IBMSecurity AppScan Standard

バージョン 9.0.3.12

ユーザー・ガイド

IBM

目次

第 1 章 概要

製品の概要、このバージョンでの新機能の概要、および連絡先情報。

製品の概要

IBM SecurityAppScan® Standard は、Web アプリケーションおよび Web サービスのセキュリティーの脆弱性をテストするツールです。このツールは、さまざまなアプリケーション・データ出力オプションに加えて、サイトをサイバー攻撃の脅威から保護するのに役立つ最も先進的なテスト方式を備えています。

IBM SecurityAppScan Standard では、以下の 3 つの異なるテスト技法を使用しています。これらは、相互を補完および強化します。

動的分析 **(**ブラック・ボックス・スキャン**)**
: これは 1 次メソッドで、実行時のアプリケーション応答をテストおよび評価します。

静的分析 **(**ホワイト・ボックス・スキャン**)**
: これは、フル Web ページのコンテキスト内の JavaScript コードを分析する固有のテクノロジーです。

対話式分析 **(Glass Box** スキャン**)**
: 動的テスト・エンジンは、Web サーバー自体に存在する専用の Glass Box エージェントと対話することができ、標準的な動的テストのみの場合と比較して、AppScan がより多くの問題を、より正確に識別することを可能にします。

AppScan の拡張機能には、以下のものが含まれます。

- すぐに使用可能な 40 を超えるさまざまなテンプレートを備えた、一般コンプライアンス・レポートおよび規制コンプライアンス・レポート
- AppScan eXtension Framework の使用、あるいは AppScan SDK を使用した既存のシステムへの直接統合によるカスタマイズと拡張性
- 悪質なサイトやその他の不要なサイトへのリンクがユーザーにもたらすリスクを識別するための、アプリケーション・セキュリティーの範囲を超えたリンク・カテゴリー化機能

AppScan Standard は、サイト配備前と実動環境での継続的なリスク・アセスメントの両方で、Web アプリケーション攻撃およびデータ侵害のリスクを軽減するのに役立ちます。

サポートされるテクノロジー

AppScan のスキャン機能に影響する可能性がある、お客様のサイトで使用されるテクノロジーについて理解する上で役立ちます。

お客様のサイトで使用されるテクノロジーの中には、AppScan のスキャン機能に影響するものと、スキャンにまったく影響しないものがあります。

- AppScan は、「ブラック・ボックス」(DAST) ツールであり、ブラウザーと同じメカニズムを使用してサイトをスキャンします。そのため、一般に、ブラウザーに対して透過的なサーバー・サイド・テクノロジーは、AppScan に対しても透過的であり、スキャンに影響しません。
- JavaScript などのクライアント・サイド・テクノロジーや HTTP プロトコル自体は AppScan に影響します。ブラウザーとは異なり、AppScan は、自動クローリング、セッション・メンテナンス、そして

無論、テストを実行できるレベルでこれらのテクノロジーを認識している必要があります。そのような場合は、正確にスキャンするように AppScan を構成する必要があります。

AppScan スキャンは、探査およびテストの、2 つの主要ステージで構成されています。次の表に、各ステージでスキャンに影響する可能性があるサーバー・サイド・テクノロジーとクライアント・サイド・テクノロジー、および構成が必要になる状況を理解するためのガイドラインを示します。

	サーバー・サイド・テクノロジー	クライアント・サイド・テクノロジー
探査ステージ	クライアントに影響しないサーバー・サイド・テクノロジー (使用されている特定のデータベースなど) は、スキャンにまったく影響しません。 クライアントに影響する 多くのメカニズム (セッション管理など) は、AppScan が正しく構成されている限り、スキャンを制限することはありません。例えば、Web サーバーおよびアプリケーション・サーバーはセッション ID の管理方法に影響を与え、AppScan はこれらの ID を追跡できる必要があります。多くの一般的なセッション ID は、事前定義されているか、AppScan が自動的に検出でき、追加の構成を必要としません。ただし、一部のカスタム・メカニズムには追加の構成が必要になります。 AppScan は、WebSphere Portal カスタム URL を明確にサポートしています。WSP は、表示されたときに追跡が困難になる方法で URL をエンコードします。AppScan は URL をデコードするため、認識して調整することが可能になります。 Glass box スキャンは、Java および .NET でのみサポートされています。	今日使用されている 2 つの主なクライアント・サイド・テクノロジーは HTML5 および JavaScript です。いずれもスキャンの探査ステージに影響します。 AppScan は、探査ステージで HTML をサポートします。つまり、リンクを抽出でき、フォームを理解して入力することができます。 AppScan は、プレーン JavaScript をサポート (実行) します。JQuery、AngularJS、および PrototypeJS など、一部の主要フレームワークは明確にサポートされています。その他の多くの JS フレームワークは明確にはサポートされていませんが、スキャンにまったく影響しません。 特定のテクノロジーが原因で自動探査ステージでページが欠落する場合、自動探査ステージの後で、テスト・ステージの前に手動でサイトを探査することにより、ページをスキャンに追加できます。
テスト・ステージ	AppScan は、サポートするテクノロジーではなく、アプリケーションをテストするよう設計されているため、それらのテクノロジーはテストに影響しません。データベースについて再び検討すると、AppScan の SQL インジェクション・テスト・スイートは、使用されているデータベースから独立しています。サード・パーティーによるテスト (共通脆弱性テスト) に対応した特定のテストも提供しています。	クライアント・サイド・テストは、JavaScript コードのみに対して実行されます。現時点では、プレーン JS の脆弱性のみが検出されます。 JS フレームワークはサポートされていないため、フレームワークを使用する JS コードは適切に分析されない可能性があります。 HTML5 は完全にサポートされています。

新機能

このセクションでは、製品の新機能およびこのフィックスパックの機能拡張について説明します。

修正の完全なリストは、 から入手可能です。 http://www.ibm.com/support/docview.wss?uid=swg27021374

IBM Security AppScan Standard 9.0.3.12 での新機能

システム要件
: Microsoft .NET Framework 4.7.2 が必要になりました。

要求ベースの **JavaScript** の実行
: アクション・ベースの JavaScript の実行の効率により、要求ベースの JavaScript の実行 (「構成」>「探査オプション」>「要求ベース」>「JavaScript を実行して URL およびダイナミック・コンテンツを見つける」) は不要になったため、デフォルトでこのチェック・ボックスが選択解除されました。このオプションが選択されているスキャンをロードした場合は選択されたままになりますが、選択を解除することを推奨します。この変更の理由については、以下のセクションを参照してください。

セキュリティー・レポート
: レポートがデフォルトでサニタイズされるようになりました (「フォームの自動入力」で定義されたパスワードはレポートに表示されません)。この設定は、「構成」>「詳細構成」>「全般: レポートのサニタイズ」で変更できます。

スキャン構成ウィザード
: ウィザードの最後のステップで、「スキャン・エキスパートを開始」チェック・ボックスがデフォルトで無効になりました。

JavaScript の実行の変更の理解

ここ数年間、当社はブラウザーの動作を模倣した「要求ベースの探査」の代替メカニズムを開発してきました。新しいメカニズムの「アクション・ベースの探査」は、実際の組み込み (Chromium ベース) ブラウザーを利用しています。どちらのメカニズムにも JavaScript の実行 (JSX) が含まれていますが、新しいテクノロジーの方が優れているため、現在は要求ベースの JSX メカニズムを廃止する過程にあります。

アクション・ベースの JSX は、ブラウザーの操作方法によりよく似ています。対象範囲と正確性が向上し、新しい JavaScript フレームワークが登場したときのサポートも向上します。そのため、要求ベースの JSX は段階的に廃止されます。

- このフィックスパックでは、要求ベースの JSX のチェック・ボックスはデフォルトで選択解除されていますが、特定のアプリケーションでアクション・ベースの探査が失敗する場合には、引き続き選択できます。
- 今後のリリースでは、このメカニズムは完全に削除される予定です。

要求ベースの JSX のチェック・ボックス (「構成」>「探査オプション」>「要求ベース」>「JavaScript を実行して URL およびダイナミック・コンテンツを見つける」) が選択されている保存済みのスキャンまたはテンプレートをロードした場合は、このチェック・ボックスは選択されたままになります。ただし、このチェック・ボックスは選択解除することを推奨します。

この変更により結果に差異が出る場合は、サポート・チケットを開くことを推奨します。その差異について説明することや、アクション・ベースのメカニズムを修正することができます。

連絡先およびサポート情報

AppScan ここでは、誤検出のテスト結果を報告するための技術サポートと、技術情報、販売情報、一般情報のための に関する連絡先情報を示します。

項目	詳細
資料	AppScan Standard 資料ライブラリーは、次の資料を含むすべてのオンライン・ユーザー文書にリンクしています。 • このユーザー・ガイドの PDF 版 • このヘルプに収録できなかった直前の情報がすべて記載された README ファイル • バージョン別に修正された APAR の詳細が記載された修正リスト • システム要件 • 現行バージョンでの主な既知の問題 (問題が検出されたときと、フィックスパックで解決されたときに更新) • AppScan Standard のダウンロード手順 http://www.ibm.com/support/docview.wss?uid=swg27024868
AppScan Standard サポート・ポータル	http://www.ibm.com/support/entry/portal/product/software/security_systems/ibm_security_appscan_standard
AppScan Standard フォーラム	https://developer.ibm.com/answers/topics/appscan-standard/
サービス要求のオープン方法	https://www.ibm.com/support/servicerequest/Home.action
「誤検出」の結果を報告するには、次のサイトをご利用ください。	http://www.ibm.com/support/docview.wss?uid=swg21295428 詳細については、 235 ページの『誤検出のテスト結果を報告』 を参照してください。
AppScan eXtensions Framework	http://www.ibm.com/developerworks/rational/downloads/08/appscan_ext_framework/ 詳細については、 312 ページの『拡張子』 を参照してください。
サポート・リソース	http://www.ibm.com/support/docview.wss?uid=swg21672099
販売および一般情報	http://www.ibm.com/software/rational/offerings/testing/webapplicationsecurity/

特定のサービス要求について AppScan Support に電話連絡するか、または問題を提出する場合は、以下の情報を準備してください。

- 実行した操作と受信したエラー・メッセージ
- 問題を把握するために必要なバックグラウンド情報
- ご使用中の AppScan Standard のバージョン
- 組織、スケジュール、期限に対する問題の影響
- ログ、データ、画面キャプチャーのチケットへのアップロード

第 2 章 インストール

インストールおよびライセンスの手続きについて説明します。

システム要件

ここでは、*AppScan Standard* を実行するマシンに必要な最低限のハードウェアとソフトウェアの概要を示します。

重要**:** 製品のリリース後に追加された更新が含まれる可能性のある、より完全なリストに以下でオンラインでアクセスできます: http://www.ibm.com/support/docview.wss?uid=swg27024155

AppScan のスキャン機能に影響する可能性がある、お客様のサイトで使用されるテクノロジーの説明については、1 ページの『サポートされるテクノロジー』 を参照してください。

ハードウェア要件

ハードウェア	最小必要要件
プロセッサー	Core 2 Duo 2 GHz (またはこれと同等のプロセッサー)
メモリー	4 GB RAM
ディスク・スペース	30 GB
ネットワーク	TCP/IP が設定されているネットワーク通信のために 1 つの NIC (100 Mbps)

オペレーティング・システムおよびソフトウェアの要件

ソフトウェア	詳細
オペレーティング・システム	サポートされるオペレーティング・システム: • Microsoft Windows Server 2016:Standard および Datacenter • Microsoft Windows Server 2012:Essentials、Standard、および Datacenter • Microsoft Windows Server 2012 R2:Essentials、Standard、および Datacenter • Microsoft Windows Server 2008 R2:Standard および Enterprise (SP1 適用済みまたは未適用) • Microsoft Windows 10:Pro および Enterprise • Microsoft Windows 8.1:Pro および Enterprise • Microsoft Windows 8:Standard、Pro、および Enterprise • Microsoft Windows 7:Enterprise、Professional、および Ultimate (SP1 適用済みまたは未適用) **注:** 32 –ビットと 64 –ビットのエディションはいずれもサポート対象ですが、64 –ビットを推奨します。すべてのフィックスパックがサポート対象です。
ブラウザー	Microsoft Internet Explorer バージョン 11 推奨:Internet Explorer Version 11.0.9600.18537、更新バージョン 11.0.38 KB3203621

ソフトウェア	詳細
その他	Microsoft .NET Framework 4.7.2 フローティング・ライセンスまたはトークン・ライセンスを使用している場合:Rational® License Key Server 8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5 (オプション) Adobe Flash Player for Internet Explorer (Flash を実行する場合と、一部のアドバイザリーで説明用ビデオを表示する場合に必要)。バージョン 9.0.124.0 から 14.0.0.125 までがサポートされています。 これより前のバージョンはサポートされていません。また、一部のバージョンでは構成作業が必要になることがあります。詳しくは、 345 ページの『Flash コンテンツ』を参照してください。 (オプション) カスタム・レポート・テンプレート用の Microsoft Word 2007、2010、2013。

重要: ローカル・ライセンスがないマシンで AppScan を使用するには、ライセンス・キー・サーバーにネットワーク接続する必要があります。

重要: AppScan と同じコンピューターで稼働しているパーソナル・ファイアウォールによって通信が妨害され、正しい検出が行われず、パフォーマンスが低下する可能性があります。最適な結果を得るには、AppScan が稼働するコンピューターでパーソナル・ファイアウォールを実行しないでください。

Glass Box サーバーの要件

Glass Box スキャン機能を使用するには、アプリケーション・サーバーに Glass Box エージェントをインストールする必要があります。詳細については、 175 ページの『Glass Box エージェントのインストール』 を参照してください。

Java プラットフォーム: Java プラットフォームでは、次のサーバー・プラットフォームとテクノロジーがサポートされています。

ソフトウェア	詳細
JRE	サポートされているのは、バージョン 6 および 7 です。JRE 8 はサポートされていません。
オペレーティング・システム	サポートされる Microsoft Windows システム (32 –ビット版と 64 –ビット版の両方): • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2 サポートされる Linux システム: • Linux RHEL 5、6、6.1、6.2、6.3、6.4 サポートされる UNIX システム: • UNIX AIX® 6.1、7.1 • UNIX Solaris (SPARC) 10、11
Java™ EE コンテナー	JBoss AS 6、7; JBoss EAP 6.1; Tomcat 6.0、7.0; WebLogic 10、11、12; WebSphere 7.0、8.0、8.5、8.5.5

.NET プラットフォーム: .NET プラットフォームでは、次のシステムとテクノロジーがサポートされます。

項目	詳細
オペレーティング・システム	サポートされるオペレーティング・システム (32 –ビット版と 64 –ビット版の両方): • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2
その他	Microsoft IIS 7.0 以降 Microsoft .NET Framework 4.0 または 4.5 をインストールする必要があります。またこのバージョンの ASP.net を使用するには、IIS がルート・レベルで構成されている必要があります。

注: アプリケーションをサーバー上で実行する場合、ユーザーには管理者特権が必要です。

注: エージェントは、テストしたいアプリケーションがサーバーに正常にインストールされた後に インストールしてください。

Cookie の使用

AppScan は、スキャンを行っているアプリケーションごとに Cookie 設定を追跡しますが、認証やその他の目的で独自の Cookie を設定することはありません。

サポート対象言語

AppScan のユーザー・インターフェースは、以下の言語で実行可能です: 中国語 (簡体字)、中国語 (繁体字)、英語 (米国)、フランス語、ドイツ語、イタリア語*、日本語、韓国語*、ポルトガル語 (ブラジル)、ロシア語*、スペイン語 (スペイン)。ユーザー・インターフェースの言語を変更するには、「ツール」>「オプション」>「全般」タブにアクセスします。

注: ユーザー・インターフェースがイタリア語および韓国語の場合、すべてのマニュアルは英語になります。ロシア語のインターフェースの場合、ヘルプは翻訳されますが、他のすべてのマニュアルは英語になります。

関連概念:

1 ページの『サポートされるテクノロジー』
AppScan のスキャン機能に影響する可能性がある、お客様のサイトで使用されるテクノロジーについて理解する上で役立ちます。

Flash Player のアップグレード

このタスクについて

スキャン中に AppScan が Adobe Flash コンテンツを実行できるようにするため、サポートされているバージョンの Adobe Flash Player for Internet Explorer がインストールされている必要があります。バージョン 9.0.124.0 から 14.0.0.125 までがサポートされています。 これより前のバージョンはサポートされていません。また、一部のサポート対象バージョンでは構成が必要になることがあります。スキャン中に Flash ファイルを実行するため、サポートされているバージョンが必要です。

注: アップグレードするまでは、「Flash の実行」チェック・ボックス (「スキャン構成」>「探査オプション」) が選択されていても Flash は実行されません。

手順

1. AppScan およびすべての Microsoft Internet Explorer ウィンドウを閉じます。

2. 最新の Flash Player をダウンロードしてインストールするには、 にアクセスしてください。
   http://get.adobe.com/flashplayer/

Flash Player の構成

このタスクについて

スキャン中に AppScan が Adobe Flash コンテンツを実行するために、サポートされているバージョンの Adobe Flash Player for Internet Explorer がインストールされている必要があります。Flash Player バージョン 10.1 以降については、場合によって、AppScan で使用するために構成が必要になることがあります。ご使用の Flash Player を構成する必要があるというメッセージが表示される場合は、以下の手順を実行してください。

注: 構成を行っていない場合、「Flash の実行 (Flash Execution)」チェック・ボックス (「スキャン構成」>「探査オプション」) が選択されていても、Flash は実行されません。

注: この手順を実行するには、管理者許可が必要です。

手順

1. AppScan を閉じます。
2. 管理者許可が付与されているユーザーとして、Flash のインストール・ファイルが含まれているフォルダーを開きます。
   - 32 ビット・システムの場合、このパスは通常、以下のようになります。

     ```
     C:\WINDOWS\System32\Macromed\Flash
     ```
   - 64 ビット・システムの場合、このパスは通常、以下のようになります。

     ```
     C:\WINDOWS\SysWow64\Macromed\Flash
     ```
3. Flash フォルダー内で、`mms.cfg` というファイルを見つけます。このファイルがない場合は、この名前を持つ空のテキスト・ファイルを作成します。
4. Microsoft ノートパッドなどのテキスト・エディターを使用して `mms.cfg` を開き、エントリー `FullFramerateWhenInvisible` を検索します。
   - これが存在している場合は、その値を 1 に設定します。
   - これが存在していない場合は、以下の行を、ファイル内の既存のどの内容よりも後に、単独の行として 追加します。

     ```
     FullFramerateWhenInvisible = 1
     ```
5. 保存します。

   これで、AppScan での Flash 実行用に Flash Player が構成されました。

インストール

インストール・ウィザードにより、簡単で迅速なインストールを実行できます。

手順

1. マシン上にバージョン 8.5 より後の AppScan Standard が存在する場合、このバージョンをインストールする前にアンインストールしてください。
2. 開いている Microsoft Office アプリケーションをすべて閉じます。

3. AppScan のセットアップを開始します。

   InstallShield ウィザードが開始し、ご使用のワークステーションが最小限のインストール要件を満たしていることが検査されます。次に、AppScan のインストール・ウィザードの「ようこそ」画面が表示されます。
4. このウィザードの指示に従って、AppScan のインストールを完了させます。

   注: GSC (Generic Service Client) をインストールまたはダウンロードするように求められます。Web サービス・スキャンを構成する場合、Web サービスの探査でこの処理が必要になりますが、Web サービスをスキャンしない場合は不要です。

サイレント・インストール

コマンド行を使用した無人インストールについて説明します。

AppScan は、コマンド行と次のパラメーターを使用して、「サイレント・モードで」インストールすることができます。

```
AppScan_Setup.exe /l"LanguageCode" /s /v"/qn INSTALLDIR=\"InstallPath\""
```

パラメーター	機能
/l	言語コード。オプションは以下のとおりです。 • 英語:**1033** • 中国語 (繁体字):**1028** • 中国語 (簡体字):**2052** • フランス語:**1036** • ドイツ語:**1031** • イタリア語:**1040** • 日本語:**1041** • 韓国語:**1042** • ポルトガル語:**1033** • スペイン語:**1034**
/s	「サイレント・モード」をアクティブにします (このパラメーターを指定しないと、通常のインストールが開始されます)。 **注:** /v"/qn" と組み合わせて使用する必要があります (次の行を参照してください)

パラメーター	機能
/v	UI モードおよび AppScan をインストールするパスなどの、追加の MSI プロパティーを設定します。 **UI モード:** 「サイレント・モード」の場合、パラメーターとして /qn (引用符で囲む) を指定してください。 パス: このインストール・パスを定義しないと、インストールではデフォルト・パス (...Program Files\IBM\AppScan Standard\) が使用されます。 異なるインストール・パスを定義するには、パラメーターとして INSTALLDIR=\"InstallPath\" (引用符で囲む) を追加してください。パスにスペースを含めることができます。 例: /v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""

例:

- デフォルト・ディレクトリーに英語版 AppScan をサイレント・インストールするには、次のように入力します。

  ```
  AppScan_Setup.exe /s /v"/qn"
  ```

- デフォルト・ディレクトリーに日本語版 AppScan をサイレント・インストールするには、次のように入力します。

  ```
  AppScan_Setup.exe /l"1041" /s /v"/qn"
  ```

- D:Program FilesAppScan に韓国語版 AppScan をサイレント・インストールするには、次のように入力します。

  ```
  AppScan_Setup.exe /l"1042" /s /v"/qn INSTALLDIR=\"D:\Program Files\AppScan\""
  ```

アンインストール

コンピューターから AppScan をアンインストールする方法について説明します。

このタスクについて

Windows の「スタート」メニューからアンインストール・ウィザードを実行するか (下記に説明)、Windows コントロール・パネルの「プログラムの追加/削除」機能を使用して、アンインストールを実行できます。 実際の手順は、インストールされている Windows のバージョンによって異なります。

手順

1. 「スタート」>「すべてのプログラム」>IBM Security AppScan Standardに移動します。
2. 「IBM Security AppScan Standard のアンインストール」を選択し、手順に従います。

   注: アンインストール・ウィザードでは、AppScan で作成されたスキャン・ファイルやレポートは削除されません。これらのファイルを削除したい場合は、手動で削除してください。

ライセンス

このセクションでは、ライセンスのインストールと管理について説明しています。

AppScan のインストールには、デフォルトのライセンスが含まれています。このライセンスにより、IBM がカスタムで設計した AppScan のテスト用 Web サイト (demo.testfire.net) をスキャンすることができます (これ以外のサイトはスキャンできません)。各自のサイトをスキャンするには、IBM® から提供される有効なライセンスをインストールする必要があります。このインストールが完了するまで、AppScan はスキャンとスキャン・テンプレートをロードおよび保存しますが、お客様のサイトに対する新規スキャンは実行しません。

IBM Security AppScan Standard ライセンス

ライセンスには次の 3 つのタイプがあります。

「ノードロック」ライセンス
このライセンスは、AppScan 実行マシンにローカルにインストールされます。各ライセンスは 1 つのマシンに割り当てられます。

「フローティング」ライセンス
このライセンスは IBM Rational License Key Server にインストールされます (AppScan 実行マシンと同じ場合があります)。AppScan を使用するサーバーはすべて、ライセンス・キー・サーバーとネットワーク接続する必要があります。ユーザーが AppScan を開くたびにライセンスがチェックアウトされ、AppScan を閉じるたびにライセンスが再びチェックインされます。

「トークン」ライセンス
このライセンスは IBM Rational License Key Server にインストールされます (AppScan 実行マシンと同じ場合があります)。AppScan を使用するサーバーはすべて、ライセンス・キー・サーバーとネットワーク接続する必要があります。ユーザーが AppScan を開くたびに必要な数のトークンがチェックアウトされ、AppScan を閉じるとトークンが再びチェックインされます。

ライセンスの状態

AppScan ライセンスを表示、編集するには、「ヘルプ」 > 「ライセンス」をクリックします。以下の 3 つのオプションがあります。

AppScan Standard License Manager を開く	現在ロードされているライセンスのリストを開くことで、次のことが可能になります。 • ノードロック・ライセンスを追加または削除する • フローティングまたはトークン・ライセンスに対しライセンス・キー・サーバーを設定する
AppScan Enterprise ライセンスの追加	自分が所属する組織が、ローカルの AppScan Standard ライセンスで許可されているユーザーに対して追加のサイトのスキャンを許可する AppScan Enterprise ライセンスを持っている場合、これらの許可をローカルのマシンにインポートして、既存のライセンスと共に使用することができます。 **注:** このオプションは、AppScan Standard のフル・ライセンス (デモ・ライセンスではなく) がロードされる場合のみ使用可能です。 323 ページの『AppScan Enterprise ライセンス許可のインポート』を参照してください。
ライセンス契約の表示	ライセンス契約を表示するにはここをクリックします。

注:  をクリックして、ダイアログ・ボックス内に表示されるライセンス情報を更新することができます。

注**:** フローティング・ライセンスまたはトークン・ライセンスが検証されたが、その後ライセンス・キー・サーバーが使用不可になった場合、AppScan は「切断モード」で最大 3 日間実行できます。この期間は、アプリケーションを通常通りにスキャンすることができます。

以下も参照してください。

351 ページの『ライセンスのトラブルシューティング』

323 ページの『AppScan Enterprise ライセンス許可のインポート』

ノードロック・ライセンスのロード

ここでは、ノードロック・ライセンスのロード方法について説明します。

このタスクについて

「ノードロック」ライセンスは、独立したサーバーにインストールされるのではなく、AppScan Standard が稼働するマシンにインストールされます。

手順

1. ライセンス・ファイルを Rational License Key Center からダウンロードして、そのファイルをご使用のマシンに保存します。
2. AppScan Standardで、「ヘルプ」>「ライセンス」>「**AppScan Standard License Manager** を開く」をクリックします。
3. 「ライセンス構成」をクリックします。
4. 上段ペイン (ノードロック・ライセンスファイル) の上部の  をクリックします。
5. ライセンスファイルをブラウズします。
6. (オプション) 2 つ以上のファイルを追加する場合、「上/下矢印」ボタンでリスト内のライセンスを昇格/降格できます。
7. 「AppScan ライセンス」ダイアログ・ボックスで、  をクリックして、ライセンスをロードします。

   注**:** ライセンス名には ASCII 文字のみ使用できます。必要に応じて、ファイル名を変更してロードします。

フローティング・ライセンスまたはトークン・ライセンスのロード

AppScan Standard Edition で使用するフローティング・ライセンスまたはトークン・ライセンスのロード方法。

このタスクについて

フローティング・ライセンスまたはトークン・ライセンスをインストールするためには、まず IBM Rational License Key Server (バージョン 8.1.2 以降) がインストールされたライセンス・キー・サーバーが必要です。ライセンス・キー・サーバーは、AppScan がインストールされているマシンとは別のマシンでも同じマシンでも構いません。以下の手順により、サーバーをセットアップして、フローティング・ライセンスをロードする方法を説明します。

手順

1. IBM Rational License Key Server (バージョン 8.1.2 またはそれ以降) を パスポート・アドバンテージからダウンロードします。
2. License Key Server をインストールします。これは、AppScan と同じコンピューター上に置くことも、中央ネットワーク・ライセンス・サーバー上に置くこともできます。
3. ライセンス・ファイルを Rational License Key Center からダウンロードして、それらのファイルを Rational License Key Server がインストールされているマシンに保存します。
4. 「スタート」>「プログラム」>「**IBM Rational**」>「**License Key Administrator (**バージョン**)**」をクリックし、Rational ライセンス・ファイル・ウィザードを使用して、ライセンス・ファイルを License Key Server にインポートします。
5. AppScan Standardで、「ヘルプ」>「ライセンス」>「**AppScan Standard License Manager** を開く」をクリックします。
6. 「ライセンス構成」をクリックします。
7. 下段ペインの上部の  をクリックします。
8. 開いたダイアログ・ボックスに、ライセンスのホストとポートを入力します。
9. (オプション) 2 つ以上のライセンス・サーバーを追加する場合、「上/下矢印」ボタンでリスト内のサーバーを昇格/降格できます。
10. 「AppScan ライセンス」ダイアログ・ボックスで、  をクリックして、ライセンスをロードします。

更新

インストール済み環境を最新の状態に維持します。

このタスクについて

サブスクリプション更新には、新しいタイプの Web アプリケーション悪用手法およびバグ修正が含まれます。これらのファイルが使用可能になったという通知を受け取った場合、すぐにインストールすることをお勧めします。

AppScan は、更新がないか IBM Web サイトを定期的に確認し、新規の更新が使用可能になると通知します。ユーザーが更新の検索を開始することもできます。

AppScan が新しく使用可能になった更新を検出すると、その新規更新ファイルをユーザーのマシンにダウンロードしてインストールする機会が与えられます。

手順

1. ツールバーで、  をクリックします。

   AppScan は、更新がないか確認します。更新が使用可能な場合、「インストール」ボタンがアクティブになります。(ユーザーの AppScan のバージョンが最新のものであれば、ボタンはグレイ表示されたままです。)
2. 更新をインストールするには、「インストール」をクリックします。

次のタスク

更新状態を 321 ページの『更新ログ』で確認できます。

一時ファイルの場所

AppScan が通常の操作中に一時ファイルを保存する場所と、その場所の変更方法を説明します。

デフォルトでは、AppScan は次の場所に一時ファイルを 保管します。

```
C:\Documents and Settings\All Users\Application Data\IBM\AppScan Standard\temp
```

何らかの理由で、このデフォルトの場所を指定変更する必要がある場合は、環境変数 APPSCAN_TEMP のパスを必要に応じて編集してください。(環境変数には、「マイ コンピュータ」を右クリックした後、「プロパティ」 > 「詳細」 > 「環境変数」と選択してアクセスします。)

制約事項: 新しい場所へのパスには、Unicode 文字を使わないでください。

第 3 章 始めに

このセクションでは、基本的な製品の機能および手順について簡単に紹介します。

自動スキャンの仕組み

このトピックでは、スキャンの「ステージ」と「フェーズ」の違いについて説明します。

AppScan フル・スキャンは 2 つのステージ (探査およびテスト) から構成されます。スキャン処理の大部分がユーザーには実際上シームレスに見え、またユーザー入力はスキャンが完了するまでほとんど必要ありませんが、この背後にある原理を理解することは役に立ちます。

探査ステージ

第 1 ステージでは、AppScan によって、リンクをクリックしてフォームのフィールドに入力を行う Web ユーザーがシミュレートされることで、サイト (Web アプリケーションまたは Web サービス) が探査されます。これが探査ステージです。

AppScan では、自身が送信した各要求への応答が分析され、潜在的な脆弱性のすべての兆候が探索されます。AppScan でセキュリティーの脆弱性を示す可能性がある応答が受信されると、この応答に基づいて 1 つ以上のテストが自動的に作成され、またどの結果が脆弱性とみなされるかを判別するために必要な検証ルール、および関連するセキュリティー上のリスクのレベルについても記述されます。

AppScan では、作成されたサイト固有のテストをアプリケーションに送信する前に、いくつかの誤った形式の要求がアプリケーションに送信され、アプリケーションでのエラー応答の生成方法が確認されます。この情報は、次に AppScan の自動テスト検証処理の精度を高めるために使用されます。

テスト・ステージ (Test stage)

第 2 ステージでは、AppScan は、探査ステージ中に作成した何千というカスタムのテスト要求を送信します。また、カスタムの検証ルールを使用して、各テストに対するアプリケーションの応答を記録および分析します。これらのルールは、アプリケーション内部のセキュリティー上の問題を特定し、またそれらのセキュリティー上のリスクのレベルをランク付けします。

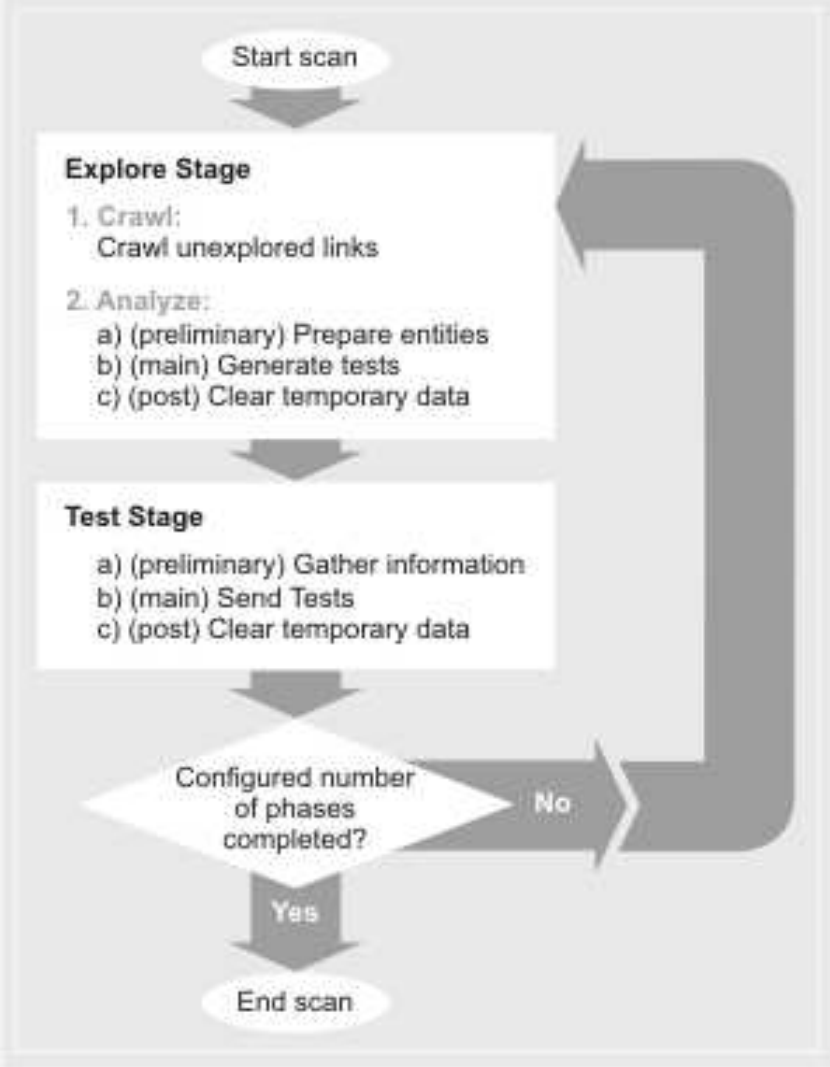
スキャン・フェーズ

実際には、テスト・ステージでサイト内の新規リンクや発生する可能性が高いセキュリティー・リスクが明らかになることがよくあります。このため、探査とテストの第 1「フェーズ」の完了後に、AppScan では、第 2「フェーズ」が自動的に開始されて新しい情報が処理されます。第 2 フェーズで新しいリンクが検出された場合は第 3 フェーズが実行され、これ以降も同じようになります。

構成された回数のスキャン・フェーズ (ユーザーが構成可能。デフォルトでは 4 回) が完了した後、スキャンが停止し、ユーザーは完了結果を確認できます。

自動スキャン・フローの図

以下の図は、自動スキャン・フローのステージとフェーズを示しています。このプロセスには、ユーザーからのアクションは不要ですが、AppScan ログ内にこれらのプロセスについて記載されている場合があります。



Web アプリケーションと Web サービスの比較

このトピックでは、AppScan によるテストの前にサイトを探査するために使用可能なさまざまな方法について説明しています。

サイトのスキャンは、最初に探査が行われ、次に収集されたデータに基づくテストが行われて実施されます。「探査データ」は、1 つ以上の探査方法を使用して収集することができます。どのケースでも、探査データが収集されると、AppScan を使用してテストが作成され、テスト・ステージ中にサイトに送信されます。

Web アプリケーションの探査 **(**ユーザー・インターフェースのあるサイト**)**

- Web サービスなしのアプリケーション (サイト) の場合は、AppScan がサイトをテストできるようにするために、開始 URL とログイン認証の資格情報を提供するだけで十分なことが多くあります。
- 必要な場合は、特定のユーザー入力によってのみ到達可能な領域にアクセスできるようにするために、 を介して*AppScan* サイトを手動で探査することができます。

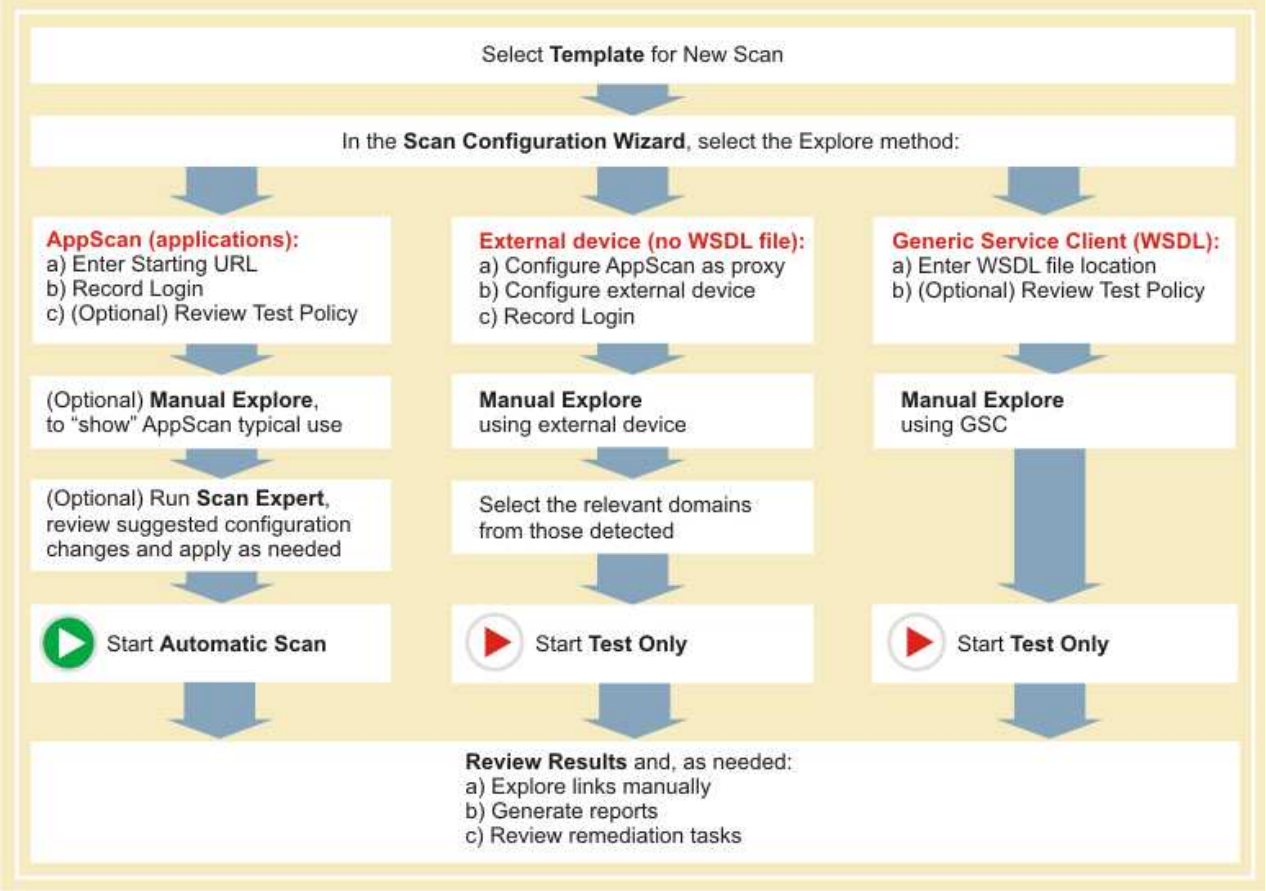
- 特定の順序でページにアクセスすることでのみ到達可能なページの場合、AppScan のマルチステップ操作を記録して使用することができます。
- 構成ウィザードではいくつかの手順でスキャンを構成して開始できますが、複雑なサイトの場合は、「構成」ダイアログ・ボックスでさらに多くの設定を微調整およびカスタマイズできます。

Web サービスの探査

- サービスの探査に使用するデバイス (携帯電話やシミュレーターなど) の記録プロキシーとして AppScan を設定できます。そうすることで、AppScan は収集された探査データを分析し、適切なテストを送信することができます。AppScan を使用して、Web サービス機能テスターなどの外部ツールでトラフィックを記録することもできます。 157 ページの『記録プロキシーとして AppScan を使用』を参照してください。
- Web サービス用の Open API 記述ファイル (JSON または YAML) がある場合、 Web サービス・ウィザードの拡張機能を使用してスキャン、およびサービスの使用に必要なマルチステップ・シーケンスを構成できます。AppScan は、サービスを自動的にスキャンします。
- 最初の 2 つの方法を使用できず、Web サービス (SOAP Web サービスなど) 用の WSDL ファイルがある場合、AppScan のインストールには、ユーザーが Web サービスに組み込まれた各種メソッドの表示、入力データの操作、サービスからのフィードバックの確認を行うことができる個別のツールがオプションで組み込まれます。まず、AppScan にサービスの URL を提供する必要があります。組み込まれている「Generic Service Client (GSC)」では、WSDL ファイルを使用して、ツリー形式で個々のメソッドが表示され、要求をサービスに送信するための使いやすい GUI が作成されます。このインターフェースから、パラメーターを入力して結果を確認できます。この処理は、AppScan によって「記録」され、AppScan によるサイトのスキャン時に、サービスに対するテストを作成するために使用されます。GSC は REST 要求のクライアントとしても使用できます (WSDL ファイルの解析なしの、単純な HTTP クライアントとして)。 161 ページの『GSC の使用』を参照してください。

基本ワークフロー

スキャン構成ウィザードを使用する単純な AppScan ワークフローを示した図です。



基本ワークフローについて詳しくは、を参照してください。 『ワークフローの説明』

Web セキュリティー分野での経験がある場合は、を参照してください。 331 ページの『上級ユーザー用のワークフロー』

ワークフローの説明

AppScan では、ご使用の Web アプリケーションに関する総合的な評価が提供されます。また、無許可アクセスやコード・インジェクションだけでなく、標準的なユーザー手法のすべてのレベルに基づく、何千というテストも実行されます。

ご使用のアプリケーションに対してスキャンを実行すると、AppScan によって各種テストがご使用の Web アプリケーションに送信されます。テストの結果は、AppScan のサイトを認識するスマート・エンジンによって作成され、強化されたレビューと操作で使用できる拡張性のあるレポートおよび推奨される修正も提供されます。

AppScan は対話式ツールです。このツールを使用して、スキャンの構成および結果に対する対応を決定します。

AppScan でのワークフローには、以下のステージが含まれています。

1. テンプレートの選択**:** 定義済みのスキャン構成が、スキャン・テンプレート です。「標準的なスキャン」テンプレート、別の定義済みのテンプレート、あるいは以前に保存したテンプレートをロードすることができます。 (構成は、後で必要に応じて現在のスキャンに合わせて調整できます。)
2. アプリケーションまたは **Web** サービスのスキャン**:** Web サービスをスキャンする場合は、AppScan にサービスを使用する方法を示すために、GSC (Generic Service Client) を使用してユーザーが多少の手動入力を行う必要があります。
   - **AppScan:** Web サービスをスキャンしない場合、またはアプリケーションの Web サービス以外の部分をスキャンする場合は、このデフォルトのオプションを選択したままにします。
   - 外部デバイスまたはクライアント**:** WSDL ファイルを使用しないサービスをスキャンする場合は、このオプションを選択します。AppScan を記録プロキシーとして構成し、AppScan を介して外部クライアントから要求を送信します。
   - 汎用サービス・クライアント**:** サービスをスキャンする場合は、このオプションを選択します。サービスに要求を送信して結果を収集できるように、GSC (Generic Service Client) が後で開きます。AppScan は、この結果を分析して、テストを作成するために使用します。
3. スキャン構成**:** サイトの詳細、ご使用の環境、および他の要件を考慮に入れて、スキャンを構成します。
4. (オプション) マニュアル探査**:** ユーザーが行うように、サイトにログインし、リンクをクリックし、フォームに入力します。これは、一般的なユーザーがサイトをブラウズする方法を AppScan に「示す」ための良い方法です。これにより、サイトの重要な部分が確実にスキャンされ、フォームに入力するためのデータが提供されます。
5. (Web サービスのみ) **GSC** を使用した要求の送信**:** GSC を開き、有効な要求をいくつかサービスに送信します。
6. (オプション) スキャン・エキスパートの実行**:** これは、構成を評価するために短時間で行うサイトの事前スキャンです。スキャン・エキスパートでは、メイン・スキャンの効率を高めるために、変更が推奨される場合があります。
7. アプリケーションまたはサービスのスキャン**:** これは、探査ステージとテスト・ステージから構成されるメイン・スキャンです。

   探査ステージ**:** AppScan がサイトをクロールし、通常のユーザーがアクセスするようにしてリンクにアクセスし、応答を記録します。また、ご使用のアプリケーションで検出された URL、ディレクトリー、ファイルなどの階層も作成されます。このリストは、アプリケーション・ツリー (22 ページの『アプリケーション・ツリー』を参照) に、表示されます。

   探査ステージは、自動または手動、あるいはこの両方を組み合わせて実行できます。探査データ・ファイルをインポートすることもできます (154 ページの『マニュアル探査データをエクスポートする』を参照)。このファイルは以前記録されたマニュアル探査シーケンスで構成されています。AppScan はサイトから収集したデータを分析し、その分析に基づいてサイト用のテストを作成します。これらのテストは、インフラストラクチャーの弱点 (市販のサード・パーティー製品またはインターネット・システムでのセキュリティー上の弱点など) とアプリケーション自体の弱点の両方を明らかにするために設計されています。

   テスト・ステージ**:** テスト・ステージ中に、AppScan は、脆弱性を明らかにし、その重大度を評価するために、探査ステージ中に受信した応答に基づいてアプリケーションをテストします。

   ご使用の AppScan の現行バージョンに組み込まれたすべてのテストの最新のリストは、「スキャン構成」ダイアログ・ボックスで確認することができます (112 ページの『「テスト・ポリシー」ビューを参照)。

AppScan で自動的に作成および実行されるテストのほかに、ユーザー定義テストを作成することもできます (289 ページの『ユーザー定義テスト』を参照)。作成したテストにより、AppScan によって生成されたテストを補完することができ、検出された結果を検査することもできます。

テスト結果は「結果リスト」に表示され、そこでテスト結果を表示および変更できます。結果の完全な詳細は、「詳細ペイン」内に表示されます。

8. (オプション) マルウェア・テストの実行: サイトで検出されたページおよびリンクを分析して、悪質なコンテンツおよび好ましくないコンテンツがないか調べます。

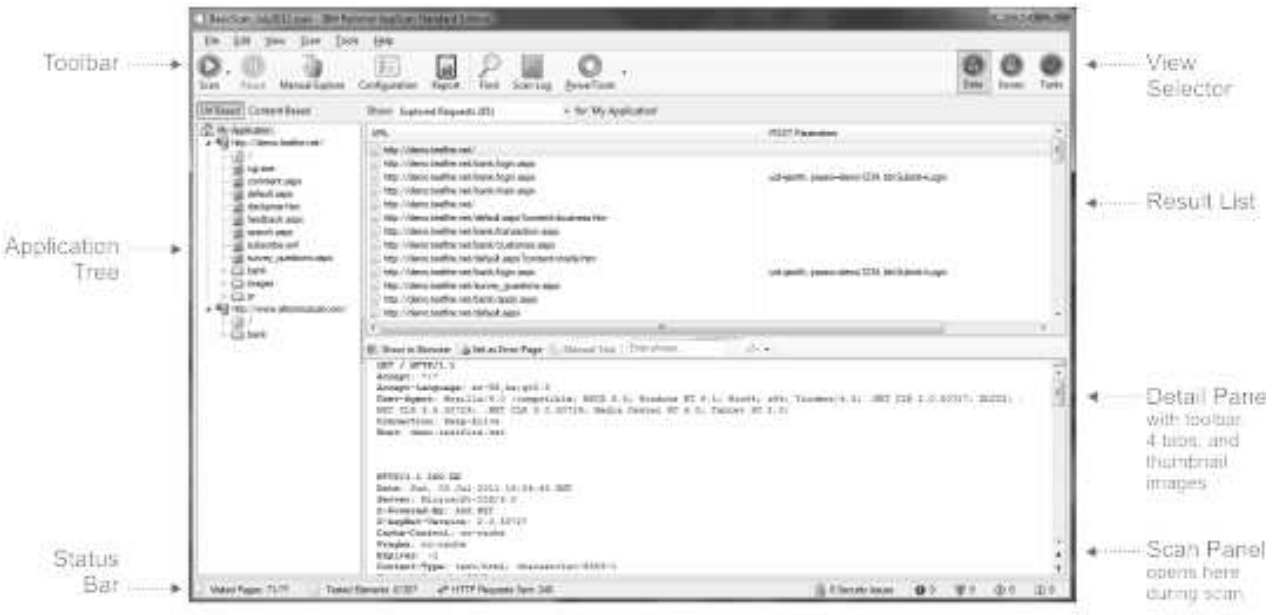
   注: 原理上はマルウェア・テストはこのステージで実行できますが (この場合、メイン・スキャンの探査ステージの結果が使用される)、実際にはマルウェア・テストは通常はライブ ・サイトに対して実行されます。一方、標準的なスキャンは、通常はテスト ・サイトに対して実行されます (スキャンによってライブ ・サイトを妨害するリスクがあるため)。

9. 結果の確認 サイトのセキュリティー状態を評価します。また、以下のことが必要な場合があります。
   - その他のリンクの手動での探査
   - 修復タスクの確認
   - レポートを印刷する
   - (必要な場合) 結果の検討に基づくスキャン構成の調整とスキャンの再実行

注: このワークフローの簡単な図については、 18 ページの『基本ワークフロー』を参照してください。

メイン・ウィンドウのツアー

AppScan のメイン・ウィンドウの構成要素、およびすべてのメニューとツールバーについて説明します。



各ペインのサイズは、スプリッター・バー (ペイン間の境界) の点線の部分をクリック・アンド・ドラッグして変更することができます。

右側の 2 つのペインは、「表示」>「レイアウト」>「垂直」/「水平」をクリックすることで、垂直方向または水平方向に調整できます。

395 ページの『第 16 章 メニュー、ツールバー、およびキーボード・ショートカット』も合わせて参照してください。

ビュー・セレクター

ツールバーの右側にある「ビュー・セレクター」アイコンを使用して、さまざまな結果ビューを切り替えます。

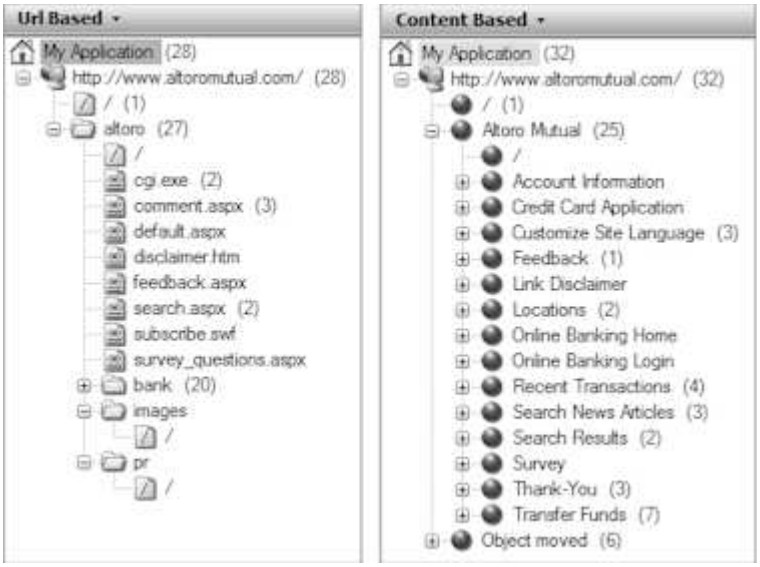
「ビュー・セレクター」で別のビューを選択すると、アプリケーション・ツリー、「結果リスト」、および「詳細ペイン」内に表示される情報が変化します。画面の 3 つの部分を以下の表にまとめます。

	データ・ビュー	探査ステージからのスクリプト・パラメーター、対話型 URL、認識された URL、リンク切れ、除外された URL、コメント、JavaScript、および Cookie が表示されます。 アプリケーション・ツリー**:** 完全なアプリケーション・ツリーです。 結果リスト**:** 表示する情報を決定するには、結果リスト上部のポップアップ・リストからフィルターを選択します。 詳細ペイン**:** スクリプト・パラメーター、対話型 URL、認識された URL、リンク切れ、除外された URL、コメント、JavaScript、および Cookie のフィルタリング済みのリスト。「アプリケーション・データ」ビューは、他の 2 つのビューとは異なり、AppScan により探査ステージのみが完了されている場合でも使用できます。データをフィルタリングするには、結果リスト上部のポップアップ・リストを使用します。 キーボード・ショートカット:**F2** 211 ページの『第 7 章 結果:アプリケーション・データ』
	問題ビュー	発見された実際の問題が、概要レベルから個々の要求/応答まで表示されます。これがデフォルトのビューです。 アプリケーション・ツリー**:** 完全なアプリケーション・ツリーです。各項目の横のカウンターは、当該項目で検出された問題の数を示します。 結果リスト**:** アプリケーション・ツリーで選択されているノードの問題と、各問題の重大度をリストします。 詳細ペイン**:** 「結果リスト」で選択した問題に関するアドバイザリー、推奨される修正、および要求/応答 (使用されているすべてのバリアントを含む) が表示されます。 キーボード・ショートカット:**F3** 219 ページの『第 8 章 結果:セキュリティー問題』

	タスク・ビュー	スキャンで検出された問題を修正するための具体的な修復タスクの To Do リストが表示されます。 アプリケーション・ツリー: 完全なアプリケーション・ツリーです。各項目の隣にあるカウンターには、その項目に関する推奨される修正の数が示されます。 結果リスト: アプリケーション・ツリーで選択されているノードの修復タスクと、各タスクの優先度をリストします。 詳細ペイン: 結果リストで選択されている修復タスクの詳細と、この修復によって解決されるすべての問題が表示されます。 キーボード・ショートカット:**F4** 243 ページの『第 9 章 結果:修復タスク』

アプリケーション・ツリー

アプリケーション・ツリーとは、AppScan によってご使用のアプリケーションで検出されたフォルダー、URL、およびファイルのツリー表示のことです。



注: 単一エントリー・ポイントのアプリケーション (例えば、MVC) などの、階層的な URL 構造を持たないアプリケーション、または階層構造が論理的でないアプリケーションの場合、論理パスをページから抜き出す 1 組の正規表現を定義して、「コンテンツ・ベース」アプリケーション・ツリーを作成することができます。 106 ページの『「コンテンツ・ベースの結果」ビュー』 を参照してください。

アプリケーション・ツリーの各アイコン

アプリケーション・ツリー内の各種ノード・タイプは、個々にそれ自身のアイコンによって示されます。

アイコン	意味
	マイ・アプリケーション、ルート・ノード。
	スキャン済みホスト。 「追加サーバー」または「ドメイン」をセットアップしている (48 ページの『「URL およびサーバー」ビュー』) か、または別のポート上にサーバーを保持している場合、このタイプのノードが複数存在する場合があります。
	ご使用のアプリケーション内で検出されたフォルダー (パス)。
	スラッシュ (斜線)。親フォルダーに対するテストの結果。
	ご使用のアプリケーション内で検出されたファイル。
	アプリケーション・ツリー内のアイコン (ここに示しているのはファイル・アイコン) 上の赤い X は、このノードとそのすべての子ノードがユーザーによってスキャンから除外されていることを示します。(このようなノードをその後のスキャンに再度含めるには、右クリックして「スキャンに含める」を選択します。) 注:子ノードは、親ノードが除外されている場合でも含めることができます。

注: アプリケーション・ツリーでは、エラー応答のみ 含まれている URL は、取り消し線の書式設定 (URL を棒線で消した状態) で表示されます。

アプリケーション・ツリーの各カウンター

アプリケーション・ツリーのカウンター (ツリーの各ノードの隣にある括弧内の数値) は、以下のように「ビュー・セレクター」で選択したビューに応じて変わります。

- セキュリティー問題: カウンターは、ノードとそのすべての子ノードに関連する問題の数を示します。(問題の総数は、 24 ページの『結果リスト』の先頭に表示されます。)
- 修復タスク: カウンターは、ノードとそのすべての子ノードに関連する修復タスクの数を示します。
- アプリケーション・データ: カウンターなし。

アプリケーション・ツリーの右クリック・メニュー

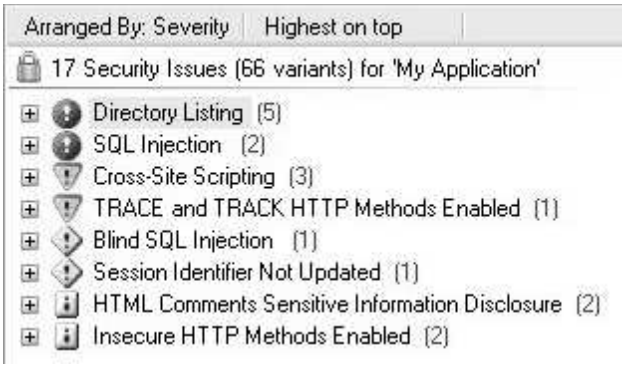
アプリケーション・ツリー内の項目 (「マイ・アプリケーション」を除く) を右クリックすると、コンテキスト・メニューに、以下のオプションの一部またはすべてが表示されます。

メニュー項目	機能
ブラウザーで表示	組み込みブラウザーを選択した URL で開きます。
マニュアル探査	選択した項目の「マニュアル探査」を開始します。詳細については、 149 ページの『AppScan の使用』 を参照してください。
マニュアル・テスト	「マニュアル・テスト」ダイアログ・ボックスが開きます。詳しくは、 236 ページの『マニュアル・テスト』を参照してください。

メニュー項目	機能
マルチステップ操作を記録	リンクを特定の順序でクリックすることによってのみ到達できるサイトの部分をテストするためのマルチステップ操作シーケンスを記録します。詳細については、 98 ページの『「マルチステップ操作」ビュー』 を参照してください。
URL をコピー	選択した URL をクリップボードにコピーします。(複数のサブノードが存在する場合は、最初のサブノードの URL がコピーされます。)
このノードのレポート	アプリケーション・ツリー内の現在選択されているノード (すべての子ノードを含む) のレポートを作成します。詳細については、 248 ページの『部分レポートの作成』 を参照してください。
スキャンから除外	選択した URL (または、選択したノードの下のすべての URL) をスキャンから除外します。 (「スキャンに含める」と切り替えます) 詳しくは、 220 ページの『URL をスキャンから除外』 を参照してください。

結果リスト

ご使用の Web アプリケーションに対するスキャンの結果は、「結果リスト」に表示されます。問題とバリアントの総数は、このリストの先頭に表示されます。



「結果リスト」のカウンター

「結果リスト」のカウンター (各ノードの隣にある括弧内の数値) は、以下のように「ビュー・セレクター」で選択したビューに応じて変わります。

- セキュリティー問題: カウンターは、ノードとそのすべての子ノードに関連する問題の数を示します。

  注: セキュリティー問題の総数 (結果リストの先頭) は、サイト内にある脆弱性のある場所の指標であり、サイトの構造化方法によってある程度左右されます。コンテンツ・ベースの構造を定義した場合、アプリケーション・ツリー内の問題の総数は、(同じ結果に対する) URL ベースのアプリケーション・ツリーでの総数と同じにならないことがあります。サイトの構造がコンテンツ・ベースで (URL ベースではなく)、コンテンツ・ベースのビューが正しく構成されている場合、コンテンツ・ベースのビュー内の問題の件数は、サイト内に存在する「脆弱性のある場所」の数をより正確に表します。バリアント の総数 (結果リストの先頭の括弧内) は、サイトの構造とは無関係で、コンテンツ・ベースのビューと URL ベースのビューの間で変化しません。
- 修復タスク: カウンターは、ノードとそのすべての子ノードに関連する修復タスクの数を示します。
- アプリケーション・データ: カウンターなし。

106 ページの『「コンテンツ・ベースの結果」ビュー』 も参照してください。

詳細ペイン

このペインには、「結果リスト」内で選択された項目の詳細が表示されます。

「詳細ペイン」で有効になる情報は、以下のように、選択した項目と選択したビューによって決まります。

- 218 ページの『アプリケーション・データ:詳細ペイン』
- 225 ページの『セキュリティー問題: 詳細ペイン』
- 246 ページの『修復タスク:詳細ペイン』

スキャンの各パネル

「進行状況」パネルおよび「通知 (Notice)」パネル

「進行状況」パネル

「進行状況」パネルは、スキャン中に「結果リスト」の下に表示されます。このパネルはスキャンを開始すると表示され、スキャンが継続している間、進行状況の情報が表示されます。

「通知 (Notice)」パネル

「通知 (Notice)」パネルは、AppScan が Web サーバーに接続できない場合、またはスキャンが完了前に停止した場合に、「進行状況」パネルの代わりに表示されます。このパネルには、詳細が表示されたダイアログを開くためのリンクが付いた簡潔な情報 (「サーバー障害」、**「スキャン未完了」**など) が表示されます。

ステータス・バー

メインウィンドウの下部のステータス・バーには、現在実行中またはロードされているスキャンについての情報が表示されます。

アイコン	意味
	アクセスしたページ: アクセスしたページの数 / アクセスするページの合計数 2 番目の数値は、スキャン中に増加した後、減少する場合があります。これは、ページがディスカバーされた後、スキャン不要として拒否されるためです。
	テストされた要素: テストされた要素の数 / テストする要素の合計数 2 番目の数値は、探査ステージ中にテスト対象の要素がディスカバーされるにつれて増加します。テスト・ステージ中には、最初 の数値が増加します。スキャン終了時までには、2 つの数値は同じになります。

アイコン	意味
	送信された **HTTP** 要求 この数値は、すべての送信された要求を表します。これには、セッション内検出要求、サーバー障害の検出要求、ログイン要求、マルチステップ操作、およびテスト要求が含まれます。つまりスキャン中には、これは AppScan が動作していることを示す指標となりますが、実際の数値にはスキャン中もスキャン後も特別な意味はありません。
	セキュリティー問題 検出されたセキュリティー問題の総数の後に、次の各カテゴリー内の数が続きます。高、中、低、情報

チュートリアル

この簡単なチュートリアルでは、スキャン構成ウィザードを使用した単純なアプリケーション・スキャンの構成、スキャンの実行、および結果の確認を行う手順を順番に示します。

この簡単なチュートリアルでは、スキャン構成ウィザードを使用して、「AltoroMutual Bank」Web サイト (デモンストレーション用に作成された Web サイト) をスキャンします。

経験のあるユーザーは、 331 ページの『上級ユーザー用のワークフロー』に記載されたより高度なワークフロー (ここでもウィザードを使用します) に従うか、 47 ページの『「スキャン構成」ダイアログ・ボックス』を使用してより詳細な構成を行うことができます。

- 『ステップ 1:スキャンの構成』
- 27 ページの『ステップ 2:スキャンの実行』
- 28 ページの『ステップ 3:スキャン結果の確認』
- 29 ページの『ステップ 4:結果の送信』

このチュートリアルは、「AltoroMutual Bank」Web サイト (デモンストレーションの目的で作成された Web サイト) を使用して進めることもできます。

URL	https://demo.testfire.net/
ユーザー名	jsmith
パスワード	demo1234

注: AppScan の評価版コピーをご利用の場合、スキャンできるサイトは AltoroMutual Bank Web サイトのみです。

注: このチュートリアルは、スキャン実行のための基本手順を簡単に示すためのものです。説明とすべての手順については、 31 ページの『第 4 章 構成』を参照してください。 331 ページの『上級ユーザー用のワークフロー』も参照してください。

ステップ 1:スキャンの構成

チュートリアルのステップ 1。

このタスクについて

「スキャン構成ウィザード」では、デフォルトの構成設定の多くを変更する必要がない場合に、スキャンの構成を簡単に行うことができます。

手順

1. AppScan を起動します。これにより「ようこそ」画面が開きます。AppScan が開いている場合は、「ファイル」>「新規」をクリックすると、同様のダイアログ・ボックスが表示されます。
2. 「スキャン構成ウィザードの起動」チェック・ボックスが選択されていることを確認して、「標準的なスキャン」テンプレートを選択します。

   「スキャン構成ウィザードへようこそ」が開きます。
3. 「**Web** アプリケーション・スキャン」ラジオ・ボタンを選択した後、「次へ」をクリックします。

   ウィザードの「URL およびサーバー」ステップが表示されます。

   注**:** 「Web サービス ・スキャン」オプションを選択した場合、ステップのフローが若干異なり、ウィザードが閉じると、 Generic Service Client (GSC) が開き、AppScan によって そのスキャンのテスト・ステージで使用されるパラメーターの入力が可能になります。(詳しくは、 44 ページの『GSC を使用した探査のウィザード』を参照してください。)
4. テキスト・ボックスにアプリケーションの URL を入力してから、「次へ」をクリックします。

   「ログイン管理」ステップが表示されます。
5. 「ログインを記録」をクリックします。

   AppScan ブラウザーが、前のステップで設定した開始 URL で開きます。現在、AppScan によってブラウズが記録されています。
6. 権限のあるユーザー名とパスワードでアプリケーションにログインします。
7. 正常にログインしたら、ブラウザーを閉じます。

   「ログイン手順」(ログイン状態を達成したリンクの順序) が表示され (詳しくは、 54 ページの『ログインの記録』を参照)、鍵アイコンの色がグレーから緑になり、セッション内検出がアクティブになったことが示されます。

    が  に変わります。
8. 「次へ」をクリックします。

   「テスト・ポリシー」ステップが表示されます。
9. 「次へ」をクリックします。

   「テストの最適化」ステップが表示されます。定期的なスキャンはデフォルト設定のままにします。
10. 「次へ」をクリックします。

    ウィザードの最終ステップが表示されます。これで、スキャンを実行する準備ができました (『ステップ 2:スキャンの実行』を参照)。

    注**:** この段階で自動スキャンを開始できますが、多くの場合は、通常のユーザーがするように、最初にアプリケーションを手動で探査することで、よりよい結果が得られます (149 ページの『AppScan の使用』を参照)。

ステップ 2:スキャンの実行

チュートリアルのステップ 2。

このタスクについて

構成が完了したら、スキャンを実行できます。

手順

1. 「自動フル・スキャンを開始」を選択して、「終了」をクリックします。

   ウィザードが閉じて、スキャン・エキスパートはサイトの現在の構成における有効性の評価を開始します。評価が完了すると、推奨の構成変更のチェックリストが表示されます。

   注: ユーザー入力を必要とする変更がある場合、それらのチェック・ボックスはぼかし表示され、選択解除されます。これらの変更用の必要な入力を指定するには、その変更のリンクをクリックします。
2. 「推奨を適用」をクリックします。

   選択した構成変更が適用されて、スキャンが開始します。「進行状況」パネルが開き、「アプリケーション・データ」と「問題」がリアルタイムで更新されます。

   探査ステージ中は、AppScan によりアプリケーションがクロールされ、そのページとコンテンツが発見されます。これらが発見されると、「アプリケーション・データ」のツリーが更新され、最終的にサイトの完全なツリーが表示されます。次のテスト・ステージ中には、AppScan により、対象のサイトに対して何千というテストが実行され、検出された問題および推奨される修正が報告されます。スキャンのこの部分では、「セキュリティー問題」ビューが自動的に選択され、「結果リスト」に発見された問題に関する動的に更新されるリストが表示されます。

   スキャンには複数のフェーズ (フェーズとは、テストがあとに続く探査のサイクルのことです) を持たせることができます。このようになるのは、AppScan でテスト・ステージ中に新しいリンクが発見され、スキャンする必要がある場合です。その場合は、これらのリンクに基づいて新しいテストが作成され、追加のスキャン・フェーズが実行されます。後続のフェーズは、新しいリンクのみがスキャンされるため、通常は前のフェーズよりも短くなります。AppScan では、構成されている「スキャン制限」に達するか、または新しい URL が検出される限り、フェーズが追加されます。この制限のデフォルトは 4 フェーズです。

   スキャンが完了すると、「進行状況」パネルが閉じて、結果を確認することができます (『ステップ 3: スキャン結果の確認』を参照)。

ステップ 3:スキャン結果の確認

チュートリアルのステップ 3。

このタスクについて

スキャンが完了すると、結果がメイン・ウィンドウ内のアプリケーション・ツリー、「結果リスト」、および「詳細ペイン」の 3 つの領域に表示されます。各領域に表示される情報の種類は、選択されたビュー (デフォルトは「セキュリティー問題」ビュー) によって決まります。

手順

ビューにアクセスするには、画面の左側にある「ビュー・セレクター」内の以下に説明されている各ビューに関連付けられているアイコンをクリックします。

表示	説明
	データ・ビュー アプリケーション内で検出されたコンテンツ項目のリストが提供されます。これは、テスト・ステージの開始前に、スキャンがアプリケーションを対象に含むように構成されているかどうかを確認するのに役立つ方法です。 • アプリケーション・ツリー: URL とフォルダーのノードが表示されます。 • 結果リスト: スキャン結果でソートされたアプリケーション・データが表示されます (211 ページの『アプリケーション・データ:結果リスト』を参照)。例えば、リンク切れ、JavaScript、Cookie などのリストの確認を選択できます。 • 詳細ペイン: 特定のページに送信された要求、および受信された応答が表示されます。 「アプリケーション・データ」ビューについて詳しくは、 211 ページの『第 7 章 結果:アプリケーション・データ』を参照してください。
	問題ビュー スキャンで発見されたセキュリティー問題に関する総合的なデータが提供されます。 • アプリケーション・ツリー: AppScan によってアプリケーションで検出されたフォルダー、URL、およびファイルがリスト表示されます。ツリーの各ノードの隣にある数値は、検出された問題の数を示しています。 • 結果リスト: 問題ごとに 1 つのアイコンが表示され、この問題に割り当てられた重大度値が示されます (220 ページの『セキュリティー問題: 結果リスト』を参照)。各問題には、この問題に対して脆弱性のある統合化された URL も保持されます。各 URL の下には、脆弱なデータのリストがあります。 • 詳細ペイン:これが問題である理由、未処理のままの場合に行われる可能性があること、推奨される修正、送信されたテスト要求のバリアント、AppScan によりテストに問題とマークが付けられたアプリケーションの応答などを理解することができる情報が表示されます。 「問題」ビューについて詳しくは、 219 ページの『第 8 章 結果:セキュリティー問題』を参照してください。
	作業ビュー セキュリティー問題に対処し、これを防止するための設計修復が表示されます。このビューでは、アプリケーションが現在抱えている問題、およびアプリケーション設計の修正方法に関して、担当者と簡潔で正確な言葉でやり取りするための容易で効率的な方法が提供されています。 • アプリケーション・ツリー: ツリーの各ノードの隣にある数値は、各項目ごとに関連している修復タスクの数を示しています。 • 結果リスト: 修復タスクごとに 1 つのアイコンが表示され、このタスクに割り当てられた優先度の値が示されます (243 ページの『修復タスク:結果リスト』を参照)。 • 詳細ペイン: 修復タスクの詳細が表示され、このタスクで対処される問題がリストされます。 「修復」ビューについて詳しくは、 243 ページの『第 9 章 結果:修復タスク』を参照してください。

『ステップ 4:結果の送信』を参照してください。

ステップ 4:結果の送信

チュートリアルのステップ 4。

このタスクについて

スキャン結果をお客様のチームに送信する基本的な方法には、以下の 2 つがあります。

レポート:
: レポート・テンプレートを、目的のレポート (QA (品質保証) 向けのレポート、経営陣向けのレポート、開発者向けのレポートなどの作成) に基づいて選択できます。ご使用のアプリケーションの開発ライフ・サイクルを進めていくに従って、コンプライアンス・レポートがますます不可欠になるでしょう。ご使用のアプリケーションが、選択した行政および業界の標準や規制にどのように耐えうるかについての完全なレポートを入手することができます。詳細については、 247 ページの『第 10 章 レポート』を参照してください。

個々の問題:
: 特定のチームまたは担当者で対処されることになっている特定の問題が存在する場合は、各テストおよびそれらの結果を関連する関係者に送信できます。 235 ページの『誤検出のテスト結果を報告』 を参照してください。

サンプル・スキャン

サンプル・スキャンは、AppScan の使用感、およびスキャン結果がどのように表示されるかを確認するのに役立ちます。

AppScan をインストールすると、4 つのサンプル・スキャンがマシンに保存されます。これらのスキャンを開き、どのように構成されているか、結果が AppScan でどのように表示されるかを確認することができます。これらのサンプル・スキャンは、AppScan Standard のメイン・フォルダー内にあります。このフォルダーのデフォルト位置は、次のとおりです。

```
C:\Program Files (x86)\IBM\AppScan Standard
```

以下のスキャンがあります。

demo.testfire.net.scan
: これは、AppScan デモンストレーション・テスト・サイトのスキャンです。構成および結果を確認することができます。また、サイトに対して追加要求を送信したり、新規データを使用してスキャンを続行したりすることもできます。

Glass_Box_DotNet_Demo.scan および **Glass_Box_Java_Demo.scan**
: これらの 2 つのスキャンは、それぞれ .NET アプリケーション・サーバーおよび Java サーバーを使用する Glass box スキャンの例です。構成を確認したり、個別の問題にドリルダウンしたりすることができます。 Glass box によって検出された問題の場合、この情報には、実際に問題があるソース・コードが含まれます。

  注: Glass box スキャンでは、スキャンされているアプリケーションのサーバーにあるエージェントへのアクセス権が必要です。このスキャンで使用されたエージェントに対するアクセス権を持っていないので、スキャンを続行することができません。

GSC_demo.testfire.scan
: これは、AppScan デモンストレーション・テスト・サイトの Web サービス・スキャンです。構成および結果を確認することができます。GSC (Generic Service Client) がインストールされている場合、これを使用してサイトに対して追加要求を送信したり、新規データを使用してスキャンを続行したりすることもできます。

第 4 章 構成

ご使用のアプリケーションと希望するテストの種類に最も当てはまる設定を選択して、スキャンを構成します。

標準的なスキャンの構成には 2 つの方法があります。

- 『スキャン構成ウィザード』 は、次の場合に役に立ちます。
  - 初めて AppScan を使用する、もしくは
  - 必要な設定のほとんどが標準である。
  - スキャン間で設定を変更する必要がなく、スキャン・テンプレートを自分自身の仕様ですでに保存してある。
- 47 ページの『「スキャン構成」ダイアログ・ボックス』 は、次の場合に役に立ちます。
  - スキャンの設定の多くをカスタマイズする必要がある、または
  - カスタム・スキャン・テンプレートを作成して保存したい。

どちらの場合も、スキャン・テンプレート (144 ページの『スキャン・テンプレート』を参照) から始めて、オプションで必要に応じて設定を変更できます。ただし、一部の詳細設定は、ウィザードではなくダイアログ・ボックスのみを使用して変更を行うことができます。

スキャンは標準的なスキャン・テンプレートを基にして行うか、以前に保存した自分自身のテンプレートをロードすることができます。(「スキャン・テンプレート」とは、単に保存してあるスキャン構成設定のセットです。) 自分自身のスキャン・テンプレートを保存してロードすることは、定期的に同じ設定をスキャンに使用する場合に最も効率的な方法です。

注: スキャンを構成した後、スキャンを開始する前に、 172 ページの『スキャン・エキスパート (Scan Expert)』を使用して特定のアプリケーション用の構成を評価し、変更を提案してそれを最適化することができます。

18 ページの『ワークフローの説明』 も参照してください。

スキャン構成ウィザード

このウィザードを使用して、基本的なスキャンを迅速に構成できます。

スキャン構成ウィザードは、デフォルト・オプションの多くを変更する必要がない場合に、スキャンを構成し、開始するための最も簡単な方法です。ただし、詳細オプションを変更する必要がある場合は、 47 ページの『「スキャン構成」ダイアログ・ボックス』 を使用することもできます。

ウィザードを使用すると、最も一般的な構成オプションにアクセスすることができ、主な違いはオプションの配列の仕方です。 (以下の表と後続のセクションのどちらにも、オプションへの相互参照がありますが、これらはウィザードでもダイアログ・ボックスでも同じで、このガイドのダイアログ・ボックスのセクションを指しています。)

探査の手段	説明
AppScan (自動または手動)	ほとんどの Web アプリケーション・スキャンではこのオプションを選択します。アプリケーションは、AppScan からアプリケーションに送信された要求によって、手動または自動 (またはその両方) で探査されます。
外部デバイス/クライアント (記録プロキシーとして AppScan を使用)	AppScan の外部トラフィック・レコーダーを記録プロキシーとして使用する場合にこのオプションを選択します。携帯電話、シミュレーター、またはエミュレーターを使用し、RESTful あるいはその他の非SOAP Web サービス (またはセキュリティー・エンベロープを必要としないSOAP サービス) を手動で探査することができます。AppScan はそのトラフィック・レコーダーにドメインと要求を表示し、入力から適切なテストを作成します。
Generic Service Client (WSDL)	WSDL ファイルを使用する Web サービスではこのオプションを選択します。Generic Service Client (GSC) は、ご使用の Web サービスの WSDL ファイルを使用して、単純なインターフェースで使用可能なサービスを表示し、ユーザーによるパラメーターの入力や結果の表示を可能にします。GSC インターフェースを使用して Web サービスを手動で探査することで、AppScan は、ユーザーの入力を使用して適切なテストを作成することが可能になります。 **注:** このオプションは、GSC (Generic Service Client) がマシンにインストールされている場合のみ使用できます。青色のリンクをクリックすると、ご使用のコンピューターに GSC がダウンロードされ、その .EXE ファイルをダブルクリックすると GSC がインストールされます。

スキャン構成ウィザードを起動する

このタスクについて

スキャン構成ウィザードは、AppScan ようこそ画面 (AppScan を起動すると表示される) から起動するか、またはツールバーの「新規スキャン」アイコンをクリックして起動できます。

注: AppScan の始動時にようこそ画面が表示されない場合、「設定」の設定が変更されています。設定を元に戻すには、 280 ページの『「全般」タブ』を参照してください。(また、ようこそ画面は「表示」メニューからいつでも開くことができます。

手順

1. ウィザードを起動するには、以下のいずれかを行います。
   - ようこそ画面で、「新規スキャンの作成」をクリックします。
   - AppScan が既に開いている場合、ツールバーの「新規スキャン」アイコン  をクリックします。
2. 「新規スキャン」ダイアログ・ボックスで、「スキャン構成ウィザードの起動」チェック・ボックスが選択されていることを確認します。
3. 「定義済みのテンプレート」リストで、スキャン・テンプレートをクリックして選択します。特定のテンプレートが必要ない場合は、「標準的なスキャン」テンプレートを選択します (詳しくは、 144 ページの『定義済みのテンプレート』を参照)。

   「スキャン構成」のようこそ画面が表示されます。
4. スキャン構成ウィザードのようこそ画面で、必要なスキャン・オプションを選択します。

探査の手段	説明
AppScan (自動または手動)	ほとんどの Web アプリケーション・スキャンではこのオプションを選択します。アプリケーションは、AppScan からアプリケーションに送信された要求によって、手動または自動 (またはその両方) で探査されます。
外部デバイス/クライアント (記録プロキシーとして AppScan を使用)	AppScan の外部トラフィック・レコーダーを記録プロキシーとして使用する場合にこのオプションを選択します。携帯電話、シミュレーター、またはエミュレーターを使用し、RESTful あるいはその他の非SOAP Web サービス (またはセキュリティー・エンベロープを必要としないSOAP サービス) を手動で探査することができます。AppScan はそのトラフィック・レコーダーにドメインと要求を表示し、入力から適切なテストを作成します。
Generic Service Client (WSDL)	WSDL ファイルを使用する Web サービスではこのオプションを選択します。Generic Service Client (GSC) は、ご使用の Web サービスの WSDL ファイルを使用して、単純なインターフェースで使用可能なサービスを表示し、ユーザーによるパラメーターの入力や結果の表示を可能にします。GSC インターフェースを使用して Web サービスを手動で探査することで、AppScan は、ユーザーの入力を使用して適切なテストを作成することが可能になります。 **注:** このオプションは、GSC (Generic Service Client) がマシンにインストールされている場合のみ使用できます。青色のリンクをクリックすると、ご使用のコンピューターに GSC がダウンロードされ、その .EXE ファイルをダブルクリックすると GSC がインストールされます。

AppScan を使用した探査のウィザード

このウィザードのステップをリストします。

1. 34 ページの『URL およびサーバー』
2. (オプション) 35 ページの『接続設定』
3. 35 ページの『ログイン管理』
4. (オプション) 36 ページの『ログイン管理の詳細』
5. 37 ページの『テスト・ポリシー』
6. 38 ページの『テストの最適化』
7. 38 ページの『完了』

URL およびサーバー

スキャンの開始 URL、およびスキャンに含める必要のある追加のサーバーおよびドメインがあれば、それらも定義します。

このタスクについて

「ようこそ」のステップで「**Web** アプリケーション・スキャン」を選択した場合、ウィザードの最初のステップは、スキャン用の開始 URL およびサーバー設定を定義することです。

手順

1. 開始 **URL:** アプリケーションの URL を入力します。スキャンはこの URL で開始します。

   AppScan は URL への到達を試み、成功した場合は、緑のチェック・マークと「サーバーへ接続済み」の確認が開始 URL の下に表示されます。構成変更により問題を修正できる場合、AppScan はどのような変更が必要であるか提示し、「構成」ダイアログ・ボックスで適切なビューにリンクします。

    入力したページをブラウザーで表示します。必要であれば、別の URL にブラウズし、ツールバーを使用して、新規ページをスキャン用の開始 URL として設定できます。ブラウザーを閉じて、スキャン構成を続行します。

    開始 URL を再度テストします。構成後、再開した際にサーバーがダウンした場合にこのボタンをクリックします。

   ヒント**:** スキャンの構成後 に、開始 URL のドメイン、スキーム、またはポートを変更する場合、構成に対する変更が必要になることがあります。AppScan によってこの構成に自動的な変更が試行されるかどうかについて確認が求められます。詳細については、 51 ページの『開始 URL ホストの変更』を参照してください。

2. 大文字と小文字を区別するパス**:** このチェック・ボックスを選択すると (デフォルト)、大/小文字のみが異なるリンクは別々のページとして扱われます。 例えば、「ReadMe.as」は「readme.as」とは異なるものと見なされます。通常、Unix ベースのサーバーの場合にはこのチェック・ボックスを選択し、Windows ベースのサーバーの場合にはチェック・マークを外します。

3. 追加のサーバーおよびドメイン**:** アプリケーションに開始 URL のもの以外のサーバーまたはドメインが含まれており、かつ *AppScan* ライセンスにそれらが含まれている場合、スキャンに組み込まれるようにここで追加する必要があります。

   a. 「プラス」アイコン  をクリックして、「サーバーおよびドメインの追加」ダイアログ・ボックスを開きます。

   b. サーバーのホスト名または IP アドレス、あるいはドメイン・ネーム (例えば、sitetoscan.com) を入力して、「**OK**」をクリックします。

   新規項目がリストに追加されます。

4. 「追加の接続設定を構成する必要があります」 デフォルトでは、AppScan は Internet Explorer のプロキシー設定を使用します。 AppScan で別のプロキシーを使用する場合のみ、このチェック・ボックスを選択します。これで、「次へ」ボタンをクリックすると、追加のステップ、 35 ページの『接続設定』が開きます。

5. 「次へ」をクリックして、ウィザードの次のステップに進みます。

次のタスク

『ログイン管理』

「追加の接続設定を構成する必要があります」を選択した場合、「『接続設定』」を続行します。

接続設定

(オプション) 必要な場合、プロキシー設定およびサーバー・レベルの認証を構成します。

このタスクについて

デフォルトでは、AppScan は Internet Explorer のプロキシー設定を使用します。このステップは、ウィザードの「URL およびサーバー」ステップで「追加の接続設定 (Additional Connection Settings)」チェック・ボックスを選択した場合にのみ開き、別のプロキシー設定を使用するか、どのプロキシー設定も使用しないように AppScan を構成することができます。

手順

1. 以下の 3 つのプロキシー・オプションの 1 つを選択します。
   - **Internet Explorer** のプロキシー設定を使用する**:** (デフォルト) これを選択すると、AppScan はアプリケーションへの接続時に、Internet Explorer 接続のアドレスおよびポートを使用します。
   - プロキシーを使用しない**:** AppScan でプロキシー設定をまったく使用しない場合は、これを選択します。
   - カスタムのプロキシー設定を使用**:** Internet Explorer で使用されるもの以外のアドレスおよびポートを使用する場合は、これを選択します。
2. プロキシーを使用するオプションのいずれかを選択した場合、接続時に使用する AppScan のユーザー名、パスワード、およびドメインを設定することもできます。これを行うには、「構成」ボタンをクリックします。
3. プラットフォームでサーバー・レベルの認証が必要な場合、「**HTTP** 認証」領域でユーザー名、パスワード、およびドメインを設定します。
4. 「次へ」をクリックします。

次のタスク

『ログイン管理』

ログイン管理

ログイン方法を構成し、必要な場合はログイン手順を記録します。

このタスクについて

ウィザードのログイン管理ステップでは、スキャン中にログイン・ページが表示される場合に AppScan が使用する 3 つの方法から 1 つを選択できます。

- 記録されたログイン:(推奨メソッド) このオプションを選択する場合、AppScan は記録されたログイン手順を使用して、実ユーザーのようにフィールドに入力し、リンクをクリックします。

  詳細については、 54 ページの『ログインの記録』を参照してください。

ログイン時に毎回人間が対応する必要がある場合 (2 因子認証、ワンタイム・パスワード、または CAPTCHA など)、「プロンプト」オプションを選択します。

- プロンプト:この場合、ログイン手順をまだ記録する必要があります。 AppScan は記録された手順を使用してログインすることはありませんが、いつログアウトするかを知るためにその手順を参照として必要とします。
- 自動ログイン: AppScan が、特別な手順がなくても、名前とパスワードのみを使用してサイトにログインできる場合、このオプションを選択し、「ユーザー名」と「パスワード」を入力します。
- ログインしない: アプリケーションがログインを必要としない場合か、何か別の理由で AppScan にログインさせない場合のみ、このオプションを選択します。

手順

1. 必要なログイン方法のラジオ・ボタンを選択します。
2. 以下のいずれかを実行します。
   - 「記録されたログイン」または「プロンプト」の場合、「記録」または「インポート」をクリックし、ログイン手順を設定します (詳しくは、 53 ページの『「ログイン」タブ』を参照してください)。
   - 自動ログインの場合、「ユーザー名」と「パスワード」を入力するだけです。

   注: ログインを記録する場合、記録が終了するとダイアログ・ボックスが開いて、AppScan が抽出したログイン・データが正しいかどうかを確認するよう求められることがあります。必要に応じて、パラメーターや値を入力または修正して、「**OK**」をクリックします。

   有効なログイン手順を記録した場合、鍵アイコンがグレー表示  から緑  になり、セッション内ページが識別されていることを示します。

   注: 鍵アイコンが赤色  に変化した場合、AppScan はスキャン中に使用できるセッション内ページのパターンを識別してログアウトしていないことを確認しようとしましたが、それができませんでした。これを修正するには、ウィザードの追加ステップを開き、AppScan に手動で ID を提供する必要があります (次のステップを参照)。
3. 「セッション内検出オプションを構成します」チェック・ボックスを選択した場合は、「次へ」をクリックすると、追加のウィザード・ステップである『ログイン管理の詳細』が開きます。ログイン手順を編集する必要がある場合のみ、これを選択してください (前のステップの注を参照)。
4. 「次へ」をクリックします。

次のタスク

37 ページの『テスト・ポリシー』

「セッション内検出オプションを構成します」を選択した場合、 を続行します。 『ログイン管理の詳細』

ログイン管理の詳細

(オプション) 記録したログイン手順を確認し、編集します。

このタスクについて

追加の「ログイン管理」設定ダイアログ・ボックスでは、記録されたログイン手順、およびログインしていることを AppScan が確認するためにスキャン中に使用するパターン (「セッション内検出パターン」) を確認して編集できます。

手順

1. ログイン手順を確認して編集し、セッション検出パターンが有効なことを確認します。オプションは、で説明されています。 56 ページの『レビューと検証タブ』
2. 「次へ」をクリックします。

次のタスク

『テスト・ポリシー』

テスト・ポリシー

スキャンを特定のタイプのテストに制限することにより、スキャン時間を短縮できます。

このタスクについて

AppScan がスキャン中に送信するテストの数は、大量になることがあります。場合によっては、スキャンを特定のタイプのみに制限することにより、スキャン時間を短縮したほうが良いこともあります。これがテスト・ポリシーです。

AppScan にはデフォルト・テスト・ポリシー、およびユーザーが選択できるいくつかの追加のテスト・ポリシー構成が備えられています。また、自分自身のユーザー定義テスト・ポリシーを使用することもできます。

ウィザードのテスト・ポリシー・ステップには、現在のポリシーの基になっているテスト・ポリシーの名前とその説明が表示されます。

手順

1. テスト・ポリシーが必要に適していることを確認します。(わからない場合は、デフォルト・テスト・ポリシーのままにしてください。)
2. 別のテスト・ポリシーをロードするには、「ポリシー・ファイル」ペインの「定義済みのポリシー」または「最近使用したポリシー」のいずれかをクリックします。詳しくは、 112 ページの『「テスト・ポリシー」ビュー』 を参照してください。
3. ログインおよびログアウト・ページに関するテストを送信します: デフォルトでは、AppScan はログイン・ページとログアウト・ページをアプリケーションの残りの部分とともにテストします。次の場合を除き、このデフォルト構成のままにしておいてください。
   - アプリケーションに、これらのページに対する不正入力を行うユーザーを締め出す安全機能が付いている。
   - これらのページがテストされると、アプリケーション・フローが変更される。

   アプリケーションがこれらのテストにどのように応答するかわからない場合、このオプションを選択したままにしておきます。
4. ログイン・ページのテスト時にセッション **ID** を送信しない: (このチェック・ボックスは、前のチェック・ボックスが選択されている場合にのみアクティブになり、デフォルトで選択されます。) ログイン・ページをテストする場合、セッション ID によってテストの成功が制限される可能性があるため、

このチェック・ボックスは選択したままにしておくことをお勧めします。ログイン・ページをテストするのに有効なセッション・トークンが必要であることが確実な場合にのみ、このチェック・ボックスを選択解除します。

アプリケーションがどのように応答するかわからない場合、このオプションを選択したままにしておきます。

5. 「次へ」をクリックします。

次のタスク

『テストの最適化』

テストの最適化

テストの最適化では高速スキャンのために機械学習を利用できます。

このタスクについて

通常の AppScan Standard の全体スキャンでは、一般的に数千ものテストを送信し、完了までに数時間、場合によっては数日かかることがあります。開発の初期段階で、または製品の現在のセキュリティ体制の全体をすばやく評価するために、テストの最適化を使用して、より短い時間フレームで必要な結果を入手できます。

当社のインテリジェントなテスト・フィルターは、統計分析に基づき、特定のテストや、特定のテストのバリアントもフィルタリングによって除外し、より一般的な脆弱性、より重大な脆弱性、またはより重要な脆弱性のみを識別する短いスキャンを生成します。AppScan のフィックスパックと iFix により、最適化フィルターが最新の状態に保たれます。テストの最適化を使用することで、徹底的で詳細なスキャンよりも迅速な結果を優先する場合に、全体のスキャン時間を大幅に短縮することができます。

手順

1. 必要なオプションを選択します (わからない場合は、デフォルト・オプションのままにしてください)。

オプション	説明
通常 (デフォルト)	詳細なテストを実行し、構成されたとおりに、適切なすべてのテストを送信します。この設定は、長いスキャンが開発ワークフローを中断させることのない場合に推奨されます。
最適化	より一般的で重大な、およびそれ以外の重要な脆弱性に対してのみテストを送信することで、スキャンを高速化します。

2. 「次へ」をクリックして、ウィザードの最終ステージに進みます。

次のタスク

『完了』

関連概念:

344 ページの『テストの最適化の理解』
このセクションでは、テストの最適化の動作と、テストの最適化を開発ライフサイクルに組み込むための最善の方法について説明します。

完了

ウィザードのステップが完了したら、構成したスキャンを開始する方法およびタイミングを決定します。

このタスクについて

スキャンをすぐに開始するオプションのいずれかを選択する場合、メイン・スキャンを開始する前にスキャン・エキスパート を実行するように選択することもできます。スキャン・エキスパートはアプリケーションにログインし、短い事前スキャンを実行して、構成した設定を評価します。その後、必要に応じて構成変更を提案します。これらの提案を (自動的にまたは手動で) 取り込むと、メイン・スキャンの効率を大幅に向上できます。

手順

1. 以下のオプションの 1 つを選択します。
   - 自動フル・スキャンを開始**:** アプリケーションのフルスキャンを開始します (探査の直後にテストが続きます)。
   - 自動探査のみを開始**:** アプリケーションを探査しますが、テスト・ステージに進みません。 (テスト・ステージを後で実行できます。)
   - マニュアル探査を開始**:** ブラウザーが開き、リンクをクリックしてフィールドに入力すると、サイトを手動で探査できます。AppScan は、テスト・ステージで使用するために結果を記録します。
   - 後でスキャンを開始します**:** スキャンを開始しないでウィザードを閉じます。次回スキャンを開始するときに、このテンプレートが使用されます。
2. スキャン構成ウィザードが完了したらスキャンを開始**:** (最初の 3 つのスキャン・オプションの 1 つが選択されている場合にのみアクティブです。) メイン・スキャンを開始する前にスキャン・エキスパートで構成を評価する場合は、このチェック・ボックスを選択します。

次のタスク

を参照してください。 167 ページの『スキャンの進行状況』

以下も参照してください。

165 ページの『スキャンを開始する』

219 ページの『第 8 章 結果:セキュリティー問題』

外部デバイスまたはクライアントを使用した探査のウィザード

このウィザードのステップをリストします。

1. 『記録プロキシー』
2. (オプション) 40 ページの『接続設定』
3. 41 ページの『SSL 証明書』
4. 41 ページの『ログイン管理』
5. (オプション) 42 ページの『ログイン管理の詳細』
6. 42 ページの『テスト・ポリシー』
7. 43 ページの『完了』

記録プロキシー

プロキシー・ポートおよびクライアント・タイプを構成します。

手順

1. 記録プロキシー・ポート**:** ユーザーがリモート・デバイスまたは外部クライアントから送信したマニュアル探査要求を AppScan が受信するポートを構成します。 AppScan が使用可能なポートを自動的に選択するようにすることができます。

   ヒント**:** 自動で選択されたポートはセッション間で変更される可能性があるため、ユーザー自身がポートを選択することをお勧めします。ただし、複数の AppScan のインスタンスを同時に開く場合は、ポートを指定しないでください。複数のインスタンスを使用する必要がある場合は、AppScan が自動的にポートを選択するように構成してください。
2. 記録の開始元**:** 記録を AppScan と同じマシン上の外部クライアント (シミュレーターやエミュレーターなど) から開始するか、リモート・デバイス (携帯電話など) から開始するかを定義します。
3. 情報ペインに表示された IP およびポートを使用するように、リモート・デバイスまたは外部クライアントを構成します。
4. 「追加の接続設定を構成する必要があります」 デフォルトでは、AppScan は Internet Explorer のプロキシー設定を使用します。 AppScan で別のプロキシーを使用する場合のみ、このチェック・ボックスを選択します。これにより、「次へ」ボタンをクリックすると追加ステップが開きます。
5. 「次へ」をクリックして、ウィザードの次のステップに進みます。

次のタスク

41 ページの『SSL 証明書』

「追加の接続設定を構成する必要があります」を選択した場合、 に進みます 『接続設定』

接続設定

(オプション) 必要な場合、プロキシー設定およびサーバー・レベルの認証を構成します。

手順

1. 以下の 3 つのプロキシー・オプションの 1 つを選択します。
   - **Internet Explorer** のプロキシー設定を使用する**:** (デフォルト) これを選択すると、AppScan はアプリケーションへの接続時に、Internet Explorer 接続のアドレスおよびポートを使用します。
   - プロキシーを使用しない**:** AppScan でプロキシー設定をまったく使用しない場合は、これを選択します。
   - カスタムのプロキシー設定を使用**:** Internet Explorer で使用されるもの以外のアドレスおよびポートを使用する場合は、これを選択します。
2. プロキシーを使用するオプションのいずれかを選択した場合、接続時に使用する AppScan のユーザー名、パスワード、およびドメインを設定することもできます。これを行うには、「構成」ボタンをクリックします。
3. プラットフォームでサーバー・レベルの認証が必要な場合、「**HTTP** 認証」領域でユーザー名、パスワード、およびドメインを設定します。
4. 「次へ」をクリックします。

次のタスク

41 ページの『SSL 証明書』

SSL 証明書

サーバーが HTTPS を使用している場合は、AppScan SSL ルート証明書を追加する必要があります (それにより、AppScan をプロキシーとして使用して送信された要求が受け入れられます)。

手順

1. 「**AppScan** 証明書をローカルにインストール」をクリックし、次に表示される Windows ダイアログ・ボックスで「はい」をクリックして変更を許可します。

   注: 証明書がインストールされると、ボタンが確認メッセージに置き換わります。次にウィザードを使用するときには、(証明書がアンインストールされない限り) このボタンは表示されません。

   注: アンインストールするには、「ツール」>「オプション」>「記録プロキシー」に進み、「削除」をクリックします。
2. リモート・デバイス (携帯電話やエミュレーター) から探査を行う場合、そのデバイスにも証明書をインストールする必要があります。
   a. デバイス上で、`http://appscan` をブラウズします。
   b. デバイス上で、「**AppScan SSL** 証明書のインストール」をクリックします。

   これで、AppScan を記録プロキシーとして使用して、ご使用のデバイスからログインを記録する準備ができました。
3. 「次へ」をクリックします。

次のタスク

『ログイン管理』

ログイン管理

ログイン手順を記録します。

始める前に

オレンジ色の鍵アイコン  は、ログインがまだ記録されていないことを示します。

手順

1. ご使用のデバイス上で、アプリケーションのログイン・ページをブラウズします。
2. AppScanで、 

をクリックします

   「外部ログイン・レコーダー」が開き、外部デバイスに接続されていることを示します。
3. ご使用のデバイス上で、アプリケーションにログインします。

   ログイン要求は、外部ログイン・レコーダーにリストされます。
4. アプリケーションにログインしたら、外部ログイン・レコーダーで「記録の停止」をクリックします。
5. オプションで、不要な要求 (例えば、別のドメインへの要求) のリストを確認し、それらを選択して - をクリックして削除します
6. 「**OK**」をクリックしてレコーダーを閉じます。

緑色の鍵アイコン  は、「セッション内」状況が検出されたことを示します。

7. 「セッション内検出オプションを構成します」チェック・ボックスを選択した場合は、「次へ」をクリックすると、追加のウィザード・ステップである『ログイン管理の詳細』が開きます。ログイン手順を編集するか、またはセッション内検出を有効/無効にする必要がある場合のみ、これを選択してください (前のステップの注を参照)。
8. ウィザードで、「次へ」をクリックします。

関連トピック:

159 ページの『外部ログイン・レコーダー』

次のタスク

『テスト・ポリシー』

「セッション内検出オプションを構成します」を選択した場合、 に進みます 36 ページの『ログイン管理の詳細』

ログイン管理の詳細

(オプション) 記録したログイン手順を確認し、編集します。

手順

1. ログイン手順を確認して編集し、セッション検出パターンが有効なことを確認します。オプションは、で説明されています。 56 ページの『レビューと検証タブ』
2. 「次へ」をクリックします。

次のタスク

『テスト・ポリシー』

テスト・ポリシー

スキャンを特定のタイプのテストに制限することにより、スキャン時間を短縮できます。

このタスクについて

AppScan がスキャン中に送信するテストの数は、大量になることがあります。場合によっては、スキャンを特定のタイプのみに制限することにより、スキャン時間を短縮したほうが良いこともあります。これがテスト・ポリシーです。

AppScan にはデフォルト・テスト・ポリシー、およびユーザーが選択できるいくつかの追加のテスト・ポリシー構成が備えられています。また、自分自身のユーザー定義テスト・ポリシーを使用することもできます。

ウィザードのテスト・ポリシー・ステップには、現在のポリシーの基になっているテスト・ポリシーの名前とその説明が表示されます。

手順

1. テスト・ポリシーが必要に適していることを確認します。(わからない場合は、デフォルト・テスト・ポリシーのままにしてください。)

2. 別のテスト・ポリシーをロードするには、「ポリシー・ファイル」ペインの「定義済みのポリシー」または「最近使用したポリシー」のいずれかをクリックします。詳しくは、 112 ページの『「テスト・ポリシー」ビュー』 を参照してください。
3. ログインおよびログアウト・ページに関するテストを送信します**:** デフォルトでは、AppScan はログイン・ページとログアウト・ページをアプリケーションの残りの部分とともにテストします。次の場合を除き、このデフォルト構成のままにしておいてください。
   - アプリケーションに、これらのページに対する不正入力を行うユーザーを締め出す安全機能が付いている。
   - これらのページがテストされると、アプリケーション・フローが変更される。

   アプリケーションがこれらのテストにどのように応答するかわからない場合、このオプションを選択したままにしておきます。
4. ログイン・ページのテスト時にセッション **ID** を送信しない**:** (このチェック・ボックスは、前のチェック・ボックスが選択されている場合にのみアクティブになり、デフォルトで選択されます。) ログイン・ページをテストする場合、セッション ID によってテストの成功が制限される可能性があるため、このチェック・ボックスは選択したままにしておくことをお勧めします。ログイン・ページをテストするのに有効なセッション・トークンが必要であることが確実な場合にのみ、このチェック・ボックスを選択解除します。

   アプリケーションがどのように応答するかわからない場合、このオプションを選択したままにしておきます。
5. 「次へ」をクリックします。

次のタスク

『完了』

完了

AppScan は、要求をアプリケーションに送信するデバイスの記録プロキシーとして構成されています。これで、アプリケーションのマニュアル探査を開始する準備ができました。

手順

1. 「終了」をクリックします。

   「外部トラフィック・レコーダー」が開き、デバイスに接続されていることを示す状況メッセージが表示されます。
2. 「外部トラフィック・レコーダー」が開き、「着信接続を待機中」状況が示されたら、ご使用のデバイス/アプリケーションから Web サービスのマニュアル探査を行います。
   a. デバイスまたはアプリケーションを使用して、Web サービスを探査します。

      探査を行うと、検出されたドメインがレコーダーの左側のペインにリストされ、URL が右側のペインにリストされます。
   b. 完了したら、AppScan で「記録の停止」をクリックします。
3. マニュアル探査データの確認および編集:

   検出されたドメイン
   : 要求が送信されたすべてのドメインがリストされ、「追加のサーバーおよびドメイン」(「構成」>「URL およびサーバー」>「追加のサーバーおよびドメイン」) のリストへの追加対象と

してデフォルトで選択されています。これにより、それらのドメインをスキャンに組み込むことができます。スキャンに組み込みたくないドメインは選択解除することができます。

ヒント: 他の企業に属しているドメインは選択解除することをお勧めします。

送信された要求数
デバイスから選択された ドメインに送信されたすべての要求が、左側のペインにリストされます。左側のペインでドメインを選択/クリアすると、要求リストは更新されます。不要な場合は、特定の要求を削除することができます。

ヒント: フィルター済みの要求の総数が 200 を超えている場合、その一部を削除することで、スキャンをより効率的に行うことができます。

注: このステージでは、「エクスポート」をクリックして、他のマシンで使用できるように探査データを保存することができます。

4. 「OK」をクリックしてレコーダーを閉じます。

AppScan では、データの処理および表示には少し時間がかかります。

5. テスト・ステージを開始するには、「スキャン」>「テストのみ」をクリックします。

テスト・ステージが開始され、完了するとスキャン結果が表示されます。

関連トピック:

-
- 278 ページの『「記録プロキシー」タブ』
- 219 ページの『第 8 章 結果:セキュリティー問題』

GSC を使用した探査のウィザード

このウィザードのステップをリストします。

1. 『URL およびサーバー』
2. (オプション) 45 ページの『接続設定』
3. 46 ページの『テスト・ポリシー』
4. 46 ページの『完了』

URL およびサーバー

サービス用の WSDL ファイルの URL を入力し、スキャンに含める追加のサーバーおよびドメインがあれば、それらを定義します。

手順

1. **WSDL URL:** サービス用の WSDL ファイルの URL を入力します。

例: `http://www.sitetoscan.com/Service1.asmx?wsdl`

2. URL が正しく入力されていることを確認するには、入力した URL を AppScan ブラウザーで開きます。
   a.  をクリックします (このボタンは、URL をテキスト・ボックスに入力した後にのみ使用可能になります)。 組み込みブラウザーが入力された URL に対して開きます。
   b. 必要な場合は、URL を訂正します。

c. ブラウザーを閉じて、スキャン構成を続行します。

3. 大文字と小文字を区別するパス**:** このチェック・ボックスを選択すると (デフォルト)、大/小文字のみが異なるリンクは別々のページとして扱われます。 例えば、「ReadMe.as」は「readme.as」とは異なるものと見なされます。通常、Unix ベースのサーバーの場合にはこのチェック・ボックスを選択し、Windows ベースのサーバーの場合にはチェック・マークを外します。
4. 追加のサーバーおよびドメイン**:**アプリケーションに開始 URL のもの以外のサーバーまたはドメインが含まれており、かつ *AppScan* ライセンスにそれらが含まれている場合、スキャンに組み込まれるようにここで追加する必要があります。

   a.  をクリックして、「サーバーおよびドメインの追加」ダイアログ・ボックスを開きます。

   b. サーバーのホスト名または IP アドレス、あるいはドメイン・ネーム (例えば、sitetoscan.com) を入力して、「**OK**」をクリックします。

   新規項目がリストに追加されます。
5. 「追加の接続設定を構成する必要があります」 デフォルトでは、AppScan は Internet Explorer のプロキシー設定を使用します。 AppScan で別のプロキシーを使用する場合のみ、このチェック・ボックスを選択します。これにより、「次へ」ボタンをクリックすると追加ステップが開きます。
6. 「次へ」をクリックして、ウィザードの次のステップに進みます。

次のタスク

46 ページの『テスト・ポリシー』

または、「追加の接続設定を構成する必要があります」チェック・ボックスを選択した場合は、以下の作業に進みます。

『接続設定』

接続設定

(オプション) 必要な場合、プロキシー設定およびサーバー・レベルの認証を構成します。

このタスクについて

デフォルトでは、AppScan は Internet Explorer のプロキシー設定を使用します。追加の「URL およびサーバー」ダイアログ・ボックスで、別のプロキシー設定を使用するか、またはプロキシー設定をまったく使用しないように AppScan を構成できます。

手順

1. 以下の 3 つのプロキシー・オプションの 1 つを選択します。
   - **Internet Explorer** のプロキシー設定を使用する**:** (デフォルト) これを選択すると、AppScan はアプリケーションへの接続時に、Internet Explorer 接続のアドレスおよびポートを使用します。
   - プロキシーを使用しない**:** AppScan でプロキシー設定をまったく使用しない場合は、これを選択します。
   - カスタムのプロキシー設定を使用**:** Internet Explorer で使用されるもの以外のアドレスおよびポートを使用する場合は、これを選択します。
2. プロキシーを使用するオプションのいずれかを選択した場合、接続時に使用する AppScan のユーザー名、パスワード、およびドメインを設定することもできます。これを行うには、「構成」ボタンをクリックします。

3. プラットフォームでサーバー・レベルの認証が必要な場合、「**HTTP** 認証」領域でユーザー名、パスワード、およびドメインを設定します。
4. 「次へ」をクリックして、テスト・ポリシー設定のステップに進みます。

次のタスク

『テスト・ポリシー』

テスト・ポリシー

マニュアル探査が完了したときに AppScan がサービスに送信するテストのテストの種類を定義します。

手順

1. 「**WSDL** スキャン構成ウィザード」>「プラットフォーム認証」ダイアログ・ボックスで、「次へ」をクリックします。

   ウィザードの **WSDL** テスト・ポリシー・ステップが表示されます (37 ページの『テスト・ポリシー』と同じです)。
2. テスト・ポリシーが必要に適していることを確認します。(カスタム・ポリシーを定義していなければ、Web サービス・テスト・ポリシーをお勧めします。)
   - 別のテスト・ポリシーをロードするには、「ロード」をクリックします。

     「テスト・ポリシーのロード」ダイアログ・ボックスが開き、事前定義ポリシーかユーザー定義ポリシーから 1 つを選択できます。
   - 現在のテスト・ポリシーを編集するには、「編集」をクリックします。

     「テスト・ポリシー・マネージャー」が開き、スキャンに組み込むテストを正確に構成することができます。

   詳細については、 115 ページの『テスト・ポリシーのインポート』を参照してください。
3. 必要な場合、「詳細テスト設定」ボタンをクリックして、追加オプションを構成できます。詳しくは、 115 ページの『テスト・ポリシーのインポート』 を参照してください。必要でなければ、「次へ」をクリックして、ウィザードの最終ステージに進みます。

次のタスク

『完了』

完了

これで、GSC を使用してサービス探査を手動で開始する準備ができました。

手順

「完了」をクリックします。
Generic Service Client (GSC) が開こうとしているというプロンプトが表示されることがあります (その場合、「**OK**」をクリックします)。その後、プログラムが開きます。

次のタスク

161 ページの『GSC の使用』

「スキャン構成」ダイアログ・ボックス

このタスクについて

「スキャン構成」ダイアログ・ボックスには、スキャンを構成するための多数のオプションがあります。メイン・オプションはスキャン構成ウィザードで使用することもできますが、デフォルト設定の多くを変更したり、既存の構成を微調整する場合にはダイアログ・ボックスを使用することをお勧めします。

手順

「スキャン構成」ダイアログ・ボックスを開くには、ツールバーの「構成」アイコン  をクリックします (または、**F10** を押します)。
「スキャン構成」ダイアログ・ボックスには、4 つのグループに分割されたさまざまなビューがあります。これらのビューにアクセスするには、左側のビュー選択ペインにある関連項目をクリックします。

注**:** スキャンを停止して構成を変更する場合、変更はすでに送信された要求には反映されません。変更をスキャン全体に適用するには、新規スキャンを開始する必要があります。

ヒント**:** 複数のビューで構成オプションを変更してから、「OK」をクリックするとすべての変更を保存できます。 (変更はビュー間を移動すると保持されますが、保存されるのは「OK」をクリックした場合のみです。)

表示	構成対象の選択**:**
探査	
48 ページの『「URL およびサーバー」ビュー』	開始 URL、システム・タイプ、および追加サーバー
52 ページの『「ログイン管理」ビュー』	ログイン方法の設定、ログイン手順の記録 (オプション)、およびセッション内検出の構成
66 ページの『「環境定義」ビュー』	アプリケーション環境に関する情報の提供
66 ページの『「除外するパスおよびファイル」ビュー』	スキャンから除外するパスおよびファイル・タイプ
72 ページの『「探査オプション」ビュー』	スキャン制限、リンク抽出方法、および一般的な探査方法
78 ページの『「パラメーターおよび Cookie」ビュー』	スキャンから除外するセッション ID およびリスト・パラメーターの識別
92 ページの『「フォームの自動入力」ビュー』	フォームを入力するための有効なパラメーター値の AppScan への指定
95 ページの『「エラー・ページ」ビュー』	カスタム・エラー・ページを識別するためのストリング、正規表現、および URL の追加
98 ページの『「マルチステップ操作」ビュー』	アプリケーションの一部にアクセスするのに必要なマルチステップ操作の記録および管理
106 ページの『「コンテンツ・ベースの結果」ビュー』	階層 URL 構造がないアプリケーション (単一エントリー・ポイント・アプリケーションなど) の場合は、AppScan でサイト・ツリーを配置する方法を定義します。
108 ページの『「Glass Box」ビュー』	AppScan Glass Box エージェントがアプリケーション・サーバーにインストールされている場合は、Glass Box のスキャンをここで構成します。
接続	

表示	構成対象の選択:
110 ページの『「通信およびプロキシー」ビュー』	通信タイムアウトおよびプロキシー・サーバー設定の構成
111 ページの『「HTTP 認証」ビュー』	サーバー側の認証およびクライアント側の証明書の追加 (アプリケーションで必要とされる場合)
テスト	
112 ページの『「テスト・ポリシー」ビュー』	テスト・ポリシーの定義および編集 (どのテストがアプリケーションに送信されるか)
117 ページの『「テストの最適化」ビュー』	製品のライフサイクルで詳細なスキャンよりも迅速なスキャンを優先する場合に、テストの最適化を適用します。
118 ページの『「テスト・オプション」ビュー』	追加のテスト・オプション
121 ページの『「権限拡張」ビュー』	AppScan は、異なるユーザー権限を使用して実行されたスキャンを参照し、アクセス許可が不十分なユーザーがアクセス可能な特権リソースを見つけます。
122 ページの『「マルウェア」ビュー』	悪質なリンクをテストします。
全般	
122 ページの『「スキャン・エキスパート」ビュー』	スキャン・エキスパートの動作およびモジュールの構成
124 ページの『「詳細構成」ビュー』	拡張スキャン・オプションの構成

「URL およびサーバー」ビュー

「スキャン構成」ダイアログ・ボックスの「URL およびサーバー」ビューです。

スキャンを開始する URL を定義する必要があります。残りの設定はオプションです。

設定	詳細
開始 URL	スキャンの開始点となるアプリケーションの URL を入力します。 AppScan は URL への到達を試み、成功した場合は、緑のチェック・マークと「サーバーへ接続済み」の確認が開始 URL の下に表示されます。構成変更により問題を修正できる場合、AppScan はどのような変更が必要であるか提示し、「構成」ダイアログ・ボックスで適切なビューにリンクします。  入力したページをブラウザーで表示します。必要であれば、別の URL にブラウズし、ツールバーを使用して、新規ページをスキャン用の開始 URL として設定できます。ブラウザーを閉じて、スキャン構成を続行します。 **注:** デフォルト・ブラウザーが使用されています。デフォルト・ブラウザーには、IE または Chromium の 2 つの内、いずれかを設定することができます。また、「ツール」>「オプション」>「参照」タブで、サポートされている外部ブラウザーを設定することもできます。  開始 URL を再度テストします。構成後、再開した際にサーバーがダウンした場合にこのボタンをクリックします。 **ヒント:** スキャンの構成後 に、開始 URL のドメイン、スキーム、またはポートを変更する場合、構成に対する変更が必要になることがあります。AppScan によってこの構成に自動的な変更が試行されるかどうかについて確認が求められます。詳細については、 51 ページの『開始 URL ホストの変更』 を参照してください。
このディレクトリー配下のリンクだけをスキャン。	これを選択すると、スキャンは開始 URL 以下のページに制限されます。他の URL へのリンクが「追加のサーバーおよびドメイン」(以下で説明) のリストに含まれている場合であってもスキャンされません。 詳しくは、『開始 URL フォルダーへのスキャンの制限』 を参照してください。
すべてのパスを大/小文字の区別をつけて扱う	これを選択すると、大/小文字でお互いに異なるリンクは、別のページであるとみなされます。例えば、「ReadMe.as」は「readme.as」とは異なるものと見なされます。 選択が解除されると、すべての URL は小文字で表示されます。 アプリケーション・ホストにおけるファイル・システムが、大/小文字を区別している場合、このチェック・ボックスを選択します。ほとんどの場合、UNIX ベースのサーバーではチェック・ボックスにチェック・マークを付け、Windows ベースのサーバーではチェック・ボックスのチェック・マークを外します。
追加のサーバーおよびドメイン	ご使用のアプリケーションに開始 URL のドメイン以外のドメインへのリンクが含まれている場合、それらのリンクをスキャンに組み込むには、リンクをここで追加する必要があります。 注: ご使用の AppScan ライセンスに含まれるサーバー/ドメインのみを追加できます。 詳しくは、 51 ページの『追加のサーバーおよびドメイン』 を参照してください。

開始 URL フォルダーへのスキャンの制限

スキャンの範囲を開始 URL のフォルダー以下に簡単に制限できます。

このタスクについて

「開始 URL」フィールドの下のチェック・ボックスを選択すると、スキャンを特定ディレクトリー以下に制限するために必要なフィルターが自動的に作成されます。

手順

1. 「スキャン構成」>「**URL** およびサーバー」を開きます。
2. スキャンの制限範囲となるディレクトリーの URL を入力するか、貼り付けます。
3. 「このディレクトリー配下のリンクだけをスキャン」チェック・ボックスを選択します。

   これで、スキャンはこの URL の下にあるパスに制限されるようになります。この範囲外のリンクはスキャンされません。

例

「開始 URL」が `http://main/bank/` と定義されている場合:

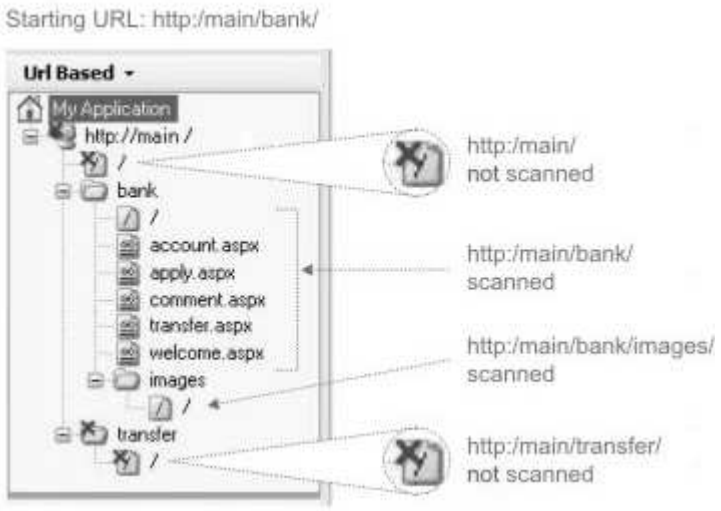
- 以下のリンクはスキャンされます。
  - `http://main/bank/transfer.aspx/`
  - `http://main/bank/transfer/page_1.aspx/`
- 以下のリンクは無視されます。
  - `http://main/transfer.aspx/`
  - `http://main/transfer/page_1.aspx/`

開始 URL を構成するときに、このチェック・ボックスを選択した場合は、「除外するパスおよびファイル」表 (「スキャン構成」>「除外するパスおよびファイル」) の最上部に次の 2 つの項目が追加されます。

項目タイプ	パス	一致	動作
除外 (開始 URL)	.*	正規表現	常に表の先頭に表示されます。降格することはできません。 編集も削除もできません。ただし、次の項目 (「例外」) が削除されると、この項目も削除されます。
例外 (開始 URL)	http://main/bank	絶対パス	常に表の 2 番目に表示されます。昇格も降格もできません。 編集は可能 です。(これは、まれに AppScan が開始 URL ディレクトリーを誤認した場合に、例外を編集できるようにするためです。) 削除されると、前の項目 (「除外」) も削除され、「開始 URL」チェック・ボックスは選択解除されます。

注**:** 他の除外や例外とは異なり、これらの 2 項目は背景がグレイ表示されており、それらが特殊な状態であることを示しています。

スキャンが開始し、左ペインにアプリケーション・ツリーが表示されると、開始 URL の下にないアプリケーションのパーツへのリンクは赤い X 印付きで示されます。これは、それらがスキャンされなかったことを示しています。



次のタスク

追加された例外が正しいかどうかの確認、またはその例外の編集は、「除外するパスおよびファイル」ビューから行えます (70 ページの『特定のフォルダーへのスキャンの制限』を参照)。

追加のサーバーおよびドメイン

スキャンに開始 URL のドメイン以外のドメインを組み込むことができます。

このタスクについて

ご使用のアプリケーションに開始 URL のドメイン以外のドメインへのリンクが含まれている場合、AppScan がスキャンにこれらのリンクを組み込むように、ここで追加する必要があります。

注: ご使用の AppScan ライセンスに含まれるサーバー/ドメインのみを追加できます。

手順

- サーバーを追加するには、  をクリックして、サーバー/ドメイン名を入力します。

  例: `demo.testfire.net` または `65.61.137.117`

  サーバーがリストに追加されます。

- リスト内のサーバーを編集するには、そのサーバーを選択して  をクリックします。

- リストからサーバーを削除するには、これを選択して  をクリックします。

開始 URL ホストの変更

構成されたスキャンの開始 URL のホスト、スキーム、またはポートを、ログイン、マルチステップ操作、およびマニュアル探査データのいずれも再記録せずに変更できます。

このタスクについて

ログイン、マルチステップ操作、またはマニュアル探査 (あるいはそのすべて) の記録を既に完了し、その後に開始 URL のホスト、スキーム、またはポートを変更する場合、これらの記録内の要求と応答の更新

および検証が必要になります。 「スキャン」 > 「ホスト/スキーム/ポートの変更」をクリックすると URL を変更できるダイアログ・ボックスが開き、AppScan によって必要な変更が自動的に更新、検証、および確認されます。

ダイアログ・ボックスには、実行されるステップが表示され、各ステップがいつ正常に完了したかを示します。 更新処理が正常に完了しなかった場合、ダイアログ・ボックスには失敗したステップが示され、変更を保存して手動で続行するか、あるいはすべての変更を元に戻すかの選択肢が示されます。

重要: 場合によって、AppScan は応答を不適切に更新することがあり、スキャンの一部またはすべてが失敗します。 その場合、問題がある手順を再記録する必要があります。

注: マニュアル 探査のデータは更新されても、開始 URL の変更時に自動 探査データとスキャン結果は削除されます。

注: このオプションを使用して変更できるのは、開始 URL のみ の、ホスト、スキーム、またはポートのみ です。開始 URL にその他の 変更を加えたり、またはスキャンのいずれかの追加 ドメインのホスト、スキーム、またはポートを変更したりする必要がある場合、このオプションは使用できません。代わりに、スキャンをテンプレートとして保存して、そのテンプレートを使用して新規スキャンを作成してください。

手順

1. スキャン (.scan) またはスキャン・テンプレート (.scant) ファイルを開きます。次に以下のようにします
   - スキャン・テンプレートの場合: ツールバーで、「スキャン構成」>「**URL** およびサーバー」をクリックします。
   - 構成されたスキャンの場合: メニュー・バーで、「スキャン」>「ホスト/スキーム/ポートの変更」をクリックします。
2. 必要に応じて開始 URL のホスト、スキーム、またはポートを変更します。

   AppScan はサーバーへの接続を試み、成功すると緑色のチェック・マークが示されます。
3. 「**OK**」をクリックします。

   AppScan は構成の更新を試みます。緑色のチェック・マークは各ステップが正常に完了したことを示します。
4. すべてのステップが正常に終了した場合: 「**OK**」をクリックし、構成の変更を保存します。

   ステップの **1** つが失敗した場合:
   - 構成の変更を保存するには、失敗したステップを手動で完了し、再試行してから「**OK**」をクリックします。
   - すべての変更を取り消して、元の開始 URL に戻すには、「キャンセル」をクリックします。

   重要: 場合によって、AppScan は応答を不適切に更新することがあり、スキャンの一部またはすべてが失敗します。 その場合、問題がある手順を再記録する必要があります。

「ログイン管理」ビュー

「スキャン構成」ダイアログ・ボックスの「ログイン管理」ビューです。

「スキャン構成」ダイアログ・ボックスの「ログイン管理」ビューは、AppScan がアプリケーションにログインする方法、およびいつログアウトしたかを認識する方法を構成するために使用します。

AppScan は、ログイン要求を自動的に検出することができ、ユーザー名とパスワード・パラメーターを入力します。ご使用のアプリケーションに、非標準のログイン手順のアクションがある場合は、これらのアクションを AppScan で使用できるように記録することができます。

「ログイン管理」ビューには、次のようなタブがあります。

- ログイン
- レビューと検証
- セッション ID
- 詳細

「ログイン」タブ

「スキャン構成」 > 「ログイン管理」 > 「ログイン」タブ

「スキャン構成」ダイアログ・ボックスの「ログイン管理」ビューは、AppScan がアプリケーションにログインする方法、およびいつログアウトしたかを認識する方法を定義するために使用します。

AppScan は、ログイン要求を自動的に検出することができ、ユーザー名とパスワード・パラメーターを入力します。ご使用のアプリケーションに、非標準のログイン手順のアクションがある場合は、これらのアクションを AppScan で使用できるように記録することができます。

設定	詳細
ログイン方法の選択	
記録済み (推奨)	(デフォルトの方法) この方法を選択すると、ブラウザーが開き、ログイン手順を記録します (HTTP 要求とユーザー・アクションの両方が記録されます)。AppScan は、アプリケーションへのログインが必要なときは必ずこの手順を使用します。 手順を記録するには、  を使用します。Web アプリケーションについては、を参照してください。RESTful (およびその他の) Web サービスについては、 157 ページの『外部トラフィック・レコーダーを使用した探査』 を参照してください。
自動ログイン	この方法を選択すると、AppScan は、ご使用のアプリケーションのログイン・フォームを自動的に検出し、指定のユーザー名とパスワードを使用することができます。 (この方法は、「記録されたログイン」方法より信頼性が劣ります。)
プロンプト	ログイン時に毎回人間が対応する必要がある (2 因子認証、ワンタイム・パスワード、CAPCHA など) 場合は、この方法を選択します。 このオプションを選択した場合でも、ログイン手順を記録する必要があるので注意してください。これは、AppScan に対して、ログインしているかどうか確認するために後で使用することができるセッション内ページを提供します。詳しくは、 54 ページの『ログインの記録』 を参照してください。
なし	アプリケーションがユーザーからのログインを必要としない場合は、このオプションを選択します。
ログイン検証状況インディケーター	

設定	詳細
鍵アイコン	鍵アイコンは、セッション内検出の状況を示します。  有効に設定され、構成されています。(セッション内ページが、ログイン手順において、自動またはユーザーによって識別されています。)  有効に設定されていますが、完全には構成されていません。  有効にされていますが、構成に失敗しました。  無効に設定されています。 詳細については、 63 ページの『「検出パターン」ダイアログ・ボックスを選択します。』を参照してください。
ログイン設定のインポートまたはエクスポート	
インポート	ログイン手順を記録すると、それはスキャンの一部として保存されます。スキャンをテンプレートとして保存する場合、ログイン手順はテンプレートの一部として保存されます。 前に保存したログイン手順を `*.login` ファイルとしてインポートするには、「インポート」ボタンをクリックします。
エクスポート	また、今後のスキャンで使用するためにログイン手順自体をエクスポートするには、「エクスポート」ボタンをクリックします。手順は `*.login` ファイルとして保存されます。

ログインの記録:
始める前に

ログイン手順を記録するには、その前に (「構成」>「URL およびサーバー」ビューまたはウィザードのいずれかで) 開始 URL が定義されていなければなりません。

このタスクについて

「記録されたログイン」では、サイトにログインする手順 (どのリンクをクリックするか、どのテキストをフォームに入力するか、およびそれらを行う順序) を AppScan に指示します。これを記録するとすぐに、AppScan は、ログインされているかを確認するために将来使用できるセッション内パターンを識別しようとします。これが完了した後、AppScan は、スキャン中にログアウトされたことを検出するたびに、そのログイン手順を使用してログインし直します。

AppScan は、サイトの応答を正確に評価できるよう、常にサイトへのログインおよびログアウト状態を把握している必要があります。スキャン中、AppScan はセッション内検出要求を繰り返し送信し、応答に「セッション内検出パターン」が含まれていることを確認して、まだログイン状態であることを検証します。 AppScan が、ページの応答でこのパターンを検出しなかった場合、AppScan は、ログアウト状態であると見なし、ログイン手順をやり直してログインを再試行します。その結果、通常はスキャン中にログイン手順が何回も繰り返されることになります。そのため、ログイン手順は可能な限り少ないステップで構成することが推奨されます。また、「セッション内」ページが小規模なページであり、追跡パラメーターや

Cookie が存在しない場合も、スキャン時間が大幅に増加する可能性があるため、ステップを少なくすることが効果的です。

手順

1. 「スキャン構成」>「ログイン管理」>「ログイン 」タブで「記録済み」を選択します。
2. 

 > 「**AppScan IE** ブラウザー」をクリックします。

   ブラウザーが開始 URL に対して開き、アクションを記録し始めます。

   注: ご使用の Web サイトのログインが Internet Explorer をサポートしていない場合、代わりに「**AppScan Chromium** ブラウザーの使用」をクリックしてください。

   注: 開始 URL がまだ定義されていない場合、先に進む前に定義するように警告されます (48 ページの『「URL およびサーバー」ビュー』を参照してください)。

   注: ログイン手順が以前に記録されている場合、新規の記録によって既存の記録が上書きされることが警告されます。

   注: スキャンに外部ブラウザーを使用するように AppScan を構成している場合 (「ツール」>「オプション」>「外部ブラウザーの使用」>「ブラウザーの選択」)、ログインの記録に AppScan ブラウザーまたは外部ブラウザーのどちらを使用するかを選択できます。可能な場合は、ログインの記録には AppScan ブラウザーを使用することをお勧めします (スキャンに異なるブラウザーを使用している場合でも)。AppScan ブラウザーではスキャン中のログインの成功率を向上させるような追加の情報を記録するためです。 AppScan ブラウザーでのログインの記録がご使用のアプリケーションでは作動しない場合は、外部ブラウザーを使用してください。

   注: ご使用のアプリケーションが Internet Explorer をサポートしていない場合、外部ブラウザーで作業するように AppScan を構成する必要があります。
3. サイトにログインし、必要に応じてフォームに入力し、リンクをクリックします。

   ヒント: デフォルトでは、ログインしたときに表示されるページが、セッション内 URL として AppScan で使用されます。AppScan は、スキャン中にこの URL を数秒間隔で送信し、この URL がまだログインしているかどうかを確認します。このページからサイズの大きな応答が送信された場合、またはこのページに追跡対象のパラメーターや Cookie が含まれている場合は、追跡対象のパラメーターや Cookie が存在せず、サイズの小さな応答を持つページ (まだログイン中のページ) に到達するまで 1 つ以上の追加のリンクをクリックすることにより、スキャンのパフォーマンスを改善することができます。次に、ブラウザーを閉じて 「レビューと検証」タブに移動し、「セッション内 URL」として後の ページを選択します。
4. サイトに正常にログインしたら、「サイトにログインしています **(I am logged in to the site)**」をクリックします。

   AppScan が、スキャン時に使用するために、ログイン情報をログイン要求から抽出しようとします。

   注: 場合によっては、ログイン・ページで提供される情報に不備があります。その場合は、ログイン後に追加のステップをクリックするように、またはサイトからログアウトするように AppScan に指示される場合があります。

注: ログイン・メカニズムが JavaScript を使用してログイン・データを操作する場合は、ダイアログ・ボックスが開き、AppScan が抽出したログイン・データが正しいかどうかを確認するよう求められることがあります。必要に応じて、パラメーターや値を入力または修正して、「**OK**」をクリックします。

「セッション情報」ダイアログ・ボックスが開き、記録したログイン要求が表示され、  が  に変わります。これは、そのセッション内検出が有効であることを示します。

注: 鍵アイコンが赤色  に変化した場合、AppScan はスキャン中に使用できるセッション内ページのパターンを識別してログアウトしていないことを確認しようとしましたが、それができませんでした。こうなった場合は、AppScan の「セッション内パターン」を識別する必要があります。詳しくは、 63 ページの『「検出パターン」ダイアログ・ボックスを選択します。』を参照してください。場合によっては、より具体的なメッセージが表示され、この問題のトラブルシューティングに関するこのヘルプ内のページへのリンクが示されることがあります。 356 ページの『ログインのトラブルシューティング』を参照してください。

5. 記録された手順に変更を加える (例えば、不要なステップを除去する) には、『レビューと検証タブ』を参照してください。

   ヒント: 一般に、ユーザーがログインで使用する URL は、「セッション内」としてマークされています (この応答は、セッション内パターンが含まれる最初の応答です)。ただし、後で、セッション内パターンも含まれるが、より小規模なページ、または追跡対象パラメーターや Cookie が含まれないページという利点がある URL を選択することが必要な場合もあります。さらに、ユーザー資格情報を使用する POST 要求が、ユーザーがログインする要求であり、最初にセッション内パターンが含まれている場合があります。セッション内ページでは、セッション内検査が毎回資格情報を送信することでセッション応答での誤検出につながるため、これは不適切な選択です。 64 ページの『セッション内検出の最適化』を参照してください。

6. 新規のログイン手順を保存するには、「**OK**」をクリックします。

   ヒント: セッション内ページに追跡対象のパラメーターと Cookie が含まれていないことがわかっている場合は、「詳細構成」>「セッション管理: セッション内ページの解析 **(Session Managment: Parse in-session page)**」設定を「False」に変更すると、スキャンのパフォーマンスを改善することができます。 124 ページの『「詳細構成」ビュー』を参照してください。

レビューと検証タブ

「スキャン構成」>「ログイン管理」>「レビューと検証」タブ

ログイン手順を記録すると、AppScan はアクションと要求の両方を記録します。これらは 「アクション」と「要求」の 2 つのサブ・タブに表示されます。ログインの再生を行う場合、AppScan は、(デフォルトでは) アクション・ベースのログインの再現を試行します。これが正常に完了しない場合、要求ベースのログインを使用します。

このタブを使用して、以下を確認および編集します。

- ログイン手順のアクション・ベース・バージョン
- ログイン手順の要求ベース・バージョン

- セッション内検出の要求
- セッション内 (またはセッション無効) 検出パターン

これは以下の場合にも使用します。

- 現在の設定の確認

表 *1.* 「レビューと検証タブ」の設定

設定	詳細
ログイン再生	このセクションは、ログイン方法に「記録されたログイン」を選択した場合にのみ表示されます
ログイン再生方法	AppScan は、記録するログイン手順の 2 つのバージョン保存します。1 つは実行したアクションをベースに、もう 1 つは実際に送信された HTTP 要求をベースにしています。 • アクション・ベース: (可能な場合はデフォルトで使用されます) AppScan は、アクション・ベースのログインを使用してログインを試行し、ユーザーのクリックとキー・ストロークを再生します。 –  再生: アクション・ベースのプレイヤーを開き、記録されたログイン手順をブラウザーで再生します。 – 編集: アクション・ベースのエディターを開き、ログイン記録の詳細の表示と編集を行います。 • 要求ベース: 最初の方法が失敗した場合、AppScan は、要求ベース・バージョンのログインを使用します。要求ベース・バージョンのログインでは、ログイン記録から未加工の HTTP 要求を再送信します。 – 編集: 要求ベースのエディターを開き、ログイン記録の詳細の表示と編集を行います。 どちらかの方法が失敗したことがメッセージに示された場合、もう一方の方法を使用してください。 **注:** アクション・ベースのログインを選択してスキャン中に失敗した場合、AppScan は要求ベースのログインを試行します。成功した場合、この設定は自動的に要求ベースに変更されます。
自動ログイン	このセクションは、ログイン方法に「自動ログイン」を選択した場合にのみ表示されます
自動検出セッション内構成ボタン	クリックして、AppScan で以下のアクションを実行します。 • 指定された資格情報を使用して、サイトへのログインを試みます。 • ログイン・ページのセッション内検出パターンを識別します (以下を参照) • セッション識別子を構成します (を参照) 64 ページの『「セッション ID」タブ』
セッション検出	AppScan は、サイトの応答を正確に評価できるよう、常にサイトへのログインおよびログアウト状態を把握している必要があります。スキャン中、AppScan はセッション内検出要求を繰り返し送信し、応答に「セッション内検出パターン」が含まれていることを確認して、まだログイン状態であることを検証します。 AppScan が、ページの応答でこのパターンを検出しなかった場合、AppScan は、ログアウト状態であると見なし、ログイン手順をやり直してログインを再試行します。その結果、通常はスキャン中にログイン手順が何回も繰り返されることになります。そのため、ログイン手順は可能な限り少ないステップで構成することが推奨されます。また、「セッション内」ページが小規模なページであり、追跡パラメーターや Cookie が存在しない場合も、スキャン時間が大幅に増加する可能性があるため、ステップを少なくすることが効果的です。
セッション内検出の要求	これは AppScan がセッション内の検証に使用する要求です。この要求は、ユーザーのログインの有無によって異なる応答を生成するものにする必要があります。 AppScan は、有効なセッション内要求を識別しようとします。これはドロップダウン・リストから 1 つ選択できます。見つからない場合、または適切なものがない場合は、詳細な要求選択ボタンを使用して独自の内容を選択できます。

表 1. 「レビューと検証タブ」の設定 (続き)

設定	詳細
詳細な要求選択ボタン	このボタンを使用するとダイアログ・ボックスが開きます。ここでログイン手順での要求を検討し、セッション内検出の要求を選択できます。詳しくは、 61 ページの『「詳細なセッション内要求の選択」ダイアログ』 を参照してください。
セッション内検出パターン:	(セッション内検出の要求が選択された場合のみアクティブになります) このフィールドには、選択したセッション内検出の要求で見つかったパターンが表示されます。これはユーザーがセッション内にいる (または、オプションによってはセッション無効である) ことを示しています。 ドロップダウン・リストで、AppScan がログイン記録で識別した候補から検出パターンを選択できます。パターン下の緑と赤のメッセージは、現在のパターンがセッション内またはセッション無効であることを示しています。 **注:** 通常、セッション内パターンを使用することが推奨されます。ただし、セッション内要求の後にセッション内パターンが必ずしも返されない場合や、定義が複雑になる場合がまれにあります。そうした場合は、セッション内パターンの代わりにセッション無効パターンを使用することができます。AppScan が有効なパターンを識別できない場合や、別のパターンを選択する必要がある場合は、「パターンの詳細な選択」ボタンを使用します (この表の次の行)。 **RegExp:** パターンを識別するために正規表現を入力するには、このチェック・ボックスを選択します。
パターンの詳細な選択ボタン	(セッション内検出の要求が選択された場合のみアクティブになります) このボタンで検出パターンを選択ダイアログ・ボックスが開き、記録したログイン手順の要求に対するセッション内およびセッション無効の応答の内容が表示されます(選択した検出パターンに基づきます)。応答のコンテキストで選択した検出パターンを確認し、コンボ・ボックスに表示されない検出パターンを定義することができます。このダイアログでは、すべての記録された応答を切り替えることができます。ボックスの上部には、AppScan が送信したセッション内およびセッション無効の要求も表示されます。
検証	
検証 ボタン	(現在のログイン手順が未検証の場合のみアクティブになります) クリックすると手順とセッション検出パターンを検証します。
鍵アイコン	鍵アイコンは、セッション内検出の構成状況を示します。  有効に設定され、構成されています。(セッション内ページが、ログイン手順において、自動またはユーザーによって識別されています。)  有効に設定されていますが、完全には構成されていません。  有効にされていますが、構成に失敗しました。  無効に設定されています。 詳細については、 63 ページの『「検出パターン」ダイアログ・ボックスを選択します。』 を参照してください。

「アクション・ベースのログインの編集」ダイアログ・ボックス:

検証に失敗した場合、「構成」 > 「ログイン」 > 「レビューと検証」 > 「(アクション・ベースの) 編集」から開くダイアログを使用して、ログイン手順をトラブルシューティングできます。

要求ベースのログインが成功した場合でも、可能であればアクション・ベースのログインをトラブルシューティングすることを推奨します。このダイアログ・ボックスでは、以下が可能です。

- 「再生」をクリックして、選択したブラウザーでログインを再生します。
- 選択したブラウザーを変更し、別のブラウザーで「再生」します。
- 「選択」 > 「待機アクション」をクリックし、要求間の待ち時間を増やします。
- 手順内の特定の要求の「タイプ」をレビューし、必要に応じて変更します。
- 「再生アクションの編集」をクリックして、XML 形式で表示および編集します。
- 1 回のログイン試行のタイムアウトを増やします。

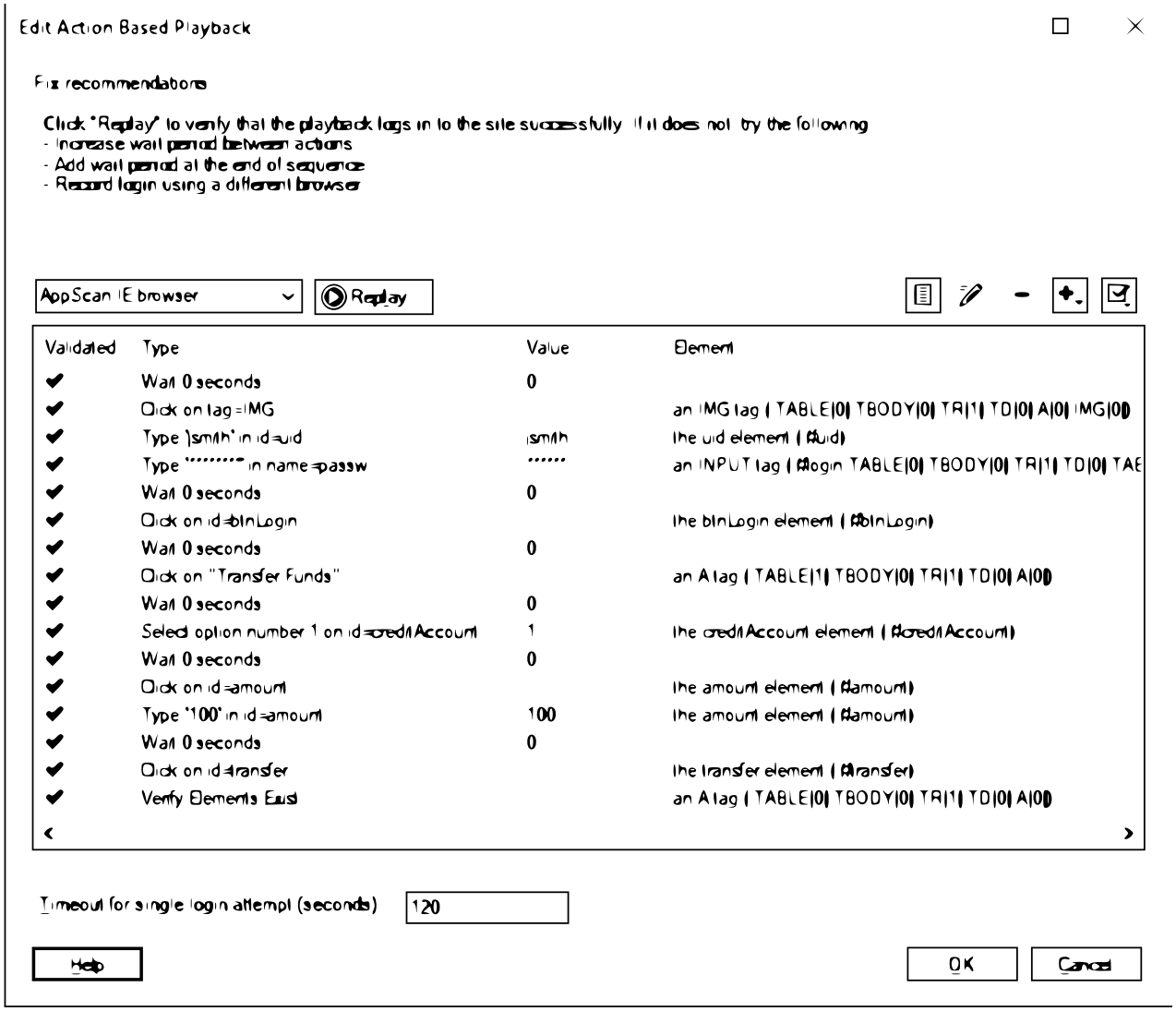


図 *1.* 「アクション・ベースの再生の編集」ダイアログ・ボックス

表 2. 「アクション・ベースの再生の編集」の設定

項目	説明
「ブラウザー」フィールド	ログイン再生のために現在選択されているブラウザーを表示します。これは、ドロップダウン・リストで変更できます。
「再生」ボタン	選択したブラウザーで、記録されたログイン手順を再生します。
要求、および要求間の待ち時間のリスト。	各アクションについて以下を表示します。 • 検証済み: 成功したアクションには緑のチェック・マーク、失敗したアクションには赤の X • タイプ: アクションの説明 (「待機」、「クリック」、または (値の) 「設定」) • 値: 待機アクション: 秒数、ユーザー・アクション: アクション名 • 要素: アクションが実行される HTML 要素 選択したアクションでは、表の上にあるアイコンを使用して以下の操作を実行できます。 •  再生アクションを XML として表示および編集 •  :アクション値の編集 •  :アクションの削除 •  :アクション間に待機時間を追加 •  :選択したアクションの前後に「待機」アクションを追加します。
単一のログイン試行のタイムアウト (分)	ログイン手順にさらに時間が必要な場合は、この設定値を増やすことができます。

「要求ベースのログインの編集」ダイアログ・ボックス:

検証に失敗した場合、「構成」 > 「ログイン」 > 「レビューと検証」 > 「(要求ベースの) 編集」から開くダイアログを使用して、ログイン手順をトラブルシューティングできます。

これは、「詳細なセッション内要求選択」ダイアログの簡易版です。

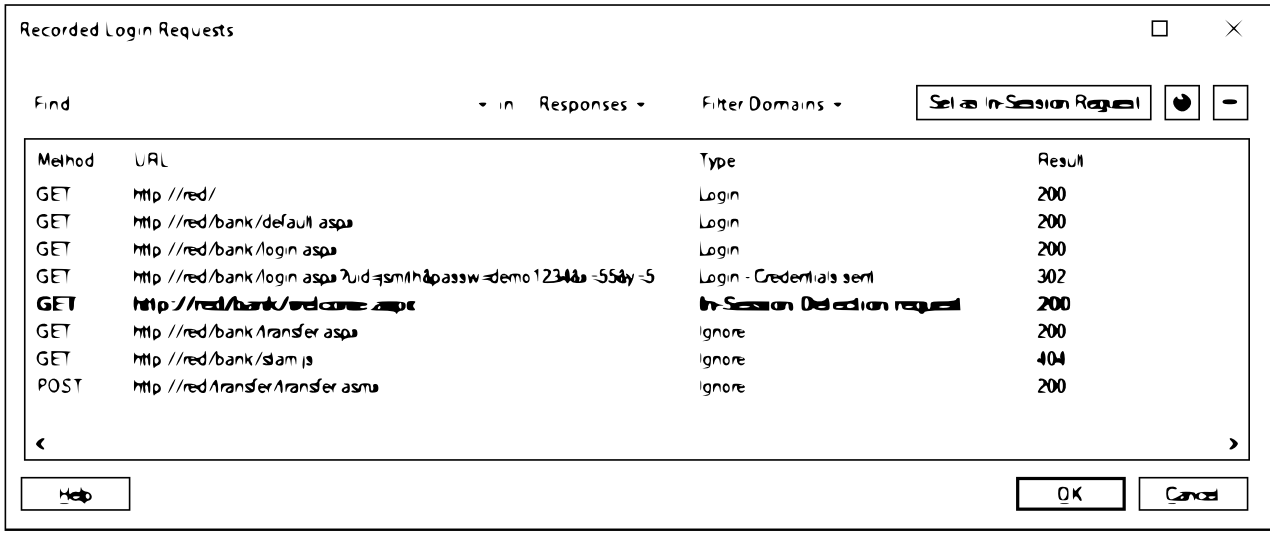


図 2. 「要求ベースの再生の編集」ダイアログ・ボックス

表 3. 「記録されたログイン要求」設定

設定	詳細
「メイン」リスト	記録されたログイン手順に含まれているすべての要求が表示されます。
検索	URL、要求、応答、またはすべてに入力したテキスト文字列が含まれている要求のみを表示します。
ドメインのフィルタリング	ドロップダウン・リストで選択したドメインからの要求のみを表示します。クリックして、AppScan で以下のアクションを実行します。
「セッション内要求として設定」ボタン	選択した要求をセッション内要求として設定します。この要求は、まだログイン中であることを確認するために、スキャン中に AppScan によって使用されます。 この操作は、リスト内の要求を右クリックして行うこともできます。
	ログインが記録されたときに受け取った、選択した要求に対する応答が表示されます。次の 2 つのタブを持つウィンドウが開きます。「ブラウザー」タブには、受け取った応答が表示されます。「要求/応答」タブには、要求と応答の未加工データが表示されます。
	選択した要求がログイン手順から削除されます。

「詳細なセッション内要求の選択」ダイアログ**:**

「詳細なセッション内要求の選択」ダイアログ・ボックスは、「構成」 > 「ログイン」 > 「レビューと検証」 > 「詳細な要求の選択」から開きます。

これは、「要求ベースのログインの編集」ダイアログ・ボックスにさらに多くのオプションが追加されたバージョンです。このダイアログ・ボックスでは、以下が可能です。

- ログイン時に送信した要求の順序を表示します。
- 「セッション内検出の要求」を表示します。

注**:** 「セッション内」とマークされたページは、最初に強調表示されるページになります。それより前の「ログイン」ページが強調表示されている場合は、セッション内パターンが正しくないか、間違ったページが「セッション内」としてマークされています。

- 手順内の URL をブラウザーに表示します。
- 別の要求をセッション内要求として設定し、この新しい要求から新しいセッション内検出パターンを選択します。
- 「セッション内」URL の前の不要な要求を削除し、AppScan がスキャン中にこれらの不要な要求を何回も繰り返すことがないようにします。
- セッション内検出要求の後に送信された、セッション内検出パターンを含み、かつ「無視」とマークされた要求を表示します。
- 手順内で要求を検索します。
- 特定ドメインからの要求のみを表示します。
- 「検出パターンの選択」ダイアログ・ボックスを開いて、AppScan によって提示されていないパターンを選択します。

表 4. 「詳細なセッション内要求の選択」の設定

設定	詳細
「メイン」リスト	記録されたログイン手順に含まれているすべての要求が表示されます。
検索	URL、要求、応答、またはすべてに入力したテキスト文字列が含まれている要求のみを表示します。
ドメインの表示	ドロップダウン・リストで選択したドメインからの要求のみを表示します。クリックして、AppScan で以下のアクションを実行します。
「セッション内要求として設定」ボタン	選択した要求をセッション内要求として設定します。この要求は、まだログイン中であることを確認するために、スキャン中に AppScan によって使用されます。 この操作は、リスト内の要求を右クリックして行うこともできます。
パターンの詳細な選択ボタン	「検出パターンを選択」ダイアログ・ボックスが開き、記録したログイン手順の要求に対するセッション内およびセッション無効の応答の内容を表示します (選択した検出パターンに基づきます)。応答のコンテキストで選択した検出パターンを確認し、コンボ・ボックスに表示されない検出パターンを定義することができます。このダイアログでは、すべての記録された応答を切り替えることができます。ボックスの上部には、AppScan が送信したセッション内およびセッション無効の要求も表示されます。 この操作は、リスト内の要求を右クリックして行うこともできます。
	ログインが記録されたときに受け取った、選択した要求に対する応答が表示されます。次の 2 つのタブを持つウィンドウが開きます。「ブラウザー」タブには、受け取った応答が表示されます。「要求/応答」タブには、要求と応答の未加工データが表示されます。
	選択した要求がログイン手順から削除されます。
検出パターン	このフィールドには、選択したセッション内検出の要求で見つかったパターンが表示されます。これはユーザーがセッション内にいる (または、オプションによってはセッション無効である) ことを示しています。 このドロップダウン・リストでは、AppScan がログイン記録で識別した候補から検出パターンを選択できます。緑と赤は、現在のパターンが有効か無効かを示しています。 **注:** 通常、セッション内パターンを使用することが推奨されます。ただし、セッション内要求の後にセッション内パターンが必ずしも返されない場合や、定義が複雑になる場合がまれにあります。そうした場合は、セッション内パターンの代わりにセッション無効パターンを使用することができます。AppScan が有効なパターンを識別できない場合や、別のパターンを選択する必要がある場合は、「パターンの詳細な選択」ボタンを使用して、独自のパターンを選択します。

「検出パターン」ダイアログ・ボックスを選択します。:

このダイアログを使用して、ログイン要求に対するセッション内およびセッション無効時の応答を比較します。これは、アプリケーションに最適な検出パターンを決定するのに役立ちます。クリックして開きます

このタスクについて

「構成」>「ログイン管理」>「レビューと検証」>「詳細なパターンの選択」とクリックすると、このダイアログ・ボックスが開きます。

以下がダイアログ・ボックスに表示されます。

- 現在のセッション検出パターンとその状況
- セッション内とセッション無効時の現在の要求と応答を表示する 4 つのペイン
- 各要求ごとの相違点が緑色で強調表示されます。
- 「セッション内応答」では、選択したパターンが緑色で強調表示されます。
- 「保存パターン」ボタンで、別のパターンを選択して設定できます。
- ダイアログの右上のページ切り替えで、要求を切り替えることができます。

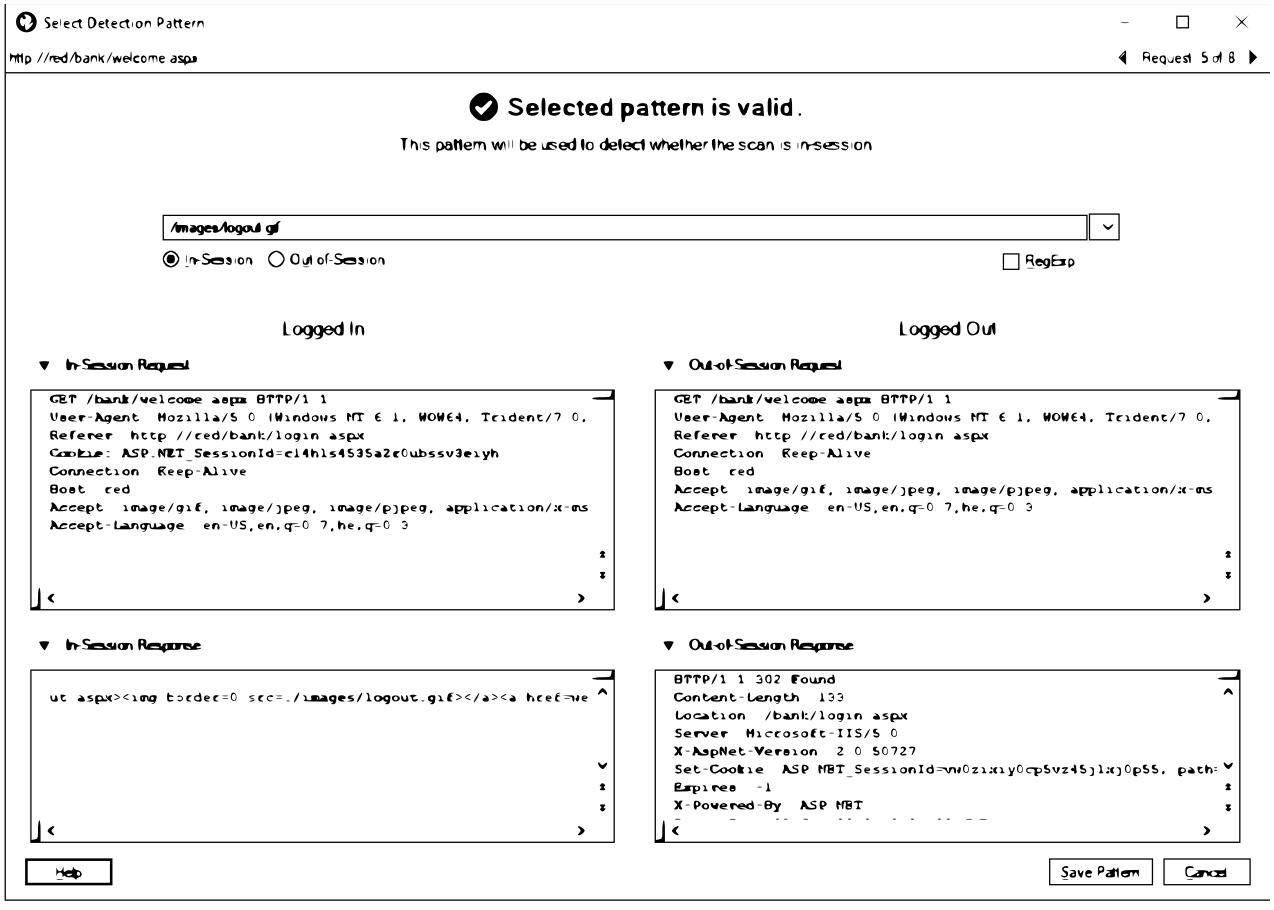


図 3. 「検出パターン」ダイアログ・ボックスを選択します。

手順

1. セッション内(またはセッション無効時)応答内で発生した、選択済みパターンをレビューします。
2. 2 つの応答を確認および比較して、他に有効なパターンがないか探します。
3. これらの応答を生成したセッション内とセッション無効時の要求(応答フィールド上部)を確認し、比較します。
4. ダイアログ・ボックスの右上隅にある矢印を使用して、記録したログインのすべての要求と応答を切り替えます。
5. 新しいパターンを選択して保存します。

セッション内検出の最適化:

ログイン手順を確認することは、セッション内検出のトラブルシューティングおよび最適化を行うのに役立ちます。

このタスクについて

AppScan は、セッション内ページで行われる「セッション内検出パターン」を自動識別しようとします。スキャン中にこのページを使用して、まだログイン状態であることを確認できます。これは、ログインしている場合にのみページ応答で発生するパターンです。例えば、「ログアウトするにはここをクリック」というテキストが示される場合があります。

スキャン中、AppScan はセッション内要求を繰り返し送信し、応答に「セッション内検出パターン」が含まれていることを確認します。 AppScan が、ページの応答でこのパターンを検出しなかった場合、AppScan は、ログアウト状態であると見なし、ログイン手順をやり直してログインを再試行します。その結果、通常はスキャン中にログイン手順が何回も繰り返されることになります。そのため、ログイン手順は可能な限り少ないステップで構成することが推奨されます。また、「セッション内」ページが小規模なページであり、追跡パラメーターや Cookie が存在しない場合も、スキャン時間が大幅に増加する可能性があるため、ステップを少なくすることが効果的です。

セッション内要求で定義済みのセッション内パターンが検出された場合 (POST 要求の直後の要求)、その要求は緑色で強調表示されます。

手順

1. 自動選択された「セッション内検出パターン」が、ユーザーがログインしていることを実際に示しているかどうかを検証します。必要に応じて、変更します。
2. ログイン手順に不要なステップがないことを確認します。不要なステップがある場合は、削除します。
3. セッション内応答が大規模でないことを確認します。また、可能であれば、追跡対象パラメーターまたは Cookie が含まれないようにします。必要に応じて、ページが小規模になるように 1 つ以上のステップを追加するか、追跡対象項目がページに含まれないようにします。
4. 追跡対象パラメーターおよび Cookie が含まれないセッション内ページを選択できれば、AppScan は、ログインするたびにそれらの項目を検査する必要がなくなります。「詳細構成」>「セッション管理:セッション内ページの解析」へ移動して、設定を「False」に変更します。
5. これらのいずれも正常に完了しない場合は、代わりにセッション無効パターンを識別し、検出方法を変更してみてください。

「セッション ID」タブ

「スキャン構成」>「ログイン管理」>「セッション ID」タブです。

「ログイン管理」ビューの「セッション **ID**」タブを使用して、記録されたログイン中に受信した変数 (セッション ID) の追跡を確認および管理します。

このタブでは、ログイン手順中に受信したすべての変数がリストされ、セッション ID を自動的に追跡対象として指定します (チェック・マークが「追跡」列の変数の隣に表示されます)。

このリスト内で変数を選択し、「追跡 **(Track)**」と「追跡の停止 **(Stop Tracking)**」ボタンを使用してそれらの状態を変更できます。「追跡対象」のパラメーターはすべて、スキャン中にその状況が追跡されるパラメーターおよび Cookie のグローバル・リストに追加されます (78 ページの『「パラメーターおよび Cookie」ビュー』を参照してください)。

ヒント**:** どの項目がセッション ID であるかが不明で、スキャンがセッション無効になる場合は、アプリケーションの開発者に連絡し、アプリケーションが使用するパラメーターおよび Cookie のリストを提供できるかを確認して、セッションを保守してください。

「詳細」タブ

「スキャン構成」>「ログイン管理」>「詳細」タブ。

「ログイン管理」ビューの「詳細」タブは、ログインの詳細設定とログアウト・ページ検出に使用します。

設定	詳細
ログインの詳細設定	「アプリケーションがすでにログインしている場合でもログインを許可します」**:** スキャン時間を節約するために、AppScan はログアウトせずに複数ログイン要求を送信します。このチェック・ボックスは、ご使用のアプリケーションでこの方法が使用できない場合にのみ選択を解除します。 「ユーザーがロックアウトされるまでの失敗ログイン試行数」**:** 特定の回数のログイン試行が失敗した後にアプリケーションでユーザーをロックアウトする場合は、このチェック・ボックスを選択して回数を構成します。AppScan Enterprise では、このしきい値に決して達しないように、失敗したログイン要求間に有効なログイン要求を送信します。このしきい値に達すると、さらなるスキャンができなくなるためです。
ログアウト・ページ検出	AppScan は、ログアウト・ページを識別するために正規表現を使用します。これにより頻繁にログアウトと再ログインを繰り返す必要がなくなるため、より効率的にスキャンを行うことができます。これは、「ログイン/ログアウト」ページをテストしないようにスキャンを構成した場合にログアウト・ページを識別するため (118 ページの『「テスト・オプション」ビュー』を参照)、および一部のセキュリティー・テストの一環として必要に応じてログアウトを行うためにも使用されます。これはデフォルトの正規表現です。 `(logout|signout|logoff|signoff|exit|quit|invalidate)` この正規表現内の標識のいずれかが URL に表示される場合、AppScan は、ページがログアウト・ページであり、したがって現在アプリケーションにログインしているものと想定します。 **注:** AppScan は、追加のインディケーターを識別すると、ログイン手順の記録時にこの表現を追加します。 必要に応じてさらにインディケーターを追加できますが、正規表現構文の規則に従うよう注意してください。 **注:** Expression Test PowerTool (「ツール」>「**Expression Test**」) は、正規表現の構文を確認するのに役立ちます。支援がさらに必要な場合は、次のリンクが役立ちます。 http://www.regular-expressions.info/quickstart.html

「環境定義」ビュー

「構成」ダイアログ・ボックスの「環境定義」ビューです。

環境定義は必須ではありませんが、AppScan でスキャン中に関連性のないテストを送信することを安全に抑制できるようになります。その結果、スキャンをさらに高速かつ正確に実施できます。

注**:** リスト内の項目の選択時に **Ctrl** キーを押しながら複数のオプションを選択できるリスト・ボックスもあります。

メトリック	コメント
オペレーティング・システム	スキャンされるアプリケーションのオペレーティング・システムを示します。
Web サーバー	該当するすべての 回答を選択します。複数のオプションを選択するには、[Ctrl] を押しながらクリックします。
アプリケーション・サーバー (ある場合)	該当するすべての 回答を選択します。複数のオプションを選択するには、[Ctrl] を押しながらクリックします。
データベースのタイプ (ある場合)	該当するすべての 回答を選択します。複数のオプションを選択するには、[Ctrl] を押しながらクリックします。
サード・パーティー・コンポーネント (ある場合)	該当するすべての 回答を選択します。複数のオプションを選択するには、[Ctrl] を押しながらクリックします。
サイトのロケーション	サイトがリモートであるかローカルであるか。
サイトのタイプ	テスト・サイトであるか、稼働中の実動サイトであるか。
デプロイメント方式	サイトが内部的にデプロイされているか (プライベート・サイト)、外部的にデプロイされているか (インターネット上)。
二次的被害の可能性	アプリケーションが脆弱な場合の損害またはデータ漏えいの可能性。
ターゲットの分布	ターゲットになる可能性がある環境内のシステムの比率。
可用性要件	(情報の) 可用性の相対的な重要性。
機密性要件	(ユーザー情報の) 機密性の相対的な重要性。
完全性要件	情報の保全性 (正確さ) の相対的な重要性。

注**:** 最後の 5 項目は、サイトの環境 CVSS メトリックです。ご使用のアプリケーション環境において、これらのメトリックの相対的な重要性を定義すると、AppScan は、スキャン中に検出された脆弱性に重大度値を割り当てる際に、この定義を考慮します。これらはグローバルな定義となります。(「詳細ペイン」 > 「重大度」 > 「CVSS パネルを開く (Open CVSS Panel)」により、この環境メトリックを特定の 問題向けに調整することができます。 227 ページの『CVSS 設定』 を参照してください。)

「除外するパスおよびファイル」ビュー

「構成」ダイアログ・ボックスの「除外するパスおよびファイル」ビューです。

アプリケーションの特定のパスや、特定タイプのファイルを無視するように AppScan を 構成することができます。ただし、除外対象には重要な問題が含まれている場合があるため、除外の適用は慎重に行ってください。ここでの変更は要求ベースの探査のみに適用され、アクション・ベースの探査には適用されません (「構成」 > 「探索オプション」 > 「探索方法」)。

設定	詳細
除外するパス	URL (絶対パス。クエリーを含む場合がある) または正規表現を「除外または包含するパス」リストに追加することにより、自動探査ステージの有効範囲をフィルタリングできます。 詳細については、『除外するパス』を参照してください。
除外するファイル・タイプ	スキャン中に特定タイプのファイルを無視するように AppScan を構成することができます。例えば、グラフィック・ファイルを除外すると、スキャンはより高速に実行されます。ただし、除外ファイルには重要な問題が含まれている場合があるため、ファイルの除外は慎重に行ってください。 詳しくは、 71 ページの『ファイル・タイプの除外』 を参照してください。

49 ページの『開始 URL フォルダーへのスキャンの制限』

除外するパス

「構成」ダイアログ・ボックスの「除外するパスおよびファイル」ビューです。

URL (絶対パス。クエリーを含む場合がある) または正規表現を「除外するパス」リストに追加することにより、自動探査ステージの有効範囲をフィルタリングできます。これを行う理由として考えられることは以下のとおりです。

- まだ開発中であり、問題があることがわかっていて、現時点ではスキャンしたくない。
- 問題がない ことがわかっており、スキャン時間を削減したい。
- スキャンをアプリケーションの特定の部分に制限することにより、スキャン時間を削減する。

定義済みの任意のパスに対して、オプションで 1 つ以上の特定のパラメーターにフィルタリングを制限することができます。これを行う理由には、以下のことが考えられます。

- 特定のパラメーター (ログイン・パラメーターやログアウト・パラメーターなど) をスキャンから除外したい大規模スクリプトのアプリケーション (URL に含まれ、そのパラメーターで制御されているアプリケーション) の場合。

この表には、以下のような 2 種類の項目があります。

- 除外: リストに含まれるパスがスキャンから除外されます。

  除外になるように構成されたパスに一致するリンクがフィルタリングされ、スキャンから除外されます。

  注: また、アプリケーション・ツリーでパスを右クリックし、「スキャンから除外」を選択することにより、パスを除外することもできます。
- 例外: リストの上方で除外されたパス内にある特定のディレクトリーを含めるために使用します。

  注: 例外機能は、除外されたパス内にあるディレクトリーを含める場合にのみ必要とされます。例えば、http://demo.testfire.net/bank を除外した場合、http://demo.testfire.net/bank/transfer.aspx を包含としてリストの下方に追加して、そのサブディレクトリーをスキャンに含めることができます。

  注: スキャンの探査ステージとテスト・ステージの間で除外を追加する場合、AppScan は除外されたパスが探査されたとしても、テストを行いません。

68 ページの『新規除外または新規例外の追加』

新規除外または新規例外の追加:

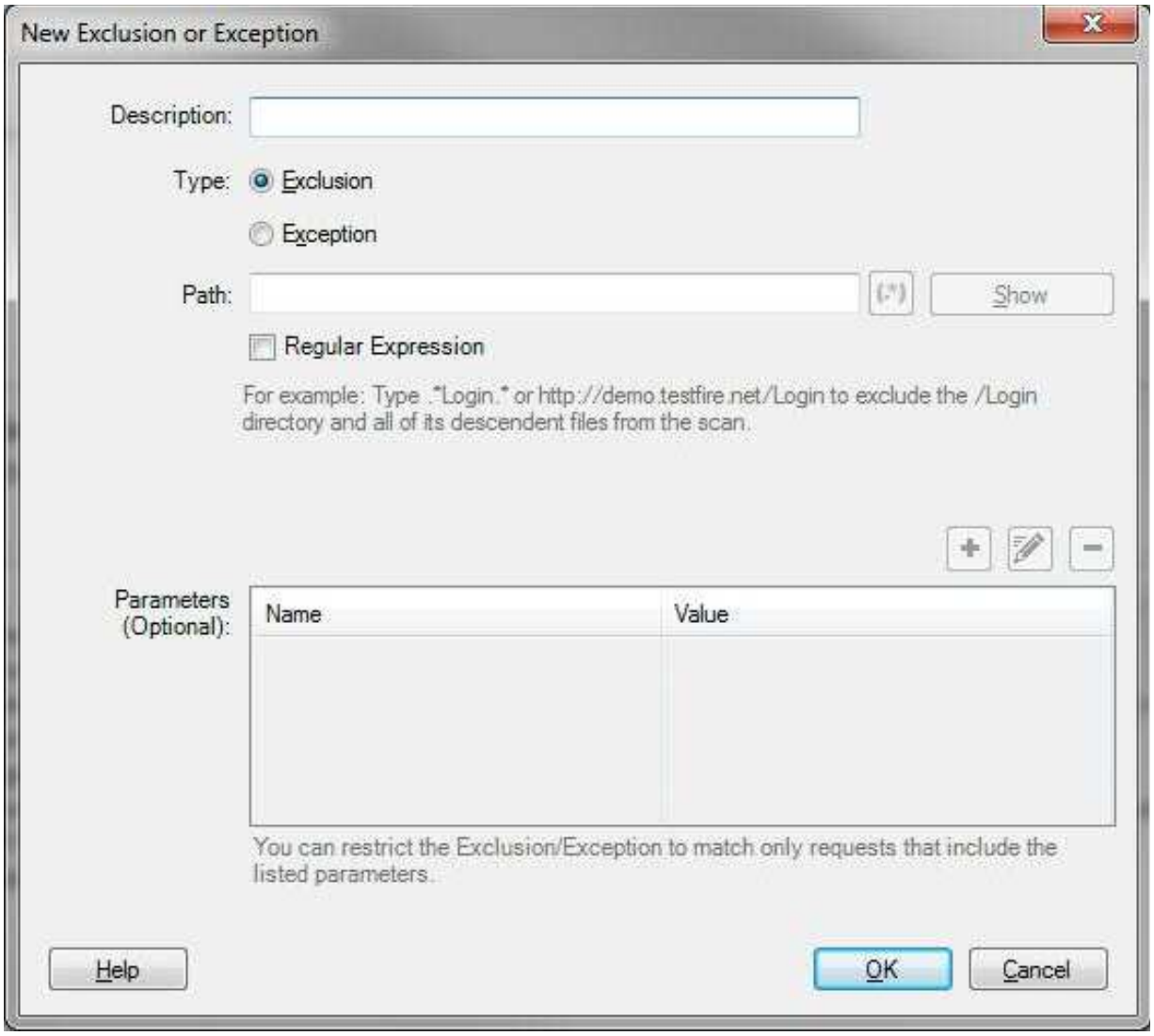
手順

1. 「構成」ダイアログ・ボックスの「除外するパスおよびファイル」タブの「除外するパス」領域で、

   をクリックして「除外」または「例外」を選択し、絶対パスまたは正規表現を入力して「**OK**」をクリックします。(「スキャン構成ウィザード」 >「開始 **URL**」>「詳細」で、「探査」をクリックします。)

   「新規除外または例外」ダイアログ・ボックスが開きます。



2. 作成するフィルターのラジオ・ボタンを選択します。
   - 除外: この項目に一致する URL をスキャンしません。
   - 例外: この項目に一致する URL がリストの上方にある除外条件によって除外されるとしても、この URL を含めます。

   注: 例外機能は、除外されたパス内にあるディレクトリーを含める場合にのみ必要とされます。例えば、http://demo.testfire.net/bank を除外した場合、http://demo.testfire.net/bank/transfer.aspx を包含としてリストの下方に追加して、そのサブディレクトリーをスキャンに含めることができます。

注: スキャンの探査ステージとテスト・ステージの間で除外を追加する場合、AppScan は除外されたパスが探査されたとしても、テストを行いません。

3. オプションで、「除外するパス」リストに表示される説明を追加します。
4. ディレクトリーのセットに一致するパスまたは正規表現を「パス」フィールドに入力し (以下の表の例を参照)、正規表現についてはチェック・ボックスを選択します。

   注: 正規表現とは、特定の構文規則に従ってストリングのセットを記述するストリングのことです。

    をクリックして Expression Test PowerTool を開くことで、正規表現の構文を検証できます。

   正規表現を作成するための支援がさらに必要な場合は、次のリンクが役立ちます。
   http://www.regular-expressions.info/quickstart.html

5. 特定のパラメーターのみを含むパスに除外または例外を適用するには、  をクリックし、1 つ以上のパラメーターをダイアログ・ボックスの下段のペインに追加します。

   注: この機能は、アプリケーション全体が URL に含まれ、そのパラメーターによって制御されている「大規模スクリプト」アプリケーション用に設計されています。 URL をフィルタリングによって除去することで、スキャンは無効にされますが、特定のパラメーターや特定のパラメーター値 (ログインあるいはログアウトのパラメーター値など) を除去することができます。

6. 「**OK**」をクリックします。

   新規項目がリストの一番下に追加されます。

   注: リスト内の 2 つの項目の間に矛盾がある場合、下の方の 項目が優先されます。必要に応じて項目の順序を調整するには、「上/下」ボタンを使用します。ある除外または包含がリストの上位にあるために、別の除外または包含が冗長になっている場合、「OK」をクリックすると、冗長項目がリストから削除されます。

例

タイプ	例および機能
除外	**http://demo.testfire.net/transfer** または **http://demo.testfire.net/transfer/** 指定された URL とすべてのサブディレクトリーおよびファイルをフィルタリングして除外します。
除外	**.*private.*** ストリング **private** を含むすべての URL を除外します。
除外	.*_bk.aspx **_bk.aspx** で終わるすべての URL を除外します。
例外	**http://demo.testfire.net/transfer/customize.aspx** 以前の除外 (この表の最初のものなど) でサブディレクトリーとファイルが除外されると、例外ではこの特定のパスをスキャンに含めます。 例外を有効にするには、除外の下 に表示する必要があることに注意してください。

除外または包含の編集**:**
手順

1. 「除外するパスおよびファイル」リストで項目を選択します。
2. 「編集」をクリックします。

   「除外または包含の編集 **(Edit Exclusion or Inclusion)**」ダイアログ・ボックスが表示され、選択した項目のプロパティーが示されます。
3. 必要に応じて変更し、「**OK**」をクリックします。

次のタスク

以下も参照してください。『特定のフォルダーへのスキャンの制限』

49 ページの『開始 URL フォルダーへのスキャンの制限』

特定のフォルダーへのスキャンの制限

除外および例外を使用して、スキャンの範囲を制限します。

このタスクについて

すべての URL を除外してから、必要なディレクトリー (複数可) を含めることにより、自動スキャンを特定の フォルダー (複数可) に制限できます。(スキャンを「開始 *URL* フォルダー」に制限するには、 49 ページの『開始 URL フォルダーへのスキャンの制限』 を参照してください。)

手順

1. 「スキャン構成」**>**「除外するパスおよびフォルダー **(Exclude Paths and Folders)**」を開きます。
2. 除外項目を、サイトのパス (**http://www.mysite.com/** など) と共に追加します (67 ページの『除外するパス』を参照してください)。
3. 1 つ以上の例外項目を、スキャンするパスと共に除外項目の下に 追加します。

   注**:** 例外項目を有効にするには、除外項目の下に 位置する必要があります。必要に応じて、「上**/**下」ボタンを使用して順序を調整してから、閉じます。
4. 開始 URL (48 ページの『「URL およびサーバー」ビュー』を参照) が除外されたパスのいずれかに含まれていないことを確認します。(含まれている場合、スキャンは開始できません。)
5. 「**OK**」をクリックして変更を保存し、リストを閉じます。

例 **1:**
このタスクについて

スキャンの開始 URL (48 ページの『「URL およびサーバー」ビュー』を参照) が **http://www.mysite.com/index.aspx** であり、スキャンをフォルダー **http://www.mysite.com/myfolder/** に制限する場合を考えてみましょう。

手順

1. 除外項目をパス `http://www.mysite.com/` と共に追加します(67 ページの『除外するパス』を参照してください)。
2. 包含項目を、開始 URL のパス (`http://www.mysite.com/index.aspx`) と共に除外項目の下に 追加します。

3. 2 番目の 包含項目を、スキャン対象のフォルダーのパス (http://www.mysite.com/myfolder/) と共に、除外項目の下に追加します。

例 **2:**
このタスクについて

ここで、スキャンの開始 URL がスキャン対象のフォルダー内にある場合を考えてみましょう。開始 URL は http://www.mysite.com/myfolder/index.aspx で、http://www.mysite.com/myfolder/ フォルダーへのスキャンを制限しようとしています。

この場合、スキャン対象のフォルダーと開始 URL が単一の包含項目でのスキャンに追加されます。

手順

1. 除外項目をパス http://www.mysite.com/ と共に追加します。
2. 包含項目を、スキャン対象のフォルダーのパス (http://www.mysite.com/myfolder/) と共に、除外項目の下に追加します。

ファイル・タイプの除外

特定のタイプのファイルをスキャンから除外します。

このタスクについて

AppScan を、すべてのページではなく、除外するパスの設定にあるような特定のファイルのタイプを無視するように構成できます。例えば、グラフィックスを除外すれば、スキャンをより高速で実行できます。ただし、除外ファイルには重要な問題が含まれている場合があるため、ファイルの除外は慎重に行ってください。

手順

1. 「スキャン構成」ダイアログ・ボックス >「探査の設定」ビューを開きます。
2. 「除外するファイル・タイプ」ペインで、スキャンしないファイル・タイプのチェック・ボックスが選択されていることを確認します。

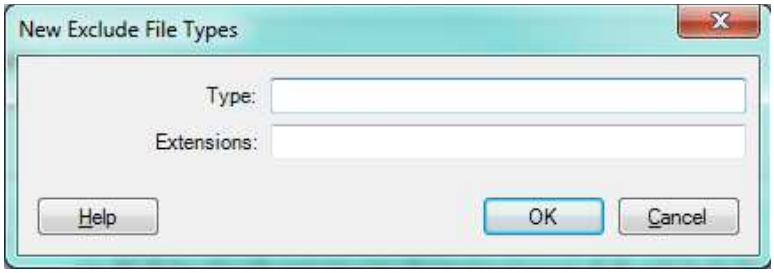
追加のファイル・タイプの除外**:**
このタスクについて

アプリケーション内に「除外するファイル・タイプ」ダイアログ・ボックスにリストされていないファイル拡張子がある場合、これらの拡張子をリストに追加できます。

手順

1. 「除外するファイル・タイプ」領域で、  をクリックします。

   「新規除外ファイル・タイプ」ダイアログ・ボックスが表示されます。



2. 「タイプ」テキスト・ボックスで、ファイル拡張子のセットを記述する語または句を入力します。
3. 「拡張子」テキスト・ボックスで、このファイル・タイプに該当する拡張子のリストを入力します。(複数の拡張子はコンマで区切ります。スペースは入れないでください。)
4. 「**OK**」をクリックします。

除外されるファイル・タイプのリストの編集**:**
手順

1. 「除外するファイル・タイプ」ダイアログ・ボックスで行を選択します。
2. 「編集」をクリックします。

   「除外するファイル・タイプの編集」ダイアログ・ボックスが表示され、選択された除外の関連拡張子が示されます。
3. 必要に応じて、タイプ名または拡張子のリストを変更します。
4. 「**OK**」をクリックします。

「探査オプション」ビュー

「構成」ダイアログ・ボックスの「探査オプション」ビューです。

「探査オプション」ビューには、次のタブが含まれます。

- 「メイン」タブは、AppScan がサイトの探査に使用する方法を選択するために使用します。
- 「アクション・ベース」タブは、アクション・ベース探査固有の設定を構成するために使用します。
- 「要求ベース」タブは、要求ベース探査固有の設定を構成するために使用します。

「メイン」タブ

「スキャン構成」 > 「探査オプション」 > 「メイン」タブ。

このタブでは、AppScan がスキャンに使用する探査方法を選択し、両方の方法に適用されるオプションを構成します。

探査方法
: AppScan は、2 つの異なる方法をスキャンの探査ステージに使用します。一方または両方を選択できます。2 つの方法の内、要求ベースの探査は一般にアクション・ベースの探査より高速で処理されます。両方とも選択した場合 (デフォルト設定であり、推奨されています）、アクション・ベース探査がまず 30 分の時間制限で実行され、その後に要求ベースの探査が実行されます。

ページ構造 **(DOM)** フィルタリング
: これらを使用すると、すでにスキャンしたページと非常に類似し、無視しても問題がないページを特定することにより、スキャン時間を大幅に減らすことができます。

スキャン制限

これらの制限により、AppScan がご使用のアプリケーションを探査する深度 (または速度) が決まります。

その他の設定

これらの設定により、クライアントが特定のサーバー・エンコードを認識し、特定のユーザー・エージェント・ヘッダーを送信するように構成します。

設定	詳細
探査方法	
アクション・ベース	任意のバージョンの Google Chrome ブラウザーを使用して、ユーザーが行うように、ブラウザーに表示されるリンクをクリックしてサイトをスキャンします。 この方法は、JavaScript や Session Storage などの新しいテクノロジーが使用されている場合、そして、RIA、Single-page Application (SPA)、または AngularJS のサイトに対して特に効果的です。
要求ベース	要求は、AppScan が検出する、すべてのページ・コンテンツに基づいて送信されます。 これには、コメント内のリンクなど、ブラウザーを使用するユーザーには表示されずに、アタッカーが見つける可能性があるコンテンツが含まれます。
ページ構造 *(DOM)* フィルタリング	
構造 (DOM) を基準にして類似ページをフィルターに掛ける	AppScan は、構造 (DOM) 類似性に関して、新規ページと既にスキャンしたページを比較します。類似性は、追加のテストが必要な新規リンクやコンテンツが新規ページに含まれていないことを示します。例えば、商用サイトでは、千単位の異なる製品が別々のページ上にあるものの、他のあらゆる点は同一のカタログがあるとします。この場合、通常はすべてのページをスキャンする必要がありません。 DOM の類似性に基づいてフィルタリングを行うことで、スキャン時間を大幅に 短縮できます。 デフォルトでは、両方のチェック・ボックスが選択されています。スキャン後、スキャン結果の「フィルター済み」タブを調べて、固有の要求がフィルター処理により誤ってスキャンから除外されていないかを確認する必要があります。 その場合は、一定した低レベルのフィルター処理を行う「フィルターに掛けるページを減らす」オプションを試行するか、DOM フィルター処理を完全に無効にする必要があります。 結果の「フィルター済み」タブには、以下の 3 種類のフィルター済み項目が表示されます。 • 類似の **DOM**:これは、ページの構造 (DOM) が以前に探査したページの構造と類似しており、テストする新規要素が含まれていない可能性が高いために、スキャンからフィルターで除外されたページを示します。 • 類似の可能性が高い **DOM**:これは、以前に探査したページと同じ構造 (DOM) が応答に含まれると AppScan が判断し、テストする新規要素が含まれていないために、送信されなかった要求を示します。 • 類似した本文:これは、応答本体のコンテンツが以前に探査された要求の応答本体のコンテンツと類似しているためにフィルタリングによってスキャンから除外された、(類似の DOM によってフィルタリングされなかったページからの) 要求を示します。 スキャン後、スキャン結果の「フィルター済み」タブを調べて、固有の要求がフィルター処理により誤ってスキャンから除外されていないかを確認する必要があります。 その場合は、「重複の可能性が高いページをフィルター (Filter likely duplicate pages)」オプション (次のオプション) をクリアするか、このチェック・ボックスをクリアして DOM フィルター処理を完全に無効にする必要があります。
構造 (DOM) を基準として類似の可用性が高いページをフィルター	この設定は、フィルター処理により、「類似の可能性が高い DOM」ページをスキャンから除外します (上記の説明を参照)。誤って固有の要求がフィルター処理によりスキャンから除外された場合は、このチェック・ボックスをクリアしてください。

設定	詳細
スキャン制限	
冗長なパスの制限	AppScan は、同じパスに対して、指定された回数を超えるアクセスは行いません。 特定のパスは、これが別のパラメーターを指定して出現すると、数回にわたってアクセスされる可能性があります。この制限は、主にスクリプトに関連して行われます。これはデフォルトでは選択解除されています。ほとんどの場合、上記のチェック・ボックス「構造 **(DOM)** を基準に重複したページをフィルター」を選択すると、スキャン時間が十分に制御されるためです。
クリックの深さの制限	AppScan は、指定された数を超えるリンクをクリックしてアクセスされたページをスキャンしません。
合計ページ制限 (Total Page Limit)	これを選択すると、AppScan は、定義されているページの最大数を超えるアクセスは行いません。ページごとに多数の URL が探査される場合があることに注意してください。
その他の設定	
エンコーディング	一般に、AppScan は、アプリケーションのエンコード方式を自動的に検出するため、自動検出がデフォルトで選択されています。 スキャン結果の応答の内容がゆがめられているように見える場合は、エンコード方式が正しく識別されていなかったことが考えられます。この問題を解決するために、ドロップダウン・リストから正しいエンコード方式を選択してください。
ユーザー・エージェント	HTTP 要求内のユーザー・エージェント・ヘッダーは、要求を送信したクライアントの種類をサーバーに提示します。これは、サーバーが返すコンテンツに影響することがあります。例えば、ユーザー・エージェントが携帯電話ブラウザーである場合にのみ、携帯電話に固有のコンテンツを送信することができます。AppScan がこのようなコンテンツをテストできるようにするには、適切なユーザー・エージェント・ヘッダーを送信するように構成する必要があります。 一般に、AppScan は、ユーザー・エージェントを自動的に検出するため、「自動検出」がデフォルトで選択されています。しかし、組み込みブラウザー以外のブラウザーを使用して、ログイン手順、マルチステップ操作、またはマニュアル探査を記録しない場合、AppScan はユーザー・エージェントを自動検出できないため、手動で選択する必要があります。 ユーザー・エージェントを変更するには、ドロップダウン・リストからエージェントを選択します。 カスタム・コンテンツを入力するには、「編集」ボタンをクリックし、コンテンツを入力します。ダイアログ・ボックスを閉じると、ボタン名が「カスタム・ユーザー・エージェント」に変更されます。 注**:** デフォルトのブラウザーを変更する場合は、 355 ページの『デフォルト・ブラウザーの変更』 にリストされている条件を参照してください。

ユーザー・エージェント・ヘッダー**:**

このセクションでは、各ユーザー・エージェントで送信されるユーザー・エージェント・ヘッダー、および「自動検出」の使用方法について説明します。

必要な場合は、「編集」ボタンをクリックして、任意のユーザー・エージェント・ヘッダーのコンテンツを編集できます。更新されたユーザー・エージェントは、「カスタム・ユーザー・エージェント」として表示されます。

「ユーザー・エージェント」ボタンをクリックしてヘッダーを選択し、「編集」ボタンをクリックしてコンテンツを編集することができます。コンテンツを編集すると、ボタン名が「カスタム・ユーザー・エージェント」に変更されます。「カスタム・ユーザー・エージェント」のコンテンツは、スキャンの保存時にそのユーザー・エージェントが選択されている場合にのみ、スキャンと共に保存されます (その後、スキャンと共に他のコンピューターに転送されます)。

「アクション・ベース」タブ

「スキャン構成」 > 「探査オプション」 > 「アクション・ベース」タブ。

このタブでは、アクション・ベース探査に影響を及ぼす設定を構成します。このタブは、「メイン」タブで「アクション・ベース探査方法」を選択した場合のみアクティブになります。

設定	詳細
全般	
探査タイムアウト (分)	サイトのアクション・ベース探査のデフォルト時間制限は 30 分です。この時間が経過すると、サイトの探査が完了していない場合でも探査ステージが停止します。 AppScan がこの時間内にサイトの重要な部分を探査できない場合には、このタイムアウトを延長できます。
ページでアクションを起動する前の最小待ち時間 (ミリ秒単位)	AppScan は、探査を開始する前に、ページが完全に読み込まれたことを識別しようとします。 最小待ち時間をここに追加した場合、AppScan は常にこの設定を最小待ち時間として使用します (ページが読み込まれたことを検出した場合でも)。ただし、ページが読み込まれていないことを検出した場合には、さらに長く待機します。 **ヒント:** 探査データをレビューしているときに、AppScan がページで可能なすべてのアクションを実行できていないことが確認された場合には、動的な待ち時間が短すぎる可能性があります。また、ブラウザーを有効にしておけば、スキャン中にこれを確認することもできます。 1. 「ツール」>「オプション」> 「詳細」に移動します 2. `SessionManagement:ShowActionBasedPlayerWindow` を見つけ、設定を `True` に変更します。 3. スキャンを実行します。スキャン時にブラウザーが開き、AppScan がサイトを探査する様子を見ることができます。現在のページが完全に読み込まれる前に新しいページへと続行されることに気づいた場合は、待ち時間を増やすと問題が解決することがあります。 **注:** この設定を変えると探査時間に影響が及ぶ可能性があるため、探査タイムアウト (上記) を増やすことも検討するとよいでしょう。
動的ページ読み込みの自動検出	デフォルトでは、AppScan はアクティブに動的ページ・コンテンツを検出して、そのようなページを処理します。まれに、これが原因でページが正しく読み込まれず、スキャン範囲に影響が及ぶことがあります。 **ヒント:** この問題を識別するには、以下を行います。 1. 「ツール」>「オプション」> 「詳細」に移動します 2. `SessionManagement:ShowActionBasedPlayerWindow` を見つけ、設定を `True` に変更します。 3. スキャンを実行します。スキャン時にブラウザーが開き、AppScan がサイトを探査する様子を見ることができます。通常のブラウザーで正しく読み込まれるページがスキャン中に正しく読み込まれないことに気づいた場合は、このチェック・ボックスをクリアすると問題が解決することがあります。
フィルター	

設定	詳細
同一 DOM 要素のアクションをスキップする	AppScan は、さまざまな基準に基づいて、前のページですでに実行したアクションを特定します。実際は異なっているのに DOM 要素が原因で同一に見えるアクションがサイトに含まれている場合、AppScan は誤ってそれらのアクションを無視することがあります。その場合は、このチェック・ボックスをクリアしてください。 **注:** AppScan は、同じアクションを数回、実際に繰り返すことでそれらが本当に同じであることを確認してから、今後の反復を無視するようになります。
重複アクションの分析およびスキップ	AppScan は、似ているように見えるアクションを特定すると、結果ページを比較します。何度か繰り返した後、すべての結果が同じに見える場合、AppScan は今後の類似のアクションを重複として無視します。 コンテンツのみ異なるページがサイトに多く含まれている場合には (ニュース・サイトなど)、この機能により大幅にスキャン時間が短縮できるため、このチェック・ボックスを選択してください。
スキップするアクション	これは、スキャン、またはアプリケーションにさえも悪影響を及ぼすため AppScan が無視すべきアクションのリストです。スキップするアクションは、アクションの DOM 要素の `Id`、`name`、または `ng-model` 属性に基づいて特定されます。DOM 要素属性の `Id`、`name`、または `ng-model` にリスト内の語句のいずれかが含まれているアクションはスキャンから除外されます。 このリストに項目を追加したり、リストの項目を編集および削除できます。

「要求ベース」タブ

「スキャン構成」 > 「探査オプション」 > 「要求ベース」タブ。

このタブでは、要求ベースの探査に影響を及ぼす設定を構成します。このタブは、「メイン」タブで「要求ベース探査方法」を選択した場合のみアクティブになります。

- **JavaScript** および「**Flash**」オプションにより、AppScan が、これらのスクリプトを無視するかスキャンするかが決まります。
- 「探査モード」により、AppScan がページ上のすべてのリンクを探査してから次のページに進むか、新しいリンクが検出されるたびにそのリンクを探査するかが決まります。
- 「**WebSphere Portal**」により、クライアントが特定のサーバー・エンコードを認識し、特定のユーザー・エージェント・ヘッダーを送信するように構成します。
- **Flash**

設定	詳細
JavaScript	
JavaScript コードを解析して URL を見つける	AppScan は、JavaScript コードをリンクを収集するためのテキスト・データとして解析します。
JavaScript を実行して URL およびダイナミック・コンテンツを見つける	AppScan は JavaScript コードを実際に実行し、その結果を分析して、リンク (構文解析のみでは発見されない可能性がある動的リンクを含む) を収集します。(この場合、構文解析よりも多くのシステム・リソースが使用されます)。 **注:** アクション・ベースの JavaScript の実行の効率が証明されているため、このオプションはデフォルトで選択解除されるようになりました。
ログインをやり直すときに JavaScript を実行する	アプリケーションのログイン・ページで JavaScript コードが使用されている場合、AppScan がスキャン中にログインするためには、このチェック・ボックスを選択しておく必要があります。

設定	詳細
探査モード	
幅優先	(デフォルト) AppScan は、ページごとに探査を行い、 ページに含まれるすべてのリンクを探査した後、次のページに進みます。 ユーザーが特定の順でリンクを訪問する必要があるアプリケーションでの制約について問題がない限り、このオプション (幅優先) のデフォルトの選択を変更しないことをお勧めします。
深さ優先	AppScan は、リンクごとに探査を行い、新しいリンクが見つかった時点でこれを探査します。 探査方法を「深さ優先」に変更すると、AppScan について、探査中に 1 個のスレッドのみ使用するように変更する必要もあります。(「構成」 > 「通信およびプロキシー」ビュー)。
WebSphere® Portal	
Enable WebSphere Portal スキャン	サイトが WebSphere Portal サイトの場合、AppScan はより効率的にスキャンするためにそのサイトから URL デコード情報を取得して、便利なアプリケーション・ツリーを作成する必要があります。 デコードを有効にするには、「**WebSphere Portal** スキャンを有効にする」を選択します。 コンテキスト・ルート URL がデフォルトの形式に従っていない場合、「コンテキスト・ルート **URL** の追加」をクリックして、1 つ以上のコンテキスト・ルート URL を追加します。 **ヒント:** ご使用のポータルのコンテキスト・ルート URL が分からない場合には、以下のようにします。 1. WebSphere Portal がインストールされているコンピュータで、`wp_profile_root/ConfigEngine/properties` ディレクトリーの `wkplc.properties` ファイルを開きます。 2. コンテキスト・ルート値が `WpsContextRoot` プロパティーによって指定されています。 **ヒント:** WebSphere Portal サイトのスキャン中は、この目的用に構成されている、定義済みの WebSphere Portal スキャン・テンプレートを使用することをお勧めします。
Flash	
Flash を解析して URL を見つける	AppScan は 、Flash コードをリンクを収集するためのテキスト・データとして解析します。

設定	詳細
潜在的な脆弱性を発見するために Flash ファイルを実行 (Execute Flash files to discover potential vulnerabilities)	AppScan は Flash ファイルを実際に再生 し、その結果を分析して、リンク (構文解析のみでは発見されない可能性がある動的リンクを含む) を収集します。(この場合、構文解析よりも多くのシステム・リソースが使用されます)。 Adobe Flash Player for Internet Explorer のバージョン 9.0.124.0 以降が必要です。サポートされているバージョンがインストールされていない場合、このチェック・ボックスを選択するとチェック・ボックスの横に警告が表示され、Flash は実行されません。 345 ページの『Flash コンテンツ』 を参照してください。 Adobe Flash Player バージョン 10.1 以降がインストールされている場合は、AppScan で使用するためには構成が必要であるというメッセージが表示されることがあります。 8 ページの『Flash Player の構成』 を参照してください。 Flash の実行が選択されている場合、3 つの Flash 実行制限を構成することもできます。以下はシステム・チューニングの基本ステージです。 • 深度限界: 最初の画面からの最大クリック数。このクリック数を超えると、特定の Flash ムービーのスキャンを停止してスキャンを先に進めます。 • クリック制限: クリック数の合計の最大値。これを超えると、特定の Flash ムービーのスキャンを停止してスキャンを先に進めます。 • 画面制限: 許容される、固有の Flash 状態の最大数。これを超えると、特定の Flash ムービーのスキャンを停止してスキャンを先に進めます。

「パラメーターおよび Cookie」ビュー

「構成」ダイアログ・ボックスの「パラメーターおよび Cookie」ビューです。

このビューを使用して、4 つの主な機能を管理します。

- 特定のパラメーターおよび Cookie に特殊な処理を割り当てます。
- パラメーターおよび Cookie のデフォルトの処理を制御します (「冗長性調整」)。
- AppScan が単独では認識しない可能性がある特殊な形式を持つパラメーターおよび Cookie を定義します。
- カスタム・ヘッダーを定義します。

設定	説明	参照
「パラメーターおよび Cookie」タブ	デフォルト以外の処理が必要なグローバル・パラメーターを表示、追加、編集、および削除できます。 例えば、ご使用のアプリケーションには、テスト中に AppScan による値の処理が不要なパラメーターおよび Cookie が含まれている可能性があります。AppScan が確実にこれらのパラメーターおよび Cookie を変更しないようにするには、テストからこれらを除外してください。例えば、ご使用のアプリケーションは、特定の Cookie またはパラメーター値が変わった場合に、ユーザー・セッションをロックすることがあります。操作からこれらのパラメーターを除外する必要があります。除外しない場合、これらの Cookie が AppScan をアプリケーションからロックアウトするため、AppScan がスキャンを正常に完了できない可能性があります。 探査ステージ中に、AppScan は、セッション ID と考えられる Cookie および HTML パラメーターを自動的に検出し、このタブのリストに追加します。セッション ID であることが分かっている Cookie とパラメーターを手動で追加することができます。 このタブの列は、下の表で定義されています。 **注:** 「テンプレート項目を表示する/テンプレート項目を非表示にする」ボタンを使用すると、現在のスキャンには関連しない可能性がある、スキャン・テンプレートから発生した項目をフィルタリングして除外できます。	80 ページの『パラメーター定義』
「カスタム・パラメーター」タブ	AppScan が単独では認識しない可能性があるカスタム・フォーマットを持つパラメーターを、追加、編集、および削除できます。	88 ページの『「カスタム・パラメーター」タブ』
「カスタム・ヘッダー」タブ	非標準 (カスタム) HTTP のヘッダーフォーマットを定義することができます。AppScan では、サイトを効果的にテストするために、応答コンテンツ内のパラメーターを特定し、サイトに送信するヘッダーに、それらのパラメーターを適切に追加できることが必要です。	91 ページの『「カスタム・ヘッダー」タブ』
冗長性調整のデフォルト	このリンク (「パラメーターおよび Cookie」タブの下部にあります) を使用することで、AppScan によって見つかった、またはユーザーによって定義されたすべてのパラメーターに適用されるデフォルトの冗長性調整にアクセスしたり、これを編集したりすることができます。 **注:** 個々のパラメーターに関する 特定の冗長性調整を変更することは、の一部として実行されます。 80 ページの『パラメーター定義』 デフォルトへの変更は、既に定義されているパラメーターまでさかのぼって適用されることはありません。これは、各パラメーターについて手動で実行する必要があります。	85 ページの『冗長性調整』

「パラメーターおよび Cookie」タブ・フィールド

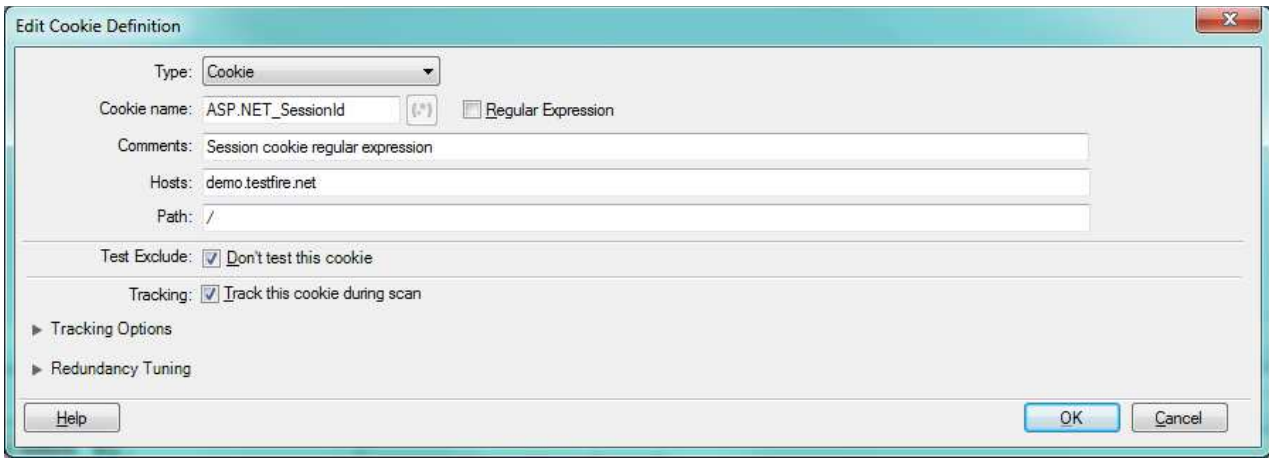
以下の表は、このタブ内のフィールドを要約したものです。

見出し	オプションおよび説明
タイプ	パラメーター/Cookie/カスタム・パラメーター
名前	
追跡	このパラメーターまたは Cookie の追跡方法: • ログイン値として • ダイナミック値として • 固定値として • 追跡しない 詳細については、 83 ページの『セッション ID』を参照してください。
テスト除外	スキャンのテスト・ステージで、このパラメーター/Cookie をテストから除外するかどうかを定義します。
冗長性調整	• デフォルト:デフォルトの冗長性調整が当該項目に適用されます。 • カスタム:当該項目の冗長性調整が、現在のデフォルト設定と異なります。
ソース	AppScan が当該項目を取得した場所を示します。 • スキャン・テンプレート:スキャン・テンプレートから発生 • ログイン・セッション ID:ユーザーによって記録されたログイン手順から発生 • マルチステップ手順変数:ユーザーによって記録されたシーケンスから発生 • スキャン・エキスパート [モジュール名]:指定されたスキャン・エキスパート・モジュールから発生 • 探査最適化プログラム:探査最適化プログラムの拡張機能から発生 • ユーザー定義

パラメーター定義

手順

新規の定義を追加するには、  をクリックします (あるいは、既存のパラメーターを編集するには、そのパラメーターを選択して  をクリックします)。
「パラメーター定義の追加」ダイアログ・ボックスが表示されます。



設定	説明
タイプ	ドロップダウン・リストからパラメーター・タイプを選択します。 パラメーター**:** この名前に一致するすべてのパラメーターが定義に組み込まれます。 **Cookie:** この名前に一致するすべての Cookie が定義に組み込まれます。 カスタム・パラメーター**:** これはカスタム・パラメーターです (「名前」ドロップダウン・リストからいずれかのカスタム・パラメーターを選択してください)。
名前	パラメーターまたは Cookie の名前。 入力する名前が正規表現の場合は、隣接するチェック・ボックスを選択します。これを行った場合、 (.*) をクリックして Expression Test PowerTool を開くことで、正規表現の構文を検証できます。 詳細については、 83 ページの『パラメーター名』を参照してください。
コメント	オプションで、自分用の参照として、このフィールドにパラメーターに関するコメントを追加できます。
ホスト	ホストが指定されている場合**:** 指定されたホスト専用にこのパラメーターを使用します。 ブランクのままになっている場合**:** すべてのホストにこのセッション ID を使用します。
パス	アプリケーションが、そのアプリケーションの別の部分から同じ名前の Cookie を提供している場合、各 Cookie のパスを定義することでそれらを区別することができます。 ブランクまたは / が指定された場合、Cookie のすべての出現が含まれます。
テスト除外	AppScan にこのパラメーターをテストさせない場合にのみ、このチェック・ボックスを選択します。
追跡	この設定は、アプリケーションによって新規値が設定されたときには必ず、スキャン中にこのパラメーターまたはセッション ID を更新する必要があることを AppScan に通知します。それにより、アプリケーションに対する要求で常に有効な Cookie/パラメーターが送信されるようになります。

設定	説明
オプションを追跡中...	(リンクをクリックして、ダイアログ・ボックスのこのオプション・セクションを開きます。) これらのオプションを使用して、追跡しているパラメーターや Cookie を処理する方法を微調整することができます。 追跡タイプ • ログイン値**:** (デフォルト、および推奨) このパラメーターを含むアプリケーションに送信される要求は、ログイン・プロセスの最後に受信したパラメーターの値を使用します。セッション内要求自体は含まれません。 **ヒント:** 「セッション内応答」のパラメーターを追跡する場合、タイプをダイナミック、ログイン値ではないに設定し、「構成」**>**「セッション管理**:** セッション内ページの解析」が「**True**」 (デフォルト値) に設定されていることを確認します。 **注:** ログインの記録がマルチステップ・シーケンスの一部である場合は、受け取ったパラメーターをログイン値として定義しても、その使用方法には影響しません。常にダイナミックとして扱われます。 • ダイナミック値**:** このパラメーターを含むアプリケーションに送信される要求は、アプリケーションから受信した最新の値を使用します。 • 固定値**:** このパラメーターを含むアプリケーションに送信される要求は常に、「値」フィールドに入力される値を使用します。 詳細については、 83 ページの『セッション ID』を参照してください。 すべての要求について **Cookie** を送信**:** これが選択されると、アプリケーションによって明示的に設定されていない場合も含めて、すべての要求に Cookie が組み込まれます。 グループとして扱う**:** Cookie 名が正規表現である場合、その正規表現に一致する別の Cookie 名をグループとして処理する (この場合、変更が行われると値だけでなく名前も更新される) か、別個の Cookie として処理するかを定義します。 応答パターン**:** 通常、AppScan は、応答 (パラメーター) または Cookie ヘッダー (Cookie) から取り出されたリンクのコンテンツに基づいて、パラメーターあるいは Cookie を更新します。AppScan が自力で値を取り出せない場合、AppScan が未加工の応答から値を取り出すのに使用できる正規表現を提供することができます。正規表現には、少なくとも 1 つのグループを含める必要があり、AppScan は、最初の一致を取り出します。 • **URL** フィルター**:** パラメーター/Cookie が特定の URL にのみ表示されることが既知である場合は、URL の絶対パスをここで定義することで、スキャン効率を改善することができます。 • エンコード**:** 取り出した値を要求に貼り付けるときにエンコードする必要がある場合は、ここでメソッドを定義します。コーディングが不明確な場合は、「コンテキストに従う」を選択します。コーディングが明確な場合は、正しい エンコードを選択してください。オプションは以下のとおりです。「なし」、「コンテキストに従う」、「URL」、「XML」、「JSON」があります。 • 一致**:** 「ヘッダーと本文」(デフォルト) または「本文のみ」を選択します。
冗長性調整...	(リンクをクリックして、ダイアログ・ボックスのこのオプション・セクションを開きます。) これらの 4 つのチェック・ボックスでは、スキャンの探査およびテスト・ステージ中に AppScan がパラメーターの変更 (または、その存在の有無) とどのように関連するかを微調整できます。 85 ページの『冗長性調整』 を参照してください。

パラメーターまたは Cookie を定義する ID

パラメーターまたは Cookie は、特定の ID に基づいて一意的に認識されます。そのため、同じ ID を持つ 2 つ以上のパラメーターまたは Cookie を定義することはできません。以下の表では、各種類の項目の ID を示しています。

パラメーター	パラメーター名、正規表現かどうか、ホスト
Cookie	パラメーター名、正規表現かどうか、ホスト、パス
カスタム・パラメーター	抽出された名前 (存在する場合)、参照名、ホスト、出現インデックス

パラメーター名

手順

「名前」テキスト・ボックスに、パラメーターか Cookie 名、またはそれに一致する正規表現を入力します。

- すべてのテキストは大文字と小文字が区別されます。正規表現の大文字と小文字を区別しない場合には、その正規表現に `(?i)` を追加してください。
- 正規表現内の文字列は部分一致と見なされます。`(.*)` を追加する必要はありません。

いくつかのデフォルト定義が提供されます。

タイプ	値	包含
パラメーター	**__VIEWSTATE**	名前にこのストリングが含まれるパラメーター
パラメーター/Cookie	**^CFID**	名前が CFID または cfid で始まるパラメーターおよび Cookie
パラメーター/Cookie	**Token**	名前に「Token」が含まれるパラメーターおよび Cookie

注**:** 正規表現とは、特定の構文規則に従ってストリングのセットを記述するストリングのことです。Expression Test PowerTool (「ツール」**>**「**Expression Test**」) は、正規表現の構文を確認するのに役立ちます。

正規表現を作成するための支援がさらに必要な場合は、次のリンクが役立ちます。 http://www.regular-expressions.info/quickstart.html

セッション ID

サイトが (Cookie またはパラメーターの形式の) 時間制限付きのセッション ID を使用する場合、サイトは有効期限が切れたトークンを含む要求を拒否します。そのため、サイトはテストに失敗します。

したがって AppScan は、時間制限付きのセッション *ID* である HTML パラメーターや Cookie を識別し、取り扱うことができる必要があります。AppScan はセッション ID に利用可能な最新の値を割り当て、アプリケーション・セッションの有効期限切れを防止します。

AppScan がセッション ID の値を自動的に更新するかどうか決定することができます。セッション ID の「状態」を設定します。

•

ログイン値**:** (推奨) このパラメーターを含むテスト要求を送信するときに、AppScan はセッション ID を、セッション内要求より先にアプリケーションから受信した値で自動的に更新します。

ヒント**:** 「セッション内応答」のパラメーターを追跡する場合、タイプを動的、ログインしないに設定し、「構成」**>**「詳細」**>**「セッション管理**:**セッション内ページの解析」が「**True**」(デフォルト値)に設定されていることを確認します。

特定の値を設定しなければならない特定の必要がない限り、ほとんどのパラメーターおよび Cookie には、この状態が推奨されます。ただし、ログイン値セッション ID が使用されると、値がデータベース内にある間に有効期限が切れる可能性があります。

注**:** ログインの記録がマルチステップ・シーケンスの一部である場合は、受け取ったパラメーターをログイン値として定義しても、その使用方法には影響しません。常にダイナミックとして扱われます。詳しくは、 98 ページの『「マルチステップ操作」ビュー』を参照してください。

データベース内のある追跡対象セッション ID を更新するには、スキャンを実行する直前に、セッション ID が送信される URL にアクセスします。新規のセッション ID が、更新された値で送信されます。

- ダイナミック: AppScan は、(例えば、シャドー Cookie と同様に) テスト前に Web アプリケーションで設定された新規の値に従って、テスト・ステージ中にセッション ID の値を自動的に更新します。

  「ダイナミック」 は、固有のセッション ID が特定の使用手順で更新されるように求めるセキュリティー手段を Web アプリケーションが実施することがわかっている場合にのみ選択してください。

-

  固定**:** 固定値を保持します。 Web アプリケーションのセキュリティーで、このセッション ID が常にこの値を持つ必要がある場合は、セッション ID に固定値を設定します。

探査ステージ中に、AppScan は、セッション ID と思われる Cookie および HTML パラメーターを自動的に検出し、それをリストに追加します。セッション ID であることがわかっている Cookie およびパラメーターは、スキャンの構成時に手動で追加できます。

URL 内のセッション **ID:**

URL パスに埋め込まれているセッション ID の追跡方法。

このタスクについて

AppScan がセッション ID を正しく追跡しない場合、セッションが頻繁に失われます。このセクションでは、URL パスに埋め込まれているセッション ID の追跡方法を説明します。

セッション ID: `abc34f3fa135`

セッション ID を含んでいる URL:`http://domain.name/dir/subdir/abc34f3fa135/anotherdir?param=val`

手順

1. このカスタム・パラメーターを認識する規則の作成:
   a. 「スキャン構成」 **>** 「パラメーターおよび **Cookie**」 **>** 「カスタム・パラメーター」タブを開きます。
   b.  をクリックして新しいカスタム・パラメーターを追加します。
   c. 参照名フィールドで、カスタム・パラメーター規則の名前を入力します。

d. パターンフィールドで、パラメーター・フォーマットを記述する正規表現を入力します。例: `(abc[a-zA-Z0-9]+)`
e. 「値グループ・インデックス」と「グループ・インデックスに名前を付ける」には変更を加えないでください。
f. ロケーションフィールドで、パスを選択します。
g. 「**OK**」をクリックして、変更内容を保管します。

2. AppScan がこのカスタム・パラメーターを追跡するように構成します。
a. 「スキャン構成」 **>** 「パラメーターおよび **Cookie**」 **>** 「パラメーターおよび **Cookie**」タブを開きます。
b.  をクリックして新しいパラメーターを追加します。
c. タイプをカスタム・パラメーターに設定します。
d. 前のステップで割り当てた参照名を選択します。
e. スキャン中にこのパラメーターを追跡チェック・ボックスを選択します。
f. 必要に応じて、追跡タイプをログイン値または動的に設定します。
g. 「**OK**」をクリックして、変更内容を保管します。

3. 記録したログイン手順に、このパス内のセッション ID を含む URL が含まれている場合、AppScan がセッション ID を追跡できるように再度ログインを記録する必要があります。
4. 必要に応じて、再度フルスキャンまたは再探査を実行します。

冗長性調整

冗長性調整を慎重に行うことで、スキャン時間を大幅に短縮できます。

AppScan は、新規情報が示されないことが明らかな場合、複数の要求を送信しないようにします。多くの場合、特定のパラメーターの値の違いは重要ではありません。また、その他のすべてのパラメーターが同じで、その値だけが異なる場合に、複数の要求を送信する必要はありません。

次の 2 つの要求を考えてみましょう。

```
.../doAction.pl?action=buy&timestamp=14:00&n=1

.../doAction.pl?action=buy&timestamp=15:30&n=1
```

これらの違いはタイム・スタンプの値だけです。

大抵の場合、どちらかの構成を使用して単一の要求を送信すれば十分であり、両方を送信する必要はありません。一方の要求に対する応答で明らかになった弱点が、もう一方の要求では明らかにならないことは、まずありません。したがって、このような場合に 1 つの要求だけが送信されるように、タイム・スタンプ・パラメーターの「冗長性調整」設定を構成する必要があります。

以下も参照してください。

86 ページの『冗長性調整オプション』

87 ページの『冗長性調整のデフォルト』

87 ページの『冗長性調整のデフォルトの変更』

88 ページの『特定のパラメーターの冗長性調整の変更』

冗長性調整オプション:

「構成」 > 「パラメーターおよび Cookie」でリストされる、特別な属性を持つパラメーターおよび Cookie の冗長性を調整するオプションです。

チェック・ボックス	選択されている場合の動作

このパラメーター/Cookie が追加または削除されるたびに、URL を再探査します。	探査ステージで、一方の URL にはこのパラメーターが含まれていて、もう一方の URL には含まれていないという点だけが異なる 2 つの URL を異なる URL として処理し、両方を探査します。
	
	例えば、以下の 2 つの URL の場合、両方 が探査されます。
	
	`...page.jsp`
	`...page.jsp?thisParam=Value`
	
	このチェック・ボックスを選択解除すると、このような場合に一方の要求のみが送信され、もう一方は破棄されます。

このパラメーター/Cookie の値が変更されるたびに、URL を再探査します。	探査ステージで、このパラメーター/Cookie の値だけが異なる 2 つの URL を異なる URL として処理し、両方を探査します。
	
	例えば、以下の 2 つの URL の場合、両方 が探査されます。
	
	`...page.jsp?thisParam=Value1`
	`...page.jsp?thisParam=Value2`
	
	このチェック・ボックスを選択解除すると、このような場合に一方の要求のみが送信され、もう一方は破棄されます。
	注: このオプションは、パラメーターまたは Cookie が追跡される場合には関係ありません。

このパラメーター/Cookie が追加または削除されるたびに、すべての隣接パラメーター/Cookie テストを繰り返します。	テスト・ステージで、このパラメーターが追加または除去された点だけが異なる 2 つの URL を異なる URL として処理し、隣接パラメーターを再テストします。
	
	例えば、以下の 2 つの URL の場合、隣接パラメーター用に 2 つの完全なセットのテストが生成されます (URL ごとに 1 セット)。
	
	`...page.jsp?adjacentParam=<test_this>`
	`...page.jsp?adjacentParam=<test_this>&thisParam=Value`
	
	このチェック・ボックスを選択解除すると、隣接パラメーター用に 1 セットのみのテストが生成されます。

このパラメーター/Cookie の値が変更されるたびに、すべての隣接パラメーター/Cookie テストを繰り返します。	テスト・ステージで、このパラメーター/Cookie の値だけが異なる 2 つの URL を異なる URL として処理し、隣接パラメーターを再テストします。
	
	例えば、以下の 2 つの URL の場合、隣接パラメーター用に 2 つの完全なセットのテストが生成されます (URL ごとに 1 セット)。
	
	`...page.jsp?adjacentParam=<test_this>&thisParam=Value1`
	`...page.jsp?adjacentParam=<test_this>&thisParam=Value2`
	
	このチェック・ボックスを選択解除すると、隣接パラメーター用に 1 セットのみのテストが生成されます。
	注: このオプションは、パラメーターまたは Cookie が追跡される場合には関係ありません。

以下も参照してください。

85 ページの『冗長性調整』

冗長性調整のデフォルト:

「構成」 > 「パラメーターおよび Cookie」でリストされる、特別な属性を持つパラメーターおよび Cookie の冗長性を調整するオプションです。

探査の最適化エクステンションが実行されない場合、冗長性調整のデフォルト設定は以下のとおりです。

チェック・ボックス	デフォルト値
このパラメーター/Cookie が追加または削除されるたびに、URL を再探査します。	
このパラメーター/Cookie の値が変更されるたびに、URL を再探査します。	
このパラメーター/Cookie が追加または削除されるたびに、すべての隣接パラメーター/Cookie テストを繰り返します。	
このパラメーター/Cookie の値が変更されるたびに、すべての隣接パラメーター/Cookie テストを繰り返します。	

探査の最適化エクステンションがアクティブ化され実行される場合、ナビゲーション・パラメーターの冗長性調整の設定は大きく なります。その一方でデフォルト設定 (すべての非ナビゲーション・パラメーターに適用) は小さく なります。

チェック・ボックス	ナビゲーション	デフォルト
このパラメーター/Cookie が追加または削除されるたびに、URL を再探査します。		
このパラメーター/Cookie の値が変更されるたびに、URL を再探査します。		
このパラメーター/Cookie が追加または削除されるたびに、すべての隣接パラメーター/Cookie テストを繰り返します。		
このパラメーター/Cookie の値が変更されるたびに、すべての隣接パラメーター/Cookie テストを繰り返します。		

以下も参照してください。

85 ページの『冗長性調整』

冗長性調整のデフォルトの変更:

冗長性調整のデフォルト設定は、手動で変更されない限り、「構成」>「パラメーターおよび Cookie」のリストに対して追加されたすべての項目に適用されます。

手順

1. 「パラメーターおよび Cookie」タブの下部にある「冗長性調整のデフォルト」をクリックします。

   「冗長性調整のデフォルト」ダイアログ・ボックスが開きます。このオプションについては、 86 ページの『冗長性調整オプション』で説明します。
2. 必要に応じて設定を調整します (詳しくは、 86 ページの『冗長性調整オプション』を参照)。

ここで行った変更は、すべての新規パラメーターに対して、それらが AppScan によって発見されるか、ユーザーによって定義されるときに、適用されます。

注: デフォルトへの変更は、既に定義されているパラメーターまでさかのぼって適用されることはありません。これは、各パラメーターについて手動で実行する必要があります。

次のタスク

参照先: 86 ページの『冗長性調整オプション』

特定のパラメーターの冗長性調整の変更:
手順

1. 「パラメーターおよび Cookie」タブで、パラメーターを選択し、 をクリックします

   「パラメーター定義 **(Parameter Definition)**」ダイアログ・ボックスが表示されます (詳しくは、 80 ページの『パラメーター定義』を参照)。
2. ダイアログ・ボックスの下部で、「追加オプション」をクリックします。

   「冗長性調整」オプションが開きます (詳しくは、 86 ページの『冗長性調整オプション』を参照)。

次のタスク

86 ページの『冗長性調整オプション』を参照してください。

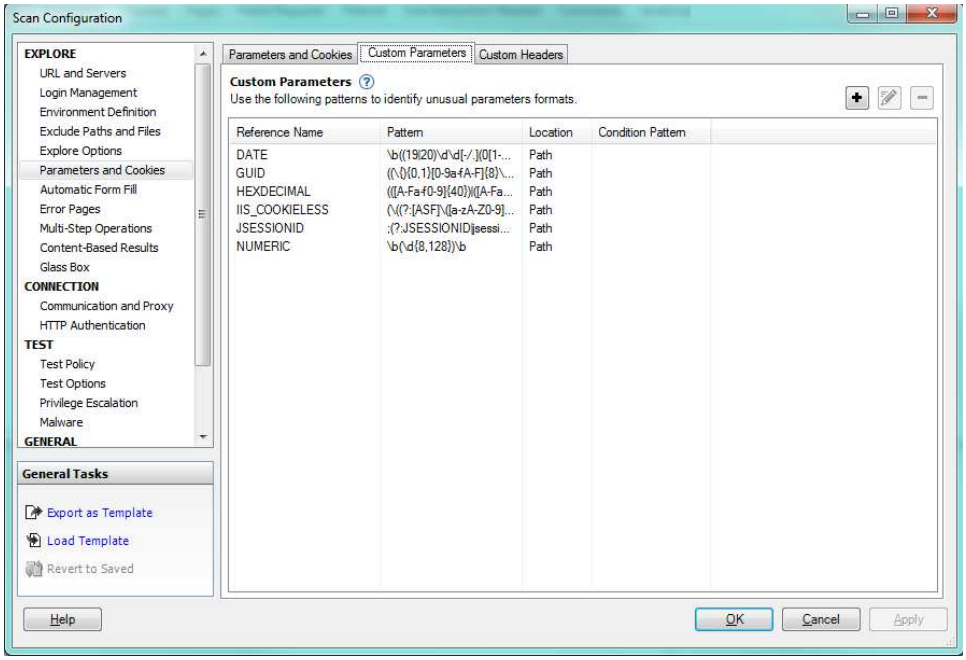
「カスタム・パラメーター」タブ

「構成」ダイアログ・ボックスの「パラメーターおよび Cookie」ビューの「カスタム・パラメーター」タブです。

このタスクについて

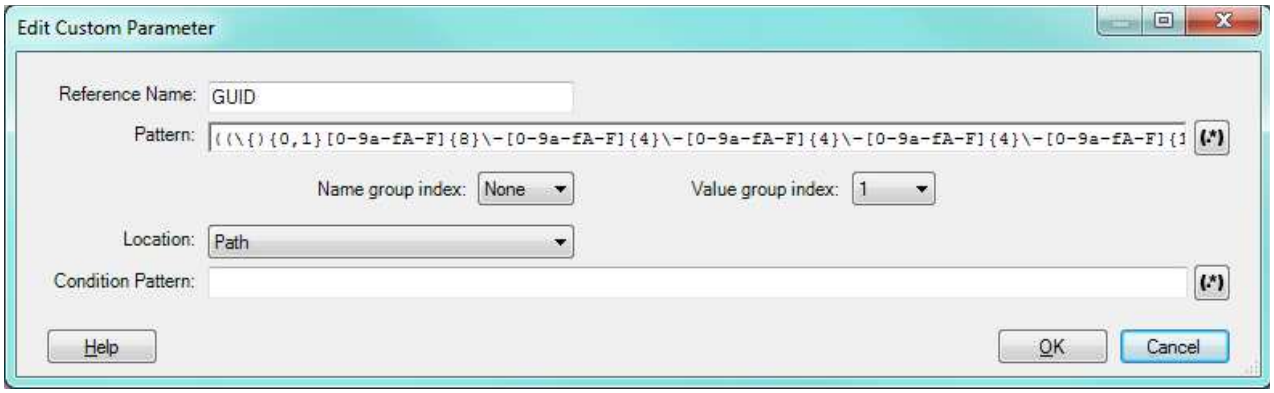
「探査:パラメーターおよび Cookie」ビューの 2 番目のタブでは、AppScan が自動的に認識できないフォーマットを持つカスタム・パラメーターを作成および管理できます。

AppScan はパラメーターを標準の HTML フォーマットで自動的に認識しますが、パラメーターが (例えば、パス内または別のパラメーター内で) 別の形式である場合、AppScan がスキャン中に認識し、それに従って操作できるように、AppScan に対してパラメーターを定義する必要があります。



手順

新規カスタム・パラメーターを定義するには、 をクリックして既存の定義を変更し、表内のパラメーターを選択し、 をクリックします
「カスタム・パラメーターの追加/編集」ダイアログ・ボックスが開きます。そのフィールドとオプションが、続く表で説明されています。



設定	説明
参照名	パラメーターにわかりやすい名前を割り当てます。 カスタム・パラメーターは、接頭部 "__patternParameter__" の後にパラメーター名が続く形で、「アプリケーション・データ」ツリーに表示されます。

設定	説明
パターン	パラメーターを定義する 1 つ以上のグループを含む正規表現。 「グループ」とは、括弧で記述された正規表現のセクションです。いずれかのグループにパラメーター値が含まれます。また、名前が含まれるグループも存在する場合があります。  をクリックして Expression Test PowerTool を開くことで、正規表現の構文を検証できます。
グループ・インデックスに名前を付ける	(オプション) 正規表現に名前が含まれる場合、どのグループ (1、2、3...) にその名前が含まれているかを示します。 AppScan は、この値を使用して「すべてのグループをカウント」し、パラメーター名を見つけます (下の例を参照)。
値グループ・インデックス	上記の正規表現のどのグループ (1、2、3...) にパラメーターの値が含まれるかを示します。 AppScan は、この値を使用して「すべてのグループをカウント」し、パラメーター値を見つけます (下の例を参照)。
場所	要求のどのコンポーネント (Body/Path/Query) にこのパラメーターが含まれるのかを示します。 注: ここで行った選択は、「パターン」にも「条件パターン」(ある場合) にも適用されますが、「応答パターン」には適用されません。
条件パターン	(オプション) パラメーターを含むコンポーネント全体 (Body、Path、または Query) を定義する正規表現を入力できます。AppScan は、コンポーネント全体がこのパターンに一致する場合のみパラメーターを作成して、スキャン時間を節約します。 例えば、パラメーターが Body にあり、Body が XML でなければならない場合、Body の始まりと終わりが XML タグであることを確認する正規表現を条件パターンとして設定できます。この条件を満たさない場合、AppScan はパラメーターを作成しません。

注: 正規表現を使用する必要がある、または正規表現を使用できるフィールドには、  ボタンがあります。このボタンを使用して Expression Test PowerTool を開くことで、正規表現の構文を検証できます。

グループ・インデックス

パターン正規表現におけるグループのインデックス付けシステムを理解するには、以下の例が参考になります。

```
Pattern: (abc)((def)(ghi))
```

この表現のグループは、次のようにインデックス付けされます。

```
Group 1: (abc)
Group 2: ((def)(ghi))
Group 3: (def)
Group 4: (ghi)
```

「グループ・インデックスに名前を付ける」および「値グループ・インデックス」ドロップダウン・リストを使用して、パラメーターに適切なグループを選択します。選択したグループは、「パターン」フィールドで強調表示されます。

注: インデックスの選択後にパターンを変更しており、選択したインデックスがパターン内にもはや存在しない場合、警告が表示されますが、値は自動的には変更されないため、手動で変更する必要があります。

「カスタム・ヘッダー」タブ

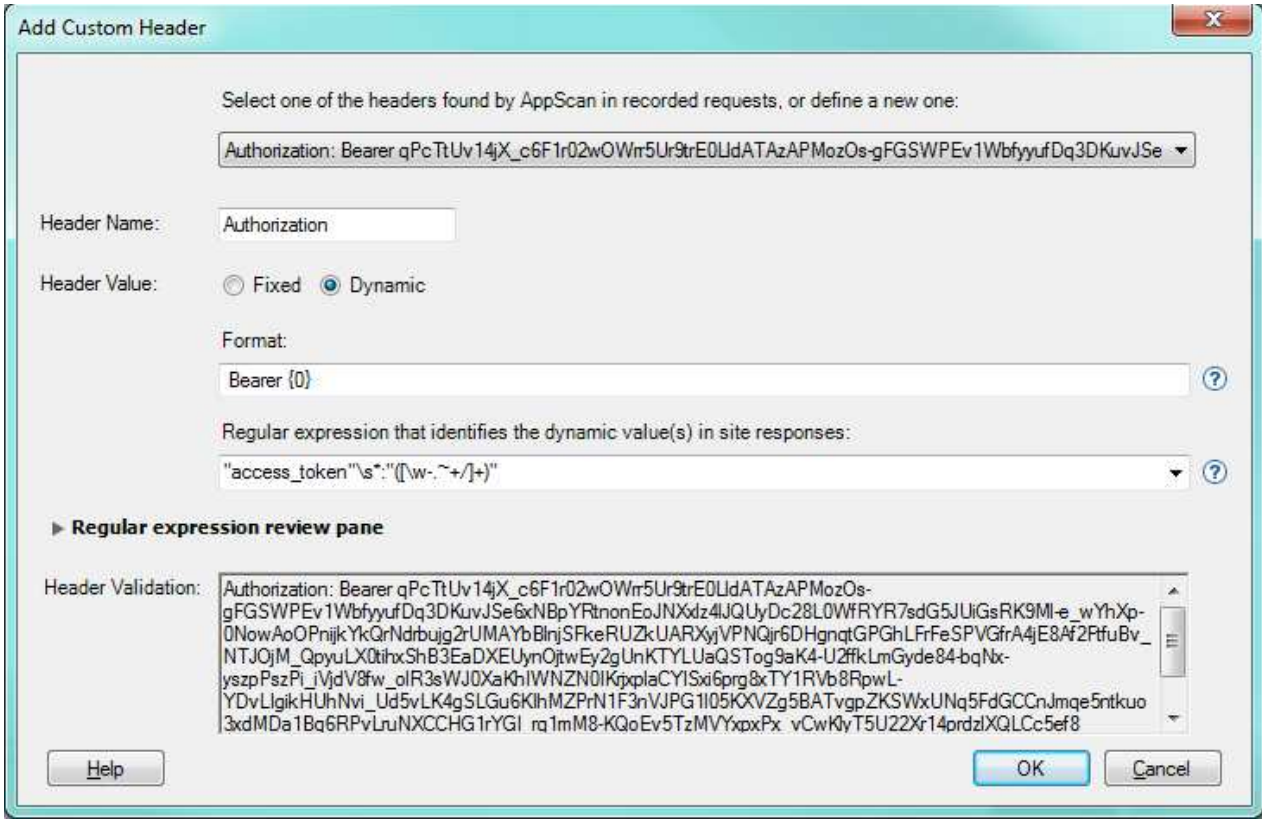
「構成」ダイアログ・ボックスの「パラメーターおよび Cookie」ビューの「カスタム・ヘッダー」タブ。

このタスクについて

「探査」の 3 番目のタブ:「パラメーターおよび Cookie」ビューでは、非標準 (カスタム) HTTP のヘッダーフォーマットを定義することができます。AppScan では、サイトを効率的にテストするために、応答コンテンツ内のパラメーターを特定し、AppScan がサイトに送信するヘッダーに、それらのパラメーターを適切に追加できることが必要です。) AppScan ではカスタム・ヘッダーを自動的に認識しようとしますが、ユーザーがこのタブを使用して定義を追加および変更することができます。また、既存の定義をアクティブにしたり、非アクティブにしたりすることができます (その場合、非アクティブになった定義はスキャンと共に保存されますが、使用されません)。

手順

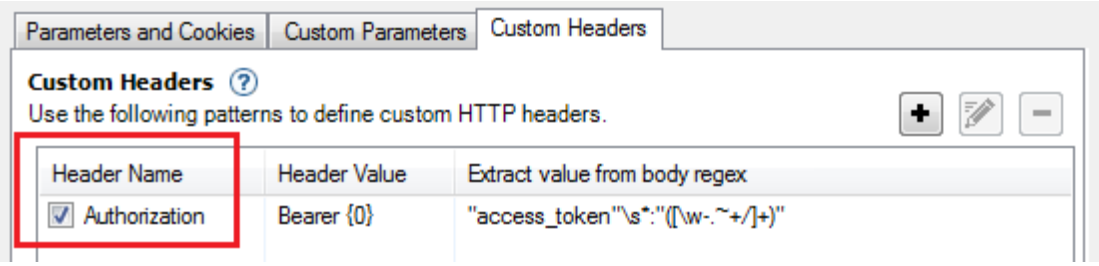
新規定義を作成するには、 をクリックして既存の定義を変更し、表内のヘッダーを選択し、 をクリックします
「カスタム・ヘッダーの追加/編集」ダイアログ・ボックスが開きます。そのフィールドとオプションが、続く表で説明されています。



設定	説明
ヘッダーの選択...	要求が記録されており、AppScan がカスタム・ヘッダーを特定した場合、ヘッダーは、ダイアログ・ボックスの上部にあるドロップダウン・リストに表示されます。 カスタム・ヘッダーが見つからない場合、このドロップダウン・リストは表示されません。 このリストからヘッダーを選択すると、残りのフィールドは自動的に入力されます。
ヘッダー名	HTTP ヘッダーの名前。
追跡タイプ	
ログイン/ダイナミック/修正済み	• ログイン値: (デフォルト、および推奨) このヘッダーを含む、アプリケーションに送信される要求は、ログイン・プロセスの最後に受信したヘッダーの値を使用します。 • ダイナミック値: このヘッダーを含む、アプリケーションに送信される要求は、アプリケーションから受信した最新の値を使用します。 • 固定値: このヘッダーを含む、アプリケーションに送信される要求は常に、「値」フィールドに入力される値を使用します。
値	(固定のみ) 値を入力します。
形式	(ダイナミックのみ) ダイナミック値の 1 つ以上のグループ (最初のグループは {0} で開始し、次のグループは {1} で開始、その後も同様に続く) を使用して完全ヘッダーの形式を定義します。
正規表現	(ダイナミックのみ) サイトの応答の値を定義する正規表現。 「形式」フィールドで定義した各値のグループを含める必要があります。
「正規表現のレビュー」ペイン	(ダイナミックのみ) クリックすると展開されます。 このペインは、正規表現を検証するために使用します。上部フィールドに完全な応答を入力すると、下部フィールドに識別されたグループとその値が表示されます。
ヘッダー検証	ヘッダー定義がスキャン時に使用するために正常に検証されたかどうかを示します。

タスクの結果

カスタム・ヘッダー定義を追加すると、カスタム・ヘッダー・リスト内に表示されます。定義の隣のチェック・ボックスが選択されていると、その定義がアクティブであることを示します。非アクティブの項目は、スキャンで保存されますが、使用されることはありません。



「フォームの自動入力」ビュー

「構成」ダイアログ・ボックスの「フォームの自動入力」ビューには、アプリケーションのフォームへの入力に使用される値が含まれています。

「フォームの自動入力」値は、AppScan が、ご使用のアプリケーションでフォームを入力するために使用する値です。値の多くにはデフォルト値が設定されており、 54 ページの『ログインの記録』 中に値が入力されると、自動的に更新されます。

これらの値は、「スキャン構成」ダイアログ・ボックスの以下のビューにおいて、表示、追加、編集を行うことができます。

設定	詳細
自動フォーム入力を有効にする	このチェック・ボックスが選択されている場合 (デフォルト)、AppScan は、「探査」ステージ中にご使用のアプリケーションのユーザー入力フォームに自動的に入力しようとします。
「フォームの自動入力」プロパティー・リスト	AppScan がスキャン中に自動でフォームに入力するために使用する値のリスト。このリストに追加したり、編集を行ったりすることができます。 詳細については、を参照してください。 『フォーム・プロパティー』
ユーザー名パラメーターおよびパスワード・パラメーター	ストリングをコンマで区切って表示します。このストリングは、AppScan がユーザー名またはパスワードを入力しなければならないフィールドを認識するために使用します。このストリングは、必要に応じて編集することができます。ストリングの間に、コンマをスペースなしで追加してください。
ユーザー名値とパスワード値	「ログイン」ビューで「自動ログイン」が選択されている場合に、ログインで使用する名前およびパスワードを表示します。この値は、ここで編集することができます。 (詳しくは、 53 ページの『「ログイン」タブ』 を参照してください。)
不明なフィールドに次の値を入力	AppScan で認識できないフィールドがあった場合に使用される文字列を入力するか (デフォルトは「1234」)、毎回 AppScan が選択するランダム値 を使用することができます。

フォーム・プロパティー

「構成」ダイアログ・ボックスの「フォーム・プロパティー」ビューには、AppScan がフォームでの自動入力に使用する値がリストされます。

このタスクについて

AppScan がスキャン中の自動フォーム入力に使用するフォーム・プロパティーに、追加または編集を実行できます。

手順

新規の定義を追加するには、  をクリックします (あるいは、既存のフォーム・プロパティーを編集するには、そのフォーム・プロパティーを選択して  をクリックします)。
「フォーム・プロパティー」ダイアログ・ボックスが表示されます。

列	説明
説明	パラメーターを表す名前。
パラメーター	HTML でこのパラメーターを定義するために使用される名前、または名前の一部。AppScan はこの名前を持つフィールドを検出すると、指定された値を入力します。 複数のパラメーター名を 1 行に入力するには、コンマをスペースなしで使用します。例: 説明:郵便番号	パラメーター: zip,postal

列	説明
値	AppScan がこのパラメーターについて送信するユーザー入力。
オーバーライド (Override)	場合によっては、特定のフィールドに対してサイトが独自のデフォルト値を入力することがあります。そのような場合、デフォルトでは、AppScan はここで入力された値ではなくサイトの提案した値を使用します。 サイトが別のデフォルト値を提供する場合でも、ここで定義された値を AppScan が使用するようにしたい場合は、このチェック・ボックスを選択します。
照合方法	AppScan がここで定義されたパラメーターを検索する方法、およびサイトによって提供されたフィールド入力オプションとの関係を定義します。オプションは、「部分一致」または「完全一致」です。 完全一致: 「パラメーター」フィールド内のいずれかのテキスト・ストリングと厳密に一致するパラメーターに対してのみ、値が入力されます。(例えば、`addr` と定義されたパラメーターは、`address` という名前のフィールドには使用されません。) さらに、フィールドにオプションのドリルダウン・リストが用意されている場合、この値は、いずれかのオプションと厳密に 一致する場合のみ使用されます。 部分一致: ここでリストされたいずれかのパラメーター・ストリングと一致、または部分的に一致するパラメーターに対して、この値が入力されます。(例えば、パラメーターが `addr` と定義されている場合、このパラメーターは `address` や `ADDR` という名前のフィールドにも使用されます。) さらに、フィールドにオプションのドリルダウン・リストが用意されていて、それらのオプションのいずれもここで入力された値と厳密に一致しない場合は、近いものが代わりに使用されます。
URL	このフィールドを空のままにした場合、この値は、URL に関係なくこのパラメーターに使用されます。 特定の URL が指定された場合、この値はこの URL に存在するパラメーターに対してのみ使用されます。(したがって、URL ごとに異なる方法でパラメーターを定義することができます。) ただし、同じパラメーターと空の URL を持つ行が他にない場合、この行の値は、他のすべての URL に対してもデフォルトになります。

例

『フォーム・プロパティーのエクスポートおよびインポート』

95 ページの『保存された ASFF ファイルのインポート』

フォーム・プロパティーのエクスポートおよびインポート:

このタスクについて

フォーム入力および認証プロパティーは、「フォーム・プロパティー」テーブルを XML ファイルとしてエクスポートすることで、将来の使用のために保存できます。

手順

1. 「探査: フォームの自動入力」ビューで、「エクスポート」をクリックします。

   「名前を付けて保存」ダイアログ・ボックスが表示され、データを ASFF ファイル (AppScan フォーム入力ファイル) として保存することができます。コンテンツは、XML 形式です。
2. ファイルに名前を付け、「保存」をクリックします。

   ASFF ファイル内容の例:

```
<FormFiller Version="1.0" Enabled="True" DefaultValue="1234"
UseDefaultValue="True">
 <Group Name="InternalAppScanUserName" Value="" MatchType="Partial" Action="">
 <MatchNames>
 <MatchName>user</MatchName>
 <MatchName>name</MatchName>
 <MatchName>uid</MatchName>
 <MatchName>login</MatchName>
 <MatchName>usr</MatchName>
 </MatchNames>
 </Group>
```

保存された **ASFF** ファイルのインポート**:**
手順

1. 「探査**::** フォームの自動入力」ビューで、「インポート」をクリックします。

   メッセージが表示され、ASFF ファイルをインポートすると、テーブル内のいずれかの現行データを削除することになることが警告されます。続行する場合は、「**OK**」をクリックします。
2. 関連 ASFF ファイルを参照し、「開く」をクリックします。

Flash ファイルのフォーム・プロパティー

Adobe Flash ファイルのフォーム・プロパティーには、特別な注意が必要となる場合があります。

このタスクについて

スキャンの構成における重要な要素は、特にフォーム・フィールドの名前が普通と異なる場合に、フォーム・フィールドに有効な値を定義することです。例えば、電子メール・フィールド名が予期しない名前である場合、AppScan は有効な電子メール・アドレス形式ではない入力を送信し、結果としてテストが失敗する可能性があります。

Flash ファイルの場合、インスタンス名 (フォーム・フィールド) にアクセスできないため、問題はより大きくなります。「スキャン構成」ダイアログ・ボックスの 92 ページの『「フォームの自動入力」ビュー』で、これらの名前にアクセスし、それらに対して有効な名前を構成します。

「エラー・ページ」ビュー

「構成」ダイアログ・ボックスの「エラー・ページ」ビューです。

AppScan があるテストに対する応答で 404 エラー・ページを受け取った場合、この応答はサイトが要求を正しくないものとして正当に認識したことを示すため、このテストは検出なしとして通常は記録されます。場合によってはその逆の例もあり、エラー・ページとして正常な結果を示すことがあります。いずれの場合も、AppScan がエラー・ページを正確に認識できるように、エラー・ページを正しく定義することが重要です。

Web アプリケーションやサーバーによって使用されているカスタマイズされたまたは動的に生成された 404 エラー・ページは、しばしば自動的に認識できないことがあります。AppScan は、カスタマイズされた 404 エラー・ページを認識しようとしますが、うまくいかない場合もあります。カスタム・エラー・ページを受け取りながら、これが認識されないと、テスト結果は実際には「検出なし」であるにもかかわらず「検出」と記録される場合、またはその逆の場合もあります。デフォルトでは、エラー・ページ・リストには標準エラー・ページ定義が含まれます。各定義ごとに、エラーのタイプと値が示されます。

ご使用のアプリケーションのエラー・ページがこのリストの定義に含まれていない場合、AppScan がエラー・ページを認識できるように、必要なストリング、正規表現、および URL を追加する必要があります。これを実行することにより、スキャン結果中の「誤検出」数を減らすことができます。そのための方法として、以下の 2 つがあります。

- スキャンを開始する前に、エラー・ページを手動で定義できます。『新規エラー・ページの定義』 を参照してください
- 探査ステージを実行した場合、見つかった URL をエラー・ページとして設定できます。 97 ページの『エラー・ページの設定』 を参照してください

重要**:** 正しく定義されていないエラー・ページは「誤検出」結果および「検出漏れ」結果の原因となることがあるため、スキャンのテスト・ステージの後 に、エラー・ページを追加または削除する場合、スキャン結果を更新する必要があります。

- 以前の定義で成功を示したテストに対しては、「現在の結果を適用」をクリックすると結果を更新できます。
- 以前の定義で失敗を示したテストに対しては、再テストを実行する必要があります。

以下も参照してください。

97 ページの『エラー・ページ変更の適用』

新規エラー・ページの定義

手順

1. 新規カスタム・エラー・ページの定義を追加するには、  をクリックします (あるいは、既存の定義を編集するには、その定義を選択して  をクリックします)。

   「カスタム・エラー・ページ」ダイアログ・ボックスが表示されます。
2. 「タイプ」リストで、以下を選択します。
   - 文字列**:** エラー・ページの HTML コンテンツで検出される文字列と突き合わせます。
   - 正規表現**:** エラー・ページの HTML コンテンツで検出される正規表現と突き合わせます。  ボタンをクリックして Expression Test PowerTool を開くことで、正規表現の構文を検証できます。
   - **URL:** 応答ページの URL を突き合わせます。
   - ページ**:** 正確な応答ページと突き合せます。(この方法は、 232 ページの『「要求/応答」タブ』で特定のバリアントに対して「エラー・ページとして設定」をクリックした場合に使用されます。)
3. 「値」テキスト・ボックスで、文字列、正規表現、または URL (相対パスおよびファイル名) を入力します。

   重要**:** 正しく定義されていないエラー・ページは「誤検出」結果および「検出漏れ」結果の原因となることがあるため、スキャンのテスト・ステージの後 に、エラー・ページを追加または削除する場合、スキャン結果を更新する必要があります。
   - 以前の定義で成功を示したテストに対しては、「現在の結果を適用」をクリックすると結果を更新できます。
   - 以前の定義で失敗を示したテストに対しては、再テストを実行する必要があります。
4. 「**OK**」をクリックします。

これ以降、この文字列、正規表現、または URL と一致するすべての応答は、AppScan によりエラー・ページとして認識されます。

例

『カスタム・ページ・フィルタリングの例』

カスタム・ページ・フィルタリングの例:

次の表は、ページを「カスタム・エラー・ページ」リストに追加する方法例を示しています。

タイプ	値	追加するもの
URL	**/fileNotFound.aspx**	特定のファイル
文字列	**"page not found"**	この文字列が含まれるページ
正規表現	**(?i)(URL|page) (.*) not found**	以下を含む任意のページ:「URL name not found」、「url name not found」、「Page page.ext not found」など。

注: 正規表現とは、特定の構文規則に従って文字列のセットを記述する文字列のことです。 Expression Test PowerTool (「ツール」>「**Expression Test**」) は、正規表現の構文を確認するのに役立ちます。

正規表現を作成するための支援がさらに必要な場合は、次のリンクが役立ちます。 http://www.regular-expressions.info/quickstart.html

エラー・ページの設定

探査結果にリストされているページを、カスタム・エラー・ページとして設定できます。

このタスクについて

「データ・ビュー」>「ページ」の探査ステージでディスカバーされた URL のリストを表示できます。ご使用のサイトのいずれかのカスタム・エラー・ページが誤ってリストされている場合、そのページをエラー・ページとして設定できます。

手順

1. アプリケーション・データ・ビューで探査結果を開きます (F2)。
2. 「結果」ペインで、「ページ」をクリックします。
3. URL を右クリックし、「エラー・ページとして設定」をクリックします。

   新規定義を取り込むために結果を更新するかどうかの確認が求められます。
4. 「開始」をクリックします。

   当該 URL がスキャン構成の「エラー・ページ」リストに追加され、必要に応じて結果が更新されます。

エラー・ページ変更の適用

このタスクについて

スキャンの後にエラー・ページのリストを編集したりそれに追加したりする場合は、変更を反映するようにスキャン結果を更新する必要があります (「誤検出」を除去します)。

編集後に、リストの上の「結果を*Current*®適用」ボタンがアクティブになります。

手順

「結果を**Current**適用」ボタンをクリックします。
結果は、新規/更新ページがエラー・ページであることを考慮に入れて更新されます。

「マルチステップ操作」ビュー

「構成」ダイアログ・ボックスの「マルチステップ操作」ビューは、リンクを特定の順序でクリックすることによってのみ到達できるサイトの部分をテストするためのビューです。

ユーザーが品目をカートに追加し、まだ支払いを行っていないオンライン・ショップなど、リンクを特定の順序で クリックすることによってのみ到達できるサイトの部分を探査するには、マルチステップ操作が必要です。以下の 3 つのページについて考えます。

1. ユーザーがショッピング・カートに 1 つ以上の品物を追加します
2. ユーザーが支払いと配送方法の詳細を入力します
3. ユーザーが、この注文が完了した確認を受け取ります

ページ 2 にはページ 1 を経由してのみ到達できます。ページ 3 にはページ 1、ページ 2 を経由してのみ到達できます。これがシーケンスです。ページ 2 とページ 3 をテストできるようにするには、AppScan が各テストの前に HTTP 要求の正しいシーケンスを送信する必要があります。

上記の例では、ページ 1 > ページ 2 > ページ 3 という単一シーケンスを記録します。AppScan は、必要に応じてこの順序から必要なサブシーケンスを抽出します。(ページ 2 のテスト中には、ページ 1 の要求が最初に送信されます。ページ 3 のテスト中には、ページ 1 に続いてページ 2 が送信されます。)

注**:** マルチステップ操作の数は 5 個以下、1 つの操作のステップ数は 25 個以下、合計ステップ数は 70 個以下に制限することをお勧めします。

注**:** マルチステップ操作の構成をマニュアル探査と混同しないようにしてください。また、上記で説明したような場合にのみ使用してください。詳しくは、AppScan を使用したマニュアル探査を参照してください。

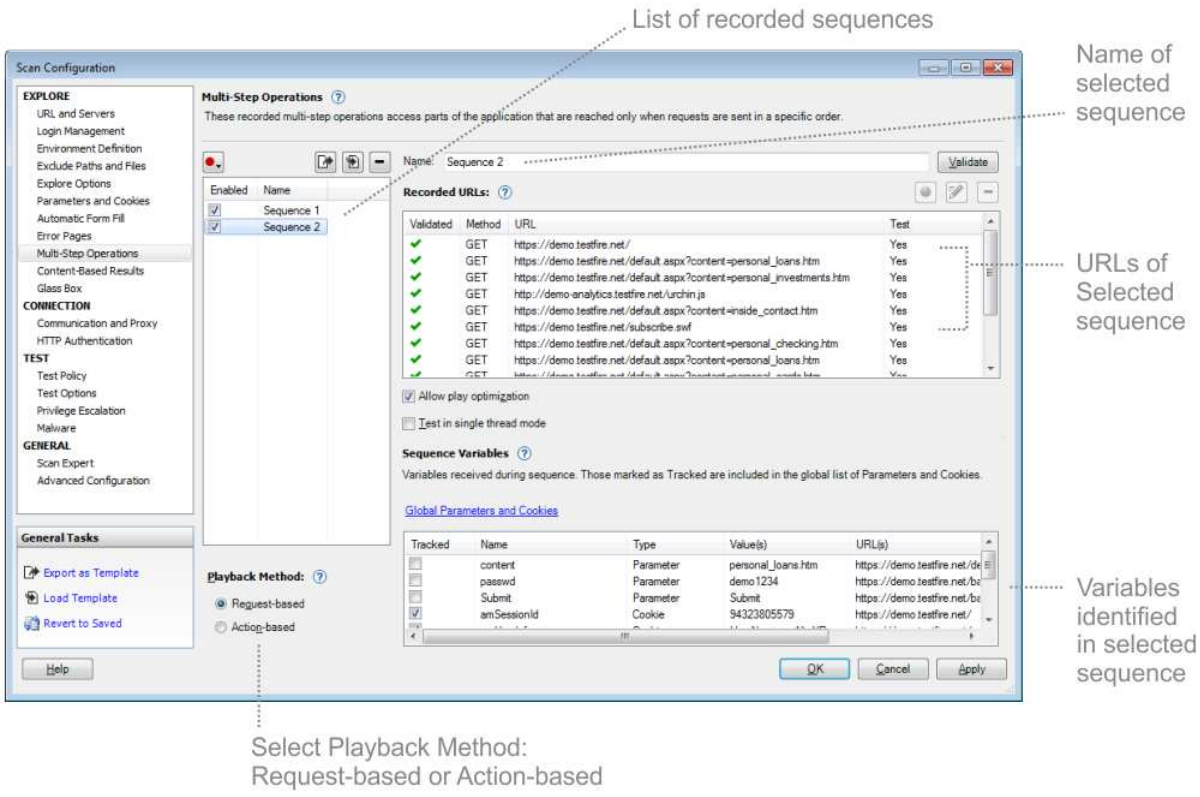

List of recorded sequences
Name of selected sequence
URLs of Selected sequence
Variables identified in selected sequence
Select Playback Method: Request-based or Action-based
Scan Configuration
EXPLORE
URL and Servers
Login Management
Environment Definition
Exclude Paths and Files
Explore Options
Parameters and Cookies
Automatic Form Fill
Error Pages
Multi-Step Operations
Content-Based Results
Glass Box
CONNECTION
Communication and Proxy
HTTP Authentication
TEST
Test Policy
Test Options
Privilege Escalation
Malware
GENERAL
Scan Expert
Advanced Configuration
General Tasks
Export as Template
Load Template
Revert to Saved
Multi-Step Operations
These recorded multi-step operations access parts of the application that are reached only when requests are sent in a specific order.
Enabled
Name
Sequence 1
Sequence 2
Name: Sequence 2
Validate
Recorded URLs:
Validated
Method
URL
Test
GET https://demo.testfire.net/ Yes
GET https://demo.testfire.net/default.aspx?content=personal_loans.htm Yes
GET https://demo.testfire.net/default.aspx?content=personal_investments.htm Yes
GET http://demo-analytics.testfire.net/urchin.js Yes
GET https://demo.testfire.net/default.aspx?content=inside_contact.htm Yes
GET https://demo.testfire.net/subscribe.swf Yes
GET https://demo.testfire.net/default.aspx?content=personal_checking.htm Yes
GET https://demo.testfire.net/default.aspx?content=personal_loans.htm Yes
Allow play optimization
Test in single thread mode
Sequence Variables
Variables received during sequence. Those marked as Tracked are included in the global list of Parameters and Cookies.
Global Parameters and Cookies
Tracked
Name
Type
Value(s)
URL(s)
content Parameter personal_loans.htm https://demo.testfire.net/de
passwd Parameter demo1234 https://demo.testfire.net/ba
Submit Parameter Submit https://demo.testfire.net/ba
amSessionId Cookie 94323805579 https://demo.testfire.net/
Playback Method:
Request-based
Action-based
Help
OK
Cancel
Apply

表 5. 「マルチステップ操作」ビューのオプション

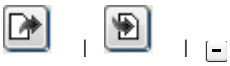
設定	詳細
記録を開始	クリックして新規シーケンスを記録します。ログイン詳細が構成されている場合は、下矢印をクリックして選択することができます。 「**AppScan IE** ブラウザー」>「ログインして記録」 AppScan は、ブラウザーが開く前にアプリケーションに自動でログイン(記録したログインを使用して)します。その後、ログイン要求を記録することなくマルチステップ操作を記録できるようになります。この方法には、このシーケンスが再生されるたびにログイン要求が再生されないという利点がありますが、AppScan がセッション無効状態の場合に限ります。 **注:** マルチステップ・シーケンスには存在し、ログイン・シーケンスには存在しないパラメーターと Cookie は、追跡をログイン値に変更した場合でも、常にダイナミックとして追跡されます。 「**AppScan IE** ブラウザー」>「ログインせずに記録」 AppScan はログインせずにシーケンスの記録を開始します。ブラウザーが開いているときに、マルチステップ・シーケンスを直接記録します。ログインする必要がある場合は、ログインが記録の一部になるため、シーケンスが再生されるたびにログインが再生され、スキャン時間が大幅に長くなる可能性があります。ログインが必要な場合は、前のオプションを使用することがベスト・プラクティスです。 **注:** このオプションを使用してシーケンスの一部としてログイン要求を記録する場合、受け取ったパラメーターと Cookie は、ログイン要求であっても、また、追跡をログイン値に変更していても、常にダイナミックとして追跡されます。 **AppScan Chromium** ブラウザー AppScan はログインすることなく、組み込み *Chromium* ベース・ブラウザーを使用して記録します。ブラウザーが開くとログインして、マルチステップ・シーケンスを記録できるようになります (必要な場合)。 **注:** このオプションを使用してシーケンスの一部としてログイン要求を記録する場合、受け取ったパラメーターと Cookie は、ログイン要求であっても、また、追跡をログイン値に変更していても、常にダイナミックとして処理されます。 詳しくは、 102 ページの『シーケンスの記録』 を参照してください。
	シーケンスを別のスキャンで使用するため (SEQ ファイルとして) エクスポートします。別のスキャンからエクスポートされたシーケンス (SEQ ファイル) をインポートします。現在のスキャンから選択したシーケンスを削除します。

表 5. 「マルチステップ操作」ビューのオプション (続き)

設定	詳細
再生方法	マルチステップ操作を記録する場合、AppScan によりアクションと要求の両方が記録されます。アクションと要求のどちらをスキャンで使用するかを選択できます。 要求ベースの再生 生の HTTP 要求を記録から送信します。一般的に早いのはこちらの方法です。 アクション・ベースの再生 ユーザーのクリックおよびキー・ストロークを再生します。この方法を選択するのは、サイトに大量の JavaScript が含まれている場合や、要求ベースの再生に含まれている要求を検証した際に、その一部に赤色の X でマークが付けられた場合などです。この方法では、スキャン時間が長くなる可能性があります。 要求ベースの再生がデフォルトの方法です。 **注:** 組み込みのブラウザー以外のブラウザーを使用するようにスキャンが構成されている (「ツール」 > 「オプション」 > 「外部ブラウザーの使用」) 場合は、常に要求ベースの再生が使用されます。 **注:** アクション・ベースの再生のサポートが行われていなかった AppScan バージョンで記録されたシーケンスをロードする場合、アクション・ベースの再生が選択されていてもそのシーケンスに対しては要求ベースの再生が選択されます。 **注:** アクション・ベースの再生をマルチステップ操作に選択する場合、ログイン方法としてもアクション・ベースを選択する必要があります。必要に応じて、ログイン手順を再び記録します (52 ページの『「ログイン管理」ビュー』を参照)。
シーケンス・リスト	このスキャンについて記録されたすべてのマルチステップ操作をリストします。
シーケンス名 (Sequence Name)	シーケンスのリストで選択されているシーケンスの名前です。それぞれの隣にあるチェック・ボックスは、このスキャンに対してそのシーケンスが有効であるかどうかを示します。 検証　これをクリックして、シーケンスが有効であることを確認します。AppScan はシーケンスを再生します。元の応答とは異なる応答を受け取る要求には赤色の X のマークが付けられ、これらがテストされないことが示されます。 **ヒント:** 要求が異なる応答を受け取る一般的な理由は、定義を必要とする動的シーケンス変数が存在しているためです。 105 ページの『シーケンス変数』を参照してください。これが問題ではなく、サイトに JavaScript が含まれている場合、アクション・ベースの再生に変更すると、結果が改善される可能性があります。

表 5. 「マルチステップ操作」ビューのオプション (続き)

設定	詳細
記録された URL	選択されたシーケンスのリンクまたはアクションを表示します。 検証済み 緑のチェック・マークは、URL が検証済みであることを示します。赤い X が未検証の URL の隣に表示されます。 テスト この URL を単独でテストするかどうかを示します (マルチステップ操作の一部としてだけでなく)。オプションは、「はい」/「いいえ」です。設定を変更するには、URL を右クリックして「テストする/テストしない」を選択します。「いいえ」を選択した場合でも、URL はマルチステップ操作の一部として再生されます。 シーケンスの再生 (テスト済みの URL のみに適用されます) この URL がテストされるたびにシーケンスの前のステップを再生するかどうかを示します。オプションは、「はい」/「いいえ」です。設定を変更するには、右クリックして「要求テスト前にシーケンスを再生」 > 「はい」/「いいえ」を選択します。 • シーケンス内の任意のリンクを選択し、ブラウザーのボタンをクリックすることにより、そのリンクを表示します (表示されるダイアログの右上にあるごみ箱アイコンをクリックすることにより、個々の要求を削除できます)。 • シーケンス内の任意のリンクを選択し、[-] をクリックすることにより、そのリンクを削除します。その後、「検証」をクリックして、更新されたシーケンスが引き続きセッション内の状態を維持しているかをチェックします。
シーケンス再生前にログイン	これを選択すると、マルチステップ操作を再生するときは必ず AppScan が最初にログインします。このオプションは、マルチステップ操作の一部としてログインを記録する場合にはクリアされます。
再生最適化を許可する	(要求ベースの再生のみ) これが選択されている場合 (デフォルト)、AppScan は、不要な再生を回避することにより、スキャン時間を最適化しようとします。この設定は、再生の最適化が原因で、AppScan でアプリケーションの一部が見つからないことが検出されない限り、無効にしないでください。 319 ページの『スキャン・ログ』は、 これを決定するのに役立ちます。
シングル・スレッド・モードでのテスト	AppScan は、複数の要求が、その間にシーケンスの再生を必要としない場合、それらを同時に送信する可能性があります。この結果、アプリケーションの一部がなくなった場合は、このチェック・ボックスを選択してください。
シーケンス変数	シーケンスの記録中に受信した変数をリストし、AppScan が決定した追跡する必要がある変数を示します。これらはセッション ID または他の変数である可能性があります。このリスト内の変数の状況を変更して、AppScan がそれらの変数を処理する方法を改善することができます (詳しくは、 105 ページの『シーケンス変数』 を参照)。

以下も参照してください。

AppScan を使用したマニュアル探査

205 ページの『マルチステップ操作のみをスキャン』

シーケンスの記録

このタスクについて

ログイン手順が構成済みの場合 (53 ページの『「ログイン」タブ』を参照)、マルチステップ操作を記録する際には以下の 2 つのオプションがあります。

「**AppScan IE** ブラウザー」>「ログインして記録」
AppScan は、ブラウザーが開く前にアプリケーションに自動でログイン(記録したログインを使用して)します。その後、ログイン要求を記録することなくマルチステップ操作を記録できるようになります。この方法には、このシーケンスが再生されるたびにログイン要求が再生されないという利点がありますが、AppScan がセッション無効状態の場合に限ります。

注: マルチステップ・シーケンスには存在し、ログイン・シーケンスには存在しないパラメーターと Cookie は、追跡をログイン値に変更した場合でも、常にダイナミックとして追跡されます。

「**AppScan IE** ブラウザー」>「ログインせずに記録」
AppScan はログインせずにシーケンスの記録を開始します。ブラウザーが開いているときに、マルチステップ・シーケンスを直接記録します。ログインする必要がある場合は、ログインが記録の一部になるため、シーケンスが再生されるたびにログインが再生され、スキャン時間が大幅に長くなる可能性があります。ログインが必要な場合は、前のオプションを使用することがベスト・プラクティスです。

注: このオプションを使用してシーケンスの一部としてログイン要求を記録する場合、受け取ったパラメーターと Cookie は、ログイン要求であっても、また、追跡をログイン値に変更していても、常にダイナミックとして追跡されます。

AppScan Chromium ブラウザー
AppScan はログインすることなく、組み込み *Chromium* ベース・ブラウザーを使用して記録します。ブラウザーが開くとログインして、マルチステップ・シーケンスを記録できるようになります(必要な場合)。

注: このオプションを使用してシーケンスの一部としてログイン要求を記録する場合、受け取ったパラメーターと Cookie は、ログイン要求であっても、また、追跡をログイン値に変更していても、常にダイナミックとして処理されます。

構成済みのログイン手順がない場合に使用できるのは、「記録」の 1 オプションだけです。

重要: マルチステップ操作の再生中は、セッション内検出はオフです (53 ページの『「ログイン」タブ』を参照)。これはつまり、AppScan はログインしていることを検証しないということです。したがって、マルチステップ操作の失敗によりユーザーがアプリケーションからログアウトすることになる場合、ログインをシーケンスの一部として記録することは重要です (これによりシーケンスが実行されるたびにログインは再生されます)。これが実行されないと、マルチステップ操作は失敗する場合があります。

注: ご使用の Web サイトが Internet Explorerをサポートしていない場合、>「**AppScan Chromium** ブラウザーの使用」を代わりにクリックします。

手順

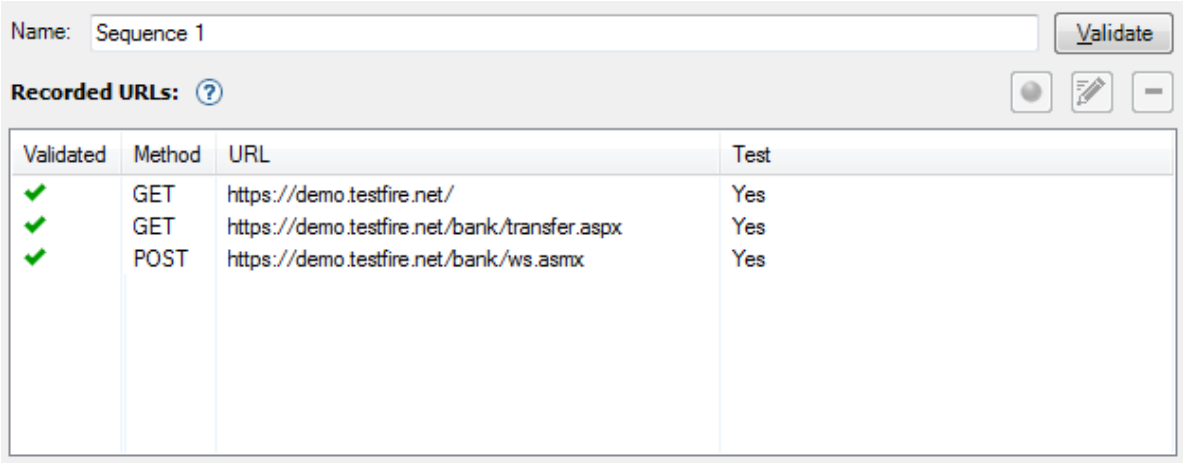
1.  をクリックし、記録オプションの 1 つを選択します (上記参照)。

   ブラウザーが開き、記録を開始します。
2. リンクをクリックし、必要なページにアクセスするために、必要に応じてフィールドに入力します。操作の一部として記録することなくリンクをクリックしたい場合は、「一時停止」  ボタンを使用することができます。
3. ブラウザーを閉じます。

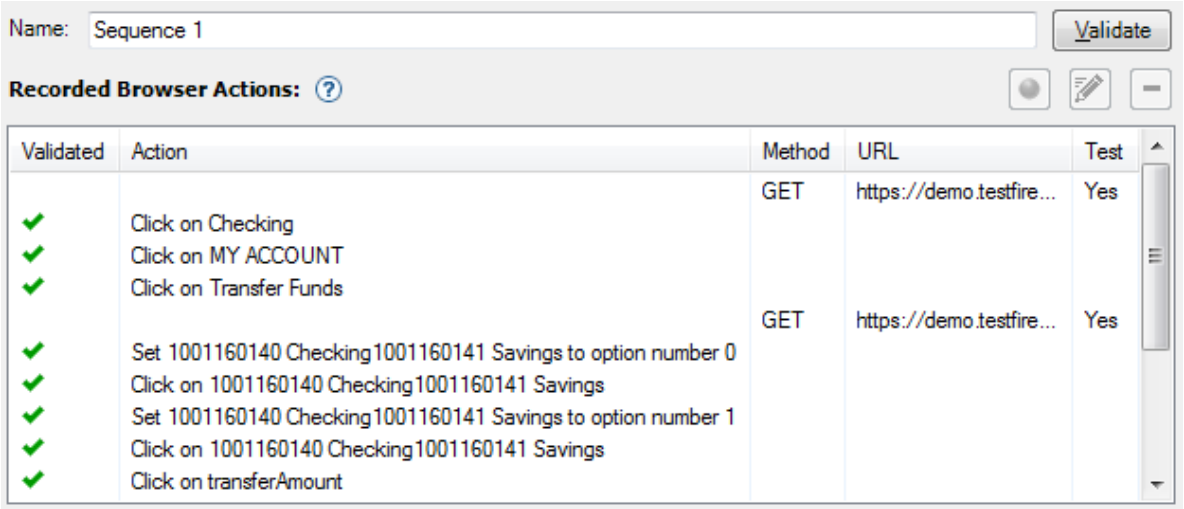
シーケンスが、「シーケンス」ペイン (右上) に表示されます。シーケンスは、順に「Sequence 1」、「Sequence 2」などと自動的に名付けられますが、「名前」フィールドに入力して名前を変更することができます。

オプションで、再生方法を変更することができます (ダイアログ・ボックスの左下)。

- 要求ベースの再生 (デフォルト) は、生の HTTP 要求を記録から送信します。一般的に早いのはこちらの方法です。



- アクション・ベースの再生は、ユーザーのクリックおよびキー・ストロークを再生します。この方法を選択するのは、サイトに大量の JavaScript が含まれている場合や、要求ベースの再生に含まれている要求を検証した際に、その一部に赤色の X でマークが付けられた場合などです。この方法は、スキャン時間が長くなる可能性があります。



注: 組み込みのブラウザー以外のブラウザーを使用するようにスキャンが構成されている (「ツール」>「オプション」>「外部ブラウザーの使用」) 場合は、常に要求ベースの再生が使用されます。

注: ユーザーのログインを必要とするサイトで、要求ベースのログインを選択した場合、要求ベースのマルチステップ操作も選択する必要があります。選択しないと、マルチステップ操作は送信されません。

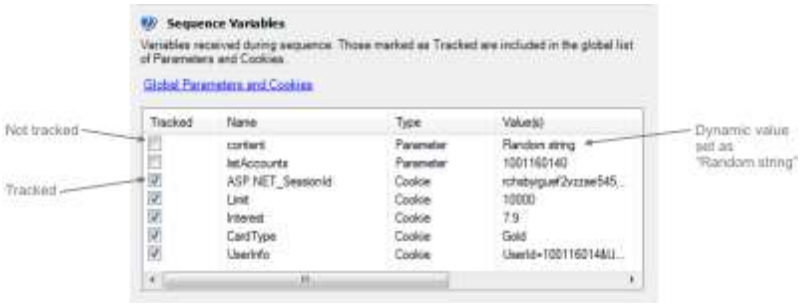
4. 「検証」をクリックします。

AppScan がシーケンスを再生し、正常に再生された各要求またはアクションの横には緑色のチェック・マークが表示されます。要求またはアクションが正常に完了しない場合、その横に赤色の X が表示されます。オプション:

- 選択して  をクリックすると、URL が表示されます。
- 不要なステップがある場合は、そのステップを選択して  をクリックすることで削除します。その後、「検証」ボタンをクリックして、シーケンスが引き続きセッション内の状態を維持しているかをチェックします。
- シーケンスの 1 つのステップを右クリックし、「テストしません」に設定します。 シーケンスの再生時、その URL は引き続き組み込まれますが、個別にテストされません。
- この URL がテストされるごとに、シーケンス内の以前のステップを再生する必要がない場合、「個別にテストする」に設定されているステップを右クリックし、「テスト要求の前にシーケンスを再生する」>「いいえ」を選択します。

シーケンス変数

「シーケンス変数」ペインには、記録されたシーケンス中に受信されたすべての変数がリストされます。AppScan がセッション ID として認識するこの変数は、スキャン中に追跡されるパラメーターおよび Cookie のグローバル・リストに自動的に追加されます (78 ページの『「パラメーターおよび Cookie」ビュー』 を参照してください)。また、これらの変数は「追跡済み」列のチェック・マークによってマークされ、追跡中であることが示されます。



変数の追跡

変数の状況を変更するには、変数を選択し、「追跡済み」チェック・ボックスを選択または選択解除します。変数が「追跡済み」である場合、AppScan は、常に最後に受信したバージョンを送信し、「セッション内」状態を保持します。

変数を「追跡対象ではない」と指定すると、パラメーターおよび Cookie のグローバル・リストから除去されることに注意してください (78 ページの『「パラメーターおよび Cookie」ビュー』 を参照)。

変数の形式の定義

パラメーターの形式を定義することで、AppScan が (テスト・ステージ中に) 有効な代替バージョンのパラメーター (場合によって異なる) を送信できるようにすることができます。パラメーターを右クリックし、以下の「ダイナミック値」オプションのいずれかを選択します。

- ランダム整数 (1 から 1000)
- 減分整数 (999999 から開始、1 ずつ減算)
- 増分整数 (1 から開始、1 ずつ追加)

- 先行ゼロの増分整数 (000001 から開始、1 ずつ追加)
- ランダム文字列 (5 個のランダム文字)
- ランダム英字文字列 (6 個のランダム英字)
- 日時 (MMddyyHHmmss)
- 日付、時間、およびミリ秒 (MMddyyHHmmssSSS)
- ランダム E メール・アドレス

例えば、シーケンスで新規ユーザーを登録し、新規 E メール・アドレスを毎回入力することがプロセスで必要となる場合 (そのため、サイトは「既存のユーザー」ページではなく登録プロセスを開始することになります)、「ランダム E メール・アドレス」として変数を定義します。 その結果、変数が含まれるテスト要求が送信されるたびに、異なる E メール・アドレスが使用され、AppScan はさまざまな登録ページをテストすることができます。

「コンテンツ・ベースの結果」ビュー

「構成」ダイアログ・ボックスのコンテンツ・ベースのビューです。AppScan が URL 構造に基づいてアプリケーション・ツリーの論理構造を定義することができない場合、このビューを使用して定義することができます。

- ご使用サイトのコンテンツが、URL がフォルダー状の階層を反映する方式の構造となっている場合、スキャン結果は自動的にこの構造を反映するため、移動が容易になります。
- ご使用のサイトで「ブレッドクラム」や他の「コンテンツ・ベース」ナビゲーション・メソッドを使用して、URL がユーザーのサイト内の「位置」を示さないようにしている場合は、サイトがどのように「ロジカル」に構成されているかを AppScan に対して「教示する」ことをお勧めします。これにより、スキャンの結果を 1 つまたは 2 つの URL に長大なリストとして置くのではなく、理解しやすいフォーマットで表すことができるようになります。この実行は必須ではありませんが、 結果に移動することが容易になるでしょう。

例えば、以下のコード・スニペットでは **Home** | **Buy** | **Books** という論理構造となっているため、"Books" が "Buy" の下に、"Buy" が "Home" の下に表示されるようにスキャン結果を 構造化すると効率的です。

```
<td class="navigation">
    <a href="http://www.onlineshop.com/">Home</a> &gt;
    <a href="http://hub.onlineshop.com/buy?ssPageName=h:h:cat:US">Buy</a> &gt;
    <b>Books<b>
</td>
```

これを実行するには、AppScan で関連コンテンツ (この例では "Home"、"Buy"、"Books") の識別と抽出を行い、コンテンツ・ベース・ツリーを構成できるようにする規則を定義します。

規則を定義すると、アプリケーション・ツリーでコンテンツ・ベース・オプションを選択してこの情報を使用した結果を表示することができるようになります。(219 ページの『セキュリティー問題: アプリケーション・ツリー』 を参照してください。)

注**:** セキュリティー問題の総数 (24 ページの『結果リスト』の先頭に表示) は、 サイト内の脆弱なロケーションを示す指標で、サイトがどのような構造になっているかによりある程度異なります。コンテンツ・ベースの構造を定義した場合、アプリケーション・ツリー内の問題の総数は、(同じ結果に対する) URL ベースのアプリケーション・ツリーでの総数と同じにならないことがあります。サイトの構造がコンテンツ・ベースで (URL ベースではなく)、コンテンツ・ベースのビューが正しく構成されている場合、コンテンツ・ベースのビュー内の問題の件数は、サイト内に存在する「脆弱性のある場所」の数をより正確に表します。

バリアント の総数 (結果リストの先頭の括弧内) は、サイトの構造とは無関係で、コンテンツ・ベースのビューと URL ベースのビューの間で変化しません。

新規コンテンツ・ベースの表示ルールの追加

サイトの論理構造を定義するルールの追加についての手順および例を示します。

始める前に

「スキャン構成」ダイアログ・ボックスの「コンテンツ・ベース」ビュー (「探査」>「コンテンツ・ベース」) で、以下の 2 つのタイプの定義を使用して、コンテンツ・ベースの構造を定義することができます。

- 論理コンテンツ・パス (ブレッドクラムなど)
- カスタム (固有のカスタム・ノードを定義するための正規表現の使用)

これにより、AppScan で 1 つのノード配下のサイトの大部分をリストする代わりに、論理的なアプリケーション・ツリーを表示できるようになります。複数の規則が定義されている場合、AppScan は各 URL を、リストされている順に規則とマッチングします。一致が見つかるとすぐに、その規則に従ってコンテンツ・ベース・ツリーにその URL が組み込まれ、次の URL に進みます。

手順

1.  をクリックして新規定義を追加します (あるいは、既存の定義を選択して  ボタン をクリックし、その定義を編集します)。フィールドの説明については、以下の表を参照してください。

設定	説明
名前	このルールの名前。
説明	(オプション) このルールの説明。
ルールのタイプ	「論理コンテンツ・パス」または「カスタム」を選択します。残りのフィールドは、選択に応じて変わります。
論理コンテンツ・パス	
コンテンツ・パス	HTML のコンテンツ・パスに一致する正規表現。
分離文字	HTML のコンテンツ・パスの階層分離文字に一致する正規表現。
ノード表示名	ノード名に一致する正規表現 (アプリケーション・ユーザーに対して表示され、アプリケーション・ツリーで使用される)。
条件	(オプション) このノード・ロケーションに組み込まれる応答を定義する正規表現。
カスタム	
ノード・ロケーション	標準 URL 形式を使用して、このルールの条件を満たすノードをアプリケーション・ツリー内で配置する場所を記述します (例えば、/Home/Buy/Books)。パスが存在しない場合は、作成されます。
条件	このノード・ロケーションに組み込まれる応答を定義する正規表現。ページ・コンテンツがこの条件に一致する場合、コンテンツ・ベース・ツリーに組み込まれます。

注: 正規表現を使用する必要がある、または正規表現を使用できるフィールドには、「正規表現」ボタン  があります。このボタンをクリックして Expression Test PowerTool を開き、正規表現の構文を検証することができます。

支援がさらに必要な場合は、次のリンクが役立ちます。 http://www.regular-expressions.info/quickstart.html

2. 上矢印/下矢印を使用して、適用される順序で定義を配列します。
3. 適用される各ルールの横のチェック・ボックスが選択されていることを確認します。
4. 「**OK**」をクリックして、変更を保存します。

例

次の表は、2 つの規則タイプのコンテンツのサンプルを示しています。

表 *6.* 「コンテンツ・ベースのビュー」規則

設定	サンプル	意味
コンテンツ・パス	**<title>(.*?)</title>**	タイトル・タグの間のすべてのテキストは、ノード名の基本として使用されます。
分離文字	**[:\->|]**	これらの 5 つの文字は、分離文字として処理されます。したがって、次のようになります。 **<title>Home:Accounts</title>** から **<title>Home:Plans</title>** 2 つの子ノード **Accounts** および **Plans** を持つ親ノード **Home** としてアプリケーション・ツリーに表示されます。
ノード表示名	**^\s*(.*?)\s*$**	テキストの前後のスペースは、ノードの命名時に削除されます。
条件	**Log out**	単語「ログアウト」を含むページのみが、この規則に従うアプリケーション・ツリーに組み込まれます。

表 *7.* カスタム規則

設定	サンプル	意味
ノード・ロケーション	**/root/child/grandchild**	条件を満たすすべてのページがアプリケーション・ツリーの **/root/child/grandchild** の下に追加されます。 **注:** 指定されたブランチ内に親ノードが存在しない場合は、作成されます。
条件		このフィールドが空の場合、規則が適用されるすべてのコンテンツがこのノード・ロケーションで追加されます。したがって、この規則が上記の規則より後に出現した場合、単語「ログアウト」を含まないすべてのページがノード **/root/child/grandchild** の下に追加されます。

「Glass Box」ビュー

「構成」ダイアログ・ボックスの「Glass Box」ビューです。

Glass Box スキャンでは、アプリケーション・サーバーにインストールされたエージェントを使用します。このエージェントは、スキャン中にサーバー・サイド・アクティビティーをモニターして、ソース・コード情報およびその他のデータを収集します。その結果、より高速で正確なスキャンを実行できます。構成された開始 URL に関連する Glass Box エージェントがデフォルトで選択され、両方の Glass Box スキャン機能が有効になります。

Glass Box スキャンにより、探査ステージで非表示の URL を検出し、テスト・ステージで追加の問題と情報を検出することができます。

設定	詳細
この glass Box エージェントを使用	Glass Box エージェントがアプリケーション・サーバー上にインストールされ、AppScan 内で定義されている場合は、このエージェントを選択してスキャンで使用できます。開始 URL を入力した場合、AppScan は、適切なエージェントの自動的な選択を試行します。 エージェントが選択されると、AppScan は、エージェントへの接続を試行し、その試行が成功したかどうかを示します。 **注:** エージェントを選択したときに「資格情報が必要です」というメッセージが表示された場合、「ツール」 > 「Glass Box 管理」に指定されている資格情報が正しいことを確認してください。 必要なサーバーがドロップダウン・リストに表示されない場合は、「**Glass Box** エージェント管理」リンクをクリックして定義できます。 **制約事項:** 1 つのスキャンで使用する Glass Box エージェントは 1 つのみ選択できます。スキャンされているアプリケーションに複数のサーバーがある場合は、各サーバー・エージェントを別個に使用してスキャンする必要があります。

Glass Box を探査ステージで使用	(デフォルトで選択されています。)
	
	この機能を使用して、サーバーの動作に影響するが応答内には表示されないパラメーターがサーバー・サイドのソース・コードに存在するかどうかを検査することにより、サイトのカバー範囲を拡大することができます。
	
	サーバー・サイド・コードの例:
	`String debugOn = request.getParameter("debug");`
	`if (debugOn == "true"){`
	`response.getWriter().println(SECRET_SERVER_DATA);`
	`}`
	
	この例では、開発者はパラメーター `"debug"` をコード内に残しています。これはサイト上のリンクには表示されませんが、攻撃者がこれを含む要求を送信した場合には、`SECRET_SERVER_DATA` が取得される可能性があります。

Glass Box をテスト・ステージで使用	(デフォルトで選択されています。) スキャンのテスト・ステージで Glass Box テストを送信するには、このチェック・ボックスを選択します。この機能は、ブラインド SQL インジェクションなどの特定のテストの成功または失敗を、より高い精度で検証できます。また、ブラック・ボックス手法によって検出できない特定のセキュリティー問題の存在を発見できます。
相当するブラック・ボックス・テストをスキップ	(デフォルトでは選択解除されています。) これは、同じぜい弱性 (WASC 脅威の分類) に対して Glass box テストとブラック・ボックス・テストの両方が送信されることを意味します。この理由は、一般的に、Glass box テストのほうが正確度が高いだけではなく、より詳細な結果を提供しますが、同等のブラック・ボックス・テストが成功する一方で Glass box テストが失敗する場合があるためです。ブラック・ボックス・テストをスキップしてもご使用のアプリケーションでの結果が変わらない場合は、このチェック・ボックスを選択することでスキャン時間を削減することができます。

注: デフォルトでは、2 つのメイン・チェック・ボックスが選択されています。これらを 2 つとも選択解除 すると、Glass Box スキャンが無効になります。

以下も参照してください。

174 ページの『Glass Box スキャン』

175 ページの『Glass Box エージェントのインストール』

189 ページの『AppScan での Glass box エージェントの定義』

192 ページの『Glass Box によるスキャン』

「通信およびプロキシー」ビュー

「構成」ダイアログ・ボックスの「通信およびプロキシー」ビュー (AppScan がテスト済みアプリケーションにアクセスするのにプロキシーが必要な場合)。

設定	詳細
通信	
スレッドの数	同時に送信される要求の最大数を設定します。 デフォルトでは、設定可能な最大値である 10 に設定されます。ご使用のサイトで同時スレッドが許可されていない場合は、この数を 1 に減らします。
タイムアウトを自動的に調整する	「スキャン中にタイムアウトを自動的に調整する」を選択して、スキャンの所要時間を短縮できる場合があります。 AppScan の選択時に、スキャン中のタイムアウトを自動的にレビューおよび調整するため、スキャン時間を大幅に短縮できる可能性があります。
タイムアウト	上記のチェック・ボックスを空欄にすると、Web サーバーから応答を待機する際の AppScan の時間制限を (秒単位で) 設定できます。デフォルトでは、タイムアウトは 10 秒となっています。
要求速度の制限	デフォルトでは、AppScan はその要求を可能な限り高速でサイトに送信します。 これにより、ネットワークやサーバーが過負荷になる場合、またはご使用のサイトが最大要求速度に関する制限をユーザーに課している場合には、このチェック・ボックスを選択して制限を低くしてください。 • 「アクション・ベースの探索」が使用されている場合 (「構成」 > 「探索オプション」 > 「探索方法」)、この設定はスキャンのテスト・ステージのみに影響を及ぼします。 • 「要求ベースの探索」が使用されている場合、この設定はスキャンの探索とテスト・ステージの両方に影響を及ぼします。
プロキシー	
プロキシー設定	AppScan がアプリケーションにアクセスするためにプロキシーが必要な場合、ここで構成します。デフォルトでは、AppScan は Internet Explorer のプロキシー設定を使用するように構成されています。 **Internet Explorer** のプロキシー設定を使用する (デフォルト) これを選択すると、Internet Explorer 接続のアドレスおよびポートを使用します。認証が必要な場合、ユーザー名、パスワード、ドメインを下に追加してください。 プロキシーを使用しない AppScan に対してプロキシーの使用を許可しない場合に選択します。 カスタムのプロキシー設定を使用 独自のプロキシー設定を定義する場合に選択します。プロキシーのアドレスおよびポートを入力します。プロキシーでの認証が必要な場合、ユーザー名、パスワード、ドメインを下に追加してください。

「HTTP 認証」ビュー

「構成」ダイアログ・ボックスの「HTTP 認証」ビューです。

このビューを使用して、必要に応じてプラットフォーム認証情報とクライアント側の証明書を構成します。AppScan は、ユーザーの個人用ストアからの複数の証明書、または PKCS#12 (PFX) 形式の単一の証明書 (スキャンごと) をサポートしています。

ヒント: PEM 証明書はサポートされていませんが、それらを PFX に変換できます (112 ページの『PEM 証明書を PFX/P12 形式に変換』 を参照)。

設定	詳細
HTTP 認証	サイトで、基本、ダイジェスト、NTLM、ネゴシエーション、または Kerberos HTTP の認証が必要な場合、スキャン中に使用する AppScan のユーザー名、パスワード、およびドメインをここに入力します。
クライアント側の証明書	サイト・サーバーがクライアント側の証明書を使用してユーザー ID を確認する場合、AppScan はスキャンの実行にこの証明書が必要です。 証明書を使用しない (デフォルト) **PFX/P12** 単一の PFX 証明書または P12 証明書を使用します。 をクリックして「証明書ファイル」を選択し、「パスワード」に入力します。 インストール済みの証明書 **(**スマート・カードを含む**)** このマシンにインストールされた証明書を使用します。 • 必要な証明書が既知の場合、またはスマート・カードを使用している場合は、次のようにその証明書を手動で追加することをお勧めします。 1. 「必要な証明書を自動的に識別」チェック・ボックスを選択解除したままにします。 2. 「追加」をクリックします。 3. 現行ユーザーの Windows 個人証明書ストアから証明書 (複数の場合あり) を選択します。 4. 「追加」をクリックします。 証明書が表に追加されます。 5. 証明書に PIN が必要な場合は、列をダブルクリックし、その列に入力します。 • 必要な証明書がどれか分からない場合: 1. 「必要な証明書を自動的に識別」チェック・ボックスを選択します。 2. PIN が必要で分かっている場合は、それを「PIN」フィールドに入力します。入力しないと、スキャンの開始時にそれを入力するようプロンプトが出されます。 **ヒント:** PIN が必要なスマート・カードは、ロックアウトされる可能性があります。可能であれば、証明書を手動で追加してください。 **注:** ほとんどのスマート・カード証明書では、スキャン時に読取装置内でカードが使用可能でなければなりません。
接続状況	48 ページの『「URL およびサーバー」ビュー』 で構成されている開始 URL を使用した接続の状況を示します。

PEM 証明書を PFX/P12 形式に変換

PEM 証明書はサポートされていないため、 PKCS#12 (PFX/P12) 形式に変換する必要があります。

このタスクについて

この変換は、以下に示す OpenSSL などの外部ツールを使用すると実行できます。

手順

1. に移動してください。 https://www.openssl.org/community/binaries.html
2. バージョン 1.0.1p をダウンロードしてインストールします。
3. 以下のコマンド形式を OpenSSL インストール bin フォルダーから実行します。

```
openssl pkcs12 -export -out Cert.p12 -in cert.pem -inkey key.pem -passin pass:root -passout pass:root
```

「テスト・ポリシー」ビュー

「構成」ダイアログ・ボックスの「テスト・ポリシー」ビューには、現在のテスト・ポリシーの詳細が表示されます。

サイトの AppScan テストの数は、何千にも達する可能性があります。大量のテストおよびテスト・バリアントを手動でフィルタリングするのではなく、アプリケーション上で実行するテストと実行しないテストのタイプの一般ポリシーを設定できます。

「テスト・ポリシー」ビューを使用して、スキャンに含めるテストを定義するテスト・ポリシーの表示、編集、および管理と、現在のスキャンのポリシーの定義を行います。

テストはグループ化されて、2 つのペインのうち上段のペインにリストされます。選択したテストのアドバイザリーと推奨される修正は、下段のペインに表示されます。

「テスト・ポリシー」ビューでは、以下のことができます。

- 現在のポリシーの詳細を表示する
- 現在のポリシーを編集して独自のユーザー定義テスト・ポリシーを作成する
- 定義済みポリシーまたは以前に保存されたユーザー定義ポリシーをインポートする

フィールド/ペイン/オプション	詳細
テスト・ポリシー	現在のテスト・ポリシーの名前を表示します。テストはグループ化されて、2 つのペインのうち上段のペインにリストされます。選択したテストのアドバイザリーと推奨される修正は、下段のペインに表示されます。
グループ化メソッド	ドロップダウン・リストを使用して、上段のペインでテストに使用するグループ化メソッドを選択します。
フィルター	ドロップダウン・リストを使用して、上段のペインでテストをフィルタリングします。以下のいずれかを選択できます。「すべて」、「DAST のみ (動的分析)」、「IAST のみ (Glass box 実行時分析)」、または「SAST のみ (静的分析)」。
検索	「検索」フィールドにテキストを入力すると、その検索ストリングを含むテストのみが表示されます。「虫眼鏡」ドロップダウン・リストを使用して、すべてのテスト・フィールドで文字列を検索するか、特定のテスト・フィールド (「テスト名」や「CVE ID」など) のみで文字列を検索するかを定義することができます。
エクスポート	現在のテスト・ポリシーを別の機会にロードできるように保存しておくには、これをクリックします。

フィールド/ペイン/オプション	詳細
インポート	定義済みテスト・ポリシーまたはユーザー定義テスト・ポリシーをロードするには、これをクリックします (115 ページの『テスト・ポリシーのインポート』 を参照)。
ポリシーの説明	右上のペインには、現在のポリシーの説明が表示されます。ユーザー定義ポリシーの場合、このフィールドを編集することができます。
テスト・ペイン	上段のメイン・ペインには、フィルター/検索基準を満たすすべての AppScan テストがリストされます。テストごとに、名前、バリアント ID、 CVE ID、 CWE ID、問題に割り当てられた重大度 (およびその重大度が CVSS かユーザー割り当てによるものか)、タイプ、安全性、WASC 脅威の分類、および XFID (X-Force ID) の各情報がリストされます。列ヘッダーをクリックすることで、これらのフィールドの一部を基準にしてテストをソートできます。 チェック・ボックスが選択されているテストが現在のポリシーに組み込まれます。テストを選択/選択解除して、ポリシーを編集できます (『テスト・ポリシーの編集』を参照)。
更新設定リンク	このリンクは、新規テストがデータベースに追加されるときにこのポリシーに追加できるテストのタイプを定義するダイアログ・ボックスを開きます。 詳しくは、 116 ページの『テスト・ポリシー更新設定』 を参照してください。
「アドバイザリーと推奨される修正」タブ	下段のメイン・ペインには、選択したテストの「アドバイザリーと推奨される修正」が表示されます。 独自の仕様に対するアドバイザリーを「編集」したり、編集されたアドバイザリーを「デフォルトにリセット」することもできます (116 ページの『アドバイザリーと推奨される修正の編集』 を参照)。
ポリシー・ファイル	「最近使用したポリシー」または「定義済みのポリシー」のいずれかをクリックするか、「参照...」をクリックして必要なポリシーを参照することにより、既存のテスト・ポリシーをロードします。

テスト・ポリシーの編集

「テスト・ポリシー」ビューを使用すると、選択されたテスト・ポリシーを微調整できます。

このタスクについて

テストの追加または削除によって現在のテスト・ポリシーを微調整できます。また、変更された構成をユーザー定義のテスト・ポリシーとして将来に使用できるようにエクスポートすることも可能です。

手順

1. 「スキャン構成」ダイアログ・ボックスで、「テスト・ポリシー」(または「スキャン構成ウィザード」>「テスト・ポリシー」) をクリックします。

   上部の領域ではすべての AppScan テストがリストされており、どれが現在のスキャンに含まれているかが示されます (チェック・ボックスが選択されている)。

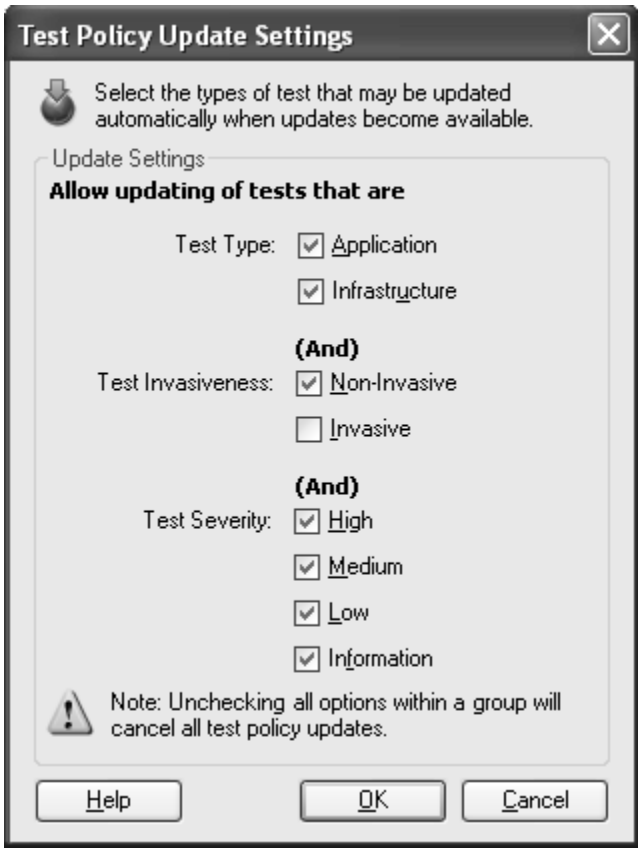
2. チェック・ボックスを選択/選択解除することで、テストまたはバリアントの組み込み/除外を行います。 (個々のバリアントを表示するには、「テスト名」の横の + アイコンをクリックします。)

   注: テストごとに、名前、バリアント ID、 CVE ID、 CWE ID、問題に割り当てられた重大度 (およびその重大度が CVSS かユーザー割り当てによるものか)、タイプ、安全性、WASC 脅威の分類、お

よび XFID (X-Force ID) の各情報がリストされます。列ヘッダーをクリックすることで、これらのフィールドのいずれかによりテストをソートできます。

注: 検索機能により、フリー・テキスト検索を使用してテストを検索できます。

3. ダイアログの右上の情報フィールドで、説明を編集することができます。
4. AppScan のテスト・データベースには、新規テストが継続的に追加されています。デフォルトでは、安全性のテストを除くすべての新規テストが、すべてのユーザー定義テスト・ポリシーに追加されます。ただし、ポリシー内のどのグループを更新するかを定義することができます。「更新設定」をクリックし、必要に応じて「テスト・ポリシー更新設定」ダイアログ・ボックスのチェック・ボックスを選択/選択解除してから、「**OK**」をクリックします。



ダイアログ・ボックスには「テスト・タイプ」、「テストの安全性」、および「テストの重大度」の 3 つのグループが存在します。 *3* つのグループすべての中の 選択したカテゴリーに属するテストだけが、新規テストが AppScan のテスト・データベースに追加されるときに、現在のポリシーに追加されます。例:例えば、重大度には「高」を選択したが、「安全でないテスト」は選択解除した場合、更新が入手可能になったときに、重大度が高くて安全でないテストはこのポリシーに追加されません。

5. オプションで、スキャンに名前を付け、将来の使用のために保存することができます (「エクスポート」をクリックし、**.policy** フォーマットで保存します)。
6. 「**OK**」をクリックして、変更を現在のテスト・ポリシーに保存します。

テスト・ポリシーのインポート

このタスクについて

最近使用したテスト・ポリシー、定義済みテスト・ポリシー、およびユーザー定義テスト・ポリシーをロードすることができます。

手順

以下のいずれかを実行します。

- 「ポリシー・ファイル」領域で、リストされた「最近使用したポリシー」または「定義済みテスト・ポリシー」のいずれかを選択します (『事前定義テスト・ポリシー』を参照)。
- 「ポリシー・ファイル」領域にリストされていないユーザー定義ポリシーを開くには、画面の上部で「インポート」ボタンをクリックします (または「ポリシー・ファイル」領域で「参照」をクリックします)。

タスクの結果

選択したポリシーがロードされ、その名前および記述がダイアログ・ボックスの上部に表示されます。

事前定義テスト・ポリシー

「テスト・ポリシー」ビューの左下にある「ポリシー・ファイル」ペインでは、最近使用されたポリシーの 1 つまたは定義済みのポリシーの 1 つを選択できます。定義済みのポリシーは、一般的な要件に合った一連の役に立つポリシーを提供します。

ポリシー名	説明
デフォルト	安全でないテストとポート・リスナー・テストを除くすべてのテストを含みます。
アプリケーションのみ (Application-Only)	安全でないテストとポート・リスナー・テストを除くすべてのアプリケーション・レベルのテストを含みます。
インフラストラクチャーのみ (Infrastructure-Only)	安全でないテストとポート・リスナー・テストを除くすべてのインフラストラクチャー・レベルのテストを含みます。
サード・パーティーのみ	安全でないテストとポート・リスナー・テストを除くすべてのサード・パーティー・レベルのテストを含みます。
安全でないテスト	すべての安全でないテスト (サーバーの安定度に影響を与える可能性があるテスト) を含みます。
完了	すべての AppScan テストを含みます。
Web サービス	安全でないテストとポート・リスナー・テストを除くすべての SOAP 関連のテストを含みます。
厳選テスト	検出の確率が高いテストとして選択されたものを含みます。これは、時間が限られているときに、サイトを評価するのに便利です。
開発者必需テスト	検出の確率が高いアプリケーション ・テストとして選択されたものを含みます。これは、時間が限られているときに、サイトを評価するのに便利です。
実動サイト	サイトに損害を与える可能性がある安全でないテストや、他のユーザーに対するサービス妨害の原因となる可能性があるテストを除外します。 **注:** 稼働中のサイトのスキャンについて詳しくは、 342 ページの『ライブ実稼働環境のスキャン』を参照してください。

テスト・ポリシー更新設定

このダイアログ・ボックスは、「スキャン構成」 > 「テスト・ポリシー」ビューから開きます。

新規テストがテストの AppScan データベースに追加されるときに、どのタイプのテスト (存在する場合) が「現在のテスト・ポリシー」に追加されるかを選択します。スキャンまたはテンプレートのロード時、またはテスト・ポリシー・ファイルのインポート時にテストは更新されます。

以下の 3 つのグループがあります。「テスト・タイプ」、「テストの安全性」、および「テストの重大度」。新規テストが使用可能になるときに、3 つのグループすべての中の 選択されたカテゴリーに属するテストだけが現在のポリシーに追加されることに注意してください。例:例えば、重大度には「高」を選択したが、「安全でないテスト」は選択解除した場合、更新が入手可能になったときに、重大度が高くて安全でないテストはこのポリシーに追加されません。

アドバイザリーと推奨される修正の編集

このタスクについて

テストのスキャン結果の「アドバイザリーと推奨される修正」タブに表示されるテキストは変更できます (229 ページの『「アドバイザリー」タブ』を参照)。(これを実行すると、編集済みファイルはコンピューター上に .xml 形式で保存されます。厳密な場所は、「ツール」>「オプション」>「設定」タブで構成します。 277 ページの『「設定」タブ』を参照してください。) 「アドバイザリーと推奨される修正」のテキストは、同じファイル内に保管されます。 (元のテキストは、「デフォルトにリセット」ボタンを使用していつでも復元できます。)

注: スキャンを別のコンピューターに送信した場合、問題に対する元のデフォルトの アドバイザリー (編集したアドバイザリーではない) が表示されます (ただし .xml ファイルをその別のコンピューターに送信し、ユーザーにそれをそのコンピューターの Custom Advisories フォルダーに保存させていない場合に限ります。 277 ページの『「設定」タブ』を参照してください)。

注: IBM が、編集済みのアドバイザリー/推奨される修正の更新バージョンをリリースした場合、(「デフォルトにリセット」ボタンをクリックして、加えた変更を廃棄しない限り) 更新されたバージョンは AppScan インターフェースには表示されません。

手順

1. 必要なテストを選択します。

   選択したテストのアドバイザリーと推奨される修正は、下段のペインに表示されます。

2. 「アドバイザリー」タブの上の「編集」アイコンをクリックします。(特定のテストのアドバイザリーと推奨される修正は、同じファイル内に保管されています。したがって、「編集」をクリックするときに 2 つのタブのどちらが上にあっても構いません。)

   アドバイザリー・ファイルが、組み込み XML エディターで開きます。
3. 必要に応じてテキストを編集し、「**OK**」をクリックします。

   注**:** 無効な XML 構文、またはアドバイザリー・ファイル・スキーマの一部ではないタグを使用している場合、警告が表示され、変更は保存されません。

   XML エディターが閉じ、変更は現在のアドバイザリーに表示されます。

デフォルトのアドバイザリーの復元**:**
このタスクについて

特定のテストのアドバイザリーがユーザーにより変更されている場合は、そのテストの選択時に「デフォルトに復元 (Restore to Default)」ボタンがアクティブになります。

手順

「テスト・ポリシー・マネージャー」で該当するテストを選択し、「デフォルトに復元 **(Restore to Default)**」をクリックします。

「テストの最適化」ビュー

テストの最適化は、AppScan のインテリジェントなテストのフィルタリングを使用してより高速なスキャンを実行します。

通常の AppScan Standard の全体スキャンでは、一般的に数千ものテストを送信し、完了までに数時間、場合によっては数日かかることがあります。開発の初期段階で、または製品の現在のセキュリティ体制の全体をすばやく評価するために、テストの最適化を使用して、より短い時間フレームで必要な結果を入手できます。

当社のインテリジェントなテスト・フィルターは、統計分析に基づき、特定のテストや、特定のテストのバリアントもフィルタリングによって除外し、より一般的な脆弱性、より重大な脆弱性、またはより重要な脆弱性のみを識別する短いスキャンを生成します。AppScan のフィックスパックと iFix により、最適化フィルターが最新の状態に保たれます。テストの最適化を使用することで、徹底的で詳細なスキャンよりも迅速な結果を優先する場合に、全体のスキャン時間を大幅に短縮することができます。

オプション	説明
通常 (デフォルト)	詳細なテストを実行し、構成されたとおりに、適切なすべてのテストを送信します。この設定は、長いスキャンが開発ワークフローを中断させることのない場合に推奨されます。
最適化	より一般的で重大な、およびそれ以外の重要な脆弱性に対してのみテストを送信することで、スキャンを高速化します。

344 ページの『テストの最適化の理解』 も参照してください。

「テスト・オプション」ビュー

「構成」ダイアログ・ボックスの「テスト・オプション」ビューです。

このビューでは、スキャンの長さおよび完成度に影響を与えるさまざまな設定を構成できます。ただし、大抵の場合、デフォルトの設定で十分です。

設定	詳細
テスト・オプション:	
最適化されたテストを行います (Use Adaptive Testing)	AppScan は何千ものテストをサイトに送信できます。ただし、スキャン時間を削減するために、送信すべきテストと省くことができるテストを賢明に判断する事前テストを送信できます。これが「適合テスト」で、効率を犠牲にせずに、スキャン時間を大幅に削減することができます。 AppScan にすべての テストをサイトに送信させる場合は、このチェック・ボックスのチェックを外します。
マルチフェーズ・スキャンを許可する	AppScan は、ご使用のアプリケーションに送信するテストに対する応答を分析します。この分析により、AppScan はしばしば、スキャンの最初の「フェーズ」では見えなかったリンクなどの、追加内容を発見します。マルチフェーズ・スキャンによって、AppScan はこの新規に検出された内容に対して探査およびテスト・ステージを繰り返すことができます。 (追加フェーズには新規リンクのみ含まれるため、通常は短くなります。) デフォルトで、マルチフェーズ・スキャンは最大 4 つのスキャン・フェーズを許可するように構成されます。 マルチフェーズ・スキャンは、フル・スキャンを実行する場合のみ適用されることに注意してください。「探査のみ」または「テストのみ」機能を使用する場合、結果は単一フェーズ・スキャンになります。
ログインおよびログアウト・ページに関するテストを送信する	ご使用のアプリケーションが不正な入力を行うユーザーをロックアウトしない限り、またはアプリケーション・フローがこれらのページをテストする AppScan によって変更されない限り、AppScan がログイン・ページとログアウト・ページのテストを行えるようにすることをお勧めします。

設定	詳細
ログイン・ページのテスト中は、セッション ID を送信しないでください。	(前のチェック・ボックスが選択されている場合のみ有効です。) ログイン・ページをテストする場合、セッション ID によってテストの成功が制限される可能性があるため、このチェック・ボックスは選択したままにしておくことをお勧めします。ログイン・ページをテストするのに有効なセッション・トークンが必要であることが確実な場合にのみ、このチェック・ボックスを選択解除します。 このチェック・ボックスがクリアされている場合でも、誤検出結果を防ぐために一部のテストは引き続きセッション ID 付きで送信されるので注意してください。
意図せずにトリガーされたセキュリティーの問題を分析	選択した場合、AppScan は、テスト対象として指定された問題に加えて、追加のセキュリティー問題に対するそれぞれのテスト応答の分析を行います。アプリケーションが非常に大きいか、またはスキャンにより大量の誤検出の結果が生成される場合には、このオプションを選択解除します。
各問題のすべてのバリアントを含める	(前のチェック・ボックスが選択されている場合のみ有効です。) 選択すると、AppScan は、意図せずにトリガーされたそれぞれの問題のすべてのバリアントを分析します。選択解除すると、問題ごとに 1 つのバリアントのみ分析されます。このチェック・ボックスを選択することは通常は不要であり、選択するとスキャン時間が大幅に増える可能性があります。
フォームの処理要求でのみ Cookie のセキュリティーに関する問題をテストする	このオプションを選択すると (デフォルト)、フォームの処理要求で使用される Cookie についてのみ、Cookie に関連するテストの実行依頼が AppScan によって送信されます。 精度を上げるには (ただし、スキャン時間は長くなります)、このチェック・ボックスを選択解除します。AppScan はすべての関連する HTTP 要求に対して Cookie テストを実行依頼します。
脆弱でなかったテスト・バリアント情報を保存	スキャン中に、AppScan は何千ものテスト・バリアントを、テスト中のサイトに送信します。これらの多くに対する応答は、どのような種類のセキュリティー上の脅威ももたらされないことを示し、デフォルトで AppScan は「脆弱でなかった」すべての結果を廃棄するので、結果データのボリュームが大幅に削減されます。 このチェック・ボックスを選択すると、AppScan は脆弱でないバリアントをすべて保存します。このオプションを選択すると、AppScan のパフォーマンスが低下し、必要なディスク領域が大幅に増加する場合があるという警告が表示されます。 詳細については、 239 ページの『脆弱でないバリアント』 を参照してください。
JavaScript セキュリティー分析を有効にする	クライアント・サイドの JavaScript コードで、特に DOM ベースのクロスサイト・スクリプティングのクライアント・サイドでの問題の範囲を検出できる静的な JavaScript 分析を有効にします。 詳細については、 120 ページの『JavaScript 分析』 を参照してください。
問題管理:	
以前のノイズ分類をこのスキャンに適用	以前のスキャンで 1 つ以上の問題を「ノイズ」(アプリケーションに無関係) に分類した場合、このチェック・ボックスを選択解除していなければ、同じ設定が将来のスキャンに自動的に適用されます。 詳細については、 221 ページの『問題の状態:「オープン」または「ノイズ」』 を参照してください。

注: スキャンの後に テスト・オプションを変更する場合、すべての変更を既存の結果に適用できるわけではないため、再スキャンするようにプロンプトが出されることがあります。

JavaScript 分析

このセクションでは、JavaScript の静的分析機能の基本と、結果の表示方法について説明します。

JavaScript 分析の結果

AppScan は JavaScript ソース・コードの静的分析を実行するため、検出された問題には脆弱なソース・コードを示すソース・レベルのトレース情報が含まれます。このトレース情報は、「詳細ペイン」の「問題情報」タブで確認できます。

コード内で番号が付けられて強調表示されている行は、アプリケーションに入力された信頼できないデータがどのように伝搬されて非セキュアな方法で使用されるかを、ソースからシンクまで、ステップバイステップで示しています。

AppScan は、高度な文字列分析テクノロジーを使用して誤検出を除去し、問題をより正確に分類します。

文字列分析の基本

AppScan は、各ページの分析において、汚染 (あるいはデータ・フロー) 分析と文字列分析という 2 つの段階を適用します。最初の段階で AppScan は、サニタイザーを通らない、ソースからシンクまでのトレースを検索します。このトレースが見つかった場合、AppScan は、文字列分析のバリアントである文字列プレフィックス分析 (SPA) を使用して、第 2 段階でそのトレースを検証します。

ソースが URL (またはその一部) であるようなケースでは、シンクにおいて攻撃者が URL のホスト部分とパス部分を制御できる場合にのみ、トレースが悪用可能となります。 SPA はソース URL を扱う文字列操作を追跡することにより、このようなケースを検証します。SPA は、URL の照会部分およびアンカー部分が以下の場合は、URL のホストとパスがアタッカーによって制御されていないと見なします。

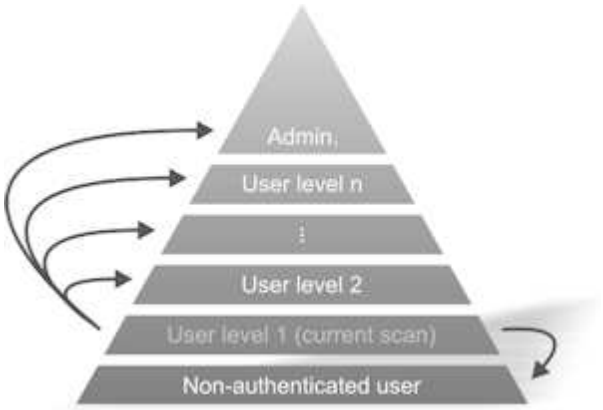
シンクにおいて、SPA はアタッカーが URL のホスト部分とパス部分を制御できるかどうかを検査します。ホスト部分とパス部分がどちらも固定されていて、アタッカーが制御していないと判断した場合は、問題が排除されます。

リダイレクトのターゲットが接頭部 `javascript:` または `mailto:` で始まる場合、問題はより正確に "「DOM ベースのクロスサイト・スクリプティング」"または"「DOM ベースの電子メール・スプーフィング」"とそれぞれ分類されます。

「権限拡張」ビュー

「構成」ダイアログ・ボックスの「権限拡張」ビューでは、異なるユーザー・レベルの結果を比較できます。

このタスクについて



AppScanは、アクセス許可が不十分なユーザーがアクセス可能な特権リソースの範囲を調査するために、異なるユーザー権限を使用して実行されたスキャンを参照できます。これは以下の 2 とおりの方法で実行できます。

- 上位権限ユーザーとの比較によって**:** AppScan が現在のスキャンよりもより高いレベルのアクセス許可を使用して生成されたスキャン結果を参照するようにします。スキャン中に、AppScan は上位レベルのユーザーがアクセス可能であった追加のリンクに、現在の (下位レベルの) アクセス許可を使用してアクセスしようとします。スキャン結果は、これらの試行が成功した箇所を示します。
- 未認証ユーザーとの比較によって**:** AppScan が、ユーザー認証なしで生成されたスキャン結果を参照するようにします。次に AppScan は、現在の認証を使用してスキャンを実行し、アクセスした新規リンクを記録します。 それからログアウトし、それらの新規リンクに認証なしで アクセスを試みます。スキャン結果は、これらの試行が成功した箇所を示します。

重要**:** 比較対象となるスキャンは、スキャン構成が同じであり、同等の探査データを持っている必要があります。例えば、スキャンの 1 つにおいてテスト前にサイトが手動で探査された場合は、そのスキャンと比較されるスキャンでテスト・ステージの前に 同じ マニュアル探査を実行する必要があります。

手順

1. **(**上位権限ユーザーと比較する場合**:)** 上部領域 (「上位権限ユーザーによるテスト」) で、  をクリックし、現在のスキャンよりも高いアクセス許可で実行されたスキャンを参照します。
2. 「開く」をクリックします。

3. スキャンで使用された認証レベルを表す名前を入力し (例えば「ゲスト」や「管理者」)、「**OK**」をクリックします。

   選択されたスキャンはリストに追加され、その役割 (管理者、オペレーター、ビジターなど) は左列に表示されます。
4. 必要に応じて、これらのステップを繰り返して、異なる認証レベルのスキャンを追加します。

   注**:** 上位権限ユーザーによるテストに対しては複数のスキャンを、各役割に対しては 1 つのスキャンを追加できます。例えば、現在のスキャンが通常ユーザーのユーザー名とパスワードを使用して構成されている場合、管理者許可で実行されたものと、スーパーバイザー許可で実行されたものという、2 つのスキャンをこのリストに追加できます。結果により、どのユーザーのリソースが通常ユーザーにアクセス可能であったかが分かります。
5. **(**未認証ユーザーと比較する場合**:)** オプションで、認証なし のスキャン実行の結果をロードすることもできます。これを実行するには、下部の領域で  をクリックし、スキャン結果を参照します。

「マルウェア」ビュー

「構成」ダイアログ・ボックスの「マルウェア」ビューを使用して、マルウェアのテストを構成します。

マルウェアのテストは、さまざまな構成オプションを持つ 2 つのモジュールで構成されています。これらのオプションは、このビューを使用して構成します。マルウェア・テストは、標準的なスキャンに影響を与えることはありません。

設定	詳細
マルウェア・テスト	悪質な外部 **Web** サイトへのリンクをチェック このチェック・ボックスを選択すると、AppScan は、望ましくない外部リンクがないかどうかについて、スキャン時にアプリケーションを検査します。インターネット接続が必要です。
有効範囲	マルウェア・テストから除外する URL を定義する正規表現のリストを作成することができます。  を使用して正規表現を追加します。また、開いたダイアログ・ボックスで  をクリックして Expression Test PowerTool を開き、正規表現の構文を検証することができます。正規表現を作成するための支援がさらに必要な場合は、次のリンクが役立ちます。 http://www.regular-expressions.info/quickstart.html
その他の結果	このセクションのチェック・ボックスを使用すると、マルウェア分析のスコープを拡大することができます。「悪質」として分類されたリンクの結果を AppScan で分析する場合、ISS によって「未分類 **(Unclassified)**」と分類されたリンク (問題が存在する可能性があります) だけでなく、「不要」および「無害」として分類されたリンクについて報告することもできます。結果に組み込みたい問題タイプを選択します。 **注:** 問題タイプが「未分類 (Unclassified)」のリンクが、実際には悪質である場合もあります。 **注:** 無害のリンクを含めると、結果のサイズが著しく増加する場合があります。

「スキャン・エキスパート」ビュー

「スキャン構成」ダイアログ・ボックスの「スキャン・エキスパート」ビューです。

スキャン・エキスパートは、メイン・スキャンが開始する前に短い探査ステージを実行します。この探査の結果を分析して、構成された設定の効率を評価し、必要に応じて変更を提案します。その後、提案された変更をインプリメントしてからメイン・スキャンを開始することにより、効率を最適化できます。 (詳しくは、 172 ページの『スキャン・エキスパート (Scan Expert)』を参照してください。)

このビューの設定では、スキャン・エキスパートの探査の完成度や、構成変更が自動的にインプリメントされるかまたは手動でインプリメントされるか、さらに構成のどの「モジュール」が評価に含まれるかを決定できます。

注**:** デフォルトでは、すべてのフル・スキャンの前に、スキャン・エキスパートが自動的に実行します。この設定は、「ツール」 **>** 「オプション**...**」 **>** 「設定」で確認または変更できます。

設定	詳細
スキャン・エキスパートの動作 (Scan Expert Behavior)	評価の制限**:** スキャン・エキスパートがアプリケーションを探査する速度 (深さ) を定義します。深く調べるほど、詳細な評価が得られます。 評価中に探査される URL の最大数、時間制限、またはその両方を定義できます。両方によって評価を制限する場合、2 つの制限の最初のもの に到達すると、評価は停止します。(注:スキャンは常に制限のとおりに停止するとは限りませんが、その後まもなく停止します。) 評価後**:** スキャン・エキスパートの推奨事項が自動的にインプリメントされてスキャンが開始するか、またはユーザーが推奨事項を確認し、承認したものを手動でインプリメントするまでシステムが待機するかを定義します。 (モジュールによっては自動的にインプリメントできないものがあるため、「自動で有効にする」を選択すると、こうしたモジュールの設定は評価されません。)
モジュール	「モジュール」ペインには、スキャン・エキスパートが評価できるすべてのモジュールがリストされます。 チェック・ボックスを選択/選択解除して、評価に組み込みたいモジュールが選択されるようにします。 上/下矢印を使用して、モジュールの順序を再配列します (これは便宜上のものであり、実行方法には影響を与えません)。 詳しくは、『スキャン・エキスパート・モジュール』を参照してください。

以下も参照してください。 172 ページの『スキャン・エキスパート (Scan Expert)』

スキャン・エキスパート・モジュール

スキャン・エキスパート・モジュールおよびその説明の表を示します。

リスト内のモジュールは、実行される順序で配列されています。2 つ以上のモジュールの推奨の間に競合がある場合は、リスト内で下にある モジュールが優先されます。

独自のモジュールを追加する場合、そのモジュールはリストの一番下に追加されます。そのため、既存のモジュールとの競合がある場合は、新規モジュールが優先されます。

必要に応じて、上矢印および下矢印を使用して、リスト内のモジュールを昇格および降格することができます。

モジュール	説明
パラメーター・ベースの移動サイトの検出	アプリケーションがパラメーター・ベースの移動を使用するかどうかを検査し、このためにスキャンを正しく構成できるように支援します。
サーバー認証	失われた、または失敗した NTLM および HTTP 認証の詳細をチェックします。
プロキシー・サーバー	プロキシー接続または認証エラーが発生していないことをチェックします。
クライアント側の証明書	クライアント証明書が必要かどうかを検出します。
記録されたログインが消失しています	ログイン・ページを自動的に検出するようにスキャンを構成している場合には、該当するページが検出されなかったときにユーザーに対して警告を行います。
AJAX フレームワークを検出します	JavaScript の実行を必要とする共通の AJAX フレームワークのマーカーを探します。
セッション ID を検出します	自動のまたは記録されたログイン・シーケンスに、セッション ID があったかどうかをチェックします。
未記入のフォーム	未記入のフォームを検出します。
未テストのサーバーを検出します	開始 URL と同じドメイン内で、開始 URL サーバー以外のサーバーへのリンクを検出します。そのようなリンクが見つかった場合、モジュールは、「追加のサーバーおよびドメイン」(「構成」 > 「URL およびサーバー」) のリストに追加することを推奨します。
通信タイムアウト	通信タイムアウト構成の精度を評価します。
スレッドの数	アプリケーションの複数のスキャン・スレッドに耐える能力を評価します。
エラー・ページを検出します	アプリケーションのカスタム・エラー・ページを検出します。
大文字と小文字を区別するパス	Web アプリケーション・サーバーで大文字と小文字を区別するかどうかをチェックします。
疑わしい URL	スキャンから除外すべきと思われる疑わしい URL を検出します。
ログアウト・リンク消失	ログアウト・ページを検出します。
深度限界	深度限界のためにリンク先に到達できなくなっていないかチェックします。到達できなくなっている場合には、深度限界を大きくするか無効にします。
Flash オブジェクトを検出します	Web アプリケーション内の Flash の利用を検出します。
Web サービス	アプリケーション内の Web サービスの存在を検出します。
環境設定を確認します	グローバルな質問が「環境設定」タブに存在する場合、これらの質問がどれも回答されていなければユーザーにアラートを出します。
WebSphere Portal の検出	テスト対象アプリケーションが WebSphere Portal に基づくものかどうかを確認します。
Scan Expert の評価	Scan Expert の評価が正常に行われたかどうかをチェックします。
Hacme Bank の検出	テスト対象のアプリケーションが McAfee Foundstone Hacme Bank であるかどうかを確認します。
WebGoat の検出	テスト対象のアプリケーションが OWASP の WebGoat であるかどうかを確認します。

122 ページの『「スキャン・エキスパート」ビュー』

「詳細構成」ビュー

「スキャン構成」ダイアログ・ボックスの「詳細」タブ (「スキャン」>「スキャン構成」>「詳細」タブ) は、特定のスキャンに影響を与える詳細レジストリー設定を変更するために使用します。このタブは、経験

を積んだ AppScan ユーザーである場合にのみ、または、問題をトラブルシューティングするためにサポート・チームから指示された場合にのみ、使用してください。

ヒント: (特定のスキャンではなく) AppScan 全般に影響を与える詳細レジストリー設定は、「オプション」ダイアログ・ボックスの「詳細」タブ (「ツール」>「オプション」>「詳細」タブ) にあります。

注: それぞれの設定には ID があります。それらの ID は、設定についてサポート・チームと話し合うときに使用できます。グリッド内の項目は、該当する列見出しをクリックすることにより、名前または ID に基づいてソートできます。

注: デフォルト設定が正規表現である場合は、その全体を削除すると、設定は未定義として扱われます (すべてを含む正規表現としては扱われません)。

名前	説明	考えられるユースケース
アクション・ベース:		
ログイン再生のブラウザー	ログイン手順を記録する場合は、常に組み込みの AppScan ブラウザーが使用され、アクション・ベースの記録が行われます。ただし、スキャン時に記録を再生 する際に AppScan が使用するブラウザーを構成することができます。オプションは以下のとおりです。 • 0 = Internet Explorer (組み込みバージョン) • 1 = Chromium • 2 = Chrome • 3 = Firefox デフォルト:0	
マルチステップ再生ブラウザー	マルチステップ・シーケンスを記録する場合は、常に組み込みの AppScan ブラウザーが使用され、アクション・ベースの記録が行われます。ただし、スキャン時に記録を再生 する際に AppScan が使用するブラウザーを構成することができます。オプションは以下のとおりです。 • 1 = Chromium • 2 = Chrome • 3 = Firefox デフォルト:1	
マルチステップ再生、非相互作用タイムアウト	マルチステップ操作の再生を停止するための非相互作用タイムアウト (秒単位)。 デフォルト:10	
単一のログイン試行のタイムアウト	ブラウザーが強制的にクローズされるまでに、単一のアクション・ベースのログイン試行のブラウザーによる再生を AppScan が待機する時間 (秒単位) デフォルト:120	
通信:		

名前	説明	考えられるユースケース
Accept-Language 要求ヘッダー値	すべての HTTP 要求の Accept-Language ヘッダーに送信されるストリング。 このストリングをユーザーが定義しなかった場合、AppScan は、ユーザーがログイン手順やマルチステップ操作を記録するため、あるいはページを表示するために開いたこのスキャンで、ブラウザーから最初に送信された値を使用します。 注:デフォルトのブラウザーを変更する場合は、 355 ページの『デフォルト・ブラウザーの変更』 にリストされている条件を参照してください。 デフォルト: en-US	探査ステージにおいて、Internet Explorer のヘッダー値が原因となって、AppScan が予期しない応答を受信する場合があります。このような場合、このサイトとの対話時にどの値を Accept-Language ヘッダーで使用すべきかを確認し、その値をこの設定 (または Internet Explorer) に定義する必要があります。

カスタム・ヘッダー	AppScan がサイトに送信するすべての要求に追加するカスタム・ヘッダーを定義できます。
	
	デフォルト: 空
		サイトで特定のヘッダー内容が予期されている場合 (例えば、特定のクライアントまたはブラウザーのプラグインによってサイトにアクセスするなどの場合) は、そのヘッダーをここで定義します。それぞれのヘッダーの前に区切り文字を指定する必要があります。ヘッダーと値の間には、コロンとシングル・スペースが必要です。
		
		形式: 区切り文字|ヘッダー|コロンとシングル・スペース|値
		
		例 1:
		`;Header: Value`
		
		(この例の場合、区切り文字は **;**)
		
		例 2:
		`,Header1: Value1,Header2: Value2`
		
		(この例の場合、区切り文字は **,**)

すべてのフォーム・アクションに対してパラメーターのない HTTP 要求を強制する	場合によっては、パラメーターが指定されていない フォームの処理要求を受け取ったときのサーバー・サイドのロジックの動作が異なることがあります。 True に設定すると、AppScan はすべてのフォームに対してパラメーターのない追加要求を送信します。その結果、追加の Web ページおよび機能へのリンクを持つカスタム・エラー・ページが返されることがあります。 デフォルト:True	スキャン中のトラフィックを確認し、パラメーターのないフォームの処理要求が原因でアプリケーションのタイムアウトや異常終了が発生することがわかった場合は、このオプションを False に設定することをお勧めします。

名前	説明	考えられるユースケース
GSC SSL ポート (GSC SSL port)	この設定により、SSL 通信の GSC で使用されるポート番号が定義されます。 デフォルト:443	GSC 探査によって提供されたリンクの場合、AppScan はこのポート番号を基にして HTTPS を識別します。SSL 通信用に異なるポートをアプリケーションで使用する場合は、そのポートをここで定義します。正しい SSL ポートを定義しない場合、AppScan はすべてのテストを HTTP として送信します。
すべての要求に AppScan デバッグ・ヘッダーを含める (Include AppScan debug headers in all requests)	True に設定されている場合は、AppScan によってサイトに送信されるすべての要求に、HTTP ヘッダーが追加されます。ヘッダー名は「X-AppScan-Debug」であり、その値には、AppScan がこの特定の要求を送信する理由 (探査、テスト、ログイン再生、サーバー障害検査など) についての情報が含まれます。 デフォルト:False	スキャンが「X-AppScan-Debug」ヘッダーを送信するように構成すると、Web デバッガー、プロキシー、アナライザー、スニファーなどの外部ツールで AppScan トラフィックを追跡するときに役立ちます。 注:一部のサイトは、このような特殊なヘッダーを含む要求をすべて拒否することがあります。
最大応答長	AppScan は、メモリー消費量に関する問題を回避するため、長い応答を切り捨てます。この設定は、許可する最大応答長をメガバイト単位で定義します。これより長い応答はエラーとして扱われます。 デフォルト:8	AppScan でリンクが認識されていないかセッションが無効になっているように見える場合、アプリケーションが長い応答を送信することが分かっているときは、最大応答長を増やすことによって問題が解決することがあります。
Accept-Encoding ヘッダーの削除	AppScan はすべてのエンコードをサポートしているわけではないため、サポートしていないエンコードを除去します。この設定が有効になっている場合、AppScan は、サポートしていないエンコードだけでなく、ヘッダー全体を除去します。 デフォルト:True	AppScan の要求をサーバーが拒否する場合、予期しない応答をサーバーが返す場合、または AppScan がセッションを維持できない場合は、トラフィック・ログを調べて、AppScan が送信する要求とご使用のブラウザーが送信する要求を比較する必要があります。ブラウザーの Accept-Encoding ヘッダーが異なっているか欠落している場合は、この設定を有効にする必要があります。
サーバー接続を再使用する	デフォルトでは、AppScan は TCP 接続を使用後に閉じます。これは、開いている接続と保存データによってスキャン結果が影響を受ける可能性があるためです。 True に設定すると、AppScan は接続を使用後も開いたままにし、可能な限り、開いている接続の再使用を試みます。 デフォルト:False	Web サーバー上でネットワーク・リソースが使い尽くされるというエラーが発生する場合は、この設定を True に変更することにより、問題を解決できる可能性があります。

名前	説明	考えられるユースケース
セキュリティー・パッケージ順序	AppScan は、基本、ダイジェスト、NTML、ネゴシエーション、および Kerberos HTTP 認証をサポートしています。特定の方式の使用または不使用を AppScan に適用する場合、またはサイト/プロキシーで複数の方式が許可されているときに、方式の選択について優先順位を適用したい場合は、この値を編集します。 例えば、「NTLM」と「基本」だけを許可し、使用可能な場合は「NTLM」を優先して使用したい場合は、この文字列を編集して `ntlm, basic` にします。 デフォルト: basic, digest, ntlm, negotiate, kerberos	特定の認証方式がサイトで使用されており、AppScan がアクセスを拒否された場合、必要な方式を唯一の方式として定義すると、問題を解決することができます。 特定の方式 (例えば、「基本」と「NTLM」など) を使用してサイトをテストしたい場合、一方のスキャンを「基本」だけを使用するように構成し、もう一方のスキャンを「NTLM」だけを使用するように構成することができます。
スラッシュ正規化 (Slash Normaliza-tion)	連続する 2 つ以上のスラッシュを 1 つのスラッシュに置き換えて、URL を正規化します。 デフォルト:True	サイト URL で連続スラッシュを利用している場合は、この設定を非アクティブにしてください。
エラー応答を有効な応答として処理	AppScan は、通常のページとは異なる方法でエラー・ページを処理します (例えば、リンクの構文解析を行わないなど)。この設定を使用すると、すべてのエラー・ページまたは開始 URL に対するエラー・ページのみを通常のページとして処理するよう AppScan に指示できます。 0 に設定すると、AppScan はすべてのエラー応答を無効として処理します。 1 に設定すると、AppScan は開始 URL に対するすべてのエラー応答 (4xx および 5xx) を有効として処理します。 2 に設定すると、AppScan は、通常のページと開始 URL の両方について、すべてのエラー応答を正しい応答として処理します。 デフォルト:0	開始 URL 応答がエラー・ページの場合、この設定を 1 に変更します。 スキャンによってエラー・ページからデータを抽出してテストしたい場合は、この設定を 2 に変更します。 デフォルト設定を変更すると、パフォーマンスに影響する可能性があることに注意してください。
Flash:		
範囲	スキャンの「範囲レベル」を定義します。1 は速度優先スキャン、2 はカバー範囲優先スキャンです。 デフォルト:1	カバー範囲を重視して Flash コンテンツをスキャンする場合は、この設定を 2 に変更できます (ただし、速度は遅くなります)。
インスタンスを除外	Flash スキャンから除外する、問題のある GUI インスタンスを定義します。このオプションを使用するのは、サポート担当者から指示された場合のみにしてください。	スキャンが失敗した場合、または、反復操作のためにエンドレスになった場合。複数のインスタンスを指定する場合はコンマで区切ります。

名前	説明	考えられるユースケース
ファイル・ダウンロード・ストリング	Flash ムービーを効率的にスキャンするためには、ファイルのダウンロードを引き起こすコントロールを AppScan が識別可能であることが重要です。ここではそのコントロールを定義します。 AppScan は、ここで定義したストリングを含むコントロールをクリックした後に「長い操作の待機時間」だけ一時停止します。この動作は、ストリングが「長い操作のストリング」設定に含まれていない場合でも同じです。 デフォルト:ダウンロード	ムービーにファイル・ダウンロードが含まれる場合は、ここでダウンロードを定義する必要があります。 複数ある場合は、セミコロンで区切ってください。 例:Download;Save;Copy
ファイル・アップロード・パス	ファイルをアップロードするためのオプションがムービーに含まれている場合に、アプリケーションに対して AppScan がアップロードできるファイルへのパス。 デフォルト: 空	ファイルをアップロードするためのオプションが Flash ムービーに含まれている場合は、ファイルへのパス (ファイル名を含む) を定義して、そのファイルがそこに存在することを確認してください。「ファイル・アップロード・ストリング」も定義する必要があることに注意してください。
ファイル・アップロード・ストリング	Flash ムービーを効率的にスキャンするためには、ユーザーがファイルをアップロードすることを許可するコントロールを AppScan が識別可能であることが重要です。ここではそのコントロールを定義します。 AppScan は、ここで定義したストリングを含むコントロールをクリックした後に「長い操作の待機時間」だけ一時停止します。この動作は、ストリングが「長い操作のストリング」設定に含まれていない場合でも同じです。 デフォルト:Upload;Browse	ユーザーがファイルをアップロードすることをムービーが許可する場合は、アップロードを行うリンクまたはコントロールのテキストをここで定義する必要があります。 複数のテキストがある場合は、セミコロンで区切ってください。 例:Upload;Browse;Add 「ファイル・アップロード・パス」も定義する必要があることに注意してください。
Flash ムービーの依存関係が存在する	サイトが持つ Flash ムービーに、そのムービーが依存する別の Flash ムービーが含まれていることを判別します。 デフォルト:False	サイトに含まれている Flash ムービーが、そのムービーが依存する別の Flash ムービーをロードする場合は、これを True に設定します。
フレーム・レート係数	Flash の再生時に、この係数 (1、2、3、4) を乗算してフレーム・レートを増加させます。 デフォルト:4	AppScan は、スキャン中に動画を再生するときに、デフォルトで係数 4 を乗算してフレーム・レートを増加させます。これが、実際の使用をシミュレートするには速すぎる場合は、より低い値を指定できます。
ムービーのロード待ち時間	AppScan がムービーのロードを待機する時間がこの時間 (ミリ秒) を超えると、ムービーの探査を開始します。 デフォルト:1600	ムービーがロードされる前に AppScan がムービーの探査を開始した場合には、結果が不正確になります。したがって、ムービーのロードにかかる時間がデフォルト時間よりも長い場合は、この設定を大きくする必要があります。

名前	説明	考えられるユースケース
長い操作のストリング	多くの場合 Flash ブラウザーは、操作後、次の操作に進む前に「通常待機時間」で定義されている時間だけ待機します。これは、ムービーが新たな状態に達する時間を確保するためです。操作に時間がかかるため新たな状態に達するまでスキャンが続行する可能性がある場合は、ブラウザーの一時停止時間を長くするために「長い操作」(ファイルのアップロードやログインなど) を定義する必要があります。 デフォルト: 空	「アップロード」リンクまたは「ログイン」リンクなどの操作を「長い操作」として定義することをお勧めします。 ファイル・アップロードの場合、ここで定義する必要があるリンクは、実際にファイルのアップロードを生じさせるリンクです。アップロード対象のファイルをユーザーに選択 させるリンクではありません。 2 つ以上のストリングを入力する場合は、シングル・スペースで区切ってください。
長い操作の待機時間	「長い操作のストリング」で定義した操作が完了して新たな状態に達するのを Flash ブラウザーが待機する時間 (ミリ秒)。 デフォルト:5000	「長い操作」が定義されている場合は、その「待機時間」をここで定義する必要があります。
サンプル間の時間	ムービーが新たな状態に達するまでの時間を確保するために、「ユーザー操作」(マウスのクリックなど) の間に待機する最小時間 (ミリ秒単位)。 デフォルト:160	ムービーに大量のアニメーションが含まれる場合は、ユーザーのクリックの間やフォーム入力の間に、デフォルト設定より長い待機時間が必要なことがあります。その場合は、ここで時間を増やすことができます。
全般:		
AppScan ブラウザーのスクリプト・エラー・ポップアップの抑止	AppScan 組み込みブラウザーで、アクション・ベースのログインの記録と再生、マニュアル探査、マルチステップの記録、ブラウザーでの表示中にスクリプト・エラー・ポップアップを抑止します。 デフォルト:False	無関係なエラー・ポップアップ・メッセージによってアクション・ベースのログインの記録と再生が妨げられる場合は、この値を True に設定することで、それらを抑止できます。「HTTP 認証」エラーおよび「ActiveX コントロールのインストール」プロンプトなどの他のポップアップも抑止されることに注意してください。
冗長なテストをマージする	True に設定すると、AppScan は、同じ 2 つ (またはそれ以上) の要求に対して 1 セットのテストのみを送信します (追加の Cookie は除く)。 False に設定すると、そのような要求は、すべて個別にテストされます。 デフォルト:True	この設定を False に変更すると、パフォーマンスが低下する可能性があります。サポートにより指示された場合のみ、False に変更してください。

名前	説明	考えられるユースケース
プロキシー・ファイル拡張子フィルター (Proxy file extension filter)	ログイン、マニュアル探査、またはマルチステップ操作を記録するときに保存される URL のリストから削除されるファイル拡張子を定義する正規表現。正規表現を使用して拡張子を削除する場合、その拡張子で終了する URL は、フィルターによって記録から除外されません。 デフォルト: ".(zip | Z | tar | t?gz | sit | cab | pdf | ps | doc | ppt | xls | rtf | dot | mp(p | t | d | e | a | 3 | 4 | ga) | m4p | mdb | csv | pp(s | a) | xl(w | a) | dbf | slk | prn | dif | avi | mpe?g | mov(ie)? | qt | moov | rmi? | as(f | x) | m1v | wm(v | f | a) | wav | ra | au | aiff | midi? | m3u | gif | jpe?g | bmp | png | tif?f | ico | pcx | css | xml)$"	CAPTCHA イメージ・ファイルなどの特定の種類のファイルを、参照のためにログイン記録に含める必要が生じる場合がまれにあります。そうした場合は、正規表現を使用してそのファイル拡張子 (この場合は `jp?g`) を削除できます。
ログのサニタイズ	ログから機密情報を除去します。 デフォルト:False	ログから機密情報を除去する必要がある場合は、このオプションをアクティブにし、除去するパターンを「機密情報パターン」オプションで定義します。 ただし、この設定を変更しても既に生成されたログには影響を与えません。
レポートのサニタイズ	レポートから機密情報を除去します。 デフォルト:True	レポートから機密情報を除去する必要がある場合は、このオプションをアクティブにし、除去するパターンを「機密情報パターン」オプションで定義します。 「構成」>「フォームの自動入力」で定義されたパスワードは、パターンが定義されていなくても、すべてのレポートから除外されます。 ただし、この設定を変更しても既に生成されたレポートには影響を与えません。

名前	説明	考えられるユースケース
GSC を使用してすべてのテストを送信 (Send all tests through GSC)	AppScan は、GSC を使用して、GSC が検出した一部またはすべてのリンク上でのテストを送信することができます。 0 = GSC を使用して SOAP メッセージのみを送信 1 = GSC を使用して、GSC が検出したリンク上でのすべてのテストを送信 2 = GSC を使用してテストを送信しない デフォルト:0	GSC でサイトを探査したときに特別なセキュリティー設定を何も定義しなかった場合、テスト・ステージ中に (GSC ではなく) AppScan がテストを送信できるようにすることで、スキャン時間が大幅に削減されます。ただし、テスト・ステージで多くのテストから応答がなかった場合、または予期しないエラー応答が返された場合は、GSC による要求の送信方法と AppScan による要求の送信方法との違いが原因で、この問題が発生している可能性があります。そのようなテストは、GSC を使用して送信することで問題が解決される場合があります。
機密情報パターン	ログおよびレポートから除外する 1 つ以上のグループを定義する正規表現。これは、「ログのサニタイズ」オプションまたは「レポートのサニタイズ」オプションがアクティブである場合に使用されます。 デフォルト: 空	レポートまたはログから機密情報を除去する必要がある場合は、対応するオプション (「ログのサニタイズ」または「レポートのサニタイズ」) をアクティブにし、ここで正規表現を使用して 1 つ以上のグループを定義します。 機密テキストは「**CONFIDENTIAL 1**」、「**CONFIDENTIAL 2**」などに置き換えられます。 「構成」>「フォームの自動入力」で定義されたパスワードは、パターンが定義されていなくても、すべてのレポートから除外されます。
JavaScript:		
マニュアル探査による JavaScript の自動実行	マニュアル探査時にトリガーされなかったリンクも含め、マニュアル探査されたページ上のすべての JavaScript 生成リンクを抽出するように、AppScan を構成できます。 デフォルト:False	これは、マニュアル探査時の範囲を広げるための方法の 1 つです。
キャッシュの消去	True に設定すると、JavaScript 実行 (有効な場合) は、ログイン中に送信された要求をキャッシュしません。これにより、スキャン時間が長くなり、ファイル・サイズが増える場合があります。 デフォルト:False	

名前	説明	考えられるユースケース
外部リンクの取り出し	JavaScript の実行が有効になっている場合に、AppScan で追加サーバーとして構成されていないサーバーが外部リンクで参照されていても、AppScan が外部リンクを取り出すことを許可します。 デフォルト:False	HTML ページは、Dojo ソース・ファイルや jQuery ソース・ファイルなどの外部 JavaScript ソース・ファイルにリンクしていることがよくあります。JavaScript の実行時に、探査ステージで検出されるすべての関連リンクにアクセスする場合は、この設定をアクティブにします。これにより、AppScan のテスト対象となる追加サーバーおよびドメインのリストにすべてのサーバーを追加せずにすむようになります。 AppScan は、リンクを取り出すときに、そのリンク先をテストしたり、そのリンク先を解析して新規リンクを抽出したりすることはありません。
JavaScript および Flash フィルター	この正規表現は、スキャンの探査ステージで JavaScript の実行対象および Flash の解析対象から除外するページを定義します。(これは JavaScript の構文解析を制限しません) デフォルト: 空	JavaScript または Flash を含む特定のページで AppScan が繰り返し異常終了またはフリーズする場合は (これはトラフィック・ログを参照することで確認できます)、ここでそのページを定義することで問題が解決します。
JavaScript リンク・パターン	AppScan は、さまざまなパターンを使用して、JavaScript コード内のリンクを識別します。通常とは異なるパターンがサイトで使用されている場合は、それらをこの正規表現で定義する必要があります。 デフォルト: 空	AppScan が JavaScript コードのリンクを識別していないように思える場合で、サイトで通常とは異なる JavaScript のリンク・パターンが使用されている場合は、ここで 1 つ以上のパターンを定義して、検索対象を AppScan に通知します。
ローカライズ:		
HTML エンコード	サイトの HTML 応答に定義されているエンコードをオーバーライドします。 デフォルト: 空	スキャン結果の応答の内容がゆがめられているように見える場合は、次のようなことが考えられます。 1) エンコード方式が AppScan によって正しく識別されなかった。または、 2) サイトの HTML でエンコード方式が間違って定義されている。 1 の解決法:「探査オプション」ドロップダウン・リストから正しい方式を選択します。 2 の解決法: 正しいエンコード方式をここに入力します。
パラメーターおよび *Cookie*		
冗長な JSON パラメーターをテストから除外	JSON コンテンツ・タイプの本文では、個別にテストする必要がない単一のパラメーターに複数の値を指定することができます。「True」に設定した場合、AppScan は、冗長な値を識別し、テストをサブセットに制限してスキャン時間の短縮を試みます。 デフォルト:True	特定の重要なパラメーターがテストされなかったことを検出した場合は、設定を「False」に変更します。

名前	説明	考えられるユースケース
冗長な XML パラメーターをテストから除外	XML コンテンツ・タイプの本文では、個別にテストする必要がない単一のパラメーターに複数の値を指定することができます。「True」に設定した場合、AppScan は、冗長な値を識別し、テストをサブセットに制限してスキャン時間の短縮を試みます。 デフォルト:True	特定の重要なパラメーターがテストされなかったことを検出した場合は、設定を「False」に変更します。
ヘッダー内のカスタム・パラメーターを追跡	この設定は、AppScan v. 8.7.0.1 以前で保存されたスキャンにのみ適用されます。 これ以降のバージョンでは、デフォルトの挙動は True に変更され、個々のパラメーターおよび Cookie の設定は以下のように制御されます。構成 > パラメーター**/Cookiee** > パラメーター定義 > オプションの追跡 > 一致**:**「ヘッダーと本文」 (デフォルト) または「本文のみ」 (80 ページの『パラメーター定義』を参照)。 デフォルトで、AppScan (8.7.0.1 以前) は、カスタム・パラメーターを応答の本文内でのみ検索し、応答のヘッダー内では検索しません。この設定を True に変更すると、AppScan はヘッダー内も検索するようになります。 デフォルト:False **注:**	応答ヘッダー内のパラメーターが変更されたことが原因となって、AppScan でセッションが無効になる場合は、この設定を変更することで問題が解決される場合があります。これを行うと、スキャン時間が長くなる場合があることに注意してください。
インライン・コンテンツが存在する場合のみテスト・ステージで動的パラメーターを追跡 (Track dynamic parameters in Test stage only when inline content exists)	テスト・ステージでの動的パラメーターの追跡により、パフォーマンス上の問題が起きる場合があります。したがって、デフォルトでは、テスト・ステージ中の動的パラメーターの追跡は、インライン・コンテンツを持つ応答でのみ行われます。 デフォルト:True	この設定を False に変更するのは、この種の追跡が不可欠な場合のみに限定してください。
サーバー障害の検出:		

名前	説明	考えられるユースケース
探査で「サーバー障害」を確認	探査ステージ中のサーバー障害を確認するために、ハートビート要求の送信を有効にします。 デフォルト:True	探査ステージで AppScan がサーバー障害エラーを受信するが、実際にはサーバー障害が発生していない場合は、頻繁なハートビート要求をサーバーがブロックしていることがエラーの原因である可能性があります。 スキャン中に AppScan で頻繁にセッションが無効になる場合は、開始 URL が Cookie なしのハートビートとしてサーバーに送信されていることが原因である可能性があります。 この設定を非アクティブにすると問題が解決される場合がありますが、AppScan がサーバーの状況を検証できなくなることに注意してください。
テストで「サーバー障害」を確認	テスト・ステージ中のサーバー障害を確認するために、ハートビート要求の送信を有効にします。 デフォルト:True	テスト・ステージで AppScan がサーバー障害エラーを受信するが、実際にはサーバー障害が発生していない場合は、頻繁なハートビート要求をサーバーがブロックしていることがエラーの原因である可能性があります。 スキャン中に AppScan で頻繁にセッションが無効になる場合は、開始 URL が Cookie なしのハートビートとしてサーバーに送信されていることが原因である可能性があります。 この設定を非アクティブにすると問題が解決される場合がありますが、AppScan がサーバーの状況を検証できなくなることに注意してください。
探査ステージの再接続の試行	AppScan が探査ステージを終了しようとしており、その前にいくつかのテストが「サーバー障害」が原因となって失敗していて、サーバーがまだ停止している場合、AppScan はサーバーへの接続を何度か試行します。 デフォルト:5	サーバーが過敏に反応することが分かっている場合、または複数の通信エラーが原因で複数のテストが失敗している一方で、1 回の通信エラーが原因でスキャンが停止している場合は、この数値を増やす必要があります。
要求再試行間隔	失敗した要求 (失敗したハートビート要求を含む) を再送するまでの秒単位の間隔。 デフォルト:1	接続環境が良くない場合や、サーバーが不安定な場合 (これは、検出漏れや、範囲の縮小につながる場合がある)、影響を小さくするためにこの間隔を増やすことができます。
要求の再試行制限	失敗した要求の送信の再試行回数。 デフォルト:2	サーバーが不安定である場合や、通信環境がよくない場合は、この設定を増やすとスキャンの効率が向上することがあります。

名前	説明	考えられるユースケース
サーバー障害のタイムアウト	AppScan がサーバーに接続できなかった場合、またはセッションが無効になった場合は、AppScan でスキャンを停止する前に、この設定で定義された期間 (秒単位)、再接続またはセッションの再確立を試行します。 デフォルト:185	接続速度が遅い場合、または障害後のサーバーの再ロードに時間がかかる場合は、この設定を増やすことをお勧めします。
サーバー障害のハートビート間隔	サーバー障害ハートビート間の秒単位の間隔。 デフォルト:3 秒 最大:60 秒	スキャン中に AppScan がサーバー障害エラーを受信する場合は、接続環境がよくないか、またはサーバーが不安定であることが原因である可能性があります。この間隔を増やすことによって問題が解決する場合があります。
テスト・ステージの再接続の試行	AppScan がテスト・ステージを終了しようとしており、その前にいくつかのテストが「サーバー障害」が原因となって失敗していて、サーバーがまだ停止している場合、AppScan はサーバーへの接続を何度か試行します。 デフォルト:5	サーバーが過敏に反応することが分かっている場合、または複数の通信エラーが原因で複数のテストが失敗している一方で、1 回の通信エラーが原因でスキャンが停止している場合は、この数値を増やす必要があります。
セッション管理*:*		
広告ドメイン	共通 Web 広告ドメインを表す正規表現。ログイン手順の記録中にこれらのドメインに送信された要求は破棄されます。 デフォルト: ad\d.googlesyndication|doubleclick\.net|coremetrics\.|webtrends\.|112\.2o7\.net|view.atdmt.com|ad.yieldmanager.com|ads.adbrite.com|oasn04.247realmedia.com| segment-pixel.invitemedia.com"	ログイン手順はスキャン中に継続的に再生されるため、これらの不要な要求をフィルターで取り除くことにより、スキャンの効率を高めることができます。 正規表現を完全に削除すると、ドメインはフィルターでは取り除かれないことに注意してください。
ログイン記録の分析	ログイン手順を記録するとき (「スキャン構成」>「ログイン管理」)、AppScan はログイン手順を分析し、セッション内検出設定 (セッション内パターン、セッション内要求、およびログイン中に受け取ったセッション ID) を更新します。 デフォルト:True	分析に時間がかかりすぎる場合、この設定を「False」に変更できます。ただし、これを行うと、セッション内検出設定を手動で構成する必要があります。
ログインをやり直す前に Cookie を消去する	ログイン手順をやり直す前に、Cookie が削除されているかどうかを判別します。 デフォルト:True	
共通の静的パラメーター値	共通の静的パラメーター値。非ランダム・パラメーター値を検出するために使用されます。非ランダム・パラメーター値は、ログイン中にトラッキングされません。 デフォルト: |true|false|\bon\b|\boff\b|\bout\b|checked|enabled|log\s?in|log\s?out|exit|submit|sign|ever|disabled| agree	

名前	説明	考えられるユースケース
探査ステージのセッション内バッファリングの無効化	探査ステージ中:要求の送信時にユーザーがセッション外であったことが要求に対する応答によって示されると、AppScan は、その要求を再送信するためにキューに格納します。これにより、可能な限り広範囲にサイトがスキャンされることになります。 デフォルト:False	サイトにより、ユーザーが頻繁にセッション外にスローされる場合は、セッション内バッファリングによって探査ステージが無限に続行されることがあります。このオプションを True に設定すると、探査ステージの処理速度は上がりますが、サイトの対象範囲が狭くなる可能性があります。
マルチステップ操作実行前のセッション内	デフォルトで、AppScan は、マルチステップ操作を再生する前にセッション内状況を検証します。 デフォルト:True	未認証ユーザーでマルチステップ操作をテストする場合、またはマルチステップ・シーケンスにログイン手順が含まれる場合は、この設定を False に変更にします。 **重要:** 「構成」 > 「ログイン管理」 > 「詳細」 > 「セッション内検出を有効にする」が選択解除されており、この詳細設定が「真」(デフォルト) に設定されている場合、各マルチステップ操作の前にログイン手順全体が再生されます。
セッション内のハートビート間隔	セッション内ハートビート間の秒単位の間隔。 デフォルト:5	スキャン中に AppScan でセッションが無効になる場合は、接続環境がよくないか、またはサーバーが不安定であることが原因である可能性があります。この間隔を増やすことによって問題が解決する場合があります。
ログイン・コンテンツ・タイプ・フィルター	ログイン手順およびマルチステップ操作手順からフィルタリングによって除去されるべきコンテンツ・タイプを定義する正規表現。ログイン手順またはマルチステップ操作手順が記録される際に、これらのコンテンツ・タイプのヘッダーを含むような応答を求める要求は、手順から除去されます。したがって、スキャン中に AppScan が手順を再生するときには、これらのコンテンツ・タイプのヘッダーを含む応答を求める要求は、手順の一部として送信されません。 デフォルト: text/javascript|application/javascript| application/x-javascript|image|text/css	サイトのログイン手順、あるいは記録したマルチステップ操作のいずれかで、ここにリストされたコンテンツ・タイプのヘッダーを含むリンクをクリックする必要がある場合には、それを正規表現から除去してください。
ログインの再試行間隔	失敗したログイン要求を再送信する前の秒単位の間隔。 デフォルト:3	AppScan でセッションが無効になり、ログイン再試行が繰り返し失敗する場合は、頻繁なログイン試行をサーバーがブロックしていることが原因である可能性があります。この間隔を増やすことによって問題が解決する場合があります。

名前	説明	考えられるユースケース
マルチパートのコンテンツ・タイプ・フィルター	不要なメモリー消費を減らすために、特定のコンテンツ・タイプが自動的にマルチパート要求 (複数のコンテンツ・タイプを含む要求) からフィルターで除外されます。この正規表現で定義したコンテンツ・タイプのみがマルチパート要求に含まれ、他のものはすべてフィルターで除外されます。 コンテンツ・タイプ・ヘッダーがない コンテンツが、デフォルトで含まれるようになっており、次の値によって定義されています。 `content_without_content_type_header` デフォルト: text/ | text/plain | application/javascript | application/json | application/rtf | application/xml | text/xml | content_without_content_type_header	重要なコンテンツ・タイプが要求からフィルターで除外される場合は、そのコンテンツ・タイプをこの正規表現に追加します。不要なコンテンツ・タイプを削除してそれらが送信されないようにすることで、メモリー消費量を減らすことができる場合もあります。
ナビゲーション・パラメーター・ホスト	ホストを表す正規表現。ナビゲーション・パラメーターを (値に基づいて) 検出するために使用されます。ナビゲーション・パラメーターはログイン手順で追跡されません。 デフォルト: https?://	サイトのナビゲーション・パラメーター内で、デフォルトの正規表現ではフィルターで除去されない独自のホストを使用している場合は、それらを追加することによりスキャン効率を高めることができます。 この項目を削除すると、ナビゲーション・パラメーターが正しく識別されなくなる可能性があります。
ナビゲーション・パラメーター・スクリプト	ナビゲーション・パラメーターを (パラメーター値に基づいて) 検出するために使用されるサーバー・サイド・スクリプトを記述する正規表現。ナビゲーション・パラメーターはログイン手順で追跡されません。 デフォルト: /[^/.]+. (htm | jsp | jsf | ws | dll | asp | php | do)	サイトのナビゲーション・パラメーター内で、デフォルトの正規表現ではフィルターで除去されない独自のサーバー・サイド・スクリプトを使用している場合は、それらを追加することによりスキャン効率を高めることができます。 この項目を削除すると、ナビゲーション・パラメーターが正しく識別されなくなる可能性があります。
ナビゲーション・パラメーター	ナビゲーション・パラメーターを表す正規表現。ナビゲーション・パラメーターはログイン手順でトラッキングされません。 デフォルト: bnav | url | page | step | redirect | request | location | target | argument | item | article | goto | node | action | ctrl | control | source | menu | frame | command	デフォルトの正規表現ではフィルターで除去されない独自のナビゲーション・パラメーターをサイトで使用している場合は、それらを追加することによりスキャン効率を高めることができます。 この正規表現を変更すると、スキャンの範囲が不十分になったり、セッションを正しく追跡できなくなったりする可能性があります。

名前	説明	考えられるユースケース
セッション内ページの解析	False に設定すると、AppScan は、セッション内ページの解析を実行しません。また、セッション内ページで変更された値を持つ追跡対象パラメーターまたは Cookie を更新しません。 デフォルト:True	セッション内ページに追跡対象 Cookie またはパラメーターが存在しない場合、この設定を False に変更することで、パフォーマンスを向上させることができます。False に設定すると、AppScan は、セッション内ページの Cookie またはパラメーターの値を更新しません。これにより、セッションが無効になる可能性があります。
ハートビート間の要求数	AppScan は、セッション内検出要求を送信した後、別のセッション内検出要求を送信する前に、少なくともここで定義した数の要求を送信します。 デフォルト:1	サーバーからの応答が遅いために、スキャンがほとんどセッション内検出要求で構成される場合は (トラフィック・ログを参照)、この値を増やすことによってスキャン時間を短縮できます。
単一のアクション・ベース・ログイン試行のタイムアウト	ブラウザーが強制的にクローズされるまでに、単一のアクション・ベースのログイン試行のブラウザーによる再生を AppScan が待機する時間 (秒単位) デフォルト:120 秒	
特別なパターン *(Special Patterns):*		
フォームの自動入力から除外	ここにリストするパラメーター名は、フォームの自動入力から除外されます。 デフォルト: ^CFID __EVENTVALIDATION __VIEWSTATE ^CFTOKEN __EVENTARGUMENT __EVENTTARGET ^BV_	値が非常に長いパラメーターを指定すると、スキャンが遅くなり、ファイル・サイズが大きくなります。値が非常に長いパラメーターをアプリケーションで使用する場合で、それらのパラメーターがフォームの入力に不要な場合は、それらのパラメーターをこのリストに追加します。
テスト *(Tests):*		
CSRF:意味のある要求のパターン	デフォルトで、AppScan は、POST 要求、および応答が「トランザクション成功 (Transaction Successful)」であった要求を対象として、クロスサイト・リクエスト・フォージェリーのテストを実行します。 この設定を使用すると、POST 要求だけでなく、その他の要求も、クロスサイト・リクエスト・フォージェリー脆弱性において「意味のある」要求として定義できます。 この定義は、「CSRF: 意味のある応答のパターン」と組み合わせて使用されます。 デフォルト: ^POST	GET 要求に対してもクロスサイト・リクエスト・フォージェリーのテストを行う場合は、この正規表現を変更してください。

名前	説明	考えられるユースケース
CSRF: 意味のある応答のパターン	デフォルトで、AppScan は、POST 要求、および応答が「トランザクション成功 (Transaction Successful)」であった要求を対象として、クロスサイト・リクエスト・フォージェリーのテストを実行します。 この設定を使用すると、「トランザクション成功 (Transaction Successful)」応答だけでなく、その他の応答も、クロスサイト・リクエスト・フォージェリー脆弱性において「意味のある」応答として定義できます。 この定義は、「CSRF: 意味のある要求のパターン」と組み合わせて使用されます。 デフォルト: トランザクション成功 (Transaction Successful)	他の種類の応答を受け取る要求についてクロスサイト・リクエスト・フォージェリー脆弱性テストを行う場合は、それらの応答をこの正規表現で定義してください。
差異のしきい値	多くの場合 AppScan ではテストが成功したかどうかを確認するために、2 つの応答を比較して、それらが「類似」しているか「差異」があるかを判別します。その際、AppScan は各種アルゴリズムを使用して「類似性の割合」 (100% は 2 つの応答が同一であることを意味する) を割り当てます。 AppScan がテスト成果を判別する際、一部の例では「類似性の割合」が「類似性のしきい値」を上回るかどうかを基準にし、別の例では「類似性の割合」が「類似性のしきい値」を下回る かどうかを基準にします。いずれのしきい値も構成可能です。 多くのテストでは、デフォルトの「類似性のしきい値」は 95%、「差異しきい値」は 75% です。 これは、次のことを示しています。 • 成果が類似性 に依存するテスト結果では、「類似性の割合」が 95% 以上 の場合、2 つのページが類似していることを示します。 • 成果が差異 に依存するテスト結果では、「類似性の割合」が 75% 以下 の場合、2 つのページに差異があることを示します。 この設定に 1 から 100 の間の値 (%) を入力すると、すべてのテストのデフォルトの「差異しきい値」値はオーバーライドされます。「類似性のしきい値」を調整することが必要な場合があります。 デフォルト: 0 (AppScan のしきい値を使用)	類似の応答にわずかな相違を生じさせる原因となる「動的」テキストがご使用のサイトにない場合は、この値を 75 未満に設定することにより、誤検出結果が少なくなる場合があります。 **ヒント:** 「類似性のしきい値」を調整することが必要な場合があります (以下を参照)。
Cookie のテストを無効にする	この設定は、Cookie テストを完全にオフにするために使用します。 デフォルト:False	アプリケーションの Cookie テストを実行するとスキャンに非常に時間がかかる場合は、テストを無効にすることもできます。ただし、これによって、セキュリティー問題が見落とされる (検出漏れが発生する) 可能性があります。

名前	説明	考えられるユースケース
静的コンテンツに対する Cookie のテストを無効にする	この拡張子を持つページに対する要求では Cookie をテストしません。 デフォルト: ;htm;html;ahtm;ahtml; chtm;chtml;fhtm;fhtml;mht; mhtm;mhtml;css;css1;js;	スキャン時間およびメモリー消費量を削減するために、その他のタイプのページ拡張子も対象から除外したい場合があります。その場合は、それらをセミコロンで区切って、除外する拡張子のリストに追加します。
ディレクトリーまたはページをテストしない	このオプションを使用すると、テスト・ステージ中の攻撃から特定のディレクトリーまたはページを除外する正規表現を定義できます。定義されたディレクトリーまたはページのみが除外され、サブディレクトリーまたはファイルは除外されないことに注意してください。 デフォルト: /wps/[^/]*/!ut/	特定のディレクトリーまたはページが脆弱でないことがわかっている場合や、特定のディレクトリーまたはページをテストするとサイトの安定性が損なわれる可能性がある場合は、それらのディレクトリーおよびページをこの正規表現で定義して、スキャン対象から除外できます。 フォルダーおよびそのすべてのサブフォルダーを除外する方法については、 66 ページの『「除外するパスおよびファイル」ビュー』を参照してください。
すべての応答からリンクを抽出	デフォルトで、AppScan は、テスト・ステージにおける新しいリンクの検索を、脆弱な応答内のみを対象として実行します。 デフォルト:False	AppScan がリンクを認識していない可能性があるか、範囲が十分ではないと考えられる場合は、この設定を有効にすることができます。ただし、これによって、スキャン時間が長くなり、ファイル・サイズが増えます。
すべての自動リンクを参照	デフォルトで、AppScan は、脆弱性が含まれている可能性がある自動リンク* のみを参照します。これらは、I フレーム、フレーム、およびリダイレクトです。すべて のタイプの自動リンクを参照するように AppScan を構成できます。 「無視する自動リンク」で定義されている正規表現に一致する要求は、この設定に関係なく、常に送信されない ことに注意してください。 デフォルト:False	他のタイプの自動リンク (スクリプトなど) の脆弱性がサイトに含まれていると考えられる場合は、この設定を有効にします。これにより、スキャン時間が長くなり、ファイル・サイズが増えます。
テスト後にログイン	テストを単一スレッドで送信して、セッション内を検証するか、各テスト後にログイン手順を送信します。 0 = False 1 = テストを単一スレッドで送信して、各テスト後にセッション内を検証します。セッション無効の場合、ログイン手順を送信します。 2 = テストを単一スレッドで送信して、各テスト後にログイン手順を送信します。 デフォルト:0	設定 1 または 2 は、重要セッションを使用するアプリケーションに必要な場合もありますが、セッションやメモリーの問題を回避するために、頻繁なログアウトを必要とします。その場合、スキャン時間がかなり長くなります。

名前	説明	考えられるユースケース
マルチステップ操作検証限界値	クロスサイト・スクリプティング・テストで検証されるマルチステップ操作シーケンスからの連続した要求の最大数。 デフォルト:0	
応答内で無視するパターン	この正規表現は、テスト応答の分析時に AppScan が無視する応答のセクションを定義します。 テストが成功したかどうかを判別するために応答を比較するときに、AppScan は、応答全体での変更率を測定します。応答が非常に長く、変更がごくわずかの場合、AppScan は差異を見逃し、脆弱性を認識しない可能性があります。 デフォルト: <input[^>]+(__VIEWSTATE|__ EVENTTARGET| __EVENTARGUMENT| __EVENTVALIDATION) [^>]+>	サイトが重要ではない長いセクションを含む応答を送信する場合は、それらのセクションをここに定義することによってスキャンの精度とパフォーマンスが向上する場合があります。
オリジナルの応答の間隔を更新する	テスト・ステージ中に (要求を再送信して) オリジナルの応答を更新するまでの間隔 (秒数)。 テスト応答がぜい弱性を示しているかどうかを AppScan が判別する方法の 1 つは、それを探査応答と比較する方法です。探査応答が、ここで設定された値より古い場合、テストを送信する前に探査要求が再送信されます。それにより、更新された探査応答を比較に使用できるようになります。これは、探査応答が時間によって変化する可能性が高く、テスト応答を古い探査応答と比較することで誤った結果になる可能性がある場合には重要です。 デフォルト:30 (秒)	ご使用のアプリケーションの応答がこの方法で古くて使用できないものになることがないことが明らかな場合は、この設定をゼロに変更してスキャン時間を削減することができます。探査ステージ要求が再送信されることはありません。
ポート・リスナー・テストの送信	デフォルトで、AppScan は、ポート・リスナー・テストを送信しません。これは、テストが失敗する可能性が高く、検証に長い時間がかかるためです。 デフォルト:False	ネットワークに外部サイトが含まれている場合は、そのサイトがローカル IP アドレスを認識できるように、このタイプのブラインド SQL 注入テストをアクティブにすることができます。

名前	説明	考えられるユースケース
類似性のしきい値	多くの場合 AppScan ではテストが成功したかどうかを確認するために、2 つの応答を比較して、それらが「類似」しているか「差異」があるかを判別します。その際、AppScan は各種アルゴリズムを使用して「類似性の割合」 (100% は 2 つの応答が同一であることを意味する) を割り当てます。 AppScan がテスト成果を判別する際、一部の例では「類似性の割合」が「類似性のしきい値」を上回るかどうかを基準にし、別の例では「類似性の割合」が「類似性のしきい値」を下回る かどうかを基準にします。いずれのしきい値も構成可能です。 多くのテストでは、デフォルトの「類似性のしきい値」は 95%、「差異しきい値」は 75% です。 これは、次のことを示しています。 • 成果が類似性 に依存するテスト結果では、「類似性の割合」が 95% 以上 の場合、2 つのページが類似していることを示します。 • 成果が差異 に依存するテスト結果では、「類似性の割合」が 75% 以下 の場合、2 つのページに差異があることを示します。 この設定に 1 から 100 の間の値 (%) を入力すると、すべてのテストの「類似性の割合」値はオーバーライドされます。 デフォルト: 0 (AppScan のしきい値を使用)	類似の応答にわずかな相違を生じさせる原因となる「動的」テキストがご使用のサイトにない場合は、このパーセンテージを大きくすることにより、誤検出結果が少なくなる場合があります。 **ヒント:** 「差異しきい値」を調整することが必要な場合があります (以下を参照)。
XSS: 反映されたプローブをすべてテスト	通常、特定のペイロード・テキストがサイトからの応答に複数含まれている場合、それらの脆弱性レベルはすべて同じであるため、AppScan はそれらのうちの 1 つだけをテストします。 デフォルト:False	単一の応答内でペイロード・テキストのすべての 出現箇所をテストする場合は、これを True に設定します。

* 自動リンク**:** ユーザーが対話することなく、ブラウザーによって自動的に送信される、Web ページ上のリンク。

SCAN ファイルの構造

AppScan Standard SCAN ファイルの基本的な構造について説明します。

AppScan Standard スキャンを保存する場合、そのデータは拡張子 SCAN が付いたファイルに保存されます。 このファイルは、以下のような複数のコンポーネントを含む ZIP アーカイブです。

RESULTSDB.FDB
データ・ビューに表示されているスキャン結果。

templateConfig.xml
スキャン・テンプレート (構成)。 このコンテンツは、同じ構成の AppScan Standard SCANT ファイルと同一です。

Manual_Explore_#.exd ファイル
マニュアル探査シーケンスの 1 つ以上の番号付きファイル。 これらは、他のスキャンにインポートできます。

スキャン・テンプレート

スキャン・テンプレートとは、再使用できるように保存された単なるスキャン構成 です。

- 「標準的なスキャン」テンプレートは、構成を全く変更しないでスキャンを実行する場合に使用できます (ただし、少なくともスキャンの開始 URL は設定する必要があります)。
- 特定のテスト・サイトまたは特定のタイプのサイトで AppScan をテストするように設計された、提供されている 『定義済みのテンプレート』 のいずれかを使用できます。
- 独自の具体的な要件に合わせて構成された、カスタム・ 146 ページの『ユーザー定義のスキャン・テンプレート』を作成できます。

スキャン・テンプレート を保存するときに、スキャンの構成定義を保存します (将来の使用のため)。スキャン を保存するときに、構成と スキャン結果の両方を保存します。

定義済みのテンプレート

このタスクについて

AppScan には、テスト・サイトで AppScan をテストするときに最善の結果を生成するように構成されている、いくつかの定義済みスキャン・テンプレートが付属しています。これらのテンプレートにより、スキャンを最適化するために多くの構成オプションを調整する必要を省くことができます。 (これらのテンプレートの更新は、時々実施される AppScan の更新に組み込まれている場合があります。)

- 定期的なスキャン
- 高速スキャン (短時間で有効な結果が得られるように構成されています)
- パラメーター・ベースの移動
- WebSphere Commerce
- WebSphere Portal
- demo.testfire.net (「Altoro Mutual Bank」Web サイトのスキャン用。このサイトはデモンストレーションの目的で作成されたものです)
- 実動サイト (稼働中の実動サイトで使用するように構成されています。詳細については、 342 ページの『ライブ実稼働環境のスキャン』を参照してください。)
- Hacme Bank
- WebGoat バージョン 5
- Worklight (IBM Worklight サーバー環境でのスキャン用)

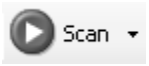
以下の表は、いくつかの定義済みテンプレートの基本構成詳細を示しています。

テスト・アプリケーション	パスの除外	パスの制限	探査方法*	大/小文字の区別	ログイン
WebGoat	.*attack?Num=.*	オフ	深さ優先	あり	ユーザー名: guest パスワード: guest
demo.testfire.net	なし	5	幅優先	なし	ユーザー名: jsmith パスワード: demo1234

* 探査方法 の詳細については、 72 ページの『「探査オプション」ビュー』を参照してください。

定義済みのテンプレートでスキャンするには、以下のようにします。

手順

1. テンプレートを以下のように選択します。
   - 「ようこそ」画面で、「定義済みのテンプレート」領域から 1 つを選択します。または
   - メイン画面で、 (または「ファイル」>「新規」) をクリックして、「定義済みのテンプレート」領域で必要なテンプレートを選択します。
2. 「名前を付けて保存」をクリックし、画面の名前を入力し、スキャンを保存します。
3. スキャンの開始 URL を定義します (48 ページの『「URL およびサーバー」ビュー』を参照)。
4. 該当する場合は、ログイン手順を記録するか、ユーザー名とパスワードを指定します (53 ページの『「ログイン」タブ』を参照)。
5. 

をクリックします

パラメーター・ベースの移動テンプレート

この定義済みのテンプレートの構成について説明します。

パラメーター・ベースの移動テンプレートには、このタイプのサイトをスキャンする際の課題に応じた以下のような設定が含まれています。

項目	場所	設定	コメント
冗長なパスの制限	探査オプション	500	必要に応じて、もっと増やすことができます。
深度限界	探査オプション	10	ASP.NET 2.0 ポストバック・リンクの処理を有効にします。
冗長性調整のデフォルト	パラメーターおよび Cookie	1 番目と 3 番目のチェック・ボックスが選択されています	
追加のパラメーター (Additional parameter)	パラメーターおよび Cookie	すべての「冗長性調整」チェック・ボックスが選択解除されています (トラッキングしない)	パラメーターは、次のような正規表現の形式になっています。 `.*(?i)(page|redirect|content|target|EVENTTARGET|EVENTARGUMENT|goto|node|action|ctrl|source.*` リストされていないナビゲーション・パラメーターがサイトで使用されている場合は、この正規表現を編集する必要があります。

以下も参照してください。

340 ページの『パラメーター・ベースの移動を使用するサイト』

341 ページの『パラメーター・ベースの移動を使用するサイトでの課題』

ユーザー定義のスキャン・テンプレート

スキャンを設定するときに、その構成を将来のスキャンで使用するためのテンプレートとして保存することができます。

このタスクについて

テンプレートを保存した後、スキャンを実行できます。または、終了したスキャンを将来のスキャンのためにテンプレートとして保存できます。また、関心のある結果を含むスキャンがある場合や、同じスキャンを開発および QA プロセス全体で再実行したい場合、スキャンをスキャン・テンプレートとして保存できます。

手順

1. 以下のいずれかを実行します。
   - 「スキャン構成ウィザード」を使用してスキャンを構成します。
   - 「スキャン構成」ダイアログ・ボックスを使用してスキャンを構成します。
   - テンプレートとして保存する構成の保存済みスキャンをロードします。
2. 「ファイル」メニューで、「名前を付けて保存」をクリックします。
3. 「名前を付けて保存」ダイアログ・ボックスで「**.scant**」ファイル・タイプを選択します。
4. テンプレートの識別しやすい名前を入力します。
5. 「保存」をクリックします。

スキャン・テンプレートのロード

このタスクについて

スキャン・テンプレートを保存した後は、それをロードし、テンプレートの定義済みスキャン構成に基づいてスキャンを実行したり、テンプレートを変更したりできます。

手順

1. 以下のいずれかを実行します。
   - SCAN ファイルまたは SCANT ファイルをそのフォルダーから AppScan インターフェースにドラッグ・アンド・ドロップします。

     Limitation: この機能は、ユーザーが管理者権限を持つ MS Windows 8 システムでは作動しません。
   - 「ファイル」>「新規」をクリックし、使用するテンプレートを選択して、「スキャン構成ウィザードの起動」チェック・ボックスを選択解除し、「**OK**」をクリックします。

   選択したスキャン・テンプレートの定義済み構成がロードされます。
2. スキャンを開始するには、以下のようにします。
   - 「スキャン」メニュー >「スキャンを開始」>「フル・スキャン/探査/テスト」をクリックします。
   - 「スキャンを開始」が使用不可の場合、「再スキャン」>「フル・スキャン/探査/テスト」をクリックします。

スキャン・テンプレートの編集

このタスクについて

スキャン・テンプレートは編集することができ、その変更はそのテンプレートに基づくすべてのスキャン用の永続変更となります。

デフォルトのスキャン・テンプレートでは永続的な編集はできません。デフォルトの構成を変更した場合、変更内容は次回のスキャンで使用されますが、デフォルトのスキャン・テンプレートには保持されません。

手順

1. スキャン・テンプレートを開きます (146 ページの『スキャン・テンプレートのロード』を参照してください)。
2. 構成設定に変更を加えます。
3. 以下のいずれかを実行します。
   - 「スキャン構成ウィザード」: このウィザードの最終ページで、「後でスキャンを開始します」を選択します。それから「ファイル」メニューで、「保存」または「名前を付けて保存」をクリックし、**scant** ファイル・タイプを選択します。
   - 「スキャン構成」ダイアログ・ボックス**:**「テンプレートとして保存」をクリックします。

スキャン中の構成の変更

スキャンを開始した後で構成を変更する場合、スキャンを再実行するか、または少なくともテスト・ステージを再実行して、変更の影響を調べる必要があります。一般に、以下のようになります。

- 探査構成を変更した場合、探査およびテスト (「スキャン」**>**「再スキャン」**>**「再スキャン **(**フル**)**」) を実行して、アプリケーションを完全に再スキャンする必要があります。
- テスト構成を変更した場合は、探査ステージを再度実行する必要はなく (探査ステージが完了している場合)、アプリケーションを再テストするだけで済みます (「スキャン」**>**「再スキャン」**>**「再テスト」)。

第 5 章 マニュアル探査

このセクションでは、スキャンのテスト・ステージを開始する前、あるいは自動スキャン (自動探査ステージと自動テスト・ステージの両方を含む) を開始する前に、アプリケーションまたはサービスを手動で探査する方法について説明します。

マニュアル探査は、AppScan がサイトをテストするときに自動探査ステージが行われていない可能性があるアプリケーションまたはサービスの一部が確実にカバーされるようにするために、ユーザーがサイトを探査して AppScanが使用できるデータを収集する場合に行います。これは、特定のユーザー入力が必要である、またはサイトが別のタイプのツールやデバイスに対してのみ応答するなどの理由で行われます。マニュアル探査は、AppScan を使用するか、AppScan を記録プロキシーとして使用するか、あるいは Generic Service Client (GSC) を使用して行うことができます。

一般に、以下のようになります。

AppScan
: サイトにサービスが含まれていない場合のマニュアル探査に使用されます。AppScan はユーザーのアクションおよび入力を記録し、スキャンのテスト・ステージ用のテストの作成に使用します。

記録プロキシーとしての **AppScan**
: 記録プロキシーとして構成された AppScan を使用して、ご使用のリモート・デバイス (携帯電話など) あるいは外部アプリケーション (モバイル・シミュレーターやエミュレーターなど) を使用して手動で探査を行いたい場合に使用します。ユース・ケースには、SOAP Web サービス、セキュリティー・エンベロープを含まない非 SOAP サービス、あるいは別のブラウザーが必要なアプリケーションなどがあります。要求は、記録プロキシーとして構成された AppScan を使用して、外部デバイスまたはアプリケーションからサイトに送信されます。これにより、AppScan が応答を記録し、その記録を使用してスキャンのテスト・ステージ用のテストを作成することが可能になります。

Generic Service Client (GSC)
: WSDL ファイルを持つ Web サービスの探査に使用されます。GSC は、サービスに要求を送信するための単純なインターフェースを作成します。応答は AppScan にインポートされ、スキャンのテスト・ステージ用のテストの作成に使用されます。

AppScan の使用

マニュアル探査を使用すると、実行中にフィールドおよびフォームを入力しながらアプリケーションの特定の部分を探査することができます。この方法を使用することで、サイトの特定のエリアが確実にカバーされ、AppScan では、すべてのフォームへの正しい入力に必要な情報を得ることができます。

AppScan ブラウザーが開き、アプリケーションを参照しながら、アクション、リンク、および入力データを記録できます。記録を停止すると、クロールしたリンクのリストが AppScan に表示され、サイトの自動探査または自動テストの実行時に使用できる関連フォームの入力データが表示されます。

マニュアル探査は、スキャンの自動探査ステージの前または後に実行でき、スキャンの自動探査ステージの代用として実行することもできます。

注**:** マニュアル探査で検出された URL は、自動探査で検出された URL と同様に、個別にテストされます。複数のリンクを特定の順序で クリックしなければアクセスできない URL を AppScan でテストする必要がある場合は、マルチステップ操作を記録する必要があります (98 ページの『「マルチステップ操作」ビュー』を参照)。

自動探査の前

自動探査の前にマニュアル探査を実行する理由としては、以下のようなものがあります。

- その都度データを手動で探査および入力することによって、フォームに入力するためのデータを AppScan に提供する手段としてマニュアル探査を使用したい。
- AppScan に、サイトの特定の重要な部分をテストさせたい。
- 特定のユーザー・プロセス (特定のシナリオを前提として、ユーザーがアクセスする URL、ファイル、およびパラメーター) をスキャンしたい場合は、このプロセスのみについてのマニュアル探査を作成することができます。このマニュアル探査は、スキャンが始まる前に実行してかまいません。
- アプリケーションで JavaScript または Java アプレットを使用しており、複数の状態 (対象の上でマウスを移動した状態やマウスを置いた状態など) が互いに特定の順序で遷移する場合にのみ、アプリケーションの特定の部分をこれら JavaScript または Java アプレットで検出する場合。これは、マルチステップ操作と同じではないことに注意してください。マルチステップ操作の場合、AppScan が特定の順序でリンクを移動する必要があるのに対し、この場合は、AppScan が一度リンクに到達すれば、他のリンクと同様に 1 つのステップでリンクをテストすることができます。

マニュアル探査の実行後、引き続き自動探査ステージ (「探査のみ」または「フル・スキャン」) に進み、スキャンでアプリケーション全体をカバーすることもできます。

自動探査の代用

以下のような場合は、自動探査の代用として マニュアル探査の実行を選択することができます。

- サイトのごく一部だけをスキャンする必要があり、テスト対象の部分をマニュアル探査によって定義したい場合。

  マニュアル探査の実行後、「テストのみ」をクリックしてスキャンを完了することができます。

自動探査の後

自動探査の後に マニュアル探査を実行する理由としては、以下の 2 つがあります。

- スキャンの結果、URL の一部が対話型 (216 ページの『ユーザーによる対話が必要』を参照) として分類された場合 (そのため、AppScan で必要なデータを自動入力できなかった場合)。データの自動入力を行うには、これらの URL を手動で探査します。

  注**:** この操作を行うと、「対話型 URL」のリストからこれらの URL が削除されます。
- サイトには SWF (Adobe Flash) ファイルが含まれています。AppScan はこれらのファイルが構成されている場合にそのテストを実行しますが (72 ページの『「探査オプション」ビュー』 を参照)、特定のファイルを見落としたことが判明した場合は、マニュアル探査を使用して、これらのファイルを AppScan 用に特定することができます。ムービー自体を探査する必要はありません。SWF ファイルをクリックしてマニュアル探査を終了し、自動探査を再実行するだけで操作が完了します。

マニュアル探査を記録する

手順

1. 「スキャン」**>**「マニュアル探査」**>**「ブラウザーの使用」をクリックします。

AppScan 組み込みブラウザーが開き、「記録」ボタン  が選択された状態 (グレイ表示された状態) になります。

注: デフォルト・ブラウザーが使用されています。デフォルト・ブラウザーには、IE または Chromium の 2 つの内、いずれかを設定することができます。また、「ツール」>「オプション」>「参照」タブで、サポートされている外部ブラウザーを設定することもできます。

2. サイトを手動で参照しながら、データを入力してリンクをクリックし、進みます。
3. 探査が終了したら、「一時停止」  をクリックするか、または単にブラウザーを閉じます。

注: アプリケーションの関連のない複数の部分を含む、マニュアル探査の記録を作成することができます。「一時停止」をクリックし、別の場所をブラウズします。次に、「記録」をクリックして記録を再開します。

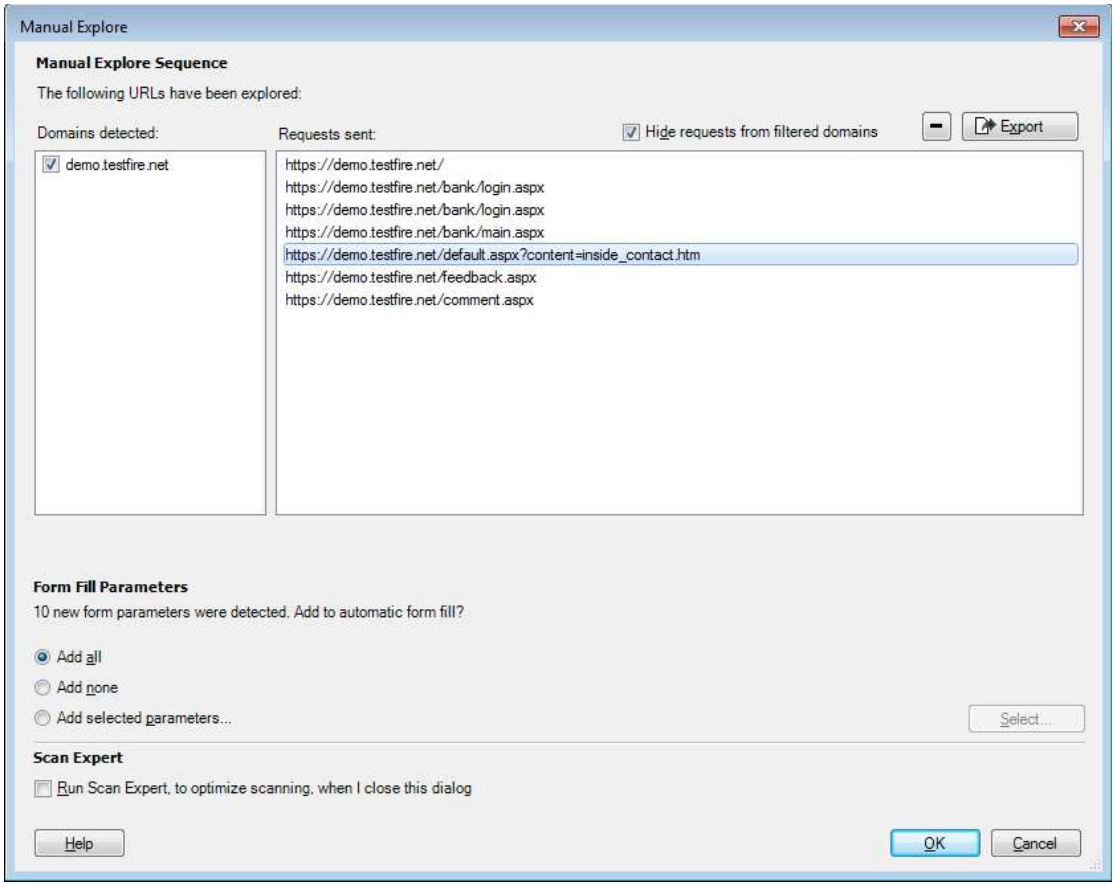
「探査済み **URL**」ダイアログ・ボックスが開き、ログイン中にアクセスした URL が表示されます。

ヒント: リンクを選択するか、  をクリックしてシーケンス内の不要なステップ (リンク) を削除できます。

マニュアル探査シーケンスの処理

シーケンスを確認、編集、およびエクスポートします。

このタスクについて



手順

1. リンクを選択するか、  をクリックしてシーケンス内の不要なステップ (リンク) を削除できます。
2. リストを検討します。

   実行されたマニュアル探査がサイトの標準手順である場合、今後のスキャンで使用するために、これを保存しておくことができます。詳しくは、 154 ページの『マニュアル探査データをエクスポートする』を参照してください。

   マニュアル探査中に HTML フォームを入力した場合、 AppScan は、どの情報を自動フォーム入力設定に追加できるか 決定します。該当する入力が見つかると、ダイアログ・ボックスの下半分にメッセージが表示され、ラジオ・ボタンが有効になります。

   `[n] new form parameters were detected. Add to Automatic Form Fill?`

   - 記録した入力のすべてを自動フォーム入力に追加する場合は、「すべてを追加 **(Add All)**」をクリックします。 入力はフォーム入力情報に自動的に追加されます。
   - 記録された入力を保存しない場合は、「追加なし」をクリックします。永久に保存されなくても、手動入力がすでに適用されています。

- 選択されたパラメーターと値のみを追加する場合は、 「選択したパラメーターの追加」をクリックし、続いて「選択」をクリックします。「自動検出されたフォームのパラメーターを追加 」ダイアログ・ボックスが表示されます (『自動的に検出されたフォームのパラメーターを追加する』を参照してください)。

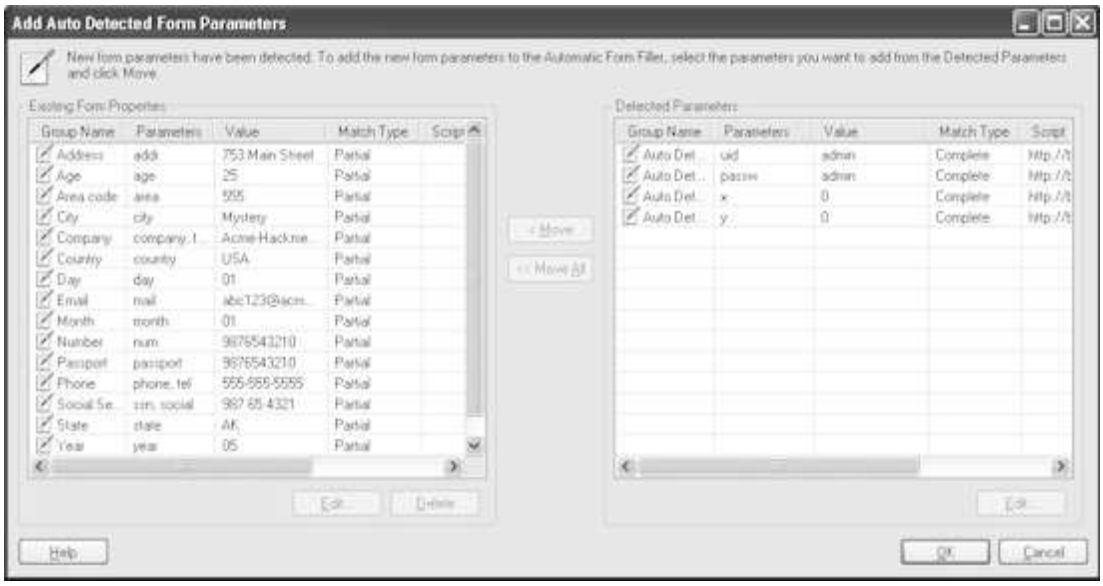
3. スキャン・エキスパート評価は、追加したリンクを使用して、構成中の脆弱性を明らかにすることができます。このダイアログ・ボックスが閉じるときにスキャン・エキスパートを実行するには、 「スキャン・エキスパート」チェック・ボックスを選択します。(詳しくは、 172 ページの『スキャン・エキスパート (Scan Expert)』を参照してください。)
4. 「**OK**」をクリックします。

   AppScan は、マニュアル探査のテスト要求を作成します。この処理には時間がかかる場合があります。

自動的に検出されたフォームのパラメーターを追加する

このタスクについて

「自動検出されたフォームのパラメーターを追加 」ダイアログ・ボックスにより、今後のスキャンで自動的に使用されるフォーム・プロパティーに追加する新しく検出されたフォームのパラメーターを 選択することができます。



手順

1. 「検出されたパラメーター」リスト (右のペイン) で 自動フォーム入力 (左のペイン) に追加する行を選択し、次に 「移動」をクリックするか、リスト内の任意のパラメーターを選択し、「すべて移動 」をクリックします。

   既存のフォーム・パラメーターに移動するパラメーターは、 これらの URL が今後スキャンされるときに有効となります。
2. 「**OK**」をクリックします。

   AppScanは、クロールした URL を分析し、この分析に基づいたテストを作成します。

マニュアル探査データをエクスポートする

標準手順をマニュアル探査の形式で「記録」し、その後、将来のスキャンに対してインポートすることができます。

このタスクについて

実行したマニュアル探査がサイトの標準手順である場合、データ (送信された要求および受信した応答) を保存して、将来のスキャンで使用することができます。データは探査データ・ファイル (.EXD) として XML 形式で保存され、必要なときにロードすることができます。これにより、毎回同じ手順を記録する手間を省くことができます。

手順

1. マニュアル探査を、前の手順の最初のステップと同様に記録します。
2. 「探査済み **URL**」ダイアログ・ボックスが表示されたら、「エクスポート」をクリックします。

   「名前を付けて保存」ダイアログ・ボックスが表示されます。
3. ファイルの名前を入力し、「**OK**」をクリックします。

   注**:** ファイルが保存されるデフォルトの場所を表示または変更するには、「オプション」>「設定」 を確認してください(277 ページの『「設定」タブ』を参照)。

次のタスク

関連タスク*:*

150 ページの『マニュアル探査を記録する』

『マニュアル探査データをインポートする』

戻る*:*

149 ページの『AppScan の使用』

マニュアル探査データをインポートする

標準手順をマニュアル探査の形式で保存した場合は、異なるサーバー上であっても、その手順を別のスキャンにインポートして再テストすることができます。

このタスクについて

新規スキャンの一部として使用するために、以前保存されたマニュアル探査手順をインポートすることができます。これは、再スキャンする必要がある標準手順の場合に役立ちます。この操作は、同じアプリケーションを別のサーバーでスキャンする場合でも実行できます (下記ステップ 3 の「注」を参照してください)。

サポートされているマニュアル探査ファイルのフォーマット:EXD、HAR、DAST.CONFIG、CONFIG。

手順

1. 「ファイル」>「インポート」>「探査データ」をクリックします。
2. 保存したマニュアル探査ファイル(EXD、HAR、DAST.CONFIGまたはCONFIG)をブラウズし、「開く」をクリックします。

「インポート」ダイアログ・ボックスが開きます。

3. デフォルトでは「応答と共にインポート」チェック・ボックスが選択されており、AppScan はサイトのテストを準備するときにこれらの応答を分析します。サイトがその応答に影響する方法で変更された場合、このチェック・ボックスをクリアすることで、AppScan が要求を再送信して最新の応答を収集するようにします。ただし、その場合は、「マニュアル探査」を再実行するほうがより効果的である可能性があります。

   注**:** 応答データを保存しないバージョンの AppScan にこのファイルが保存されていた場合、チェック・ボックスはクリアされ、グレー表示されています。「続行」を選択することで、要求をインポートしてサイトに送信し、新規 の応答を収集してテスト用に分析することができます。ただし、その場合は、「マニュアル探査」を再実行するほうがより効果的である可能性があります。

4. スキャンを開始するには、「続行」をクリックします。
   a. AppScan は、探査ステージ・データを分析して、ホスト競合がないかを確認します。

      ファイルが現行の構成に含まれていないホストをカバーしている場合、「探査データ・ファイル中での競合」ダイアログ・ボックスが表示されます。各ホストに対して適切な「アクション」を選択して、すべての競合を解決します。
      - 無視:このホストを探査しません。
      - テスト済みホストに追加:リストされたホストをスキャンのサーバーに追加します。
      - **<hostname>** と置換:スキャンで定義されている各ホストについて、競合するホストをスキャン構成にすでに含まれているホストで置換するためのオプションが用意されています。

        注**:** この機能によって、1 つのホストにおいてマニュアル探査を記録し、同じアプリケーションをホスティングする別のサーバーにおいて、このプロセスを再生することができます。例えば、ステージング・サーバーにおいてプロセスを記録し、実動サーバーにおいてこれを再生するために使用することができます。

   b. スキャンの開始:
      - インポートされたデータに応答が含まれている場合、テスト・ステージに備えてキャッシュ・データが分析されます。
      - インポートされたデータに応答が含まれていない 場合は、最初にフル探査ステージが実行され、その後にテスト・ステージ用のテストを作成するための応答の分析が実行されます。
   c. 探査ステージおよび分析が完了すると、スキャンが一時停止されます。
5. この時点で、ユーザーはオプションでマニュアル探査または自動探査を続行することができます。
6. スキャンのテスト・ステージを続行するには、「スキャン」>「続行」>「テスト」をクリックします。

次のタスク

関連タスク*:*

150 ページの『マニュアル探査を記録する』

154 ページの『マニュアル探査データをエクスポートする』

戻る*:*

149 ページの『AppScan の使用』

AppScan をプロキシー・サーバーとして使用する

プロキシー・サーバーとして機能するように AppScan を設定し、AppScan を介してサード・パーティーのブラウズ・ユーティリティー (ブラウザー、Web サービス・クライアント、自動探査スクリプト、携帯電話など) を使用して、アプリケーションを手動で探査することができます。この操作モードでは、AppScan は、自身を経由する HTTP/HTTPS トラフィック状況を記録し、その記録を分析し、適切なテストを作成します。

このタスクについて

注: プロキシー・サーバーとして AppScan を使用する探査は、SOAP Web サービスと非 SOAP Web サービスを探査する場合や、アプリケーション・クライアントが Internet Explorer と互換性がない場合に使用することができます。AppScan をプロキシーとして使用するように Web サービスを構成することで、AppScan は、Web サービスに対する要求を、そのクライアントが送信したものとして収集します。AppScan に付属の GSC (Generic Service Client) は、この目的で SOAP Web サービスで使用されます。 157 ページの『外部トラフィック・レコーダーを使用した探査』を参照してください。

注: AppScan ブラウザーがエラー・メッセージを生成し、一方ご使用の外部ブラウザーはエラー・メッセージを生成しない場合、 AppScan をプロキシーとして、外部ブラウザーから手動で表示するためにこの機能を使用することができます。(この状況が発生した場合は、AppScan サポート・チームにお問い合わせください。問題を解決できることがあります。)

手順

1. AppScan が Internet Explorer のプロキシー設定を使用するように 構成されていないことを確認します。「スキャン構成」>「接続ビュー」で、以下のいずれかを実行します。
   - 「プロキシーを使用しない」を選択します。
   - 「カスタムのプロキシー設定を使用」を選択し、プロキシー・アドレス、ポート、および認証情報を入力します。

   注: これを行わない場合、探査を開始すると設定は自動的に「プロキシーを使用しない」に変更されます。
2. AppScan リスニング・ポートを検索します。「ツール」>「オプション」>「記録プロキシー」タブを開きます (278 ページの『「記録プロキシー」タブ』を参照)。

   「プロキシー・ポート」エリアには、AppScan が Web アプリケーションに対するトラフィック状況を listen するために使用しているポートが示されます。これは、AppScan 自身に割り当てられているポート (検索しているポート番号はグレイになります) か、手動で選択したポートである可能性があります。
3. AppScan をご使用の Web ブラウザーのプロキシーとして使用するように、ブラウザーを構成します。

   ご使用のブラウザーで、プロキシー・サーバーを構成するセクションを検索します。ホスト名またはアドレスを、AppScan を実行しているマシンで使用されている IP アドレス (通常、localhost が受け入れ可能な項目です) に変更し、ポートを AppScan リスニング・ポートに変更します。
4. 次の手順で、ご使用のアプリケーションのマニュアル探査を実行します (完全な詳細については 149 ページの『AppScan の使用』を参照してください)。
   a. 「スキャン」>「マニュアル探査」をクリックして AppScan 内部ブラウザーを開きます。
   b. 内部ブラウザーを閉じずに、外部ブラウザーを開きます。
   c. アプリケーションを必要に応じて手動で探査します。

d. 外部ブラウザーを閉じます。
e. AppScan 内部ブラウザーを閉じます。

AppScan をプロキシーとして使用するご使用のブラウザーの構成

AppScan をプロキシーとして使用するようにブラウザーを構成する方法の例を示します。

手順

1. AppScan において、「ツール」>「オプション」>「スキャン・オプション」タブをクリックします。

   ポートを「自動」に設定し、**4744** とします。
2. **Microsoft Internet Explorer** >「ツール」>「インターネット オプション」 >「接続」タブ >「**LAN** の設定」を開き、「プロキシ サーバー」セクションのチェック・ボックスを選択します。

   「アドレス」および「ポート」テキスト・ボックスが有効になります。
3. Internet Explorer で、AppScan で検出された構成を入力します。

   アドレス: `localhost` および ポート: `47444744`

記録プロキシーとして AppScan を使用

AppScan の外部トラフィック・レコーダーを記録プロキシーとして使用する場合にこのオプションを選択します。携帯電話、シミュレーター、またはエミュレーターを使用し、RESTful あるいはその他の非SOAP Web サービス (またはセキュリティー・エンベロープを必要としないSOAP サービス) を手動で探査することができます。AppScan はそのトラフィック・レコーダーにドメインと要求を表示し、入力から適切なテストを作成します。

注**:** WSDL ファイルを持ち、SOAP セキュリティー・エンベロープを使用する Web サービスの場合、代わりに GSC を使用してサービスを探査する必要があります (詳しくは、 161 ページの『GSC の使用』を参照)。

注**:** アプリケーションが中間者保護を使用している場合、AppScan をプロキシーとして使用して、そのアプリケーションをスキャンすることはできません。

外部トラフィック・レコーダーを使用した探査

これは、非 SOAP Web サービス・スキャンの単純なワークフローの例です。

このタスクについて

このサンプル・ワークフローは、概念的な各ステップを個別に示しています。

注**:** 外部トラフィック・レコーダーの同じインスタンスを介して、複数のモバイル・デバイスから構成および要求を行うことができます。すべてのドメインおよび要求が一緒にリストされます。

手順

1. テンプレートの選択

   「ファイル」>「新規」をクリックし、テンプレートを選択します。
   - IBMWorklight開発者の場合:
     a. Worklight テンプレートを選択します。

b. Worklight アプリケーション・コードでアプリケーション認証(認証性)を使用している場合:Worklight サーバーで Worklight コンソールを開き、アプリケーション認証(認証性)が無効になっていることを確認します。有効の場合は、アプリケーションコードで無効にします。

- その他の環境の場合:「標準的なスキャン」テンプレートを使用します。

注: ご使用のマシンの Internet Explorer で AppScan をプロキシーとして使用するように構成されている場合、AppScan が Internet Explorer のプロキシー設定を使用するように構成されていないことを確認する必要があります。そのように構成されていると、ループが発生するためです。この競合を解決するには、「構成」>「通信およびプロキシー」タブで、他の 2 つのオプションのいずれかを選択します。

- プロキシーを使用しない
- カスタムのプロキシー設定を使用

これを行わずに外部トラフィック・レコーダーを使用してマニュアル探査を記録した場合、設定が自動的に「プロキシーを使用しない」に変更されます。チェック・ボックスが選択されているかどうかに関係なく、テスト・ステージの冗長性調整が使用されます。

2. ウィザードの「ようこそ」ダイアログ・ボックスで、外部デバイス/クライアント (AppScan を記録プロキシーとして使用) を選択し、「次へ」をクリックします。
3. ウィザードのステップに従います。
   a. 39 ページの『記録プロキシー』
   b. (オプション) 40 ページの『接続設定』
   c. 41 ページの『SSL 証明書』
   d. 41 ページの『ログイン管理』
   e. (オプション) 42 ページの『ログイン管理の詳細』
   f. 42 ページの『テスト・ポリシー』
   g. 43 ページの『完了』
4. 「外部トラフィック・レコーダー」が開き、「着信接続を待機中」状況が示されたら、ご使用のデバイス/アプリケーションから Web サービスのマニュアル探査を行います。
   a. デバイスまたはアプリケーションを使用して、Web サービスを探査します。

      探査を行うと、検出されたドメインがレコーダーの左側のペインにリストされ、URL が右側のペインにリストされます。
   b. 完了したら、AppScan で「記録の停止」をクリックします。
5. マニュアル探査データの確認および編集:

   検出されたドメイン
   : 要求が送信されたすべてのドメインがリストされ、「追加のサーバーおよびドメイン」(「構成」>「URL およびサーバー」>「追加のサーバーおよびドメイン」) のリストへの追加対象としてデフォルトで選択されています。これにより、それらのドメインをスキャンに組み込むことができます。スキャンに組み込みたくないドメインは選択解除することができます。

     ヒント: 他の企業に属しているドメインは選択解除することをお勧めします。

   送信された要求数
   : デバイスから選択された ドメインに送信されたすべての要求が、左側のペインにリストされます。左側のペインでドメインを選択/クリアすると、要求リストは更新されます。不要な場合は、特定の要求を削除することができます。

ヒント: フィルター済みの要求の総数が 200 を超えている場合、その一部を削除することで、スキャンをより効率的に行うことができます。

注: このステージでは、「エクスポート」をクリックして、他のマシンで使用できるように探査データを保存することができます。

6. 「OK」をクリックしてレコーダーを閉じます。

AppScan では、データの処理および表示には少し時間がかかります。

7. テスト・ステージを開始するには、「スキャン」>「テストのみ」をクリックします。

テスト・ステージが開始され、完了するとスキャン結果が表示されます。

関連トピック:

-
- 278 ページの『「記録プロキシー」タブ』
- 219 ページの『第 8 章 結果:セキュリティー問題』

外部ログイン・レコーダー

AppScan を記録プロキシーとして使用してマニュアル探査を行う場合、このレコーダーには、ログイン中に受信したトラフィックが表示され、ユーザーはそれを編集および承認してスキャン時のアプリケーションへのログインに使用することができます。

「構成」 > 「ログイン管理」 > 「記録を開始」 > 「外部デバイスの使用」をクリックすると「外部ログイン・レコーダー」が開き、ログイン手順の記録に使用されます。ここには、送信された要求が表示されます。

項目	説明
プロキシーの接続状況	着信接続が記録されているか、およびその他の状況メッセージが表示されます。
ポートでの listen	レコーダーに割り当てられている現行ポートを表示します。
記録プロキシー構成	「ツール」 > 「オプション」 > 「記録プロキシー」タブを開き、ポートあるいはその他の任意の記録プロキシー構成を変更します (詳しくは、 278 ページの『「記録プロキシー」タブ』 を参照)。
送信されたログイン要求	マニュアル探査中に記録されたすべての要求を表示します。左側のペインで選択されたドメインからの要求は黒色で表示され、その他はグレー表示されます。
記録の停止	着信要求の記録を停止しますが、ダイアログ・ボックスは開いたままで、ログイン手順の確認および編集を行うことができます。 スキャンに関係ない個別の要求をリストから削除するには、その要求を選択し、 をクリックします。
OK	レコーダーを閉じます。

完全なワークフローについては、 157 ページの『外部トラフィック・レコーダーを使用した探査』を参照してください。

以下も参照してください。

- 278 ページの『「記録プロキシー」タブ』
- 85 ページの『冗長性調整』

外部トラフィック・レコーダー

AppScan を記録プロキシーとして使用してマニュアル探査を行う場合、このレコーダーには、検出されたドメインと受信したトラフィックが表示され、ユーザーがテスト対象を制御することができます。制限付きバージョンのレコーダーは、ログイン手順を記録するのに使用されます。

「マニュアル探査」 > 「外部デバイスの使用」をクリックすると、「外部トラフィック・レコーダー」が開きます。

項目	説明
プロキシーの接続状況	着信接続が記録されているか、およびその他の状況メッセージが表示されます。
ポートでの listen	レコーダーに割り当てられている現行ポートを表示します。 ポートあるいはその他の記録プロキシー構成を変更するには、「記録プロキシー構成」をクリックします (詳しくは、 278 ページの『「記録プロキシー」タブ』を参照)。
記録されたトラフィック	
検出されたドメイン (左側のペイン)	記録されたトラフィック内で検出されたすべてのドメインのリスト。 スキャンに組み込む必要があるドメインを選択します。レコーダーを閉じると、選択したすべてのドメインが「追加のサーバーおよびドメイン」リスト (「構成」 > 「URL およびサーバー」 > 「追加のサーバーおよびドメイン」) に追加され、スキャンに組み込まれます。
送信された要求 (右側のペイン)	マニュアル探査中に記録されたすべての要求を表示します。左側のペインで選択されたドメインからの要求は黒色で表示され、その他はグレー表示されます。 • 選択されたドメインからの要求のみ を表示するには、「フィルター済みドメインからの要求を非表示にする」チェック・ボックスをクリックします。 • スキャンに関係ない個別の要求をリストから削除するには、その要求を選択し、 - をクリックします。
エクスポート	クリックすると記録がエクスポートされ、別のマシンで使用することができます。このボタンは、記録が停止された後にのみアクティブになります。
探査ステージの冗長性調整	(デフォルトで選択済み) 選択されている場合、探査ステージの冗長性調整 (「構成」 > 「パラメータおよび Cookie」タブ > 「冗長性調整のデフォルト」 > 「探査」) は、ダイアログ・ボックスを閉じると現行の記録に適用され、重複する要求を回避することができます。 チェック・ボックスは、選択するとマニュアル探査からの Cookie が失われる場合にのみクリアしてください。
記録の停止	リストを表示および編集するために、ダイアログ・ボックスを開いたまま記録を停止します。 **注:** 記録を停止すると、現行データを破棄しなければ記録を再開することはできません。
OK	ダイアログ・ボックスを閉じ、現在選択されているすべてのドメインを、スキャンに組み込む「追加のサーバーおよびドメイン」のリストに追加します (「構成」> 「URL およびサーバー」 > 「追加のサーバーおよびドメイン」)。

ワークフローについては、 157 ページの『外部トラフィック・レコーダーを使用した探査』を参照してください。

以下も参照してください。

- 278 ページの『「記録プロキシー」タブ』

- 85 ページの『冗長性調整』

GSC の使用

Generic Service Client (GSC) は、ご使用の Web サービスの WSDL ファイルを使用して、単純なインターフェースで使用可能なサービスを表示し、ユーザーによるパラメーターの入力や結果の表示を可能にします。GSC インターフェースを使用して Web サービスを手動で探査することで、AppScan は、ユーザーの入力を使用して適切なテストを作成することが可能になります。

注**:** GSC は、WSDL ファイルで定義されている Web サービスの探査に使用されます。ただし、ご使用のサービスに WSDL ファイルがないか、サービスが SOAP セキュリティー・エンベロープを使用しない場合、あるいはステージの探査に使用したい独自のアプリケーションを持っている場合は、代わりにモバイル・デバイス、エミュレーター、またはシミュレーターと、記録プロキシーとして構成されている AppScan の組み込み外部トラフィック・レコーダーを使用することができます (詳しくは、 157 ページの『記録プロキシーとして AppScan を使用』を参照)。

いくつかのパラメーターをサービスに送信して応答を受信し、GSC を閉じたら、「テストのみ実行 **(Run Tests Only)**」をクリックして、入力に基づいた自動スキャンを開始します。(探査ステージは GSC を使用したマニュアル探査中に完了するため、このスキャンは実際にはテスト・ステージのみです。)

クライアント側の証明書なしで SSL を使用する場合、(AppScan 8.0 に付属しているバージョンの GSC を使用するのであれば) GSC を特別に構成する必要はありません。CCS の場合の構成の詳細については、GSC インフォメーション・センターを参照してください。GSC インフォメーション・センターにはメイン GSC ツールバーからアクセスすることができます。

注**:** AppScan GSC が開いている間は は開いたままですが、GSC が閉じられるまで機能しません。

注**:** GSC ヘルプ・ファイルで説明されているいくつかの機能は、AppScan を通じて使用している場合には適用されないことがあります。

GSC を使用した探査

これは、SOAP Web サービス・スキャンの単純なワークフローの例です。

始める前に

テストを Web サービスに送信するには、GSC がシステムにインストールされている必要があります。インストールするかどうかは、AppScan のインストール中に尋ねられています。そのときに GSC をインストールしていない場合は、メインの AppScan フォルダー内にある GSC_Setup.exe ファイルをクリックすれば、いつでもインストールを実行できます。

手順

1. 「スキャン構成」ダイアログ・ボックスの「URL およびサーバー」ビューを開き、「開始 URL」フィールドで以下のいずれかを追加します。
   - WSDL ファイルの URL
   - ローカル・ネットワーク上の WSDL ファイルへのパス (次の形式):

     ```
     file////c:/mywsdlfile.wsdl
     ```

制約事項**:** WSDL ファイルがローカルで提供されている場合、GSC はファイルからドメイン・ネームを取り出すことができません。したがって、2 つ目のオプションを選択する場合は、「追加のサーバーおよびドメイン」エリアでドメイン・ネームと一緒に GSC を指定する必要があります。以下に例を示します。 `demo.testfire.net`

2. 該当する場合は、「大文字と小文字を区別する (Case Sensitive)」チェック・ボックスを選択します。
3. 「**OK**」をクリックして、「スキャン構成」ダイアログ・ボックスを閉じます。
4. 「スキャン」**>**「**Web** サービスの探査」をクリックします。

   GSC が開き、Web サービスのツリーが左ペインに表示されます。 (ツリーを展開して個々の Web サービスを表示するには、  アイコンをクリックします。)
5. 以下のようにして、サービスを探査します。
   a. ツリー内のサービスをクリックして選択します。 要求をサービスに送信するためのインターフェースが、右ペインに表示されます。
   b. 右ペインの「メッセージ (Message)」タブで、送信する値を入力します。
   c. 「起動」をクリックして、要求を送信します。

      メイン・ペインに結果が表示され、要求が、画面の左下の「呼び出しヒストリー」ペインに追加されます。
   d. 必要に応じてさらに他のサービスに対してこれを繰り返します。
6. 要求を十分に送信したら、GSC を閉じます。

   GSC が閉じ、データに基づいてテストが作成されます。
7. スキャンを開始するには、「スキャン」**>**「テストのみ」をクリックします。

タスクの結果

スキャンが完了すると、結果が表示されます。

例

219 ページの『第 8 章 結果:セキュリティー問題』 を参照してください。

SOAP Web サービスがサイトの一部 として組み込まれているサイトをスキャンする

サイトに Web サービスと、スキャンする必要があるその他のページの両方が含まれている場合は、この手順を使用します。

このタスクについて

サイトに、Web サービスと、スキャンする必要があるその他のページの両方が含まれている場合は、GSC を使用して手動で Web サービスを探査する必要がありますが、その後は AppScan にサイトの残りの部分を自動的に探査させて、サイト全体 をテストすることができます。この場合は、Web サービス WSDL ファイルの URL および、サイトを探査するための開始 URL の両方を AppScan に提供する必要があります。

手順

1. 「スキャン」>「スキャン構成」>「**URL** およびサーバー」をクリックし、「開始 **URL**」フィールドで、Web サービスの WSDL ファイルの URL を入力します。
2. 「追加のサーバーおよびドメイン」領域で、  をクリックして、アプリケーションをスキャンするための開始 URL を入力します。
3. 「**Web** サービスの探査」をクリックします。

   GSC が開きます。
4. 要求をサービスに送信し、GSC を閉じます。
5. 「スキャン」>「フル・スキャン」をクリックします。

   AppScan はアプリケーションを探査し、それからサイト全体をテストして、結果を提示します。

   以下も参照してください。

   219 ページの『第 8 章 結果:セキュリティー問題』

第 6 章 スキャン中

スキャンの開始方法、スキャン中に何が行われるか、探査ステージの手動による操作方法、スキャン結果のエクスポート方法について説明します。

スキャンを開始する

注: スキャン・エキスパートが構成されていると、スキャンの開始時に、メイン・スキャンの前にこれが実行されます。構成内容を評価し、メイン・スキャンを最適化するための変更点を提案します。詳しくは、172 ページの『スキャン・エキスパート (Scan Expert)』 を参照してください。

「スキャン構成ウィザード」からスキャンを開始する

このタスクについて

「スキャン構成ウィザード」(31 ページの『スキャン構成ウィザード』を参照してください) を使用してスキャンを作成する場合、ウィザードの最終ステップで、スキャンを開始するオプションが提供されます。

手順

オプション (下記の表を参照してください) を選択し、「終了」をクリックします。

オプション	クリックで実行される機能
自動フル・スキャンを開始	ウィザードで作成したばかりの構成を使用して、スキャンを開始します。スキャンは自動探査で開始され、テスト・ステージに自動的に進みます。
自動探査のみを開始	スキャンの自動探査ステージを開始しますが、自動的にテスト・ステージには進みません。
マニュアル探査を開始	ブラウザーを開いてアプリケーションを手動で探査します (149 ページの『AppScan の使用』を参照してください)。
後でスキャンを開始します	スキャンを開始せずにウィザードを閉じます (例えば、スキャン構成をさらに編集してからスキャンを開始したい場合、またはスキャンを後ほど開始したい場合があります)。
「スキャン構成ウィザード」が完了したらスキャンを開始	スキャン・エキスパートがご使用の構成を分析し、スキャンの効率を向上させるために、構成の変更を提案します。 (詳細については、 172 ページの『スキャン・エキスパート (Scan Expert)』を参照してください。) このオプションを選択すると、ウィザードを閉じるとすぐにスキャン・エキスパートが実行されます。

「スキャン」メニューまたはツールバーからスキャンを開始する

このタスクについて

AppScan が開いていると、「スキャン」メニューまたはツールバーから現在の構成を使用してスキャンを開始することができます。

手順

「スキャン」メニューで、またはツールバーの  ボタンから、以下のいずれかを選択します。

構成にマニュアル探査データも自動探査データも含まれていない 場合

アイコン	オプション	説明
	フル・スキャン	フルスキャンを実行します。認識されていない URL がなくなるまでアプリケーションを探査し、続いてテスト・ステージを自動的に続行します。 (マルチフェーズ・スキャンが構成されている場合は、必要に応じてマルチフェーズを完了させます。)
	探査のみ	サイトを探査しますが、テストは実行しません。これによって、探査結果を調査し、テスト・ステージに進む前に、必要に応じて手動でサイトを探査できます。
	テストのみ	(テストする探査データがない場合、このオプションは使用不可になっています。)

構成にマニュアル探査データまたは自動探査データが含まれている場合

アイコン	オプション	説明
	フルスキャンを継続	既存の自動探査データおよびマニュアル探査データを含め、この構成を使用してサイトの探査とテストを行います。
	探査のみを継続	サイトを自動的に探査して、既存の自動探査データおよびマニュアル探査データにデータを追加します。これによって、探査結果を調査し、テスト・ステージに進む前に、必要に応じて手動でサイトを探査できます。
	テストのみを継続	既存の自動探査データおよびマニュアル探査データを使用して、サイトのテストのみを行います。

注**:** 1 つ以上のマルチステップ操作が構成済みで、この操作がスキャン対象のサイトの重要なサブセットを構成している場合、この操作のシーケンスに対してのみスキャンを実行することができます (205 ページの『マルチステップ操作のみをスキャン』を参照してください)。

「ようこそ」ダイアログ・ボックスからスキャンを開始する

AppScan が開始されると、 「ようこそ」ダイアログ・ボックスが表示されます。

注**:** 「ようこそ」ダイアログ・ボックスが開始時に表示されない場合は、 280 ページの『「全般」タブ』を参照して、 「ようこそ」ダイアログ・ボックスを再表示させる方法を確認してください。

以下の項目を実行できます。

- 『新規スキャンの作成』 または
- 167 ページの『既存スキャンのロード』

新規スキャンの作成

手順

1. 「新規スキャンの作成」を選択します。
2. 以下のいずれかを実行します。

- 定義済みの構成のいずれかを使用してスキャンを実行する場合、「スキャン構成ウィザードの起動」チェック・ボックスを選択します。(171 ページの『自動スキャン』を参照してください。)
- スキャンを開始する前に構成を変更したい場合、「スキャン構成ウィザードの起動」チェック・ボックスをクリア します。(31 ページの『スキャン構成ウィザード』を参照してください。)

3. スキャン・テンプレートをクリックします。特定のテンプレートが必要ない場合は、「標準的なスキャン」を選択します。

既存スキャンのロード

手順

1. 「既存のスキャンを開く」を選択します。
2. リストから保存済みスキャンを選択するか、「参照」をクリックしてリストにない保存済みスキャンを開きます。
3. 「**OK**」をクリックします。

「新規スキャン」ダイアログ・ボックスからスキャンを開始する

「新規スキャン」ダイアログ・ボックスは、(「ファイル」>「新規」) でいつでも開くことができます。このボックスにより、「スキャン構成ウィザード」を開くか、ただちにフル・スキャンを実行できるスキャン・テンプレートを選択します。

スキャン構成ウィザードを起動するには、以下のようにします。

1. 必要に応じて、「スキャン構成ウィザードの起動」チェック・ボックスの選択またはクリアを確認します。
2. 「定義済みのテンプレート」リストで、必要なテンプレートをクリックします。特定の テンプレートが必要ない場合は、「標準的なスキャン」をクリックします。

   注**:** 保存したテンプレートを使用するには、「参照」をクリックし、必要な SCANT ファイルを参照して「オープン」をクリックします。

スキャンの進行状況

スキャンが開始されると、結果リストの下に「進行状況パネル」が表示されます。

このパネルには、以下が表示されます。

- 探査またはテストされている Current URL。
- 探査ステージまたはテスト・ステージの完了率。
- これが後続のスキャン・フェーズである場合、現在のフェーズ番号 (172 ページの『自動マルチフェーズ・スキャン』を参照してください)。
- スキャンが始まってから経過した時間 (mm:ss、hh:mm:ss、または dd:hh:mm:ss 形式)。

通信上の問題または要求によってスキャンが停止すると、「進行状況」パネルの代わりに「スキャン通知」パネルが表示されます。

「スキャン通知パネル」には以下の項目が表示されます。

- 自動再開の前の通信上の問題とタイムアウト。
- スキャンが未完了であるという通知。
- 今までのスキャンの実行内容と、その続行方法を説明したダイアログ・ボックスを開く「詳細情報」リンク。

スキャンの一時停止と続行

スキャンはいつでも一時停止することができます。また、後で再開することができます。接続上の問題でスキャンが一時停止していた場合は、この問題が解決されてからスキャンを続行することができます。

注: スキャンを一時停止しても、実際に停止する前にしばらく続行する場合があります。

1. スキャンを一時停止するには、ツールバーの「一時停止」ボタン をクリックします (または「スキャン」>「一時停止」をクリックします)。

   「通知パネル **(Notice Panel)**」が表示され、「**スキャン未完了**」と表示されます。

2. 一時停止されたスキャンを継続するには、ツールバーの「スキャン」ボタン をクリックして、以下のいずれかのオプションを選択します。

   - フル・スキャン: フル・スキャンを再開します。(認識されていない URL がなくなるまで探査ステージを続行し、続いてテスト・ステージを自動的に続行します。マルチフェーズ・スキャンが構成されている場合は、必要に応じてマルチフェーズを完了させます。)
   - 探査のみ: 探査ステージを再開してこれを完了しますが、テスト・ステージは続行しません。
   - テストのみ: テスト・ステージを再開しますが、スキャンが一時停止したときに探査されておらず、認識されていない URL は、いずれも無視されます。

接続上の問題で停止したスキャン

接続上の問題が、AppScan とスキャン中のサーバー、または AppScan とローカル Web プロキシー・サーバーとの間で発生したために、スキャンが停止する場合があります。

接続上の問題が検出されると、90 秒のカウントダウンが始まり、その間 AppScan はこの問題が解決するまで待機します。カウントダウン中にこの問題が解決すると、「スキャン通知」パネルが閉じてスキャンが再開されます。

通信上の問題がある場合、「通知パネル **(Notice panel)**」に、以下のメッセージが表示されます。

```
Trying to connect to: <IP> Explore/Test stops in <n>
```

- ここで示される IP アドレスは、スキャンされているサーバーの IP、プロキシーの IP (接続上の問題が Web プロキシーに関するものである場合)、または、スキャンが複数のサーバーに接続していて、そのうちの複数がダウンしている場合には、IP のリストとなります。
- 数値 <n> は 90 秒のカウントダウンです。
- カウントダウンがゼロに達するまで問題が解決しない場合、スキャンは停止します。

- 問題が解決すると、スキャンが一時停止していたところから続行 (「スキャン」>「続行」) するか、またはスキャンを再実行 (「スキャン」>「再スキャン」) することができます。

アプリケーションの問題で停止したスキャン

このタスクについて

スキャンが停止して、「通知 **(Notice)**」パネルに「詳細情報」のリンクが表示されることがあります。

手順

1. 「詳細情報」をクリックします。

   次に実行する指示が含まれたメッセージ・ボックスが表示されます。この指示には、対話型 URL のリスト、または NTLM 認証がないために発生するリンク切れのリストを検索する方法が記述されています。スキャンがこれらのいずれかを検出し、それを自動的に解決することができない場合、「詳細情報」メッセージ・ボックスに、問題が要約されます。
2. 必要に応じて、以下の手順を使用します。
   - 『対話型 URL の処理』
   - 『失敗した要求の処理』

対話型 URL の処理

ユーザーによる対話が必要なスキャン URL に組み込む方法。

このタスクについて

入力フォームの中に自動で入力ができなかったものがあるためにスキャンが停止した場合は、手動で探査を完了することができます。

手順

1. 「アプリケーション・データ」ビューを選択します。
2. 「ユーザーによる対話が必要」表示を選択します。
3. これらの URL のマニュアル探査を作成 (216 ページの『対話型 URL の手動による探査』を参照してください) し、 フォーム入力値を挿入します。
4. スキャンを続行します。できれば、別の自動探査ステージを使用してください。

失敗した要求の処理

NTLM 認証がないために失敗した要求を処理する方法。

このタスクについて

スキャン中に NTLM 認証がないためにリンク切れが発生すると、スキャンは停止します。

手順

1. 「アプリケーション・データ」ビューを選択します。
2. 「失敗した要求」表示を選択します。
3. 「スキャン構成」ダイアログ・ボックス >「ログイン/ログアウト」で、ご使用のプラットフォーム認証の詳細を入力します。
4. 探査ステージの再実行でスキャンを続行します。

スキャンの保存とロード

スキャンを保存するときに、スキャン構成と、AppScan が (探査ステージとテスト・ステージの両方で) これまでに収集したデータすべてが .SCAN ファイルとして保存されます。

スキャンの保存後、.SCAN ファイルをロードして、スキャンを再開したり再実行することができます。

スキャンを保存する

このタスクについて

終了または一時停止、あるいは外部要因により停止したいずれのスキャンも保存することができます。

手順

「ファイル」>「保存」をクリックします (または **[Ctrl] + S** を押します)。

注**:** スキャンが保存されるデフォルトのフォルダーを表示または変更するには、「ツール」>「オプション」>「設定」をクリックします。詳しくは、 277 ページの『「設定」タブ』を参照してください。

自動スキャン保存

このタスクについて

スキャン中にデータを .SCAN ファイルに自動的に保存するように、AppScan を 設定することができます。このオプションが選択されると、AppScan は、スキャン中に周期的 (定義した間隔で) および特定のマイルストーンの両方の方法で保存を行います。

手順

「ツール」>「オプション」>「スキャン・オプション」タブ をクリックして「スキャン中に自動的に保存」チェック・ボックスを選択します。保存の間隔を調整することもできます。
実行中のスキャンは、選択した間隔で保存されます。以下の時点でも保存が行われます。

- スキャンの任意の部分を開始または続行した時点
- 探査ステージが終了した時点
- テスト・ステージが終了した時点

新規スキャンが開始され、自動保存が有効になると、自動保存がオンになっているため、スキャンを保存する必要があると通知するメッセージが表示されます。

- 「はい」をクリックすると、スキャンを保存するための「名前を付けて保存」ダイアログ・ボックス が開きます。
- 「いいえ」をクリックすると、現在のスキャンのみについて「スキャン中に自動的に保存」機能を 無効にします。
- 「無効」をクリックすると、このスキャンと今後のスキャンについて、「スキャン中に自動的に保存」機能を無効にします。

保存済みスキャンをロードする

手順

「ファイル」>「開く」をクリックしてスキャンを選択します。
「ロード中」進行状況表示バーがしばらく開き、続いてスキャンが前回保存されたときに探査またはテストされた状態で、スキャンの 「アプリケーション・ツリー」がメイン・ウィンドウに表示されます。

レガシー・スキャン・テンプレートのインポート

8.6 より前のバージョンの AppScan に保存されているスキャンからスキャン・テンプレートをインポートする方法。

AppScan バージョン 8.6 でスキャン・ファイルのフォーマットが再設計されたので、旧バージョンで保存されているスキャンを現行バージョンで開くことはできません。必要に応じて、新規スキャンで使用するためにテンプレートをインポートできます。

スキャン・テンプレートをインポートするには、以下のようにします。

1. スキャン・ファイルの拡張子を SCAN から ZIP に変更します
2. ZIP ファイルを開き、`templateconfig.xml` を見つけて抽出します
3. その拡張子を XML から SCANT に変更します
4. AppScan で開きます。

自動スキャン

完全自動スキャンは、1 サイクル以上の探査ステージと、その後のテスト・ステージから構成されます。

172 ページの『自動マルチフェーズ・スキャン』

探査ステージ

完全自動スキャンが始まると、まず探査ステージが開始されます。このステージ中、AppScan では以下を実行します。

- アプリケーションについて、スキャン構成 (48 ページの『「URL およびサーバー」ビュー』を参照してください) で指定した開始 URL からアプリケーションで除外されていないすべての URL まで、ユーザーがクロールするようにクロールを行います。

  注: スキャン構成によって、 探査ステージをフィルターに掛ける (66 ページの『「除外するパスおよびファイル」ビュー』を参照してください) ことが できます。特定のパスを除外する、または固有の探査制限を設定すると、これらのフィルターが探査ステージに適用されます。
- アプリケーションにおける URL の階層モデルである「アプリケーション・ツリー」 を構築します。
- 探査済み URL を分析し、テストを生成します。

テスト・ステージ (Test stage)

テスト・ステージ中に AppScan では以下を実行します。

- アプリケーションにログインします。
- URL に対して予備的なテストを実施します。これは結果の解釈に役立ちます。
- 脆弱性を明らかにする目的で設計された要求を送信することにより URL をテストします。
- 各要求に対する応答を記録します。

- テスト結果を提供します。

テスト・ステージ中に、「結果リスト」の「セキュリティー問題」ビューにスキャンの結果が表示されます。

自動マルチフェーズ・スキャン

このタスクについて

一部のテストでは、Web サイトを通常にブラウズしていてはアクセスできない新領域の Web アプリケーション (ディレクトリー・リストや robots.txt ファイルの内容など) が明らかになることがあります。マルチフェーズ・スキャンが有効であると、AppScan は、テスト・ステージ中に見つかった URL を探査対象の URL のリストに追加します。テスト・ステージが完了すると、AppScan は次に新規に見つかった URL を自動的に探査して、これらについて新しいテストを作成し、そのテストを実施します。

デフォルトでは、スキャンには (必要な場合) フェーズを 4 個まで含めることができます。 1 個から 10 個のフェーズ間で実行できるように、AppScan を構成することができます。

注**:** マルチフェーズ・スキャン設定は、フル・スキャンが実行されている場合のみ適用されます。「探査のみ」および「テストのみ」機能を有効にすると、結果は単一フェーズ・スキャンとなります。

手順

1. 「スキャン構成」**>**「テスト・オプション」ビューを開きます。
2. 「マルチフェーズ・スキャンを有効にする **(Enable Multiphase Scanning)**」チェック・ボックスを選択します。
3. 「最大フェーズ数 **(Max. Phases)**」テキスト・ボックスで、許可するフェーズの最大数 (**1** から **10** までの数値で、デフォルトは **4** です) を入力します。

   AppScan がサイトをテストすると、当初の探査ステージではアクセスできなかった追加の URL に対するテスト応答が分析されます。続いて、これらの新規リンクについて、追加の探査ステージとテスト・ステージが実行されます。ここで入力した数値は、AppScan がこの動作を実行する回数を決定します。(デフォルトでは、マルチフェーズ・スキャンは 4 フェーズで有効です。)

   注**:** 「進行状況」パネル (167 ページの『スキャンの進行状況』を参照してください) には、 スキャンが現在処理中のフェーズが示されます。

   注**:** ご使用のアプリケーションを再スキャンする (「スキャン」**>**「再スキャン」) 場合、フェーズ番号は 1 から再開します。

   注**:** スキャンを保存すると、現在のフェーズ番号が保存されます。このスキャンを後からロードしてスキャンを再度実行すると、保存されたフェーズ番号からスキャンが開始されます。

スキャン・エキスパート (Scan Expert)

スキャン・エキスパートは、ご使用のアプリケーションとネットワークの動作を探査して、スキャン構成の効率を評価する機能です。スキャン・エキスパートの結果に基づき、より厳密なスキャンにするために必要な構成への変更を推奨することができます。

スキャン・エキスパートはご使用のアプリケーションに接続し、このアプリケーションに関して簡単な探査ステージを実行します。このステージ中、「スキャン・パネル」には進行状況が表示され、アプリケーショ

ン・ツリーには、通常のスキャン中と全く同様に、探査されたアプリケーションの部分が表示されます。「スキャン・エキスパート」ペインも同時に開きます (このスキャンが通常のスキャンでないことを示します)。

スキャン・エキスパートの使用手順は以下のとおりです。

- スキャン・エキスパートは、フルスキャンの前に自動的に実行されるように構成できます。構成方法によって、スキャン・エキスパートは次のように動作します。
  - 推奨が提示されます。これを了承するか、または手動で拒否します。あるいは、
  - 自動で有効になっている推奨を自動的に適用し (すべての推奨が自動で有効になっているわけではありません)、スキャンに進みます。

  (詳しくは、 122 ページの『「スキャン・エキスパート」ビュー』を参照してください。スキャン開始時のスキャン・エキスパートの自動実行を有効または無効にするには、「ツール」>「オプション...」>「設定」を選択します。)
- スキャン・エキスパートを単独で随時実行し、ご使用の構成を評価します。
  - スキャン・エキスパートがアプリケーションに対して簡単な探査ステージを実行し、応答を分析して構成を評価するようにするには、「スキャン」>「スキャン・エキスパート評価の実行」をクリックします。
  - アプリケーションをすでに探査済みの場合、スキャン・エキスパートによる探査ステージを実行せずに、既存の データの分析を実行することによって、時間を節約することができます。「スキャン」>「スキャン・エキスパート分析のみ実行」をクリックします。
- スキャンを開始しようとしたときに、構成の重大な問題が AppScan によって検出された場合、問題の解決を図るために、スキャン・エキスパートがたとえ自動的に実行されるように構成されていない場合でも実行されることがあります。

スキャン・エキスパート推奨

スキャン・エキスパートの探査ステージが完了すると、受信した応答が分析され、構成への変更が推奨されます。スキャン・エキスパートをどのように構成しているかにより (122 ページの『「スキャン・エキスパート」ビュー』 を参照してください)、提案された変更が自動的に適用されるか、またはインタラクティブ・リストとして表示されます。

以下の表は、スキャン・エキスパート推奨リストで有効なオプションをまとめたものです。

オプション	説明
推奨	AppScan が、追加のユーザー入力なしで実装できる推奨が自動的に選択されます。必要に応じて、チェック・ボックスを選択または選択解除します。 実装にユーザーの入力が必要な推奨は、青いリンクで表示されます。リンクをクリックすると、「構成」ダイアログ・ボックスが開いて関連するタブが表示されるため、必要な入力を行います (ログイン手順の記録など)。
詳細	クリックすると、選択された推奨に関する詳細ウィンドウが開きます。 このウィンドウには、推奨の背景にある論拠と、この推奨を手動で適用する方法に関する指示が含まれます。
マニュアル編集	「スキャン構成」ダイアログ・ボックスを該当するビューで開き、現在選択されている推奨を手動で適用することができます。

オプション	説明
推奨を適用	スキャン構成を更新して、チェック・ボックスが選択されているすべての推奨に適合させてからスキャン・エキスパート・ペインを閉じます。
すべて無視	推奨をすべて破棄してスキャン・エキスパート・ペインを閉じます。

Glass Box スキャン

概要

Glass box スキャンの原理とそのセットアップの概要を説明します。

通常のスキャンでは、アプリケーションを「ブラック・ボックス」として認識し、ボックスの「中身」を確認することなく、その出力 を分析します。これに対して Glass Box スキャンでは、アプリケーション・サーバーにインストールされたエージェントを使用して、スキャン中にコード自体を調査します。「Glass Box (ガラスの箱)」という用語は、このことに由来しています。これを行うには、AppScan Glass Box エージェントが、AppScan 自体がインストールされているローカル・マシン上ではなく、テストしたいアプリケーションと同じサーバー上にインストールされている必要があります。

Glass Box スキャンには、以下のような利点があります。

- 探査ステージでは、サーバー・サイドに影響するが応答からは検出できない (従って、ブラック・ボックス・スキャンだけでは検出できない) HTTP パラメーターを、Glass Box スキャンによって検出することができます。
- テスト・ステージ中に、Glass Box スキャンは、ブラインド SQL インジェクションなどの特定のテストの成功または失敗を、より高い精度で検証できます。これにより、「誤検出」の結果が少なくなります。また、ブラック・ボックス・スキャンでは検出できない一部のセキュリティー問題を検出することもできます。
- Glass Box スキャンにより、AppScan で実際のソース・コードに存在する脆弱性を表示できるため、レポート作成と修復を簡素化することができます。

Glass box スキャンを組み込むことで、検出できる問題の種類と数だけでなく、提供される問題情報という点でも、スキャンの範囲を広げることができます。

Glass Box スキャンをセットアップして操作するには、以下のタスクを実行します。

タスク	説明
1.エージェントのインストール	AppScan Glass Box エージェントをアプリケーション・サーバーにインストールします。 この操作は、***1*** つのサーバーに対して ***1*** 回だけ行います。 **注:** このエージェントは複数のサーバーにインストールできますが、Glass Box スキャンに使用できるサーバーは 1 つだけです。
2.エージェントの定義	インストールしたエージェントを AppScan で定義して、 とエージェントが通信できるようにします。 この操作は、各 ***AppScan*** マシンで一度だけ行います。 **注:** AppScan の複数のインスタンス (別々のマシン上のインスタンス) で同じ Glass Box Web サーバー・エージェントを使用することはできますが、同時に使用することはできません。

タスク	説明
3.スキャンの構成	必要な Glass Box エージェントを使用するようにスキャン を構成します。この構成はデフォルトで自動的に行われますが、「スキャン構成」>「**Glass Box**」で、構成を調整することができます。 この操作は、各スキャンで一度だけ行います。
4.スキャンの実行	有効にした Glass box スキャンを使用して、アプリケーションをスキャンします。
5.エージェント・ルールの更新	自動更新プロセスでサーバー・エージェント・ルールの更新プロンプトが表示されたら、サーバー・エージェントを更新します。これにより、Web サーバー上の規則のバージョンと、ローカルの AppScan 上のバージョンとの同期が維持されます。 **注:** 更新処理の実行後は、Web アプリケーション・サーバーを再始動する必要があります。

Java プラットフォームの場合

Java サーバーでの Glass box エージェントのインストールおよび使用。

Glass Box エージェントのインストール

このセクションでは、サーバー・サイドの Glass Box エージェントをセットアップして、Glass Box スキャンを有効にする方法について説明します。

ご使用のアプリケーション・サーバー (複数可) に AppScan のインストール済み環境から特定のファイルをコピーして、AppScan Glass Box エージェントをアプリケーション・サーバーにインストールする必要があります。

注**:** Glass Box エージェントは、専用の Java エージェント (`gbAgent.jar`) をインストールして使用することによって機能します。他の Java エージェントが Web サーバー上で定義されている場合は、アプリケーション・サーバーのコマンド行で以下のように指定することにより、Glass Box エージェントを追加することができます (正確なパスは、現在のインストール済み環境によって異なります)。

```
java ... -javaagent:c:\otherAgent\otherAgent.jar
  -javaagent:c:\glassbox\gbAgent.jar ...
```

システム要件

次のプラットフォームとテクノロジーがサポートされています。

ソフトウェア	詳細
JRE	サポートされているのは、バージョン 6 および 7 です。JRE 8 はサポートされていません。
オペレーティング・システム	サポートされる Microsoft Windows システム (32 –ビット版と 64 –ビット版の両方): • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2 サポートされる Linux システム: • Linux RHEL 5、6、6.1、6.2、6.3、6.4 サポートされる UNIX システム: • UNIX AIX 6.1、7.1 • UNIX Solaris (SPARC) 10、11

ソフトウェア	詳細
Java EE コンテナー	JBoss AS 6、7; JBoss EAP 6.1; Tomcat 6.0、7.0; WebLogic 10、11、12; WebSphere 7.0、8.0、8.5、8.5.5

始める前に

インストールを開始する前に、以下に示す情報を準備しておくと、時間の節約になります。これらの情報を準備するには、Web アプリケーション・サーバー管理者への問い合わせが必要になる場合があります。

- 使用しているサーバーのオペレーティング・システム (Windows、Linux、Unix)
- ご使用の Java EE アプリケーション・サーバー (WebSphere、WebLogic、Tomcat、JBoss) と、そのサーバーをインストールするモード (標準インストールまたはオペレーティング・システム・サービスとしてインストール)
- Java EE アプリケーション・サーバーの Web アプリケーションのデプロイメント場所 (例: `D:\apache-tomcat-6.0.32\webapps`)
- Java EE アプリケーション・サーバーで使用される Java ランタイムの場所 (例: `C:\Program Files (x86)\Java\jre6`)
- Java EE アプリケーション・サーバー管理用の資格情報 (新しい Web アプリケーションをデプロイするため)

注**:** このサーバーをセキュア・モードで実行する場合は、特別な権限が必要になります。参照先 187 ページの『セキュア・モードで作業する場合に必要な権限』

ログ

Glass box ログは次の場所に保存されます。

`[Installation folder]\instrumentation.log`

Glass Box エージェント・インストーラーを使用した自動的なインストール**:**

このセクションでは、ユーザー・インターフェースを使用して Glass Box エージェントを自動的にインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. `...\Program Files\IBM\AppScan Standard\Glass box` を開きます。

   正確なパスは、AppScan をインストールした場所によって異なります。
2. 以下の関連セットアップ・ファイルを Web サーバーにコピーします。
   - **Linux** サーバー**:** ファイル `GB_Java_Setup.bin` をコピーします。
   - **Windows** サーバー**:** ファイル `GB_Java_Setup.exe` をコピーします。
3. GB_Java_Setup アプリケーションを起動して、オンラインの説明に従います。このプロセス中に、以下の操作を要求する画面が表示されます。

- Web アプリケーション・サーバーを選択します。サーバーがリストされていない場合は (例えば、JBoss Service、Tomcat Service、WebLogic Service など)、 「その他」を選択します。
- エージェント用のユーザー名とパスワードを定義します。後で、エージェントを AppScan で定義する際に、この資格情報が必要になります。この資格情報により、製品とエージェント間の通信が有効になります。ASCII 文字の英語以外は使用できません。

注: 「その他」を選択した場合は、ステップ 5 から、関連する手動 インストールについて続行してください。

注: また、フレームワークの関連 JAVA_HOME (JDK) または JRE_HOME (JDK または JRE) フォルダーへのパスを指定する画面が表示される場合があります。

ヒント: インストーラー・インターフェースの言語オプションには、ご使用のオペレーティング・システムでサポートされる言語のみが含まれます。インストーラーを異なる言語で実行する場合は、インストーラーをコマンド行から開始して、希望する言語のフラグを追加することができます。 例えば、英語の OS 上で日本語でインストーラーを実行するには、`GB_Java_Setup.bin -l ja` というコマンドを実行します。

- Glass box エージェントのインストール・フォルダー内に開始スクリプトが作成されます。
- デスクトップを使用する場合、Glass box エージェントが有効になった状態で、サーバーを始動するためのショートカットが作成されます。

重要: Glass Box スキャンを有効にするには、これらのいずれかを使用してアプリケーション・サーバーを始動する必要があります。これにより、Glass box エージェントがアクティブな状態でサーバーが始動されます。

コマンド行を使用した自動インストール:

このセクションでは、コマンド行を使用して Glass Box エージェントをインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. `...\Program Files\IBM\AppScan Standard\Glass box` を開きます。

   正確なパスは、AppScan をインストールした場所によって異なります。
2. 以下の関連セットアップ・ファイルを Web サーバーにコピーします。
   - Linux サーバーの場合は、ファイル `GB_Java_Setup.bin` をコピーします。
   - Windows サーバーの場合は、ファイル `GB_Java_Setup.exe` をコピーします。
3. 現在のサーバーに適用される、スペースで区切られた以下のすべて の引数を含むコマンド行を実行します。

コマンド	説明
`GB_Java_Setup.bin` (Linux) または `GB_Java_Setup.exe` (Windows)	設定ファイル。

コマンド	説明
-i console	
-l en	インストールの言語を設定します。使用する言語のコードを指定します (英語の場合は「en」)。
-DCHOSEN_INSTALL_SET=JBoss / WebSphe / Tomcat / WebLogic / Other	エージェントをインストールするサーバーのタイプ。 **注:** 対象のサーバーがリスト対象のサーバーではない場合は (例えば、JBoss Service、Tomcat Service、WebLogic Service など)、「**Other**」を設定します。
-DUSER_INSTALL_DIR=value	エージェントがインストールされるパスを設定します。
-DGLASS_USERNAME=value	エージェントにアクセスするためのユーザー名を設定します。英字と数字以外は使用できません。
-DGLASS_PASSWORD=value	エージェントにアクセスするためのパスワードを設定します。英字と数字以外は使用できません。
-DWEBLOGIC_PATH / -DJBOSS_PATH / -DTOMCAT_PATH / -DWEBSPHERE_PATH=value	Web サーバーのインストール・ディレクトリーのパスを設定します。 例 (実際の場所は、システムによって異なります): WebLogic: C:\weblogic\user_projects\domains\base_domain\ JBoss: C:\jboss-6.0.0\ Tomcat: C:\apache-tomcat-6.0.32\ WebSphere: C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\
-DJBOSS_SERVER_NAME=value / -DWEBSPHERE_SERVER_NAME=value	サーバー名。
-DWEBLOGIC_USERNAME / -DWEBSPHERE_USERNAME=value -DWEBLOGIC_PASSWORD / -DWEBSPHERE_PASSWORD=value	アプリケーション・サーバーにアクセスするためのユーザー名とパスワード。
-DWEBLOGIC_LIB=value	LIB フォルダーへのパス。例: C:\weblogic\wlserver_10.3\server\lib\
-DWEBLOGIC_TARGET=value	サーバー/ターゲット名。
-DWEBLOGIC_PORT=value	管理ポート。
-DSELECTED_JBOSS_TYPE=value	以下のいずれかの値を使用してください。 JBoss AS JBoss EAP Standalone JBoss EAP Managed Domain

WebSphere の例**:**

```
GB_Java_Setup.bin –i console –l en -DCHOSEN_INSTALL_SET=WebSphe
-DUSER_INSTALL_DIR=/opt/glass_box -DGLASS_USERNAME=jsmith
-DGLASS_PASSWORD=1234
```

```
-DWEBSPHERE_PATH=/opt/IBM/WebSphere/AppServer/profiles/AppSrv01
-DWEBSPHERE_SERVER_NAME=server1
-DWEBSPHERE_USERNAME=admin -DWEBSPHERE_PASSWORD=admin_pw
```

4. ご使用の Web サーバーが手順の最後で停止したことを確認してください。停止しなかった場合は、手動で停止してください。
5. デスクトップ・ショートカット、または Glass box エージェント・インストール・フォルダー内の開始スクリプトを使用して Web サーバー を再始動してください。再始動すると Glass Box エージェントがアクティブになります。

JBoss サーバーまたは **JBoss Service** サーバーでの手動インストール**:**

このセクションでは、JBoss サーバーまたは JBoss Service サーバーに Glass Box エージェントを手動でインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. `...\Program Files\IBM\AppScan Standard\Glass box` を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。
2. `GB_Java_Manual_Setup.zip` を探し、使用している Web サーバーにコピーします。
3. このフォルダーの内容を、Web サーバー上の任意の場所に解凍します。
4. エージェント用のユーザー名とパスワードを定義します (ASCII 文字の英語以外は使用できません)。
   - **Linux** サーバー**:** `AgentCredentials.sh <username> <password>` を実行します。

     注**:** `AgentCredentials.sh` には実行権限が必要です。
   - **Windows** サーバー**:** `AgentCredentials.bat <username> <password>` を実行します。
5. 以下の手順で、GBootStrap Web アプリケーションをデプロイします。
   a. JBoss 管理コンソールにログインします。デフォルトの場所は `http://<server_name>:<port_number>/admin-console/` です。
   b. 「アプリケーション **(Applications)**」**>**「**Web** アプリケーション **WAR (Web Application WARs)**」をクリックしてから、「新規リソースの追加 **(Add a new resource)**」をクリックします。
   c. `GBootStrap.war` (解凍した Glass Box フォルダーに格納されています) へのパスを入力し、「続行 **(Continue)**」をクリックします。

   リソースが正常に作成されたことを示すメッセージが表示されます。
6. JBoss サーバー/サービスをシャットダウンします。
7. 次のいずれか を実行して、Java エージェントの gbAgent.jar (解凍したフォルダーに格納されています) を JVM 引数として指定します。
   - 環境変数を使用する場合:JAVA_OPTS 環境変数 (存在しない場合は作成してください) を使用し、次の値に設定して JBossの JVM を構成します。

```
-javaagent:"<path_to_gbAgent.jar>/gbAgent.jar"
-Djava.net.preferIPv4Stack=true
-Djboss.modules.system.pkgs=com.ibm.glassbox.asm.agent,
  com.ibm.glassbox.agent,com.ibm.glassbox.logger,
  com.ibm.glassbox.jsp,org.jboss.byteman
```

- バッチ・スクリプト/シェル・スクリプトを使用する場合: サーバー付属の構成ファイルを編集することにより、JBoss を実行する JVM に引数を渡します。

  Linux サーバー:

  a. JBoss フォルダーで、以下の適切なファイルを見つけ (通常、/bin 内にあります)、エディターで開きます。
     - **JBoss AS:** run.sh
     - **JBoss EAP** スタンドアロン: standalone.sh
     - **JBoss EAP** 管理ドメイン: domain.sh

  b. JAVA_OPTS で始まる行を探し、その下に次のコードを追加します。

```
export JAVA_OPTS=$JAVA_OPTS "-javaagent:<path_to_gbAgent.jar>/gbAgent.jar"
-Djava.net.preferIPv4Stack=true
-Djboss.modules.system.pkgs=com.ibm.glassbox.asm.agent,
  com.ibm.glassbox.agent,
  com.ibm.glassbox.logger,
  com.ibm.glassbox.jsp,org.jboss.byteman
```

  c. ファイルを保存して閉じます。

  Windows サーバー:

  a. JBoss フォルダーで、以下の適切なファイルを見つけ (通常、/bin 内にあります)、エディターで開きます。
     - **JBoss AS:** run.conf
     - **JBoss EAP** スタンドアロン: standalone.conf
     - **JBoss EAP** 管理ドメイン: domain.conf

  b. set JAVA_OPTS= で始まる行を探し、その下に次の行を追加します。

```
set JAVA_OPTS=$JAVA_OPTS "-javaagent:<path_to_gbAgent.jar>\gbAgent.jar"
-Djava.net.preferIPv4Stack=true
-Djboss.modules.system.pkgs=com.ibm.glassbox.asm.agent,
  com.ibm.glassbox.agent,com.ibm.glassbox.logger,
  com.ibm.glassbox.jsp,org.jboss.byteman"
```

  c. ファイルを保存して閉じます。

  重要: 他の JAVA_OPTS 割り当てによって -javaagent が上書きされることがないよう、JAVA_OPTS が上記の行より前に 1 回だけ初期化されることを確認してください。

  注: JAVA_OPTS に引数を追加するには、%JAVA_OPTS% / $ JAVA_OPTS 規則を使用します。

8. JBoss サーバー/サービスを再始動します。

Tomcat サーバーでの手動インストール:

このセクションでは、Tomcat サーバーで Glass Box エージェントを手動でインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. `...\Program Files\IBM\AppScan Standard\Glass box` を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。
2. `GB_Java_Manual_Setup.zip` を探し、使用している Web サーバーにコピーします。
3. このフォルダーの内容を、Web サーバー上の任意の場所に解凍します。
4. エージェント用のユーザー名とパスワードを定義します (ASCII 文字の英語以外は使用できません)。
   - **Linux** サーバー**:** `AgentCredentials.sh <username> <password>` を実行します。

     注**:** `AgentCredentials.sh` には実行権限が必要です。
   - **Windows** サーバー**:** `AgentCredentials.bat <username> <password>` を実行します。
5. GBootStrap Web アプリケーションをデプロイします。
   - 推奨方法:
     a. Tomcat Manager にログインします。デフォルトの場所は `http://<server_name>:<port_number>/manager/html` です。
     b. 「デプロイ・テーブル **(Deploy table)**」**>**「デプロイする **war** ファイル **(War file to deploy)**」で、「ファイルの選択 **(Choose file)**」をクリックします。
     c. GBootStrap.war (解凍した Glass Box フォルダーに格納されています) を探し、「開く **(Open)**」をクリックします。
     d. 「デプロイ」をクリックし、GBootStrap がアプリケーション・リストに追加されたことを確認します。
   - 代替方法:
     a. ファイル GBootStrap.war を、解凍した Glass Box フォルダーからコピーします。
     b. そのファイルを `\webapps` フォルダー (デフォルト・ロケーション) に貼り付けます。

        `C:\apache-tomcat-[version]\webapps`
6. Tomcat をシャットダウンします。
7. 以下のいずれか を実行して、常に Glass Box エージェントを使用するように Tomcat を構成します。
   - 環境変数を使用する場合**:** JAVA_OPTS 環境変数 (存在しない場合は作成してください) を使用し、次の値 `-javaagent:<path_to_gbAgent.jar>/gbAgent.jar` に設定して Tomcat の JVM を構成します。
   - バッチ・スクリプト**/**シェル・スクリプトを使用する場合**:** サーバー付属の構成スクリプトを編集することにより、Tomcat を実行する JVM に引数を渡します。

     Linux サーバー**:**

     a. Tomcat フォルダー (通常は `<path_to_Tomcat_folder>/bin` にあります) で `startup.sh` を開きます
     b. `CATALINA_OPTS` で始まる行を探し、その下に次の行を追加します。

        `export CATALINA_OPTS = $CATALINA_OPTS -javaagent:<path_to_gbAgent.jar>/gbAgent.jar`

c. ファイルを保存して閉じます。

Windows サーバー**:**

a. Tomcat フォルダー(通常は `<path_to_Tomcat_folder>\bin` にあります)で `startup.bat` を開きます。

b. `set CATALINA_OPTS=` で始まる行を探し、その下に次の行を追加します。

```
set CATALINA_OPTS = %CATALINA_OPTS% -javaagent:<path_to_gbAgent.jar>/gbAgent.jar
```

c. ファイルを保存して閉じます。

重要**:** 他の CATALINA_OPTS 割り当てによって `-javaagent` が上書きされることがないよう、CATALINA_OPTS が上記の行より前で 1 回だけ初期化されることを確認してください。

注**:** CATALINA_OPTS に引数を追加するには、%CATALINA_OPTS% / $ CATALINA_OPTS 規則を使用します。

8. Tomcat を再始動します。

Tomcat Service サーバーでの手動インストール**:**

このセクションでは、Tomcat Service/Daemon サーバーで Glass Box エージェントを手動でインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. `...\Program Files\IBM\AppScan Standard\Glass box` を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。

2. `GB_Java_Manual_Setup.zip` を探し、使用している Web サーバーにコピーします。
3. このフォルダーの内容を、Web サーバー上の任意の場所に解凍します。
4. エージェント用のユーザー名とパスワードを定義します (ASCII 文字の英語以外は使用できません)。
   - **Linux** サーバー**:** `AgentCredentials.sh <username> <password>` を実行します。

     注**:** `AgentCredentials.sh` には実行権限が必要です。
   - **Windows** サーバー**:** `AgentCredentials.bat <username> <password>` を実行します。
5. 以下の手順で、GBootStrap Web アプリケーションをデプロイします。
   - Tomcat Manager にログインします。デフォルトの場所は `http://<server_name>:<port_number>/manager/html` です。
   - 「デプロイ・テーブル **(Deploy table)**」>「デプロイする **war** ファイル **(War file to deploy)**」で、「ファイルの選択 **(Choose file)**」をクリックします。
   - GBootStrap.war (解凍した Glass Box フォルダーに格納されています) を探し、「開く **(Open)**」をクリックします。
   - 「デプロイ **(Deploy)**」をクリックし、GBootStrap がアプリケーション・リストに追加されたことを確認します。

6. Tomcat をシャットダウンします。
7. 以下の手順を実行して、Glass Box エージェントを使用するように Tomcat を構成します。
   a. ...\Tomcat 7.0\bin\tomcat7w.exe で Tomcat JVM を探します。
   b. これをダブルクリックして、「プロパティー **(Properties)**」>「**Java**」タブを選択します。
   c. Java オプション領域で -javaagent:<path_to_gbAgent.jar>/gbAgent.jar を新しい行として追加します。

      注: Web サーバーに他の Java エージェントが定義されている場合でも、以下のように、「Java オプション (Java Options)」領域に Glass Box エージェントを追加 することができます (正確なパスはインストール済み環境によって異なります)。

      ```
      ... -javaagent:c:\...\otherAgent.jar -javaagent:c:\glassbox\gbAgent.jar ...
      ```
   d. 「**OK**」をクリックします。
8. Tomcat を再始動します。

WebLogic サーバーでの手動インストール:

このセクションでは、WebLogic サーバーで Glass Box エージェントを手動でインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. ...\Program Files\IBM\AppScan Standard\Glass box を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。
2. GB_Java_Manual_Setup.zip を探し、使用している Web サーバーにコピーします。
3. このフォルダーの内容を、Web サーバー上の任意の場所に解凍します。
4. エージェント用のユーザー名とパスワードを定義します (ASCII 文字の英語以外は使用できません)。
   - **Linux** サーバー: AgentCredentials.sh <username> <password> を実行します。

     注: AgentCredentials.sh には実行権限が必要です。
   - **Windows** サーバー: AgentCredentials.bat <username> <password> を実行します。
5. 以下の手順で、GBootStrap Web アプリケーションをデプロイします。
   a. WebLogic 管理コンソールにログインします。デフォルトの場所は http://<server_name>:<port_number>/console/ です。
   b. 「ドメイン構造 **(Domain Structure)**」ペインで、「デプロイメント **(Deployments)**」をクリックして「インストール **(Install)**」をクリックします。
   c. 「パス **(Path)**」フィールドに GBootStrap.war へのパスを入力して、「次へ **(Next)**」をクリックします。
   d. 「このデプロイメントをアプリケーションとしてインストールする **(Install this deployment as an application)**」ラジオ・ボタンを選択して、「次へ **(Next)**」をクリックします。
   e. 「名前 **(Name)**」フィールドのテキストが「**GBootStrap**」になっていることを確認します。

f. 「**Finish (**終了**)**」をクリックして「保存 **(Save)**」をクリックします。

g. 「ドメイン構造 **(Domain Structure)**」ペインで「デプロイメント **(Deployments)**」をクリックして、 **GBootStrap** が追加されていることを確認し、「正常性 **(Health)**」列に緑のチェック・マーク・アイコンが表示されていることを確認します。

6. WebLogic サーバーをシャットダウンします。
7. 次のいずれか を実行して、Java エージェントの gbAgent.jar (解凍したフォルダーに格納されています) を JVM 引数として指定します。
   - 環境変数を使用する場合:JAVA_OPTS 環境変数 (存在しない場合は作成してください) を使用し、次の値に設定して複数の WebLogic の JVM を構成します。
     - **Linux** サーバー**:** `-javaagent:<path_to_gbAgent.jar>/gbAgent.jar`
     - **Windows** サーバー**:** `-javaagent:<path_to_gbAgent.jar>\gbAgent.jar`
   - バッチ・スクリプト**/**シェル・スクリプトを使用する場合**:** サーバー付属の構成スクリプトを編集することにより、WebLogic を実行する JVM に引数を渡します。

     Linux サーバー**:**

     a. WebLogic フォルダー(通常は `<path_to_Weblogic_folder>\bin` にあります)で、エディターを使用してスタートアップ・ファイルを開きます。
        - **Admin** サーバー**:** `DOMAIN_NAME/bin/startWebLogic.sh` を開きます。
        - **Managed** サーバー**:** `DOMAIN_NAME/bin/startManagedWebLogic.sh` を開きます。

     b. `JAVA_OPTIONS` で始まる行を探し、その下に次の行を追加します。

     ```
     export JAVA_OPTIONS = $JAVA_OPTIONS -javaagent:"<path_to_gbAgent.jar>/gbAgent.jar"
     ```

     c. ファイルを保存して閉じます。

     Windows サーバー**:**

     a. WebLogic フォルダー (通常は `<path_to_WebLogic_folder>\bin` にあります) で `startWebLogic.bat` を開きます

     b. `set JAVA_OPTIONS` で始まる行を探し、その下に次の行を追加します。

     ```
     set JAVA_OPTIONS = %JAVA_OPTIONS% -javaagent:<path_to_gbAgent.jar>/gbAgent.jar
     ```

     c. ファイルを保存して閉じます。

     重要**:** 他の JAVA_OPTIONS 割り当てによって `-javaagent` が上書きされることがないよう、JAVA_OPTIONS が上記の行より前で 1 回だけ初期化されることを確認してください。

     注**:** JAVA_OPTIONS に引数を追加するには、%JAVA_OPTIONS% / $ JAVA_OPTIONS 規則を使用します。
8. WebLogic サーバーを再始動します。

WebLogic Service サーバーでの手動インストール**:**

このセクションでは、WebLogic Service/Daemon サーバーで Glass Box エージェントを手動でインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. ...\Program Files\IBM\AppScan Standard\Glass box を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。
2. GB_Java_Manual_Setup.zip を探し、使用している Web サーバーにコピーします。
3. このフォルダーの内容を、Web サーバー上の任意の場所に解凍します。
4. エージェント用のユーザー名とパスワードを定義します (英字と数字以外は使用できません)。
   - **Linux** サーバー**:** AgentCredentials.sh <username> <password> を実行します。

     注**:** AgentCredentials.sh には実行権限が必要です。
   - **Windows** サーバー**:** AgentCredentials.bat <username> <password> を実行します。
5. 以下の手順で、GBootStrap Web アプリケーションをデプロイします。
   a. WebLogic 管理コンソールにログインします。デフォルトの場所は http://<server_name>:<port_number>/console/ です。
   b. 「ドメイン構造 **(Domain Structure)**」ペインで、「デプロイメント **(Deployments)**」をクリックして「インストール **(Install)**」をクリックします。
   c. 「パス **(Path)**」フィールドに GBootStrap.war へのパスを入力して、「次へ **(Next)**」をクリックします。
   d. 「このデプロイメントをアプリケーションとしてインストールする **(Install this deployment as an application)**」ラジオ・ボタンを選択して、「次へ **(Next)**」をクリックします。

      注**:** インストール・オプションが使用不可にされている (グレー表示されている) 場合、ロックおよび編集モードの設定を変更して、これを使用可能にする必要がある場合があります。
   e. 「名前 **(Name)**」フィールドのテキストが「**GBootStrap**」になっていることを確認します。
   f. 「**Finish** (終了)」をクリックして「保存 **(Save)**」をクリックします。
   g. 「ドメイン構造 **(Domain Structure)**」ペインで「デプロイメント **(Deployments)**」をクリックして、 **GBootStrap** が追加されていることを確認し、「正常性 **(Health)**」列に緑のチェック・マーク・アイコンが表示されていることを確認します。
6. WebLogic サービスをシャットダウンします。
7. レジストリー・キー HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<WEBLOGIC_SERVICE> を探し、-javaagent:<path_to_gbAgent.jar>/gbAgent.jar を含むように CmdLine の値を編集することで、Glass Box エージェントを使用するように WebLogic を構成します。
8. サービスを再始動します。

WebSphere サーバーでの手動インストール**:**

このセクションでは、WebSphere サーバーで Glass Box エージェントを手動でインストールする方法について説明します。

このタスクについて

AppScan をインストールすると、サーバー・エージェントのインストールに必要なファイルが、ご使用のマシンの専用フォルダーに保存されます。このタスクを実行するには、このフォルダーとアプリケーション・サーバーにアクセスできる必要があります。

手順

1. ...\Program Files\IBM\AppScan Standard\Glass box を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。
2. GB_Java_Manual_Setup.zip を探し、使用している Web サーバーにコピーします。
3. このフォルダーの内容を、Web サーバー上の任意の場所に解凍します。
4. エージェント用のユーザー名とパスワードを定義します (ASCII 文字の英語以外は使用できません)。
   - **Linux** サーバー: AgentCredentials.sh <username> <password> を実行します。

     注: AgentCredentials.sh には実行権限が必要です。
   - **Windows** サーバー: AgentCredentials.bat <username> <password> を実行します。
5. 以下の手順で、GBootStrap Web アプリケーションをデプロイします。
   a. WebSphere の Integrated Solutions Console にログインします。デフォルトの場所は http://<server_name>:<port_number>/ibm/console/ です。

      注: 複数のプロファイルが定義されている場合は、該当するプロファイルにログインしてください。
   b. 「新規アプリケーション」>「新規エンタープライズ・アプリケーション」を選択します。
   c. 「新規アプリケーションへのパス」領域で、GBootStrap.war ファイルへの絶対パスを追加します。
   d. 「コンテキスト・ルート」フィールドに「GBootStrap」と入力して、「次へ」をクリックします。

      「新規アプリケーションのインストール」ウィザードが開きます。
   e. どのデフォルト・オプションも変更しない場合は、ウィザードが完了するまで「次へ」をクリックします。構成の保存画面が表示されたら、構成を保存します。 ウィザードが完了すると、アプリケーション・リストに GBootstrap.war が表示されます。「アプリケーション状況」列の赤の X アイコンまたは緑の矢印アイコンは、アプリケーションが有効になっているかどうかを示しています。有効になっていない場合 (赤の X が表示されている場合) は、アプリケーションを選択して「開始」をクリックします。緑の矢印が表示されている場合は、GBootstrap.war が有効になっています。
6. ここで、「サーバー」>「アプリケーション・サーバー」を選択します。
7. 右側のペインで、使用しているサーバーの名前をクリックします。
8. 「構成」タブをクリックして前面に移動します。
9. 「サーバー・インフラストラクチャー」で、「**Java** およびプロセス管理」>「プロセス定義」をクリックします。
10. 「アプリケーション・プロパティー」で「**Java** 仮想マシン」をクリックします。
11. 以下の引数を「汎用 JVM 引数」に追加します。

    -javaagent:c:/path/to/gbAgent.jar (この例は Windows オペレーティング・システム用のもので、他のシステムの場合は、必要に応じてパスを変更する必要があります)。

    注: パスにスペースを使用することはできません。

注: 他の Java エージェントが Web サーバーに定義されている場合でも、以下のように、「汎用 JVM 引数」領域に Glass Box エージェントを追加 することができます (正確なパスはインストール済み環境によって異なります)。

```
... -javaagent:c:\otherAgent\otherAgent.jar -javaagent:c:\glassbox\gbAgent.jar ...
```

12. 「適用」をクリックします。構成の保存画面が表示された場合は、構成を保存します。
13. WebSphere サーバーを再始動します。

セキュア・モードで作業する場合に必要な権限

このセクションでは、スキャン中に Web アプリケーション・サーバーをセキュア・モードで実行する場合に追加する必要のある特別な権限について説明します。

サーバーをセキュア・モード (つまり、Java Security Manager を有効にした状態) で実行する場合、以下に示す特別な権限を GBootStrap Web アプリケーションに追加する必要があります。

- 「getClassLoader」(java.lang.RuntimePermission) にアクセスするための権限
- 「accessClassInPackage.sun.net.www.protocol.*」(java.lang.RuntimePermission) を使用するための権限
- 「java.io.tmpdir」プロパティー (java.util.PropertyPermission) に対する読み取り権限
- 「ALL FILES」に対する読み取り/書き込み/削除権限

必要に応じて、これらの Java セキュリティー権限を追加する方法と場所の説明について、使用している Web サーバーのマニュアルを参照してください。 以下の各セクションでは、これらの権限を追加する際に役立ついくつかのソースと例を紹介します。ただし、これらはあくまでも例であるため、実際に作業する場合には調整が必要になります。

IBM WebSphere

ガイド:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.express.doc/info/exp/ae/tsec_waspolicyfile.html

追加される行の概要:

```
grant codeBase "file:${application}" {
 permission java.lang.RuntimePermission "getClassLoader";
 permission java.lang.RuntimePermission
"accessClassInPackage.sun.net.www.protocol.*";
 permission java.io.FilePermission "<>", "read, write, delete";
 permission java.util.PropertyPermission "java.io.tmpdir", "read";
};
```

場所:

```
<profile_root>/config/cells/<cell_name>/applications/<ear_file_name>
/deployments/<application_name>/META-INF/was.policy
```

追加される行の例:

```
"C:\Program Files (x86)\IBM\WebSphere\AppServer\profiles\AppSrv01
\config\cells\ROIS-PSNode01Cell\applications\GBootStrap_war.ear
\deployments\GBootStrap_war\META-INF\was.policy")
```

Apache Tomcat

ガイド:

http://tomcat.apache.org/tomcat-6.0-doc/security-manager-howto.html#Configuring_Tomcat_With_A_SecurityManager

追加される行の概要:

```
grant codeBase "file:${catalina.base}/webapps/GBootStrap/-"{
 permission java.lang.RuntimePermission "getClassLoader";
 permission java.lang.RuntimePermission
"accessClassInPackage.sun.net.www.protocol.*";
 permission java.io.FilePermission "<<ALL FILES>>">>", "read, write, delete";
 permission java.util.PropertyPermission "java.io.tmpdir", "read";
};
```

場所:

```
<CATALINA_HOME>/conf/catalina.policy
```

追加される行の例:

```
"C:\Software\Tomcat\apache-tomcat-6.0.33\conf\catalina.policy"
```

Weblogic

ガイド:

http://download.oracle.com/docs/cd/E13222_01/wls/docs81/security/server_prot.html

具体的には、『Setting Application-Specific Security Policies』セクションを参照してください。

追加される行の概要:

```
<security-permission>
 <description>
  Allow getting the J2EEJ2SETest4 property
 </description>
 <security-permission-spec>
  grant {
    permission java.util.PropertyPermission
"welcome.J2EEJ2SETest4","read";
  };
 </security-permission-spec>
</security-permission>
```

追加される行:

```
weblogic.xml
```

JBoss

ガイド:

http://docs.jboss.org/jbossweb/latest/security-manager-howto.html

追加される行の概要:

```
grant codeBase "file:${catalina.base}/webapps/GBootStrap/-"{
 permission java.lang.RuntimePermission "getClassLoader";
 permission java.lang.RuntimePermission
"accessClassInPackage.sun.net.www.protocol.*";
 permission java.io.FilePermission "ALL FILES", "read, write, delete";
 permission java.util.PropertyPermission "java.io.tmpdir", "read";
};
```

追加される行:

```
CATALINA_HOME/conf/catalina.policy
```

AppScan での Glass box エージェントの定義

このセクションでは、サーバー・サイドの Glass Box エージェントにアクセスするために AppScan を構成する方法について説明します。

このタスクについて

アプリケーション・サーバーに Glass Box エージェントをインストールしたら、このエージェントを AppScan に定義して、製品がエージェントにアクセスできるようにする必要があります。この処理を実行すると、AppScan は、すべての関連スキャンについて、Glass Box スキャン用に Glass Box エージェントを自動的に使用します (スキャン構成で選択解除した場合を除く)。

制約事項: 同じサーバー・エージェントを複数の AppScan マシンで定義できますが、1 つのエージェントは、同時に 1 つのスキャンに対してのみ使用できます。

制約事項: 複数のエージェントを定義できますが、1 つのスキャン構成で選択できるエージェントは 1 つだけです。

手順

1. 「構成」>「**URL** およびサーバー」タブで、「開始 **URL**」を設定します。この例では、URL にポート 8080 が含まれるので注意してください。

   ```
   https://altoro.testfire.net:8080/
   ```

2. 「**OK**」をクリックして、「構成」ダイアログ・ボックスを閉じます。
3. 「ツール」>「**Glass Box** エージェント管理」をクリックします。

   「Glass Box エージェント」ダイアログ・ボックスが表示され、すでに定義されているすべてのエージェントがリストされます。

4. 新規エージェントをリストに追加するには、  をクリックします。

   「Glass Box エージェント定義」ダイアログ・ボックスが表示されます。「Glass box エージェント URL」は、前のステップで入力した「開始 URL」に基づいて自動的に入力されます。

   重要: 「Glass box エージェント URL」には、「開始 URL」から抽出されたポート値 (この場合は 8080) が自動的に入力されます。別のポートにエージェントをインストールした場合は、ポート値を正しい値に置き換えてください。この例では、ポート値は 8888 に変更されています。

   ```
   http://altoro.testfire.net:8888/GBootStrap/
   ```

5. 必要に応じて、残りのフィールドとオプションを入力します。

オプション	説明
ユーザー名およびパスワード	エージェントをサーバーにインストールしたときに定義したユーザー名とパスワードを入力します。
エージェント・ログ設定:	(オプション) クリックすると、これらの設定が開きます。 **注:** エージェント・ログ設定は、サーバー・サイドのエージェントに保存されます。

オプション	説明
最大ログ行数	(オプション) スライダーを使用して、ログのサイズを制限します。
ログ・コンテンツ	(オプション) ログに含める情報レベルを選択します。エラー: エラー・メッセージのみを含めます。警告: エラー・メッセージと警告メッセージを含めます。情報: エラー、警告、通知メッセージを含めます。デバッグ: すべてのメッセージを含めます。 Glass box ログは次の場所に保存されます。 `[Installation folder]\instrumentation.log`

AppScan はエージェント・サーバーへの接続を試行します。接続に成功すると、緑色の「接続済み」アイコンが表示されます。問題が発生した場合は、赤色のアイコンと、「エージェントに接続できません」や「資格情報が必要です」などのメッセージが表示されます。

注: お客様のサイトで HTTP と HTTPS の両方が提供されている場合、開始 URL が HTTPS であることを確認してください (そうなっていない場合は、HTTPS に変更してください)。

注: エラー・メッセージを受信した場合は、以下の Web サイトを参照してください。

http://www.ibm.com/support/docview.wss?uid=swg21567723

6. 「**OK**」をクリックして、定義ダイアログ・ボックスを閉じます。

   エージェントがリストに追加されます。
7. 「**OK**」をクリックして、リストを閉じます。

   これで、このマシン上でエージェントが定義されました。

ユーザー資格情報の変更:

このセクションでは、Glass Box エージェントにアクセスするためのユーザー名とパスワードを変更する方法について説明します。

このタスクについて

Glass Box エージェントのインストール時に、エージェントにアクセスするためのユーザー名とパスワードを定義する画面が表示されます。 この資格情報により、AppScan だけがエージェントにアクセスできるようになります。インストール後に資格情報を変更する必要がある場合は、以下の手順を実行します。

手順

1. アプリケーション・サーバーで、インストール・ディレクトリーに対してコマンド行を開きます。
2. 以下のように、新規の資格情報を定義します。

- Linux サーバーの場合:`AgentCredentials.sh <newusername> <newpassword>` を実行します。
- Windows サーバーの場合:`AgentCredentials.bat <newusername> <newpassword>` を実行します。

3. サーバーから GBootStrap をアンデプロイします。
4. Glass Box インストール・フォルダーの新しい変更済み GBootStrap.war をサーバーにデプロイします。

Glass box スキャンの構成

スキャンは自動的に構成されますが、このセクションでは、変更することが推奨されるオプションについて説明します。

手順

1. 普通にスキャンを構成します。
2. 「構成」>「**Glass Box**」タブで、ドロップダウン・リストから定義済みの Glass box エージェントの 1 つを選択し、必要に応じて設定を調整します。

設定	詳細
この glass Box エージェントを使用	Glass Box エージェントがアプリケーション・サーバー上にインストールされ、AppScan 内で定義されている場合は、このエージェントを選択してスキャンで使用できます。開始 URL を入力した場合、AppScan は、適切なエージェントの自動的な選択を試行します。 エージェントが選択されると、AppScan は、エージェントへの接続を試行し、その試行が成功したかどうかを示します。 **注:** エージェントを選択したときに「資格情報が必要です」というメッセージが表示された場合、「ツール」 > 「Glass Box 管理」に指定されている資格情報が正しいことを確認してください。 必要なサーバーがドロップダウン・リストに表示されない場合は、「**Glass Box** エージェント管理」リンクをクリックして定義できます。 **制約事項:** 1 つのスキャンで使用する Glass Box エージェントは 1 つのみ選択できます。スキャンされているアプリケーションに複数のサーバーがある場合は、各サーバー・エージェントを別個に使用してスキャンする必要があります。

Glass Box を探査ステージで使用	(デフォルトで選択されています。)
	
	この機能を使用して、サーバーの動作に影響するが応答内には表示されないパラメーターがサーバー・サイドのソース・コードに存在するかどうかを検査することにより、サイトのカバー範囲を拡大することができます。
	
	サーバー・サイド・コードの例:
	`String debugOn = request.getParameter("debug");`
	`if (debugOn == "true"){`
	`response.getWriter().println(SECRET_SERVER_DATA);`
	`}`
	
	この例では、開発者はパラメーター `"debug"` をコード内に残しています。これはサイト上のリンクには表示されませんが、攻撃者がこれを含む要求を送信した場合には、`SECRET_SERVER_DATA` が取得される可能性があります。

Glass Box をテスト・ステージで使用	(デフォルトで選択されています。) スキャンのテスト・ステージで Glass Box テストを送信するには、このチェック・ボックスを選択します。この機能は、ブラインド SQL インジェクションなどの特定のテストの成功または失敗を、より高い精度で検証できます。また、ブラック・ボックス手法によって検出できない特定のセキュリティー問題の存在を発見できます。

設定	詳細
相当するブラック・ボックス・テストをスキップ	(デフォルトでは選択解除されています。) これは、同じぜい弱性 (WASC 脅威の分類) に対して Glass box テストとブラック・ボックス・テストの両方が送信されることを意味します。この理由は、一般的に、Glass box テストのほうが正確度が高いだけではなく、より詳細な結果を提供しますが、同等のブラック・ボックス・テストが成功する一方で Glass box テストが失敗する場合があるためです。ブラック・ボックス・テストをスキップしてもご使用のアプリケーションでの結果が変わらない場合は、このチェック・ボックスを選択することでスキャン時間を削減することができます。

ステータス・バーが、Glass box スキャンが有効にされ、スキャンを開始する準備ができたことを示します。

Glass Box によるスキャン

このセクションでは、Glass Box スキャンについて説明します。

このタスクについて

Glass Box エージェントを AppScan に定義すると、Glass Box スキャンがデフォルトで有効になります。「スキャン構成」ダイアログ・ボックスを使用すると、正しいサーバー・エージェントが選択されていること、およびスキャンの一部として Glass Box スキャンが実行されるように構成されていることを確認することができます。

Glass Box スキャンにより、探査ステージで非表示の URL を検出し、テスト・ステージで追加の問題と情報を検出することができます。

手順

1. 「構成」>「**Glass Box**」ビューをクリックします。
2. 使用したいエージェントをドロップダウン・リストから選択します。

   注: 必要なエージェントがリストに表示されていない場合は、「**Glass Box** エージェント管理」リンクをクリックして、エージェントを定義します。
3. 2 つの主要な Glass box スキャン・オプションのいずれかまたは両方が選択されていることを確認します。
   - Glass Box を探査ステージで使用
   - Glass Box をテスト・ステージで使用

   注: 「相当するブラック・ボックス・テストをスキップ」チェック・ボックスは、デフォルトでクリアされています。これは、同じぜい弱性 (WASC 脅威の分類) に対して Glass box テストとブラック・ボックス・テストの両方が送信されることを意味します。この理由は、一般的に、Glass box テストのほうが正確度が高いだけではなく、より詳細な結果を提供しますが、同等のブラック・ボックス・テストが成功する一方で Glass box テストが失敗する場合があるためです。ブラック・ボックス・テストをスキップしてもご使用のアプリケーションでの結果が変わらない場合は、このチェック・ボックスを選択することでスキャン時間を削減することができます。
4. 「スキャン」>「フルスキャン」をクリックし、スキャンを開始します。

スキャンが開始され、Glass box スキャンがアクティブであることを示すステータス・バー・メッセージが表示されます。

スキャン結果には、「問題情報」タブの Glass box データが含まれます (使用可能な場合)。

Glass Box エージェントのアンインストール

このセクションでは、サーバー・サイドの Glass Box エージェントをアンインストールする方法について説明します。

- 『自動アンインストール』
- 『JBoss サーバーでの手動アンインストール』
- 194 ページの『JBoss Service サーバーでの手動アンインストール』
- 195 ページの『Tomcat サーバーでの手動アンインストール』
- 195 ページの『Tomcat Service サーバーでの手動アンインストール』
- 196 ページの『WebLogic サーバーでの手動アンインストール』
- 196 ページの『WebLogic Service サーバーでの手動アンインストール』
- 197 ページの『WebSphere サーバーでの手動アンインストール』

自動アンインストール:

このセクションでは、ユーザー・インターフェースを使用して Glass Box エージェントを自動的にアンインストールする方法について説明します。

このタスクについて

Glass Box エージェントは、Glass Box エージェント・インストーラーを使用して自動的にインストールした場合にのみ、自動的にアンインストールすることができます。手動でインストールした場合は、このガイドの次のセクションにある説明に従って、手動でアンインストールする必要があります。

このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. サーバーで Glass Box ディレクトリーを開きます。
2. アンインストーラーを以下のように起動します。
   - **Linux** サーバー: `Uninstall.bin` をダブルクリックします
   - **Windows** サーバー: `Uninstall.exe` をダブルクリックします
3. オンラインの指示に従って、Glass Box を完全にアンインストールします。

JBoss サーバーでの手動アンインストール:

このセクションでは、JBoss サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンイン

ストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. JBoss 管理コンソールにログインします。デフォルトの場所は `http://<server_name>:<port_number>/admin-console/` です。
   b. 「アプリケーション **(Applications)**」>「**Web** アプリケーション **WAR (Web Application WARs)**」をクリックしてから、GBootStrap.war エントリーで「削除 **(Delete)**」をクリックします。
   c. 確認画面が表示されたら「**OK**」をクリックします。
2. JBoss サーバーをシャットダウンします。
3. JAVA_OPTS から Java エージェントを削除します。 手動インストールの実行中に、JAVA_OPTS が編集されて gbAgent.jar が組み込まれます。JAVA_OPTS から gbAgent.jar を削除し、JAVA_OPTS を元の状態に復元するには、インストールの説明を参照してください。
4. 他の Web アプリケーション・サーバーで使用される場合を除き、JBoss サーバーから Glass Box ディレクトリーを削除します。
5. JBoss サーバーを再始動します。

JBoss Service サーバーでの手動アンインストール**:**

このセクションでは、JBoss Service サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンインストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. JBoss 管理コンソールにログインします。デフォルトの場所は `http://<server_name>:<port_number>/admin-console/` です。
   b. 「アプリケーション **(Applications)**」>「**Web** アプリケーション **WAR (Web Application WARs)**」をクリックしてから、GBootStrap.war エントリーで「削除 **(Delete)**」をクリックします。
   c. 確認画面が表示されたら「**OK**」をクリックします。
2. JBoss サービスをシャットダウンします。
3. JAVA_OPTS から Java エージェントを削除します。 手動インストールの実行中に、JAVA_OPTS が編集されて gbAgent.jar が組み込まれます。JAVA_OPTS から gbAgent.jar を削除し、JAVA_OPTS を元の状態に復元するには、インストールの説明を参照してください。
4. 他の Web アプリケーション・サーバーで使用される場合を除き、JBoss サーバーから Glass Box ディレクトリーを削除します。
5. サービスを再始動します。

Tomcat サーバーでの手動アンインストール**:**

このセクションでは、Tomcat サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンインストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. Tomcat Manager にログインします。デフォルトの場所は `http://<server_name>:<port_number>/manager/html` です。
   b. アプリケーション・リストで「**GBootStrap.war**」を選択し、「コマンド **(Commands)**」**>**「アンデプロイ **(Undeploy)**」をクリックします。
   c. 確認画面が表示されたら「**OK**」をクリックします。
2. Tomcat サーバーをシャットダウンします。
3. CATALINA_OPTS から Java エージェントを削除します。 手動インストールの実行中、CATALINA_OPTS が編集されて gbAgent.jar が組み込まれます。CATALINA_OPTS から gbAgent.jar を削除して CATALINA_OPTS を元の状態に復元するには、インストールの説明を参照してください。
4. 他の Web アプリケーション・サーバーによって使用される場合を除き、Tomcat サーバーから Glass Box ディレクトリーを削除します。
5. Tomcat サーバーを再始動します。

Tomcat Service サーバーでの手動アンインストール**:**

このセクションでは、Tomcat Service サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンインストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. Tomcat Manager にログインします。デフォルトの場所は `http://<server_name>:<port_number>/manager/html` です。
   b. アプリケーション・リストで「**GBootStrap.war**」を選択し、「コマンド **(Commands)**」**>**「アンデプロイ **(Undeploy)**」をクリックします。
   c. 確認画面が表示されたら「**OK**」をクリックします。
2. Tomcat Service をシャットダウンします。

3. JVM 引数から Java エージェントを削除します。
   a. `...\Tomcat 7.0\bin\tomcat7w.exe` で Tomcat JVM を探します。
   b. これをダブルクリックして、「プロパティー **(Properties)**」>「**Java**」タブを選択します。
   c. 「Java オプション (Java Options)」領域に `-javaagent:c:/path/to/gbAgent.jar` という行がある場合は、これを削除します。
   d. 「**OK**」をクリックします。
4. Tomcat Service を再始動します。

WebLogic サーバーでの手動アンインストール**:**

このセクションでは、WebLogic サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンインストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. WebLogic 管理コンソールにログインします。デフォルトの場所は `http://<server_name>:<port_number>/console/` です。
   b. 「ドメイン構造 (Domain Structure)」ペインで「デプロイメント **Deployment)**」をクリックし、「**GBootStrap**」チェック・ボックスを選択して「削除 **(Delete)**」をクリックします。
   c. 「ドメイン構造 (Domain Structure)」ペインで「デプロイメント **(Deployment)**」をクリックし、GBootStrap が削除されていることを確認します。
2. WebLogic サーバーをシャットダウンします。
3. JAVA_OPTIONS から Java エージェントを削除します。 手動インストールの実行中、JAVA_OPTIONS が編集されて gbAgent.jar が組み込まれます。JAVA_OPTIONS から gbAgent.jar を削除して JAVA_OPTIONS を元の状態に復元するには、インストールの説明を参照してください。
4. 他の Web アプリケーション・サーバーによって使用される場合を除き、WebLogic サーバーから Glass Box ディレクトリーを削除します。
5. WebLogic サーバーを再始動します。

WebLogic Service サーバーでの手動アンインストール**:**

このセクションでは、WebLogic Service サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンインストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. WebLogic 管理コンソールにログインします。デフォルトの場所は `http://<server_name>:<port_number>/console/` です。
   b. 「ドメイン構造 (Domain Structure)」ペインで「デプロイメント **Deployment)**」をクリックし、「**GBootStrap**」チェック・ボックスを選択して「削除 **(Delete)**」をクリックします。
   c. 「ドメイン構造 (Domain Structure)」ペインで「デプロイメント **(Deployment)**」をクリックし、GBootStrap が削除されていることを確認します。
2. WebLogic Service をシャットダウンします。
3. JAVA_OPTIONS から Java エージェントを削除します。 手動インストールの実行中、JAVA_OPTIONS が編集されて gbAgent.jar が組み込まれます。JAVA_OPTIONS から gbAgent.jar を削除して JAVA_OPTIONS を元の状態に復元するには、インストールの説明を参照してください。
4. サービスを再始動します。

WebSphere サーバーでの手動アンインストール**:**

このセクションでは、WebSphere Service サーバーで Glass Box エージェントを手動でアンインストールする方法について説明します。

このタスクについて

Glass Box がアプリケーション・サーバーにインストールされている場合、そのインストール済み環境には Java エージェントと GBootStrap Web アプリケーションが含まれています。 Glass Box をアンインストールするには、その両方を削除する必要があります。このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

1. GBootStrap Web アプリケーションのアンデプロイ:
   a. WebSphere の Integrated Solutions Console にログインします。デフォルトの場所は `http://<server_name>:9043/console/` です。

      注**:** 複数のプロファイルが定義されている場合は、適切なプロファイルのコンソールにログインしてください。
   b. 「アプリケーション」**>**「アプリケーション・タイプ」**>**「**WebSphere** エンタープライズ・アプリケーション」を選択します。
   c. 「エンタープライズ・アプリケーション」領域で「**GBootStrap**」ボックスを選択し、「アンインストール」をクリックします。
   d. ウィザードの指示に従って、GBootStrap アプリケーションを削除します。

      GBootStrap がアプリケーションのリストから除去されます。
   e. 「サーバー」**>**「アプリケーション・サーバー」を選択します。
   f. 右側のペインで、使用しているサーバーの名前をクリックします。
   g. 「構成」タブをクリックして前面に移動します。
   h. 「サーバー・インフラストラクチャー」で、「**Java** およびプロセス管理」 **>**「プロセス定義」をクリックします。
   i. 「追加プロパティー」で、「**Java** 仮想マシン」をクリックします。

2. 「汎用 JVM 引数」で `-javaagent:c:/path/to/gbAgent.jar` をクリアすることにより、Glass Box エージェントを削除します。

   注: この例が該当するのは、Windows オペレーティング・システムの場合です。他のシステムの場合は、システムに合わせてパスを調整してください。
3. 「適用」をクリックします。構成の保存画面が表示された場合は、構成を保存します。
4. WebSphere を再始動します。

.NET プラットフォームの場合

.NET サーバーでの Glass box エージェントのインストールおよび使用。

Glass Box エージェントのインストール

このセクションでは、.NET サーバーで Glass Box エージェントをインストールする方法について説明します。

始める前に

ご使用のアプリケーション・サーバー (複数可) に AppScan のインストール済み環境から特定のファイルをコピーして、AppScan Glass Box エージェントをアプリケーション・サーバーにインストールする必要があります。これを行うには、アプリケーション・サーバーにアクセスする必要があります。サポートされているシステムとテクノロジーは以下のとおりです。

項目	詳細
オペレーティング・システム	サポートされるオペレーティング・システム (32 –ビット版と 64 –ビット版の両方): • Microsoft Windows Server 2012 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2008 R2
その他	Microsoft IIS 7.0 以降 Microsoft .NET Framework 4.0 または 4.5 をインストールする必要があります。またこのバージョンの ASP.net を使用するには、IIS がルート・レベルで構成されている必要があります。

手順

1. `...\Program Files\IBM\AppScan Standard\Glass box` を開きます。

   絶対パスは、AppScan をインストールした場所によって異なります。
2. `GB_DotNET_Setup.exe` を探し、使用している Web サーバー・マシンにコピーします。
3. このファイルをダブルクリックし、ウィザードを開始します。
4. ウィザードのステップに従います。

5. 新規の Web サイトにインストールするか、既存の Web サイトにインストールするかを尋ねられたら、(どちらが良いかが不明確な場合は) 推奨オプションを選択します。

   注: 2 つのオプションのどちらが推奨されるかは、ご使用のシステムによって異なります。「既存の Web サイト」が推奨される可能性が高いですが、必ずこちらが推奨されるわけではなく、「新規の Web サイト」が推奨される場合もあります。通常は、新規のポートが不要なために「既存の Web サイト」が優先されます。新規のポートは、AppScan で構成する必要があり、AppScan にアクセスできるように追加のファイアウォール構成も必要になる場合があります。
6. このステップは、前のステップでの選択によって異なります。
   a. 既存のサイト: 「既存のサイト」を選択した場合、ここで既存のサイトのリストからサイトを選択するように要求されます。

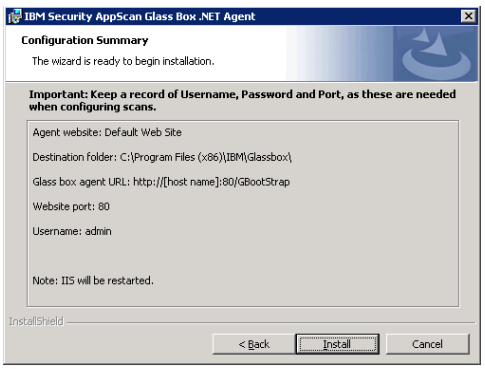
      注: 複数のサイトがある場合、ウィザードには、それらのサイトが優先順にリストされます。ウィザードは、いくつかのサイトに潜在的な問題があることを識別すると、それらのサイトを下にリストし、「非推奨」のラベルを付けます。ただし、順序や「非推奨」はあくまでも提案であり、場合によっては、「非推奨」のラベルが付いたサイトを選択しなければならない場合もあります。

      ヒント: どちらを選択した場合も、すべてのサイトのモニターが有効になりますが、可能な場合は、最初の スキャンの開始 URL として構成する予定のサイトを選択するようにしてください。
   b. 新規サイト: 「新規サイト」を選択した場合、ここでポートを割り当てるように要求されます。リモート・マシンからスキャンを行う場合に AppScan へのアクセスを許可するポートを定義する必要があります。

      重要: AppScan を構成する際にポート番号を提供する必要があります。

      注: 「テスト」ボタンを使用して、選択したポートが現在使用可能であるかを確認することができます。ただし、これは、「次へ」をクリックすると自動的に実行されます。
7. Glass box Web アプリケーション・エージェントのエージェント・ユーザー名およびパスワードを設定します。

   重要: Glass box を使用したスキャンの構成時に、これらの資格情報を提供する必要があります。
8. 実際のインストール・タスクを実行する前に、「概要」画面が表示されます。



重要: 「インストール」をクリックする前に、ユーザー名、パスワード、およびポートの記録を準備してください。これらは、AppScan の構成時に必要です。

9. 「インストール」をクリックします。

注: インストールには、IIS の再始動も含まれます。
このプロセスが完了すると、プロセスが成功したか失敗したかを示す最終メッセージが表示されます。

注: 何らかの理由でインストールが失敗した場合、最終ダイアログでトラブルシューティングに使用するインストール・ログへのリンクが提供されます。サーバー上の別のサイト (「非推奨」のラベルが付けられていた場合でも) または新規サイトへのインストールを試行することも有効な場合があります。どのような場合も、インストールを再試行する前に、アンインストールする必要があります。2 つのインストール・ログの場所は、%temp% フォルダーです。2 つのインストール・ログの名前は次のとおりです。

```
glassbox_setup_api.txt
glassbox_setup_msi.txt
```

アンインストール・プロセスには、IIS の再始動が含まれるので注意してください。

注: Glass box ログは次の場所に保存されます。

```
C:\Program Files (x86)\IBM\Glassbox\GBootStrap\GlassBoxLog.log
```

AppScan での Glass box エージェントの定義

このセクションでは、サーバー・サイドの Glass Box エージェントにアクセスするために AppScan を構成する方法について説明します。

このタスクについて

アプリケーション・サーバーに Glass Box エージェントをインストールしたら、このエージェントを AppScan に定義して、製品がエージェントにアクセスできるようにする必要があります。この処理を実行すると、AppScan は、すべての関連スキャンについて、Glass Box スキャン用に Glass Box エージェントを自動的に使用します (スキャン構成で選択解除した場合を除く)。

制約事項: 同じサーバー・エージェントを複数の AppScan マシンで定義できますが、1 つのエージェントは、同時に 1 つのスキャンに対してのみ使用できます。

制約事項: 複数のエージェントを定義できますが、1 つのスキャン構成で選択できるエージェントは 1 つだけです。

手順

1. 「構成」>「**URL** およびサーバー」タブで、「開始 **URL**」を設定します。この例では、URL にポート 8080 が含まれるので注意してください。

   ```
   https://altoro.testfire.net:8080/
   ```

2. 「**OK**」をクリックして、「構成」ダイアログ・ボックスを閉じます。
3. 「ツール」>「**Glass Box** エージェント管理」をクリックします。

   「Glass Box エージェント」ダイアログ・ボックスが表示され、すでに定義されているすべてのエージェントがリストされます。

4. 新規エージェントをリストに追加するには、  をクリックします。

   「Glass Box エージェント定義」ダイアログ・ボックスが表示されます。「Glass box エージェント URL」は、前のステップで入力した「開始 URL」に基づいて自動的に入力されます。

   重要: 「Glass box エージェント URL」には、「開始 URL」から抽出されたポート値 (この場合は 8080) が自動的に入力されます。別のポートにエージェントをインストールした場合は、ポート値を正しい値に置き換えてください。この例では、ポート値は 8888 に変更されています。

   ```
   http://altoro.testfire.net:8888/GBootStrap/
   ```

5. 必要に応じて、残りのフィールドとオプションを入力します。

オプション	説明
ユーザー名およびパスワード	エージェントをサーバーにインストールしたときに定義したユーザー名とパスワードを入力します。
エージェント・ログ設定:	(オプション) クリックすると、これらの設定が開きます。 **注:** エージェント・ログ設定は、サーバー・サイドのエージェントに保存されます。
最大ログ行数	(オプション) スライダーを使用して、ログのサイズを制限します。
ログ・コンテンツ	(オプション) ログに含める情報レベルを選択します。エラー: エラー・メッセージのみを含めます。警告: エラー・メッセージと警告メッセージを含めます。情報: エラー、警告、通知メッセージを含めます。デバッグ: すべてのメッセージを含めます。 Glass box ログは次の場所に保存されます。 `[Installation folder]\instrumentation.log`

AppScan はエージェント・サーバーへの接続を試行します。接続に成功すると、緑色の「接続済み」アイコンが表示されます。問題が発生した場合は、赤色のアイコンと、「エージェントに接続できません」や「資格情報が必要です」などのメッセージが表示されます。

注: お客様のサイトで HTTP と HTTPS の両方が提供されている場合、開始 URL が HTTPS であることを確認してください (そうなっていない場合は、HTTPS に変更してください)。

注: エラー・メッセージを受信した場合は、以下の Web サイトを参照してください。

http://www.ibm.com/support/docview.wss?uid=swg21567723

6. 「**OK**」をクリックして、定義ダイアログ・ボックスを閉じます。

   エージェントがリストに追加されます。

7. 「**OK**」をクリックして、リストを閉じます。

   これで、このマシン上でエージェントが定義されました。

Glass box スキャンの構成

スキャンは自動的に構成されますが、このセクションでは、変更することが推奨されるオプションについて説明します。

手順

1. 普通にスキャンを構成します。
2. 「構成」>「**Glass Box**」タブで、ドロップダウン・リストから定義済みの Glass box エージェントの 1 つを選択し、必要に応じて設定を調整します。

設定	詳細
この glass Box エージェントを使用	Glass Box エージェントがアプリケーション・サーバー上にインストールされ、AppScan 内で定義されている場合は、このエージェントを選択してスキャンで使用できます。開始 URL を入力した場合、AppScan は、適切なエージェントの自動的な選択を試行します。 エージェントが選択されると、AppScan は、エージェントへの接続を試行し、その試行が成功したかどうかを示します。 **注:** エージェントを選択したときに「資格情報が必要です」というメッセージが表示された場合、「ツール」 > 「Glass Box 管理」に指定されている資格情報が正しいことを確認してください。 必要なサーバーがドロップダウン・リストに表示されない場合は、「**Glass Box** エージェント管理」リンクをクリックして定義できます。 **制約事項:** 1 つのスキャンで使用する Glass Box エージェントは 1 つのみ選択できます。スキャンされているアプリケーションに複数のサーバーがある場合は、各サーバー・エージェントを別個に使用してスキャンする必要があります。

設定	詳細

Glass Box を探査ステージで使用	(デフォルトで選択されています。)
	
	この機能を使用して、サーバーの動作に影響するが応答内には表示されないパラメーターがサーバー・サイドのソース・コードに存在するかどうかを検査することにより、サイトのカバー範囲を拡大することができます。
	
	サーバー・サイド・コードの例:
	
	`String debugOn = request.getParameter("debug");`
	`if (debugOn == "true"){`
	`response.getWriter().println(SECRET_SERVER_DATA);`
	`}`
	
	この例では、開発者はパラメーター `"debug"` をコード内に残しています。これはサイト上のリンクには表示されませんが、攻撃者がこれを含む要求を送信した場合には、`SECRET_SERVER_DATA` が取得される可能性があります。

Glass Box をテスト・ステージで使用	(デフォルトで選択されています。) スキャンのテスト・ステージで Glass Box テストを送信するには、このチェック・ボックスを選択します。この機能は、ブラインド SQL インジェクションなどの特定のテストの成功または失敗を、より高い精度で検証できます。また、ブラック・ボックス手法によって検出できない特定のセキュリティー問題の存在を発見できます。
相当するブラック・ボックス・テストをスキップ	(デフォルトでは選択解除されています。) これは、同じぜい弱性 (WASC 脅威の分類) に対して Glass box テストとブラック・ボックス・テストの両方が送信されることを意味します。この理由は、一般的に、Glass box テストのほうが正確度が高いだけではなく、より詳細な結果を提供しますが、同等のブラック・ボックス・テストが成功する一方で Glass box テストが失敗する場合があるためです。ブラック・ボックス・テストをスキップしてもご使用のアプリケーションでの結果が変わらない場合は、このチェック・ボックスを選択することでスキャン時間を削減することができます。

ステータス・バーが、Glass box スキャンが有効にされ、スキャンを開始する準備ができたことを示します。

Glass Box によるスキャン

このセクションでは、Glass Box スキャンについて説明します。

このタスクについて

Glass Box エージェントを AppScan に定義すると、Glass Box スキャンがデフォルトで有効になります。「スキャン構成」ダイアログ・ボックスを使用すると、正しいサーバー・エージェントが選択されていること、およびスキャンの一部として Glass Box スキャンが実行されるように構成されていることを確認することができます。

Glass Box スキャンにより、探査ステージで非表示の URL を検出し、テスト・ステージで追加の問題と情報を検出することができます。

手順

1. 「構成」>「**Glass Box**」ビューをクリックします。
2. 使用したいエージェントをドロップダウン・リストから選択します。

注: 必要なエージェントがリストに表示されていない場合は、「**Glass Box** エージェント管理」リンクをクリックして、エージェントを定義します。

3. 2 つの主要な Glass box スキャン・オプションのいずれかまたは両方が選択されていることを確認します。
   - Glass Box を探査ステージで使用
   - Glass Box をテスト・ステージで使用

   注: 「相当するブラック・ボックス・テストをスキップ」チェック・ボックスは、デフォルトでクリアされています。これは、同じぜい弱性 (WASC 脅威の分類) に対して Glass box テストとブラック・ボックス・テストの両方が送信されることを意味します。この理由は、一般的に、Glass box テストのほうが正確度が高いだけではなく、より詳細な結果を提供しますが、同等のブラック・ボックス・テストが成功する一方で Glass box テストが失敗する場合があるためです。ブラック・ボックス・テストをスキップしてもご使用のアプリケーションでの結果が変わらない場合は、このチェック・ボックスを選択することでスキャン時間を削減することができます。
4. 「スキャン」>「フルスキャン」をクリックし、スキャンを開始します。

   スキャンが開始され、Glass box スキャンがアクティブであることを示すステータス・バー・メッセージが表示されます。

   スキャン結果には、「問題情報」タブの Glass box データが含まれます (使用可能な場合)。

Glass Box エージェントのアンインストール

このセクションでは、.NET サーバーから Glass Box エージェントをアンインストールする方法について説明します。

このタスクについて

このタスクを実行するには、アプリケーション・サーバーにアクセスする必要があります。

手順

以下のいずれかを実行します。

- Microsoft Windows の「プログラムの追加と削除」機能を使用します。
- GB_.NET_Setup.exe を再実行し、ウィザードで「アンインストール」オプションを選択します。

部分スキャン

スキャン・メニューのいくつかのオプションによって、スキャンの一部分を実行したり、ご使用のサイトの一部分をスキャンしたりすることができます。

タスク	説明
探査のみ	AppScan で、ご使用のサイトを探査し、サイト・モデルを構築しますが、スキャンのテスト・ステージへは進みません。要件を満たしているかどうか確認するために収集されたサイト・モデルとアプリケーション・データを調査し、さらに、必要な場合は手動で探査を行い、その後フル・スキャンに進みます。

タスク	説明
テストのみ	事前に「探査のみ」を実行している場合、または、フル・スキャンを完了前に停止した場合、AppScan で、既存の探査結果を使用して、ご使用のサイトをテストすることができます。この機能は、例えば、サイトの構造には変更がないけれども、実施されたセキュリティー上の変更の反映を確認したい場合などに、スキャン時間を節約することができます。 **注:** 多くの場合、フルスキャン中に、テスト・ステージで明らかになるサイトの部分が存在します。 その場合、AppScan は、探査ステージおよびテスト・ステージの追加フェーズを実行します。1 つのスキャンには、このような複数のフェーズが含まれることがあります。「探査のみ」または「テストのみ」の機能を使用してスキャンを実施すると、結果は単一フェーズ・スキャンとなります。 これには、サイトのすべての部分が含まれていない可能性があります。
再スキャン (フル)	現在のスキャン結果を削除して、現在の構成を使用してフルスキャンを実行します。
再探査	現在のスキャン結果を削除して、現在の構成を使用して探査ステージのみ実行します。
再テスト	現在のテスト結果を削除して、新規テスト・ステージを現在の構成と探査結果を使用して実行します。 **Limitation:** 再テスト中の応答がオリジナルの応答と同じ場合は、結果は更新されず、オリジナルの応答のタイム・スタンプが表示されます。

マルチステップ操作のみをスキャン

マルチステップ操作を定義し、それを使用してサイトのその部分だけをテストすることができます。

このタスクについて

マルチステップ操作は、アプリケーションの特定の部分に到達するために特定の順序で送信される必要のある一連の要求です。 (詳細については、 98 ページの『「マルチステップ操作」ビュー』を参照してください。) これらの操作は、スキャンするアプリケーションの一部にすぎない場合もあります。

手順

1. 少なくとも 1 つのマルチステップ操作を含むスキャンを構成します。 (98 ページの『「マルチステップ操作」ビュー』 を参照してください。)
2. 推奨: スキャン・エキスパートを実行して構成を評価します。(172 ページの『スキャン・エキスパート (Scan Expert)』 を参照してください。)
3. 「スキャン」メニューで、「マルチステップ操作のみをスキャン」をクリックします。

   AppScan は構成された操作をスキャンし、結果を表示します。

   注**:** シーケンスに直接関連するテストのみが送信されます。 (例えば、サイト・インフラストラクチャー・テストは送信されません。) これは、スキャンが終了したときに、ステータス・バー (左下にあります) に、送信されるテストが他にもあることが示される可能性があることを意味します。サイトの一部 でフル・スキャンを実行する方法としてスキャンのマルチステップ操作機能を使用している場合、(次のステップである)「テストのみ」を続行してこれらのテストを送信する必要があります。
4. (オプション) 「スキャン」**>**「テストのみ」をクリックして、テスト対象となっているサイトの部分のフル・スキャンを実行します。

   インフラストラクチャーおよび他の残りのテストがサイトに送信され、結果がスキャン結果に追加されます。

スキャン中の構成の変更

スキャンを開始した後で構成を変更する場合、スキャンを再実行するか、または少なくともテスト・ステージを再実行して、変更の影響を調べる必要があります。一般に、以下のようになります。

- 探査構成を変更した場合、探査およびテスト (「スキャン」>「再スキャン」>「再スキャン **(フル)**」) を実行して、アプリケーションを完全に再スキャンする必要があります。
- テスト構成を変更した場合は、探査ステージを再度実行する必要はなく (探査ステージが完了している場合)、アプリケーションを再テストするだけで済みます (「スキャン」>「再スキャン」>「再テスト」)。

スキャン結果をエクスポートする

スキャンが完了すると、結果がメイン・ウィンドウに表示されます。 別のビュー (問題、修復、アプリケーション・データ) では、スキャン結果を用途に応じてフィルタリングして提供します。

以下のさまざまな方法で、スキャン結果を AppScan からエクスポートすることができます。

- AppScan レポートを構成し生成します。PDF または他の読み取り可能でポータブルなフォーマットにエクスポートします。 247 ページの『第 10 章 レポート』を参照してください。
- テスト・バリアントを問題から選択し、AppScan でそのバリアント情報の zip ファイルを新規 E メールに添付できるようにします。 219 ページの『第 8 章 結果:セキュリティー問題』を参照してください。
- 完全なスキャン結果からデータベースまたは XML ファイルを生成します。後述の 『スキャン結果 DB と XML ファイルを生成する』を参照してください。

スキャン結果 DB と XML ファイルを生成する

始める前に

完全なスキャン結果を XML ファイルまたはリレーショナル・データベースとしてエクスポートできます。データベース・オプションでは、結果が Firebird データベース構造にエクスポートされます。これはオープン・ソースで、ODBC および JDBC 標準に準拠します。)

XML 出力のスキーマの名前は **ScanExport.xsd** で、AppScan **\Docs** フォルダーで見つけることができます。例えば、次の場所にあります。

```
[AppScan Standard installation folder]\Docs\ScanExport.xsd
```

手順

1. 「ファイル」>「エクスポート」をクリックして **XML** または **DB** を選択します。
2. エクスポート先の場所を参照し、ファイルの名前を入力します。
3. 「保存」をクリックします。

次のタスク

『エクスポートされたデータベース・ファイルで情報にアクセスする』

エクスポートされたデータベース・ファイルで情報にアクセスする

手順

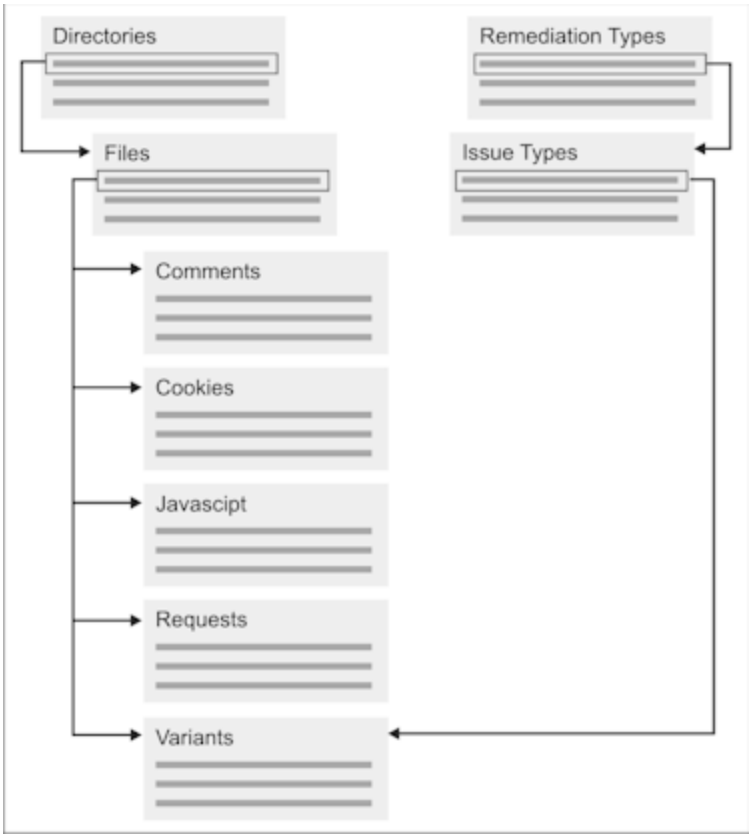
1. Firebird データベース・エンジンを次のサイトからダウンロードします。http://firebird.sourceforge.net/index.php?op=files&id=engine

2. Firebird ドライバーをダウンロードします (いずれかを選択します)。
   - **Firebird ODBC** ドライバー**:** http://firebird.sourceforge.net/index.php?op=files&id=odbc
   - **Firebird JDBC** ドライバー**:** http://firebird.sourceforge.net/index.php?op=files&id=jaybird
3. ODBC または JDBC 準拠クライアントを使用して、ユーザー名 `SYSDBA` とパスワード `masterkey` で Firebird を開きます。

Firebird データベース構造

スキャン結果が Firebird データベース構造にエクスポートされると、多くの ODBC および JDBC データベース・ビューアーのいずれかを使用して表示することができます。関連するデータベース・コンポーネントの構造を下記の図に示し、次のサブセクションで説明します。

注**:** データベースのフィールドの一部は AppScan の内部フィールドで、ユーザーに関連しません。これらのフィールドは、以下の表で「AppScan 内部」としてマークされています。



ディレクトリー

データベースのディレクトリー・セクションには、スキャンからの個々のディレクトリーまたはサブディレクトリーの行があります。

フィールド名	説明/コメント
ID	ディレクトリーの AppScan ID。
NAME	ディレクトリー名
PARENTID	このディレクトリーが含まれるディレクトリー (これがサブディレクトリーの場合)

フィールド名	説明/コメント
PATH	ディレクトリー・パス
DIRTYPE	ディレクトリー・タイプ:ホスト/アプリケーション

ファイル

データベースのファイル・セクションには、個々のファイルの行があります。

フィールド名	説明/コメント
ID	ファイルの AppScan ID。
FILENAME	ファイル名
PARENTID	このファイルが含まれるディレクトリーの ID

コメント

コメント・セクションには、サイト・ページで検出された個々の HTML コメントの行があります。

フィールド名	説明/コメント
ENGINEID	コメントの AppScan ID
FILEID	コメントが検出されたファイルの ID
SHORTTEXT	コメントのテキスト (切り捨てられることがあります)

Cookie

Cookie セクションには、検出された個々の Cookie の行があります。

フィールド名	説明/コメント
ID	Cookie の AppScan ID
REQCOOKIEID	AppScan 内部
RESPCOOKIEID	AppScan 内部
NAME	Cookie ファイルの名前
COOKIEVALUE	Cookie の値
SETINURL	Cookie のソース URL
FILEID	Cookie が保存されるファイルの AppScan ID
PATH	Cookie のパス属性
COOKIEDOMAIN	Cookie のドメイン属性
EXPIRES	Cookie の期限切れ日付
SECURE	Cookie のセキュア属性

問題のタイプ

問題のタイプ・セクションには、検出された個々の問題の行があります。

フィールド名	説明/コメント
ENGINEID	この問題の AppScan ID

フィールド名	説明/コメント
NAME	GUI に表示される問題の名前
INVASIVE	問題が安全でないかどうか: Y/N
SEVERITY	AppScan GUI で示される、この問題の重大度コード: 4 = すべて 3 = 高 2 = 中 1 = 低 0 = 情報
THREATCLASS	GUI に表示される脅威の分類
THREATCLASSREFERENCE	この分類におけるインターネット参照への URL (関連する場合)
REMEDIATIONTYPEID	修復タイプの AppScan ID
ADVISORYID	AppScan 内部
ENTITYTYPE	AppScan 内部
INFRASTRUCTURE	AppScan 内部

Javascript

JavaScript セクションには、サイト・ページで検出された個々の Javascript の行があります。

フィールド名	説明/コメント
ENGINEID	JavaScript の AppScan ID
FILEID	Javascript が検出されたファイルの ID
SHORTTEXT	JavaScript のテキスト (切り捨てられることがあります)

修復タイプ

修復セクションには、個々の修復の行があります。

フィールド名	説明/コメント
ENGINEID	修復タイプの AppScan ID
NAME	GUI に表示される修復タイプの名前
REMEDIATIONPRIORIY	修復の優先順位コード (1 = 最優先)

要求

要求セクションには、送信された個々のテスト要求の行があります。

フィールド名	説明/コメント
ENGINEID	テスト要求の AppScan ID
FILEID	要求が送信されたファイルの AppScan ID
URL	要求の URL

フィールド名	説明/コメント
QUERY	要求に送信されたパラメーター
STATUS	AppScan 内部
REASONID	AppScan 内部
XMLTYPE	AppScan 内部
LOGINTYPE	AppScan 内部

スクリプト・パラメーター

このセクションには、テスト要求に送信された個々のパラメーターの行が含まれています。

フィールド名	説明/コメント
ENGINEID	パラメーターの AppScan ID
FILEID	パラメーターが送信されたファイルの ID
NAME	送信された実パラメーター
PARAMETERTYPE	パラメータ・タイプ:Get/Post

バリアント

バリアント・セクションには、個々のバリアントの行が含まれています。

フィールド名	説明/コメント
ENGINEID	バリアントの AppScan ID
ENTITYNAME	バリアントが送信される Cookie の名前 (該当する場合)
FILEID	バリアントが送信されたファイルの ID
ISSUETYPE	GUI に表示される問題のタイプの名前
REMEDIATIONTYPE	AppScan 内部
SEQUENCEINDEX	AppScan 内部

第 7 章 結果:アプリケーション・データ

AppScan では、「アプリケーション・データ」、「セキュリティーの問題」、および「修復タスク」といった 3 つの方法でスキャン結果の表示と処理を行うことができます。本セクションでは、「アプリケーション・データ」ビューについて説明します。

このビューは、スキャンのテスト・ステージを開始する前に、スキャンでカバーしたいサイトのすべての部分が実際に探査されたかどうかを確認する場合に便利です。このビューでは、テスト・ステージを参照せずに、探査ステージの結果のみを表示します。

「ビュー・セレクター」で、次のアイコンをクリックします。

アプリケーション・データ:アプリケーション・ツリー

「アプリケーション・ツリー」には、探査したフォルダー、URL、ファイルが表示されます。

探査ステージ後、「アプリケーション・ツリー」を照会すると、ご使用のアプリケーションが見やすく表示され、すべてが探査されたことが確認できます。

「アプリケーション・ツリー」でノードを選択すると、「結果リスト」にリストされるデータをフィルタリングできます。特定のタイプのデータに対する結果がない場合は、ツリー内の上位ノードを選択してください。「マイ・アプリケーション」を選択すると、特定のタイプのすべてのデータがリストされます。

アプリケーション・データ:結果リスト

「結果リスト」には、アプリケーション・ツリー内で選択されたノードについて、探査ステージ中に検出された URL、パラメーター、スクリプトのリストが表示されます。以下の表に、データのカテゴリーを示します。

データ・タイプ	説明
212 ページの『要求』	AppScan がアクセスした URL。
212 ページの『パラメーター』	AppScan が検出したスクリプトおよびそれに関連するパラメーター。
213 ページの『Cookie』	AppScan が検出した Cookie。
ページ	AppScan によって探査されたすべてのページ。
214 ページの『失敗した要求』	要求に応答しなかったリンク。
215 ページの『フィルタリングされた URL』	AppScan のデフォルト設定、またはユーザーが定義した探査フィルター (66 ページの『「除外するパスおよびファイル」ビュー』を参照) が原因で、探査されなかった URL。

データ・タイプ	説明
216 ページの『ユーザーによる対話が必要』	AppScan では自動で設定できなかった、ユーザー入力が必要な URL。フォーム・パラメーター入力の定義方法については、 53 ページの『「ログイン」タブ』を参照してください。
217 ページの『コメント』	ユーザーがアクセスできる Web ページ上のコメント。
217 ページの『JavaScript』	AppScan が検出した JavaScript。

「結果リスト」で以下のようにします。

- 各データ・カテゴリー (要求、パラメーターなど) 上にマウスを移動し、そのカテゴリー内の (アプリケーション・ツリー内で選択したノードに関する) 項目数を確認します。
- カテゴリーをクリックすると、そのカテゴリー内の項目が (結果リストに) 表示されます。
- 結果リスト内の項目をクリックして、その項目の詳細を詳細ペインに表示します。

「結果リスト」と、各データ・タイプの「詳細ペイン」については、次のセクションで説明します。

要求

このビューには、AppScan が有効な応答を受信した要求がリストされます。この応答を基に、AppScan はサイトの弱点を明らかにするテストを生成します。テストは、テスト・ステージ中に送信されます。

要求または応答の本文に XML (XHTML または SOAP を含む) が含まれる場合は、「認識された URL」アイコンは、「XML」アイコン  に置き換わります。

結果リストの要求

「結果リスト」には、AppScan によって認識された各ページの URL と、方式およびパラメーターが表示されます。

- 認識された URL を表示するには、要求を右クリックして「ブラウザーで表示」をクリックするか、URL を選択して「詳細ペイン」の「ブラウザーで表示」リンクをクリックします。
- URL のマニュアル・テストを作成するには、「アクセスした **URL**」項目を右クリックし、「マニュアル・テスト」をクリックするか、URL を選択して、「詳細ペイン」の「マニュアル・テスト」リンクをクリックします。(詳しくは、 236 ページの『マニュアル・テスト』 を参照してください。)

「詳細ペイン」の要求

「詳細ペイン」には、「ブラウザーで表示」と「マニュアル・テスト」へのリンクが表示されます。これらのリンクは、「結果リスト」での右クリック・コマンドと同様に動作します。

「要求/応答」タブが表示され、このタブには「結果リスト」で選択した URL の、要求および即時の応答が示されます。

パラメーター

「パラメーター」とは、1 つ以上のパラメーターを含む要求のことです。

「結果リスト」には、探査ステージ中に検出されたパラメーターがすべて表示されます。このリストの URL は、悪意のあるアタックに対して脆弱である可能性が最も高い URL です。このリストは、一連の有用なテスト要求をスキャンが生成したかどうかを評価する際に非常に重要となります。

AppScan は、「スクリプト・パラメーター」リストのパラメーターごとに、名前、タイプ、値、URL (結果ペイン) と値 (詳細ペイン)、追跡されるかどうかを表示します。同じパラメーター名が複数回リストされることがありますが、URL が異なるか、同じ URL でも値が異なる場合です。

以下の表は、リスト内の項目を右クリックして選択可能なオプションを示しています。

表 *8.* 右クリック・オプション

オプション	機能
URL をコピー	選択した URL をクリップボードにコピーします。
「パラメーターおよび Cookie」タブのリストに追加	右クリックして「パラメーターおよび **Cookie** に追加」リストを選択することで、選択したパラメーター名 (すべての値) を「構成」ダイアログ・ボックス内のリストに追加します。AppScan によるこのパラメーターの処理方法を構成するために「パラメーター定義」ダイアログ・ボックスが開きます。
スキャンから、このパスとパラメーター値の組み合わせを除外する	特定のパラメーター値を、特定の URL で発生した場合にスキャンから除外します。このオプションを選択すると、関連データが指定された状態で「除外または例外を編集」ダイアログ・ボックスが開きます。 例 URL が `http://site/command` であるサイトと「action」という名前のポスト・パラメーターについて考えます。この値はサーバーから以下のようにそれぞれ異なる応答をトリガーします。 • `action=login` は、ログイン・ページにリダイレクトします。 • `action=logout` は、セッションの期限が切れます。 • `action=clean` は、サーバーがユーザー・データを削除します。 AppScan がこのサイトをスキャンできるようにするためには、`action=logout` のときには `http://site/command` を、もしくは `action=login` またはその他の値ではないときに `clean` を除外する必要があります。パラメーター名 `action` と値 `logout` または `clean` を持つ `http://site/command` を除外するこの機能を使用して、除外を実行できます。 詳細については、 68 ページの『新規除外または新規例外の追加』 を参照してください。
選択したパラメーターをテストしない	1 つ以上のパラメーター名 (すべての値) をスキャンのテスト・ステージから除外します。この設定は、指定したパラメーターのすべての値に適用されます。これは、探査ステージには影響しません。 「構成」ダイアログ・ボックスの「パラメーターおよび Cookie」ビュー内のリストにパラメーター名が追加され、その「テスト除外」値が「はい」に設定されます。 詳細については、 78 ページの『「パラメーターおよび Cookie」ビュー』 を参照してください。

Cookie

Cookie はスキャン中に AppScan が検出したすべての Cookie をリストします。対象となる Cookie が応答によって設定されたか、Javascript で生成されたか、スキャン前からホスト上にあったかに関わりません。

- 「結果リスト」には、探査ステージ中に検出されたすべての Cookie が表示されます。各 Cookie のリストには、追跡されているかどうか、名前、Set-cookie URL、値、テストから除外するかどうか、パス、ドメイン、有効期限が切れる日付、セキュアかどうか、およびコンテキストが表示されます。

  注: リストされる URL は、(Set Cookie コマンドなどの他のものがあった場合でも) Cookie を設定した応答につながっている URL です。応答によって設定された Cookie ではない場合 (Javascript によって生成された、もともとホスト上にあった、など) は、「応答 URL」フィールドには「なし」が表示されます。
- 右クリックして「この **Cookie** をパラメーターおよび **Cookie** タブに追加」リストを選択することで、「構成」ダイアログ・ボックスのリストに任意の Cookie を追加することができます。AppScan によるこの Cookie の処理方法を構成するために「パラメーター定義」ダイアログ・ボックスが開きます。
- 特定の Cookie が選択された場合は、「詳細」ペインに次のものが表示されます。

項目	説明
パス	その Cookie の送信先である、アプリケーション内の特定のフォルダーまたはサブフォルダー。パスの属性は、その Cookie が有効になっているドメインの URL のサブセットを指定するために使用されます。Cookie がすでにドメイン・マッチングを通過している場合 (次の項目)、URL のパス名コンポーネントとパス属性が比較され、一致するとその Cookie は有効と判断され、URL 要求とともに送信されます。
ドメイン	その Cookie の送信先のドメインまたはサブドメイン。(ドメインが設定されていない場合は、Cookie は Set Cookie コマンドを発行したドメインとすべてのサブドメインに送信されます。)
期限切れ	Cookie が期限切れとなり、ユーザーのマシンから削除される日付と時刻。
セキュア	**はい** (保護された) または **いいえ**。「セキュア」のマークが付くと、Cookie はホストとの通信チャネルがセキュアな場合にだけ送信されます (現在は HTTPS サーバーのみ)。「セキュア」が指定されていない場合、Cookie はすべてのチャネル経由で送信しても安全だと判断されます。
要求 URL	AppScan が Cookie とともに送信した最初の要求。

失敗した要求

失敗した要求とは、有効な応答を返さなかった送信済みの要求のことです。リンク切れが発生するのは通常、サイトがダウンしているか、通信上のその他の問題が発生したか、要求したページの代わりにエラー応答の状況を要求が返したときです。

注: アプリケーション・ツリーでは、エラー応答のみ 含まれている URL は、取り消し線の書式設定 (URL を棒線で消した状態) で表示されます。

- エラー・ページが期待される応答である場合
- スキャン全体を繰り返すのではなく、リンク切れについてのみ、要求を再送できます。探査ステージ実行後にアプリケーションを変更または修正した場合は、次の手順を実行してリンク切れを再探査します。

  注: ログインが必要なアプリケーションの場合は、AppScan を手動でログイン (53 ページの『「ログイン」タブ』を参照) してから次の手順を実行してください。ログインせずに実行すると、リンク切れは通常の使用パターン外で探査されます。
- 「結果」ペインの「失敗した要求」を選択すると、すべてのリンク切れを表示することができます。
- 「失敗した要求をすべて再試行」をクリックすると、それらのリンクは「リンク切れ」リストから削除され、「アクセスされていないリンク」リストに追加されます。AppScan は探査ステージを続行し、可能な場合に「アクセスされていないリンク」リストのリンクにアクセスします。「アクセスされていないリンク (Unvisited Links)」の探査がすべて終わると、探査ステージは終了します。

注: スキャン中に AppScan とサーバー間の通信に問題が発生すると、一部のリンクに「リンク切れ」のマークが付くことがあります。通信の問題が発生すると、AppScan は 90 秒間、要求の再送を試みます。90 秒の間に接続が回復しないと、スキャンは停止します。メイン・ウィンドウの「通知 (Notice)」パネルによって問題が通知され、タイムアウトのカウントダウンが表示されます。この通知が表示されたら、リンクのトラブルシューティングを試みる前に、AppScan とご使用のアプリケーションとの間の接続を修復してください。

- 「詳細ペイン」では、「ブラウザーで表示」ボタンをクリックすると、特定のリンク切れの応答ページが表示されます。

フィルタリングされた URL

フィルタリングされた URL とは、標準のフィルター、またはスキャンの構成時に定義されたフィルター(66 ページの『「除外するパスおよびファイル」ビュー』 を参照) によって探査から除外されたために、AppScan がアクセスしなかった URL のことです。

「結果リスト」のフィルタリングされた URL

「結果リスト」には、探査されなかった URL と、「フィルター・タイプ」(そのページがフィルタリングされた理由) が表示されます。

フィルタリングされた URL を表示するには、フィルタリングされた URL を右クリックし、「ブラウザーで表示」をクリックします。

以下の表は、構成可能な主要フィルターをリストしています。

フィルター名	意味および構成方法
深度限界	「構成」>「探査オプション」>「スキャン制限」>「クリックの深さ制限」で構成された制限のために、URL がフィルタリングされました。
ファイル拡張子フィルター	拡張子は、「構成」>「除外するパスおよびファイル」>「除外するファイル・タイプ」にリストされているうちのいずれかです。
類似の可能性が高い DOM	以前に探査したページと同じ構造 (DOM) が応答に含まれると AppScan が判断し、テストする新規要素が含まれていないために、フィルタリングによってスキャンから除外されたページ。「構成」>「探査オプション」>「メイン」>「構造 **(DOM)** を基準として類似の可能性が高いページをフィルター」によって制御されます。
パス・フィルター	パスは、「構成」>「除外するパスおよびファイル」>「除外するパス」にリストされているうちのいずれかです。
パスの制限	「構成」>「探査オプション」>「スキャン制限」>「冗長なパスの制限」で構成された制限のために、URL がフィルタリングされました。
類似した本文	応答本体のコンテンツが以前に探査された要求の応答本体のコンテンツと類似しているためにフィルタリングによってスキャンから除外された、(類似の DOM によってフィルタリングされなかったページからの) 要求。「構成」>「探査オプション」>「メイン」>「構造 **(DOM)** を基準にして類似ページをフィルター」によって制御されます。
類似の DOM	ページの構造 (DOM) が以前に探査したページの構造と類似しており、テストする新規要素が含まれていない可能性が高いために、フィルタリングによってスキャンから除外されたページ。「構成」>「探査オプション」>「メイン」>「構造 **(DOM)** を基準にして類似ページをフィルター」によって制御されます。
合計リンク・アクセス数の制限	「構成」>「探査オプション」>「スキャン制限」>「合計ページ制限」で構成された制限のために、URL がフィルタリングされました。

フィルター名	意味および構成方法
未テストの Web サーバー	ドメインが「開始 URL」のドメインと異なっており、「構成」>「**URL** およびサーバー」>「追加のサーバーおよびドメイン」で構成された追加ドメインの 1 つではありません。

「詳細ペイン」のフィルタリングされた URL

「詳細ペイン」には、ブラウザーで URL を表示するリンク「ブラウザーで表示」が表示されます。 これは、「結果リスト」で、「ブラウザーで表示」を右クリックしたときと同じ機能です。

「要求/応答」タブには、URL がフィルタリングで除外されなければ URL に送信されたはずの要求が表示されます。

関連資料:

66 ページの『「除外するパスおよびファイル」ビュー』
「構成」ダイアログ・ボックスの「除外するパスおよびファイル」ビューです。

72 ページの『「探査オプション」ビュー』
「構成」ダイアログ・ボックスの「探査オプション」ビューです。

ユーザーによる対話が必要

「ユーザーによる対話が必要」とは、AppScan では設定できないユーザー入力を必要とするために、送信されなかった要求のことです。入力を設定するように AppScan を構成できます。 92 ページの『「フォームの自動入力」ビュー』 を参照してください。一部のアプリケーション・パラメーターが足りないか、自動フォーム入力を使用しない選択をした場合、確認のために AppScan が対話型 URL のリストを表示します。

- 対話型 URL のリストを確認することができます。これらのページをスキャン対象にするには、「マニュアル探査」で、必要なユーザー情報を入力します。
- 対話型 URL のリストを十分に確認したうえで、必要なデータを入力し、要求を送信することをお勧めします。AppScan はテスト・ステージでそれらの URL を含めます。
- AppScan がこれらの要求を送信できるようにすることで、以前にアクセス不能であったサイトの新規部分がアクセス可能になる場合があります。したがって、対話型 URL にアクセスした後は、アプリケーションを再探査 (「スキャン」>「再スキャン」>「探査」) する必要があります。

『対話型 URL の手動による探査』を参照)。

対話型 URL の手動による探査

このタスクについて

対話型 URL とは、AppScan では設定できず、ユーザーによる入力を必要とするために、送信されなかった要求のことです。一部のアプリケーション・パラメーターが足りないか、自動フォーム入力を使用しないことを選択した場合、スキャンの最後に AppScan が対話型 URL のリストを表示します。

手順

1. 「データ・ビュー」>「結果リスト」で「ユーザーによる対話が必要」をクリックします。

   対話型入力の URL のリストが表示されます。

   注**:** 同じ URL が複数回表示される場合がありますが、各インスタンスはフォームが異なります。
2. リストの URL を右クリックし、「この **URL** を手動で探査」をクリックします。

「マニュアル探査」ボタンが表示されたブラウザーが表示され、その URL が開きます。マニュアル探査を実行します (150 ページの『マニュアル探査を記録する』を参照)。

マニュアル探査が終了したら、AppScan が新しい探査を分析します。

新しい URL が検出されると、探査の継続 (「スキャン」>「スキャンを継続」>「探査」) を促すメッセージが表示されます。

- 新しい URL は検出されなかったが新しいテストが作成された場合は、引き続きテスト・ステージを実行 (「スキャン」>「スキャンを継続」>「テスト」) するように促すメッセージが表示されます。
- 新しい URL が検出され、新しいテストも作成された場合は、探査とテストの両方を継続 (「スキャン」>「スキャンを継続」>「フル・テスト **(Full Test)**」) するように促すメッセージが表示されます。

コメント

コメント とは、探査ステージ中に AppScan が検出した HTML コメントのことです。HTML のページに隠されているコメントには、ハッカーにとって役に立つ情報が書かれていることがあります。意図的にまたは偶然に、開発者が最後のページに開発者自身やその他の開発者のためのコメントを残していることが時折あります。ハッカーはこうしたコメントから、デバッグのパスワードといった役立つ内部情報を入手します。

「結果リスト」のコメント

コメントのリストには、コメントの 1 行目とコメントが記載されている最初の URL が表示されます。AppScan が同じコメントを複数回検出した場合、最初のインスタンスのみリストされます。

「詳細ペイン」のコメント

「詳細ペイン」には、「結果リスト」で選択した項目のコメント全体が表示されます。ここでコメントを検討し、最終的なアプリケーションからどのコメントを削除する必要があるかを判断します。

JavaScript

JavaScript は、探査ステージ中に AppScan が検出した JavaScript のコードをリストします。

「結果リスト」の JavaScript

このリストには、JavaScript の 1 行目と、その JavaScript が検出された最初の URL が表示されます。同じスクリプトが複数の URL で検出された場合は、最初のインスタンスのみがリストされます。

「詳細ペイン」の JavaScript

「詳細ペイン」には、「結果リスト」で選択した項目のスクリプト全体が表示されます。ここでコメントをもとにコードを検討し、最終的なアプリケーションからどれを削除する必要があるかを判断します。

アプリケーション・データ:詳細ペイン

「アプリケーション・データ」ビューの「詳細ペイン」には、選択したデータ・タイプに応じて各種データおよびツールバー・オプションが表示されます。

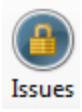
データ・タイプ	ツールバー・オプション
要求	「ブラウザーで表示」、「エラー・ページとして設定」、「マニュアル・テスト」、「検索」(単語/句)
パラメーター	「要求」(切り替え)、「ブラウザーで表示」、「エラー・ページとして設定」、「マニュアル・テスト」、「検索」(単語/句)
Cookie	なし。
ページ	ページ情報タブ。 「要求/応答」タブ:「要求」(切り替え)、「ブラウザーで表示」、「エラー・ページとして設定」、「マニュアル・テスト」、「検索」(単語/句)
失敗した要求	「ブラウザーで表示」、「エラー・ページとして設定」、「検索」(単語/句)
フィルター済み	「ブラウザーで表示」、「エラー・ページとして設定」、「検索」(単語/句)
ユーザーによる対話が必要	「この URL を手動で探査」、「検索」(単語/句)
コメント	なし。
JavaScript	「検索」(単語/句)。

第 8 章 結果:セキュリティー問題

AppScan では、「アプリケーション・データ」、「セキュリティーの問題」、および「修復タスク」といった 3 つの方法でスキャン結果の表示と処理を行うことができます。このセクションでは、「セキュリティー問題」ビューについて説明します。

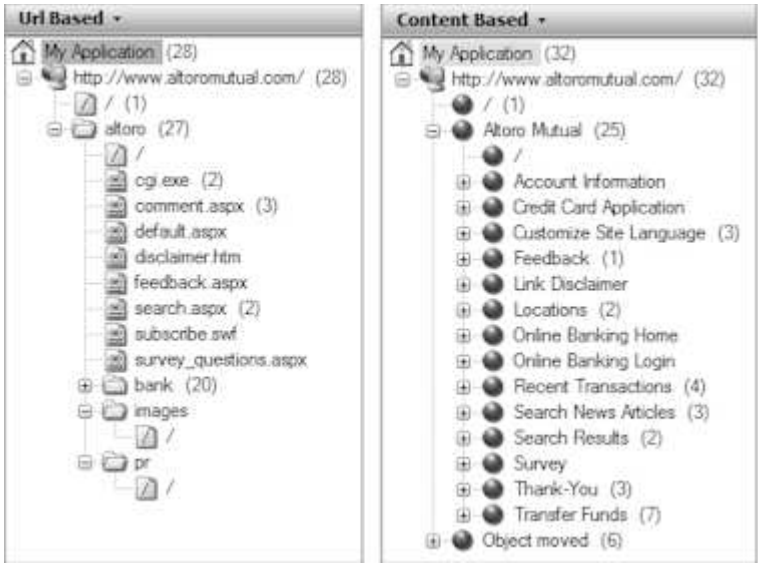
「セキュリティー問題」ビューには、スキャンの結果に関する結果へのアクセスが含まれています。結果を概略レベルで表示することも、特定のテストまたはオブジェクトを選択して詳細にアクセスすることもできます。これらの詳細には、アドバイザリー、推奨される修正、要求/応答、および問題が発生したテスト・バリアント間の差が含まれます。問題の重大度を操作したり、(修正ありまたは修正なしで) テストを再送したり、問題に基づいたレポートを作成したりできます。

「ビュー・セレクター」で、次のアイコンをクリックします。



セキュリティー問題: アプリケーション・ツリー

「アプリケーション・ツリー」には、スキャンされたアプリケーションのフォルダーとファイルが表示されます。ツリーの各ノードには、カウンターがあります。ここには、ノードに含まれる問題の数が示されます。



アプリケーション・ツリーでは、次のことができます。

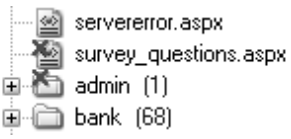
- ノードを選択して、「結果 リスト」に表示する問題をフィルターに掛けます。
- 右クリック・メニューを使用して、「ブラウザーで表示」、「マニュアル探査」、「マニュアル・テスト」、「URL をクリップボードにコピー」、「URL をスキャンから除外」を実行できます。(23 ページの『アプリケーション・ツリーの右クリック・メニュー』 を参照してください。)

- コンテンツ・ベースの表示ルールを定義しておくと、ペインの上部にあるコンボ・ボックスをクリックして、URL ベースのビューとコンテンツ・ベースのビューの間で切り替えを行うことができます。(106 ページの『「コンテンツ・ベースの結果」ビュー』 を参照してください。)

URL をスキャンから除外

アプリケーション・ツリーの URL またはノードを右クリックして「スキャンから除外」を選択すると、それらを今後のスキャンから除外することができます。(その URL またはノードをスキャン対象に戻すには、再度右クリックして「スキャンに含める」を選択するだけです。)

URL またはノードがスキャンから除外されると、アプリケーション・ツリーのアイコン上に赤い **X** が 表示されます。



この方法で URL を除外すると、「除外」項目は「除外するパスおよびファイル」リスト (66 ページの『「除外するパスおよびファイル」ビュー』を参照してください) に追加されます。

セキュリティー問題: 結果リスト

「結果リスト」には、「アプリケーション・ツリー」で選択されたノードに関係する問題が表示されます。「マイ・アプリケーション」ノードを選択していると、「結果リスト」にはご使用の Web アプリケーションで検出されたすべての問題が表示されます。

問題はタイプ別にグループ分けされます。個々のタイプの下にはすべての URL がリストされます。各 URL の下には、すべての問題がリストされます。(問題の個別のバリアントは、「結果リスト」には表示されませんが、「詳細ペイン」から参照することができます。)

ツリーの各ノードには、問題の重大度を示す重大度アイコンと、このタイプの問題が検出された数を示すカウンターが含まれます。タイプと URL では、重大度アイコンは、ノードの下に含まれる最も重大な問題の重大度を示します。

問題を分類する方法を変更したり、問題の重大度値を操作することができます (221 ページの『重大度レベル』 を参照してください)。

現時点で「ノイズ」として処理したくない問題を指定するには、これを結果表示から完全に削除するか、取り消し線付きで表示させます (221 ページの『問題の状態:「オープン」または「ノイズ」』 を参照してください)。

セキュリティー問題の合計数 (リストの先頭に表示) は、サイト内の脆弱なロケーションを示す指標で、サイトがどのような構造になっているかによりある程度異なります。コンテンツ・ベースの構造 (106 ページの『「コンテンツ・ベースの結果」ビュー』を参照してください) を定義すると、 アプリケーション・ツリー内の問題の合計数は、(同じ結果に対する) URL ベースのアプリケーション・ツリーでの合計数と同じでないことがあります。サイトの構造がコンテンツ・ベースで (URL ベースではなく)、コンテンツ・ベースのビューが正しく構成されている場合、コンテンツ・ベースのビュー内の問題の件数は、サイト内に存在する「脆弱性のある場所」の数をより正確に表します。バリアント の合計数 (リストの先頭の括弧内) はサイト構造とは無関係であり、 コンテンツ・ベースのビューと URL ベースのビューの間で変わりません。

重大度レベル

重大度アイコンは、問題では、その問題の重大度レベルを示し、問題のタイプと URL では、ノードの下に含まれるすべての問題について最も重大なものを示します。

アイコン	意味	説明	例
	高重大度	アプリケーション、Web サーバー、または情報に対する直接的な危険	サーバー上でのコマンド実行、顧客情報の盗聴、サービス妨害
	中重大度	プライベート・エリアへの無許可アクセスによる脅威 (データベースおよびオペレーティング・システムへの危険性はない)	スクリプト・ソースの暴露、強制ブラウズ
	低重大度	無許可の調査の許容	サーバー・パスの開示、内部 IP アドレスの開示
	情報	認識しておくべき問題 (必ずしもセキュリティー問題ではない)	有効化された安全ではないメソッド

関連タスク:

『重大度レベルを変更する』

重大度レベルを変更する

手順

ノードに割り当てられている重大度は、そのノードを右クリックして「重大度 >」を選択し、次に新しい値を入力することで変更できます。

注: タイプまたは URL ノードの重大度レベルを変更すると、このノードに含まれる問題はすべて新しいレベルに変わります。

問題の状態:「オープン」または「ノイズ」

ご使用のアプリケーションに関係しない問題は、「ノイズ」として指定して結果から削除できます。

このタスクについて

AppScan によって検出された特定の問題が、 ご使用のアプリケーションに関係しない (アプリケーションにとって、この問題が事実上「誤検出」結果である) 場合、 (例えば、問題が、開発環境には存在するけれども、デプロイメント環境には存在しない場合)、これを「ノイズ」として分類することをお勧めします。

「ノイズ」として分類した問題を表示するための 2 つのオプションがあります。1 つは、「結果リスト」には入れるが、取り消し線付きのグレイ表示にする方法、もう 1 つは「結果リスト」に全く入れない方法です。

手順

2 つの表示オプションを切り替えるには、「表示」>「ノイズとしてマークされた問題を表示」をクリックします。

タスクの結果

チェック・マークがメニュー項目の横に表示され、「ノイズ」とマークされた問題は、「結果リスト」に含まれますが、取り消し線付きのグレイ・テキストで表示されます。

例

ノイズ定義は以下の方法で適用されます。

- スキャンが構成されているワークステーションでは、 ノイズ指定を保存すると、この指定はスキャンを保存した時点で自動的に今後のスキャンに適用されます。(ノイズ分類ファイルの場所は、「ツール」>「オプション」>「全般」タブで定義されます。)
- 保存済みスキャンを別のワークステーション上で 開いた場合、 これらの問題は、ワークステーションに別の定義があっても、このスキャンでは ノイズとして 指定されます。(ただし、2 番目のワークステーションにこのスキャンを保存 すると、 その定義がワークステーションに保存され、ワークステーションにあった以前のノイズ分類ファイルが上書きされます。)

次のタスク

以下も参照してください。

『問題の状態を変更する』

118 ページの『「テスト・オプション」ビュー』

問題の状態を変更する

ノードに割り当てられている状態は変更することができます。

手順

ノードを右クリックして、「状態 >」を選択し、次に新しい値 (ご使用のアプリケーションに関連する問題には「未解決」、関連性のない問題には「ノイズ」) を選択します。

注: タイプまたは URL ノードの状態を変更すると、このノードに含まれる問題はすべて新しい状態に変わります。

問題の状態のエクスポートおよびインポート

特定の問題を「ノイズ」(アプリケーションに無関係) として指定した場合、この指定を他のワークステーションで使用するためにエクスポートすることができます。

このタスクについて

ノイズ指定を他のワークステーションで使用するためにエクスポートするには、以下のようにします。

手順

「ファイル」>「エクスポート」>「クロス・スキャン・データ」をクリックして、データを XML ファイルとして保存します。

次のタスク

状態を別のワークステーションにインポートするには、「ファイル」>「インポート」>「クロス・スキャン・データ」をクリックします。

テストを再送する

このタスクについて

完全フル・スキャンまたはテスト・ステージを実行せずに、テストを再送することができます。例えば、あるテストの結果が前のスキャンの結果と矛盾しているように見える場合、テストを再送することができます。

手順

1. 「結果リスト」で、ノードを右クリックします。
2. 表示されるメニューで、「再テスト」をクリックします。

   AppScan は、選択されたノードに含まれているすべてのテスト要求を送信し、新規の結果が「結果リスト」に追加されます。

右クリック・メニュー

「セキュリティー問題」の「結果リスト」の右クリック・メニューには、次のオプションが含まれます。

項目	説明
重大度	選択された項目の重大度値を変更します (高、中、低、情報を選択)
状態	問題の状態は、デフォルトでは常に「未解決」です。何らかの理由で、関連付けが不要な特定の問題がある場合、これらの問題は「ノイズ」として定義することができます。(オプション:「未解決」/「ノイズ)」
再テスト	選択されたテストを再送し、その結果をスキャン結果に追加します
マニュアル・テスト	マニュアル・テストを作成します (236 ページの『マニュアル・テスト』を参照してください)
削除	選択された項目をテスト結果から削除します (復元できません)
脆弱でないとして設定	結果を脆弱でないとして設定すると、これはテスト結果には含まれません (ただし、脆弱でないバリアント・リストからは表示と復元が可能です。 239 ページの『脆弱でないバリアント・リスト』を参照してください)
誤検出を報告	テスト情報を zip し、AppScan サポートまたはお客様の組織のメンバーに E メールで送信します (235 ページの『誤検出のテスト結果を報告』 を参照)。
問題情報の生成	選択した結果のデータのみ「問題情報」タブに取り込みます。 **ヒント:** すべての 結果についての問題情報を更新する場合は、このオプションではなく、「ツール」 > 「すべての問題情報の生成」を選択します。

「結果リスト」でセキュリティー問題をフィルタリングする

問題のタイプについて「結果リスト」を フィルターに掛けるか、特定の問題を検索することができます。

手順

1. 「編集」メニューで、「検索」をクリックします (または **Ctrl + F** を押します)。

   「検索」バーがメイン・ウィンドウの「結果リスト」の下に表示されます。
2. 「アプリケーション・ツリー」でノードを選択します。
   - 「マイ・アプリケーション」ノードを選択すると、すべての結果について検索が行われます。
   - ツリー内のいずれかのノードを選択すると、選択したノードとそのサブノードについて検索が行われます。
3. 「検索」バーの「検索」テキスト・ボックスに、 ストリングまたはストリングの一部を入力します。
4. 「検索対象」コンボ・ボックスで、結果内で文字列を検索する場所を選択します。オプションは以下のとおりです。「テストの ID 番号」、「セキュリティー問題」、「URL」、「CVE ID」、「CWE ID」、「XFID (X-Force ID)」、「要求/応答データ」、「バリアントの説明」、「パラメーター/Cookie 名」、またはそれらの「すべて」があります。
5. 「ただちに検索」をクリックするか、**Enter** キーを押します。

   検索結果が、以前表示されていたリストに上書きされて「結果リスト」に表示されます。

   別の「検索」ストリングを入力して「ただちに検索」を再度クリックすると、新規検索は、表示されている直前の検索結果についてではなく、「アプリケーション・ツリー」で選択されているノードについて実行されます。

検索内容:	検索文字列:	検索対象:
ID: "5016" のバリアント (「詳細ペイン」の「プロパティー」サブタブを参照してください)	"5016"	ID
クロスサイト・スクリプティング	"cross"	テスト名
問題のあるログイン・ページ	"login"	テスト URL
パスワード操作に関係する問題	"passwd"	要求/応答

「結果リスト」をソートする

このタスクについて

「結果リスト」の問題を再配列することができます。デフォルトでは、問題は重大度でソートされています。

手順

1. 列見出しの「表示順」をクリックします。
2. メニューのコマンドをクリックして、問題をソートします。
   - 重大度 - テスト名は、重大度の高いものから、情報レベルへと重大度順にリストされます。
   - カウント - 各テストの問題の数。最も多くの問題を検出したテストが先頭にリストされます。
   - 名前 - テスト名をアルファベット順にリストします。

   問題は「結果リスト」で再ソートされます。

   ソートの順序を逆にする (昇順または降順) には、「結果リスト」の 2 番目の列をクリックします。2 番目の列を再度クリックすると、順序をリセットすることができます。

セキュリティー問題: 詳細ペイン

「詳細ペイン」には、選択されたテストに関係する情報と、「結果リスト」で選択されたすべてのテストのバリアント が示されます。

「詳細ペイン」には、『「問題情報」タブ』、 229 ページの『「アドバイザリー」タブ』、 232 ページの『「推奨される修正」タブ』、および 232 ページの『「要求/応答」タブ』 という 4 つのタブがあります (タブをクリックすると、そのコンテンツが前面に表示されます)。

「問題情報」タブ

「詳細ペイン」の最初のタブには、入手可能な情報の要約が示されています。

スキャン中に問題が検出されてツリーに追加されると、「問題情報」タブには、他の「詳細ペイン」タブで使用可能な情報の要約が表示されます。また、問題に関する CVSS メトリックのスコアリングおよび関連の画面キャプチャーなどの有用な追加情報も表示されます。これらの情報は、結果と一緒に保存し、レポートに組み込むことができます。

領域/アイコン	説明
ヘッダー	「URL」、「エンティティー」、および「セキュリティー・リスク」(高、中、低、または情報) を含む問題ヘッダー。
CVSS メトリックのスコア	3 つの CVSS メトリック・グループ: (基本、一時的、および環境) に基づく平均スコア。リンクをクリックして編集します (227 ページの『CVSS 設定』を参照)。
	画面キャプチャー、ユーザーが選択した他の関連イメージ、およびユーザー独自のコメントを、スキャン結果と一緒にレポートに組み込むことを可能にします (226 ページの『問題情報を編集』を参照)。
ヒント (黄色のボックス)	この情報は、(下の) コンテンツ領域を参照し、ここに表示されるイメージまたは HTML で検索する内容を説明します。
コンテンツ (画面キャプチャーまたは HTML コード)	問題により、この領域には、1 枚の画面キャプチャー、比較用に 2 枚の画面キャプチャー、シミュレート・ポップアップ付きの 1 枚の画面キャプチャー、または HTML コードが含まれます。 HTML の場合、コンテンツ領域の右上にある  をクリックすることで、テキスト折り返しのオン/オフを切り替えることができます。
論拠 (青のボックス)	AppScan の実行内容と、問題であると認識した 理由を説明します。
技術的要約 (グレイのボックス)	この問題についてテストするために AppScan が実行した内容の技術的な詳細 と、応答の検証方法を説明します。

「問題情報」ツールバー

「詳細」ペインの上にあるツールバーには、選択された問題の現在の重大度と、問題の状態が表示されます。ツールバーでは問題間での切り替えが可能です。

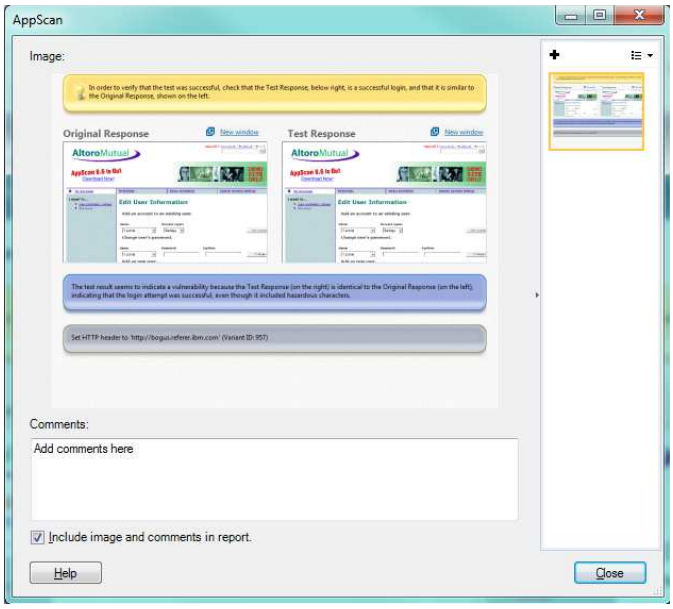
- 重大度: 4 種類の標準重大度設定のうちいずれか 1 つを選択するか、この問題について CVSS 設定を手動で調整します。
- 状態: オプションは「未解決」または「ノイズ」です。デフォルトは「未解決」です。重要でない問題には、「ノイズ」を選択します。デフォルトでは、「ノイズ」と指定された結果は、取り消し線を引かれて結果リストに表示されます。これを表示から完全に取り除くには、「ツール」 > 「ノイズとしてマークされた問題を表示」の選択を解除します。

問題情報を編集

レポートに組み込むために、問題情報にイメージおよびコメントを追加します。

「問題情報」タブの画面キャプチャー、ユーザーが選択した他の関連イメージ、およびユーザー独自のコメントをスキャン結果と一緒に保存し、レポートに組み込むことができます。

- 「問題情報」タブの右上隅にある アイコン をクリックし、問題情報を編集します。

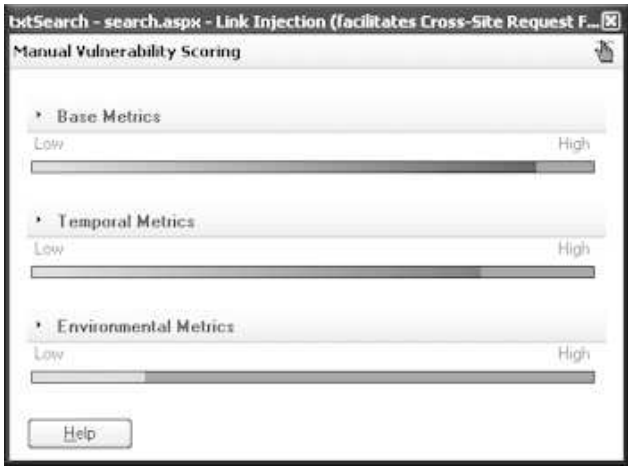


領域/アイコン	説明
イメージ	使用可能なサムネールから現在選択されているイメージを右側のペインに表示します。
	スキャン結果でこの問題にイメージを追加する場合にクリックします。
>	現行イメージをコンピューターに保存する場合にクリックします。
>	現行イメージをスキャン結果から削除する場合にクリックします。
コメント	現在表示されているイメージに関するコメントを入力し、スキャンと一緒に保存します。

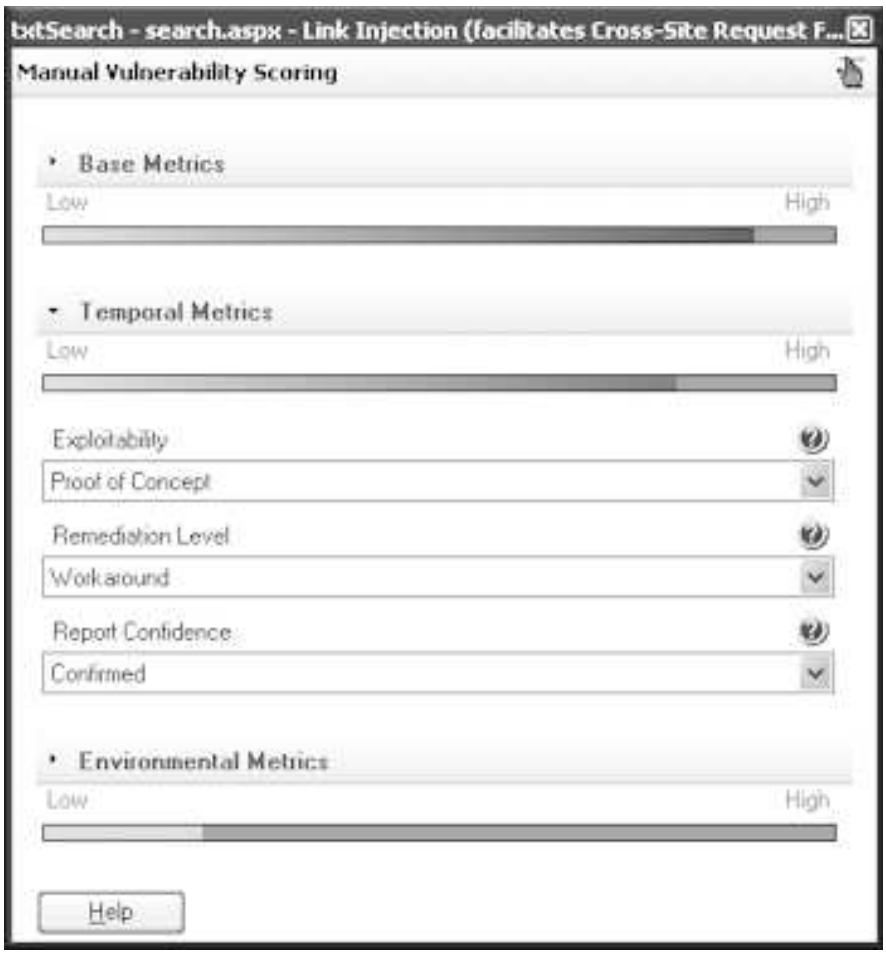
領域/アイコン	説明
イメージおよびコメントをレポートに含める	現在表示されているイメージおよびコメント をレポートに組み込む場合に選択します。各イメージを個別に構成することができます。デフォルトでは、すべてのイメージが組み込まれます。

CVSS 設定

CVSS メトリックに基づいた特定の問題について、重大度の設定を手動で微調整することができます。これは、「問題情報」ツールバーから「重大度」>「**CVSS** 設定」をクリックして実行されます。



CVSS ウィンドウから、3 つのセクションのいずれかの名前をクリックすると、そのセクションが開き、構成が表示されます。 をクリックすることで、デフォルト設定を復元することができます。このアイコンは、変更が行われた場合にのみアクティブになります。



基本メトリック

時間およびユーザー環境が変わっても一定である脆弱性メトリックです。

メトリック	説明	オプション
アクセス・ベクトル	脆弱性をローカルのみで悪用できるか、隣接ネットワークからも悪用できるか、あるいはすべてのネットワーク接続から悪用できるか (リモートから悪用可能)。	ローカル、隣接ネットワーク、ネットワーク
アクセスの複雑性	この脆弱性の悪用に関する難易度。	高、中、低
認証	脆弱性を悪用するために攻撃者が認証する必要がある回数。	なし、1 回、複数回
機密性への影響	この脆弱性を悪用された場合の機密性への影響。	なし、部分一致、完全一致
完全性への影響	この脆弱性を悪用された場合、システム保全性 (アプリケーションによって提供される情報の正確さ) が損なわれる程度。	なし、部分一致、完全一致
可用性への影響	この脆弱性を悪用された場合の情報リソースの可用性への影響。	なし、部分一致、完全一致

一時的メトリック

時間の経過に伴って変化する脆弱性のメトリックがあります。

メトリック	説明	オプション
悪用の可能性	この脆弱性につけこむ悪用手法の現在の状態。	未検証、PoC (概念検証)、実用的、高、未定義
修復レベル	脆弱性の保護に使用可能な修復レベル。	公式のフィックス、一時的なフィックス、回避策、利用不可、未定義
レポートの信頼性	脆弱性の存在および技術詳細についての信頼性の度合い。	未確認、裏づけなし、確認済み、未定義

環境メトリック

これらのメトリックはアプリケーション環境を反映し、「構成」ダイアログ・ボックス > 「環境メトリック」タブを使用してグローバルに設定する必要があります。これらをここで変更するのは、異なる特性を持つアプリケーション環境の一部に対してこの脆弱性が固有の場合に限られます。

メトリック	説明	オプション
二次的被害の可能性	アプリケーションが脆弱な場合の損害またはデータ漏えいの可能性。	なし、低、低から中、中、中から高、高、未定義
ターゲットの分布	ターゲットになる可能性がある環境内のシステムの比率。	なし、低、中、高、未定義
可用性要件	(情報の) 可用性の相対的な重要性	なし、低、中、高、未定義
機密性要件	(ユーザー情報の) 機密性の相対的な重要性。	なし、低、中、高、未定義
完全性要件	情報の保全性 (正確さ) の相対的な重要性。	なし、低、中、高、未定義

デフォルトの重大度設定を復元する

手順

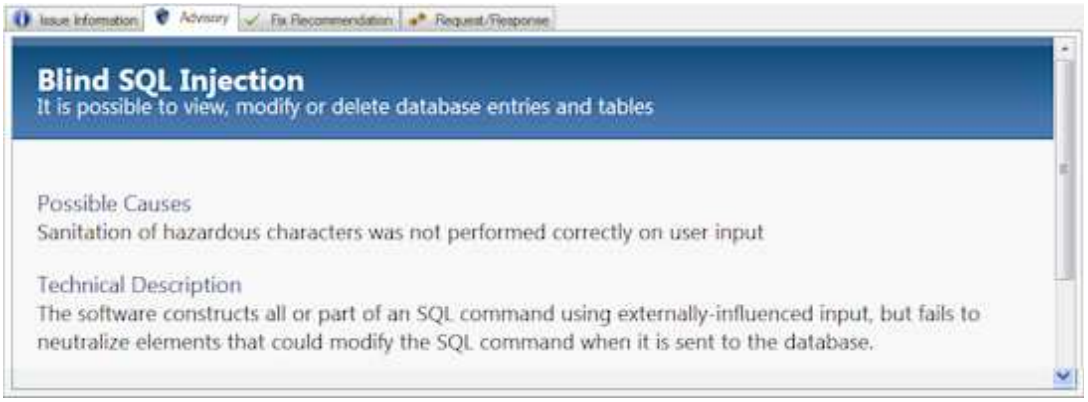
特定の問題について、 (別の重大度を選択するか、CVSS 設定を調整して) 重大度設定を手動で変更した場合、前の設定を復元することができます。

- マニュアル設定 (高/中/低/情報) を、この問題に関する現在の CVSS 設定に基づいた設定に置き換えるには、「問題情報」ツールバーで「重大度」>「**CVSS** を使用して重大度を計算」をクリックします。
- デフォルトの CVSS 設定を復元するには、「問題情報」ツールバーで「重大度」>「**CVSS** 設定」をクリックし、開いた CVSS 設定ウィンドウで、  をクリックします

「アドバイザリー」タブ

「詳細 (Detail)」ペインの 2 番目のタブは「アドバイザリー」です。

「アドバイザリー」タブの情報には、選択された問題の技術詳細と、詳細情報への参照リンクが含まれています。この情報は、修正すべき内容と修正理由を説明する必要がある場合には欠くことができません。



「アドバイザリー」タブには、 以下のセクションが含まれます。

テスト名
: 「結果リスト」に表示されるテストの名前。

重大度
: この脆弱性に割り当てられる重大度。

タイプ
: この脆弱性がアプリケーション・レベルであるのか、インフラストラクチャー・レベルであるのか。

WASC 脅威の分類
: このクラスの脅威を説明する Web Application Security Consortium のページへのインターネット・リンク。

CVE ID(s)
: このタイプの脆弱性の業界標準番号 (231 ページの『CVE サポート』を参照)。

CWE ID(s)
: この問題の業界標準番号 (231 ページの『CWE サポート』を参照)。

XFID この問題の X-Force ID (232 ページの『X-Force サポート』を参照)。

セキュリティー上のリスク
: この問題がアプリケーションに対してどれほどのセキュリティー・リスクを持つかについて説明。

研修モジュール
: 問題を説明し、示す Adobe Flash プレゼンテーション。

考えられる原因
: 問題がご使用のアプリケーションにどのようにして存在するようになったかを示します。

技術的な説明
: 問題の詳細な技術的な説明。

影響を受ける製品
: 問題によって影響を受ける可能性のあるサード・パーティー製品。

参考資料と関連リンク
: 追加情報へのリンク。

CVE サポート

CVE (Common Vulnerabilities and Exposures) は、公的に認識されている情報セキュリティーの脆弱性と暴露に関する一般名を提供する業界標準のリストです。これを使用すると、別個のデータベースとツールにまたがるデータを共有することが容易になります。(詳細については、CVE Web サイト (http://cve.mitre.org/) を参照してください)

AppScan CVE ID が割り当てられている脆弱性に対する アドバイザリーには、CVE Web サイト上の説明にリンクする参照が含まれます。(CVE ID は、受け入れられた脆弱性は CVE で、脆弱性候補は CAN で始まります。)

以下の項目を実行できます。

- テストに関するアドバイザリーで、テスト結果の CVE ID を確認する (229 ページの『「アドバイザリー」タブ』を参照)
- CVE ID のリンクをクリックして、CVE Web サイト上の説明に移動する
- レポートに CVE ID (アドバイザリーの一部として) を含める
- 特定のテストによってテストされた CVE ID を「テスト・ポリシー」ビューで確認する (「スキャン構成」>「テスト・ポリシー」。 112 ページの『「テスト・ポリシー」ビュー』 を参照)
- 「テスト・ポリシー」ビューで CVE および CAN 文字列を検索することによって CVE ID を持つすべてのテストをリストする
- 「テスト・ポリシー」ビューで ID を検索することによって特定の CVE を検索する

CWE サポート

共通脆弱性タイプ一覧 (Common Weakness Enumeration) は、公的に認識されているソフトウェアの脆弱性に関する一般名を提供する業界標準のリストです。これを使用すると、別個のデータベースとツールにまたがるデータを共有することが容易になります。(詳細については、CWE Web サイト (http://cwe.mitre.org/) を参照してください)

AppScan CWE ID が割り当てられている脆弱性に対する アドバイザリーには、参照番号、および CWE Web サイト上の説明へのリンクが含まれます。特定の脆弱性が独自の CWE ID (問題 の ID に加えて) を持つ場合は、「バリアントの詳細」ペインに表示されます。

以下の項目を実行できます。

- 問題に対するアドバイザリーに問題の CWE ID を表示する (229 ページの『「アドバイザリー」タブ』を参照)
- バリアントの CWE ID、および上位の問題を「バリアントの詳細」タブに表示する (234 ページの『バリアントの詳細』を参照)
- CWE Web サイト上の説明にリンクする CWE ID をクリックする
- レポートに CWE ID (アドバイザリーの一部として) を組み込む
- 「テスト・ポリシー」ビューで参照番号を検索することによって特定の CWE を検索する

AppScan の現行バージョンで使用されている CWE データベースのバージョンについては、リリース・ノート ([AppScan Standardinstallation directory]\Docs) を参照してください。使用されるデータベースが毎日の更新で変更される場合、その変更は「更新のログ」(「ヘルプ」メニュー>「更新のログ」) にリストされます。

X-Force サポート

X-Force は、脅威および脆弱性に関する世界で最も包括的なデータベースの 1 つです。脆弱性に関するすべての AppScan アドバイザリーには、それぞれの XFID および X-Force サイトへのリンクが含まれます。X-Force サイトでは、セキュリティー問題に関する追加情報を見つけることができます。

以下のことが可能です。

- 問題に対するアドバイザリーに問題の XFID を表示する (229 ページの『「アドバイザリー」タブ』を参照)
- バリアントの XFID、および上位の問題を「バリアントの詳細」タブに表示する (234 ページの『バリアントの詳細』を参照)
- X-Force Web サイト上の説明にリンクする XFID をクリックする
- レポートに XFID (アドバイザリーの一部として) を含める
- 「テスト・ポリシー」ビューで参照番号を検索することによって特定の XFID を検索する

「推奨される修正」タブ

「詳細 (Detail)」ペインの 3 番目のタブは「推奨される修正」です。

「推奨される修正」タブの情報は、選択された特定の問題に対して、ご使用の Web アプリケーションをセキュアにするために、絶対に実行しなければならないタスクです。

「推奨される修正」タブには、選択された問題を修正するための既知の推奨が表示されます。これらの解決方法は、非常に複雑で、段階的な説明である可能性があります。

推奨される修正は次のように分類されます。

- 全般 - 常に選択されます
- **.Net** - Microsoft© .NET
- **Java EE** - Sun© Java Platform, Enterprise Edition

  注**:** 関連性がない推奨される修正を非表示にするよう AppScan を設定できます。詳しくは、 277 ページの『「設定」タブ』 を参照してください。

「要求/応答」タブ

「詳細」ペインの 4 番目のタブは「要求/応答」です。

「要求/応答」タブには、テストに関する情報とテスト特定のバリアントが含まれます。これらは、ご使用の Web アプリケーションのどこに脆弱性があるかを発見するためにアプリケーションに送信されたものです。テストによっては複数のバリアントが含まれる場合があります。バリアントとは、AppScan が Web アプリケーション・サーバーに送信した元のテスト結果とわずかに違うものです。(AppScan はまず、正当な、アプリケーションのビジネス・ロジックに沿った要求を送信します。次に、不正または誤った要求がアプリケーションでどのように処理されるかを確認する目的で変更された同様の要求を送信します。個々のテスト要求は、AppScan データベース全体におけるすべてのセキュリティー規則を網羅するために必要な数だけ、バリアントを持つことができます。

例えば、特定のパラメーターのユーザー入力規則が守られていることを確認するために送信されるテストについて考えて見ましょう。あるバリアントは、アポストロフィが有効な入力でないことを検査し、別のバリアントは引用符が許可されていないことを検査します。

バリアント自体は赤のテキストで表示され、検証 (セキュリティー問題の存在を示す応答の一部) が黄色で強調表示されます。

「要求/応答」タブには、大量の説明情報の他に、スキャン結果の認識と使用に関する拡張機能が用意されています。

「要求/応答」タブには、2 つのペインがあり、上部にそのタブ独自のツールバーがあります。ツールバーとタブは以下の図のように表示されます。要約については下記の表を参照してください。

ツール	機能
バリアント < >	現行のテストのバリアントの数を示します。 < と > アイコンをクリックして、それぞれ前のバリアントと次のバリアントに切り替えることができます。
テスト/オリジナル	オリジナル情報とテスト情報で切り替えます。
次の強調表示	(検証テキストが強調表示されている場所で有効です。) カーソルを次の強調表示テキストに移動します。
ブラウザーで表示	ブラウザーから画面キャプチャーを取得するオプションがある標準装備のブラウザーを開いて現行ページを表示します。 ブラウザーが開くと、ブラウザーのツールバーにあるカメラ・アイコン  をクリックして、そのページの画面キャプチャーを取得することができます。画面キャプチャーは、「問題情報」タブに追加されます。
「オプション」 > 「誤検出を報告」	現在のバリアントを AppScan サポート・チーム、またはお客様の企業内に E メールで送信するために使用します。(235 ページの『誤検出のテスト結果を報告』 を参照してください。)
「オプション」 > 「マニュアル・テスト」	テストを変更し、これをマニュアル・テストとして保存します。(236 ページの『マニュアル・テスト』 を参照してください。)
「オプション」 > 「バリアントを削除」	選択されたバリアントをテスト結果から永久に削除します (復元できません)。これは、「結果」ペインでバリアントを右クリックすることによっても実行できます。
「オプション」 > 「脆弱でないとして設定」	選択されたバリアントの定義を「脆弱でない」に変更します。 ユーザーにより「脆弱でない」に変更された検出応答は、スキャン結果から削除され、レポートには含まれません。ただし、「脆弱でないバリアント」リストから参照 (および復元) することができます。(239 ページの『脆弱でないバリアント・リスト』 を参照してください。)

ツール	機能
「オプション」 > 「エラー・ページとして設定」	現在のページをエラー・ページ (「スキャン構成」ダイアログ・ボックス >「エラー・ページ」) のリストに追加し、結果を更新して、この応答がエラー・ページであるという事実を反映させます。
「オプション」 > 「問題情報に追加」	現在の問題について結果の検討を実行し、新しい情報が有効になった場合、これを「問題情報」タブに追加します。
検索	特定のストリングを検索するためのテキストを入力します。(223 ページの『「結果リスト」でセキュリティー問題をフィルタリングする』 を参照してください。)
バリアントの詳細	右側のペインには、現行バリアントの詳細が表示されます。この詳細には、ID、説明、差 (このバリアントとオリジナルの要求の間の差)、推理、および CWE ID が含まれます。

バリアントを表示する

このタスクについて

個々のテストには複数の関連するバリアントがあります。各バリアントは、要求をわずかに変更して、多数の攻撃手口に対するご使用のアプリケーションのセキュリティーを検査します。

手順

1. 「テスト」をクリックします。
2. 右矢印または左矢印ボタンをクリックすると、バリアント要求を表示することができます。

   送信されるバリアント・テストごとに、要求の変更部分が赤で強調表示されます。バリアントの詳細については、「バリアントの詳細」タブを参照してください。

バリアントの詳細

「バリアントの詳細」は、「詳細ペイン」の「要求/応答」タブのサイド・タブです。

「バリアントの詳細」タブは、「詳細ペイン」の 「要求/応答」タブ内にあり、バリアントとその目的について説明します。

セクション	説明
ID	検索および管理を簡単にするために、ID 番号が各バリアントに割り当てられています。
説明	テストの要旨。
差	このテストの元の要求に対して行われた変更を示します。変更は、赤で強調表示されます。(変更には、パラメーター、Cookie、またはメソッドの値の変更、パスの変更、パラメーターの削除、HTTP ヘッダーの削除または追加、ボディに対するパラメーターの削除または追加などが含まれます。)
推理	このテスト結果が脆弱性を示している理由を説明します。
CVE ID	脆弱性の CVE ID (231 ページの『CVE サポート』を参照)。
CWE ID	バリアントおよびその上位問題の CWE ID。(231 ページの『CWE サポート』を参照)。

画面キャプチャーの取得

ぜい弱性を示すアプリケーションの画面キャプチャーを取得し、レポートに組み込むことができます。

手順

1. 「結果リスト」で項目を選択し、必要なバリアントまで切り替えます。
2. 「詳細ペイン」>「要求/応答」タブで、「ブラウザーで表示」をクリックします。
3. ブラウザーで、「カメラ」アイコン  をクリックします。

   現行ページの画面キャプチャーが、「問題情報」タブのデータに追加され、レポートに組み込まれます。

誤検出のテスト結果を報告

以下の目的で、テスト情報を AppScan サポートに E メールで送信することができます。

- AppScan では「検出」 (ぜい弱性を含む) と分類されたが「検出なし」(ぜい弱性を示さない) でないかと思われる結果をレポートします。
- AppScan サポートに対して、結果が「検出」と分類された理由を尋ねます。

さらに、この機能を使用して、結果を適宜 zip して、組織内の開発者と監査員に E メールで送信することができます。

注**:** デフォルトでは AppScan は、データを暗号化フォーマットで保存します。これは、サポート担当者のみがアクセス可能です。ご自分の組織内にファイルを送信する場合、情報を .zip ファイルとして保存するように AppScan を構成しなければなりません。「ツール」>「オプション」>「全般」タブで、「添付ファイルの暗号化 **(Encrypt Attachments)**」チェック・ボックスの選択を解除します。

単一の誤検出バリアントのレポート

手順

1. 「結果リスト」で項目を選択します。
2. 「詳細ペイン」>「要求/応答」タブで、選択された問題のバリアント全体を表示します。
3. 送信したいバリアントが表示されたら、詳細ペインのツールバーで「誤検出を報告」をクリックします。

   「誤検出を報告」ダイアログ・ボックスが開きます。
4. 「ファイルの保存」をクリックしてファイルをディスクに保存します。

   ご使用の暗号化設定 (下記を参照) により、ファイルは暗号化または .zip フォーマットで保存されます。
5. ファイルを AppScan サポートに送信するには、「サポート・プロバイダーを表示」リンクをクリックしてログインし、ファイルをアップロードします。

誤検出バリアント・セットのレポート

このタスクについて

「結果リスト」の右クリック・メニューを使用して、任意の問題、URL、または 1 つの添付ファイル中の下位項目に関するすべてのバリアント情報をレポートすることができます。

手順

1. 「結果リスト」で、問題、URL、またはパラメーターを右クリックし、「誤検出を報告」を選択します。

   「誤検出を報告」ダイアログ・ボックスが開きます。
2. 「ファイルの保存」をクリックしてファイルをディスクに保存します。

   ご使用の暗号化設定 (下記を参照) により、ファイルは暗号化または .zip フォーマットで保存されます。

   注**:** デフォルトでは、ファイルは暗号化されています。この設定を変更するには、「ツール」>「オプション」>「全般」>「誤検出を報告」に進み、「添付ファイルの暗号化」チェック・ボックスを選択解除します。
3. ファイルを AppScan サポートに送信するには、「サポート・プロバイダーを表示」リンクをクリックしてログインし、ファイルをアップロードします。

誤検出レポートの暗号化

このタスクについて

デフォルトでは、「誤検出を報告」機能は、 AppScan サポート担当者のみが開けるように、データを暗号化フォーマットで保存します。

ご自分の組織内に添付ファイルを送信する場合、受信者は暗号化を解除できないため、この暗号化機能を無効にする必要があります。

手順

1. 「ツール」>「オプション」>「全般」>「誤検出を報告」をクリックします。
2. 「添付ファイルの暗号化 **(Encrypt attachments)**」チェック・ボックスを必要に応じて選択するか、選択を解除します。

マニュアル・テスト

このタスクについて

マニュアル・テスト機能により、レポートに含めるためにご自分のテストを送信し、これをセキュリティー問題として保存する ことができます。

探査結果が出たら、すぐにマニュアル・テストを作成することができます。マニュアル・テストは現在のスキャンに対してのみ保存されます。再スキャンを実行すると、テストが失われることに注意してください。

マニュアル・テストを既存のテストに基づいて実施するか、最初から新規に作成することができます。

手順

1. マニュアル・テストを既存のバリアントに基づいて実施するには、以下のようにします。
   - 「結果リスト」で、テスト・バリアントをクリックするか、または

- 「結果リスト」で、テストをクリックし、次に「詳細ペイン」でツールバーを使い、必要なバリアントを表示します。

最初から新規バリアントを作成する場合は、(次のステップである)「マニュアル・テスト」ダイアログ・ボックスを既存のバリアントを選択せずに開きます。

2. 「マニュアル・テスト」ダイアログ・ボックスを開きます。
   - 「ツール」メニューで、「マニュアル・テスト」をクリックするか、または
   - 「アプリケーション・ツリー」または「結果リスト」でノードを右クリックし、ポップアップ・メニューから「マニュアル・テスト」を選択するか、または
   - 選択されたバリアントの「アプリケーション・データ」>「詳細ペイン」 で、「マニュアル・テスト」ボタンをクリックします。

   「マニュアル・テスト」ダイアログ・ボックスが表示され、選択されたテストのバリアントのプロパティーを表示します。
3. 「ホスト名/**IP** アドレス」フィールドで、テストの送信先であるサーバーを入力します。
4. 「ポート」フィールドに、サーバーに到達するために AppScan で使用されるポートを入力します。

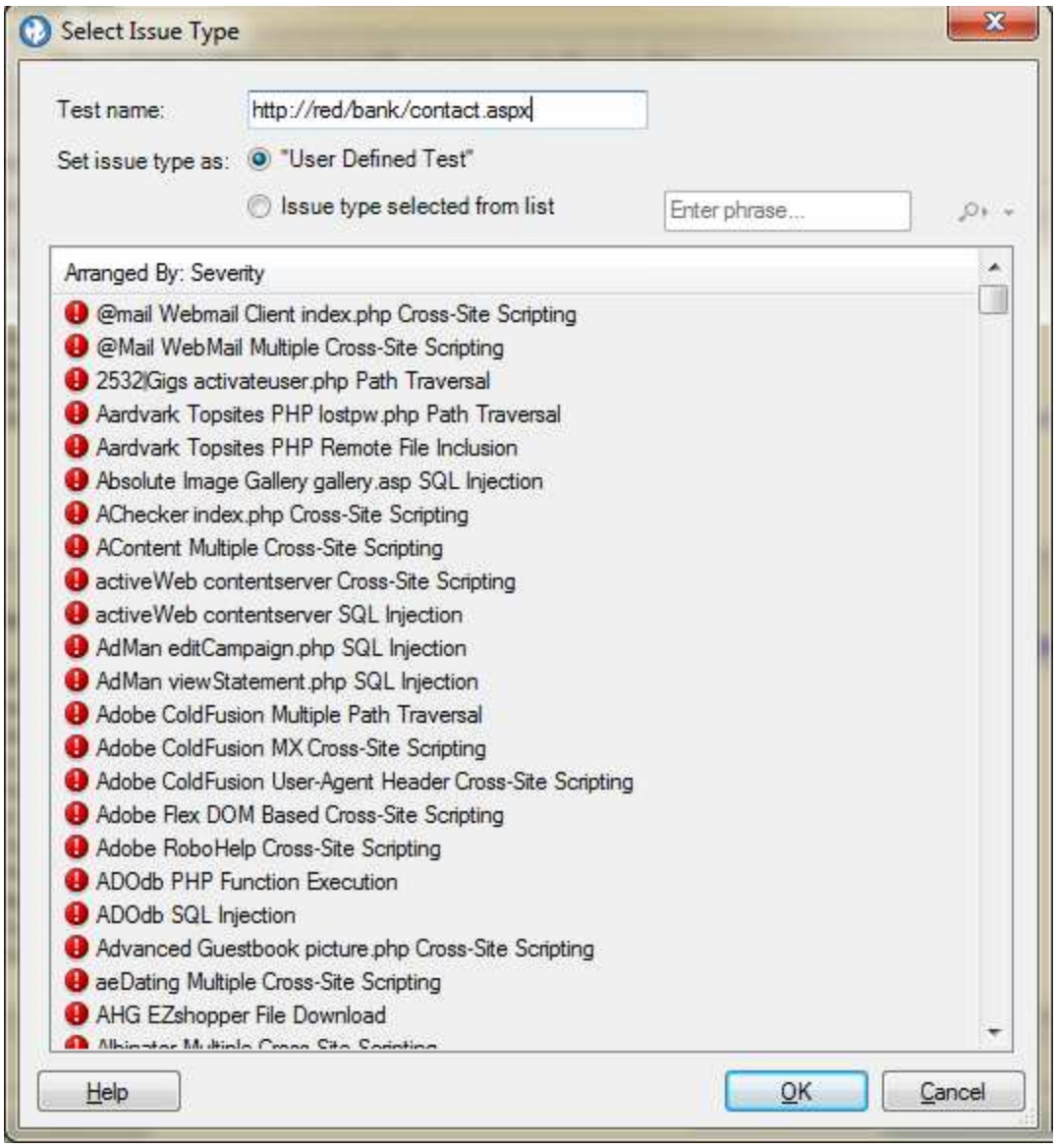
   デフォルトのポートは **80** です。 SSL が選択されていない場合は、**443** がデフォルトのポートです。
5. 必要な場合は、「要求」自体を編集してもかまいません。
6. 「オプション」リストでは、以下のオプションを選択またはクリアします。

オプション	クリックで実行される機能
SSL	SSL 内の要求を送信します。
要求送信前にログイン	ログイン要求をアプリケーションに送信してからマニュアル・テストを送信します。
自動的にコンテンツ長を計算	要求内のコンテンツ長 **HTTP** ヘッダーを、要求を編集する際の要求内容と同じ値に自動的に更新します。 このオプションを選択すると、ユーザーはコンテンツ長の値を編集できません。 要求ヘッダーにコンテンツ長パラメーターがない場合、このオプションは無効です。

7. 「送信」をクリックします。

   要求が送信され、応答が「応答」テキスト域 (下のペイン) に表示されます。
8. 組み込みブラウザーで応答を表示するには、「ブラウザーで表示」をクリックします。
9. このマニュアル・テストを現在のスキャンに追加するには、「保存」をクリックします。

「問題タイプを選択」ダイアログ・ボックスが表示されます。「ユーザー定義テスト」ラジオ・ボタンがデフォルトで選択されています。



10. 「テスト名」フィールドでは、デフォルト名 (URL) のままにすることも、新しい名前を定義することもできます。
11. (デフォルトのユーザー定義テスト・タイプではなく) 既存のテスト・タイプの下にテストを保存するには、 2 番目のラジオ・ボタンを選択して、リスト内のテスト・タイプをクリックします。

    注: 検索機能を使用してリスト内の問題を探すには、「検索」フィールドに問題名の一部を入力します。ある検索結果から次の検索結果に移動するには、拡大鏡アイコンをクリックします。
12. 「**OK**」をクリックします。

    ダイアログ・ボックスが閉じます。新規テストが結果に追加され、現在のスキャンを続行すると (「スキャン」>「続行」>「スキャン/テスト」)、このテストが組み込まれます。

    注: 再スキャンを実行しても、このテストは組み込まれません。

脆弱でないバリアント

スキャン中に、AppScan は何千ものテスト・バリアントを、テスト中のサイトに送信します。これらの多くに対する応答は、どのような種類のセキュリティー上の脅威も引き起こされないことを示します。デフォルトでは、AppScan はこれらの「脆弱でない」結果をすべて破棄します。

- 必要な場合は、脆弱でないバリアントをすべて保存するように AppScan を構成することができます。
- さらに、個々の結果の状況を「脆弱でない」に変更することができます。

『すべての脆弱でないバリアントを保存する』

『バリアントを脆弱でないとして定義する』

『脆弱でないバリアント・リスト』

240 ページの『バリアントの削除』

すべての脆弱でないバリアントを保存する

このタスクについて

すべての「脆弱でない」テスト・バリアントを検討する場合、これらを保存するように、AppScan を構成することができます。

注意:
脆弱でないテスト・バリアント情報を保存すると **AppScan** のパフォーマンスが低下し、必要なディスク領域が大幅に増加する場合があります。

手順

「スキャン構成」>「テスト・オプション」で、「脆弱でなかったテスト・バリアント情報を保存」チェック・ボックスを選択します。

バリアントを脆弱でないとして定義する

このタスクについて

テスト・バリアントを「脆弱でない」として定義すると、これはスキャン結果に表示されず、レポートに含まれませんが、 (『脆弱でないバリアント・リスト』経由で) その詳細を表示し、必要な場合にあとで復元することもできます。

手順

以下のいずれかを実行します。

- 「結果リスト」を右クリックし、「脆弱でないとして設定」を選択します。
- 「結果リスト」で変数を選択し、「要求/応答」ツールバーで 「脆弱でないとして設定」をクリックします。

バリアントがスキャン結果表示から削除され、レポートに含まれなくなります。

脆弱でないバリアント・リスト

脆弱でないバリアント・リストにより、スキャン結果とともに保存されていた脆弱でないバリアントの詳細を表示し、必要な場合には復元することができます。

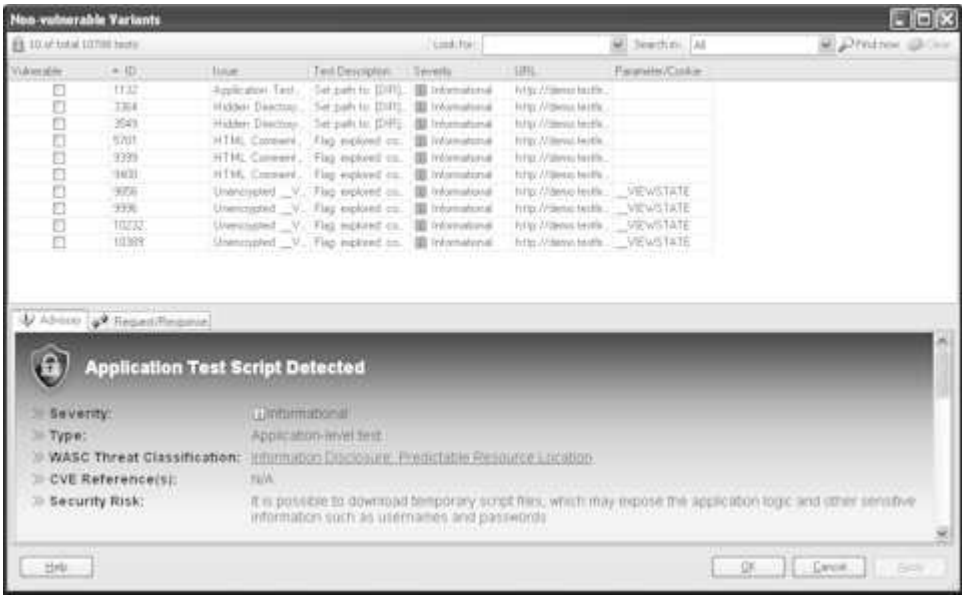
バリアントをこのリストに追加するには、以下の 2 つの方法があります。

- 脆弱でなかったテスト・バリアント情報を保存する (118 ページの『「テスト・オプション」ビュー』を参照してください) ように、AppScan が構成されている
- AppScan が「脆弱」として分類した結果を (前のセクションで説明したように)「脆弱でない」に手動で変更した

脆弱でないバリアントを表示する

手順

「表示」メニューで「脆弱でないバリアント」をクリックします。



脆弱でない変数を脆弱に復元する

手順

1. 脆弱として復元する、脆弱でないバリアント・リストに含まれる 1 つ以上のバリアントについてチェック・ボックスを選択します。
2. ダイアログ・ボックスの下部で「適用」をクリックします。
3. 「**OK**」をクリックして確認します。

バリアントの削除

このタスクについて

(バリアントを脆弱でないとして定義するのではなく) バリアントを削除する場合、これらはスキャン結果から完全に削除され、後で復元することができなくなります。 (再度アクセスするには、新規スキャンを実行する必要があります。)

手順

以下のいずれかを実行します。

- 「結果リスト」を右クリックし、「削除」を選択します。

- 「結果リスト」でバリアントを選択し、「要求/応答」ツールバーで「バリアントを削除」をクリックします。

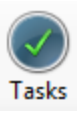
バリアントがスキャン結果から削除され、レポートに含まれなくなります。

第 9 章 結果:修復タスク

AppScan では、「アプリケーション・データ」、「セキュリティーの問題」、および「修復タスク」といった 3 つの方法でスキャン結果の表示と処理を行うことができます。このセクションでは、「修復タスク」ビューについて説明します。

「修復タスク」ビューには、スキャンで検出された問題を解決する目的で設計されたソリューションが用意されています。通常、1 つの修復タスクで複数のセキュリティー問題を解決します。

「ビュー・セレクター」で



をクリックします

修復タスク:アプリケーション・ツリー

「アプリケーション・ツリー」には、スキャンされたアプリケーションのフォルダーとファイルが表示されます。ツリーの各ノードには、カウンターがあります。ここには、ノードに含まれる修復タスクの数が示されます。各ノードのカウントは、1 つの修復タスクで複数の問題が解決できる場合があるため、「問題」ビューのカウントと同じであるか、これより小さくなります。

「アプリケーション・ツリー」には、以下のレベルで修復タスクが表示されます。

- タスク名
- **URL**
- パラメーターまたは **Cookie**

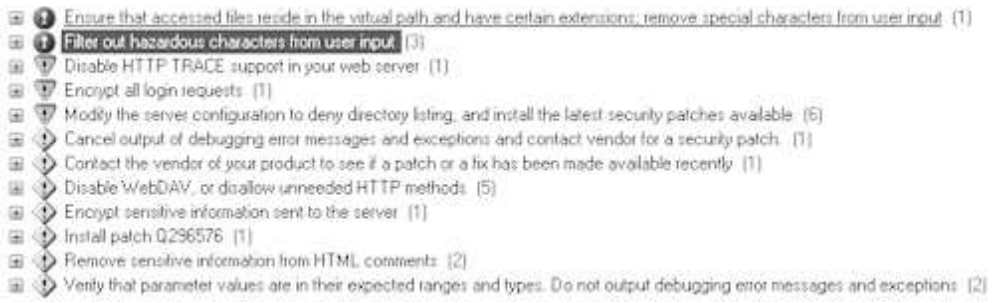
複数の URL で検出された 1 つの問題に対応して設計されたシングル・タスクが、問題の下に URL を伴って一度リストされます。

「アプリケーション・ツリー」のノードを選択して、「結果リスト」をフィルターに掛けます。このリストには、選択されたノードの結果のみが表示されます。

修復タスク:結果リスト

「結果リスト」には、「アプリケーション・ツリー」で選択されたノードに関係する修復タスクが表示されます。「マイ・アプリケーション」ノードを選択していると、「結果リスト」にはご使用のアプリケーションに関係するすべての修復タスクが表示されます。

修復タスクは、問題を解決するために実行される修復のタイプ別にまとめられます。修復項目ごとにアイコンがあり、実行されるタスクの優先順位を示します。また、カウントは、この修復により影響を受けるファイル数、パラメーター数、Cookie 数を示します。



個々のタスクには、URL が含まれている場合があります。ここには、ファイル、パラメーター、Cookie が含まれます。修復を分類する方法を変更したり、修復の優先順位の値を操作することができます。

「結果リスト」で修復タスクを検索する

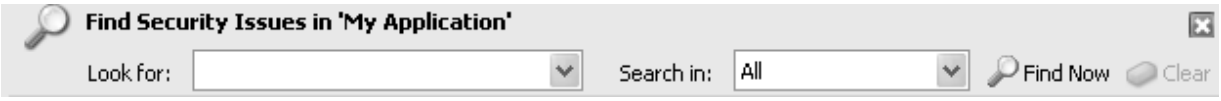
このタスクについて

修復タスクのタイプについて「結果リスト」をフィルターに掛けるか、特定の修復を検索することができます。

手順

1. 「編集」メニューで、「検索」をクリックします (または **Ctrl + F** を押します)。

   「検索」バーがメイン・ウィンドウの「結果リスト」の上に表示されます。

2. 「アプリケーション・ツリー」でノードを選択します。
   - 「マイ・アプリケーション」ノードを選択すると、すべての結果について検索が行われます。
   - ツリー内のいずれかのノードを選択すると、選択したノードとそのサブノードについて検索が行われます。
3. 「検索」バーの「検索」テキスト・ボックスに、ストリングまたはストリングの一部を入力します。
4. 「検索対象」リストで、検索の対象にする修復の部分を以下から選択します:

検索対象	文字列の検索対象
修復	「結果リスト」に表示されるときの修復の名前
URL	修復結果が関係する URL のパス名
詳細	修復タスクの詳細
すべて	上記オプションのすべて

5. 「ただちに検索」をクリックするか、**Enter** キーを押します。

検索結果が、以前表示されていたリストに上書きされて「結果リスト」に表示されます。別の「検索」ストリングを入力して「ただちに検索」を再度クリックすると、新規検索は、表示されている直前の検索結果についてではなく、「アプリケーション・ツリー」で選択されているノードについて実行されます。

例

検索内容	検索文字列	検索対象
仮想ディレクトリーに関係する修復タスク	"virtual direc"	修復
ログイン・ページの修復タスク	"login"	URL

修復タスクをソートする

このタスクについて

修復タスクを「結果リスト」で再配列することができます。デフォルトでは、タスクは優先度順にソートされています。

手順

1. 列見出しの「表示順」をクリックします。

   メニューが表示されます。
2. メニューのコマンドをクリックして、修復をソートします。
   - 優先順位 - タスク名は、優先度の高いものから、低いものへと優先度順にリストされます。
   - カウント - 影響を受ける URL、パラメーター、Cookie の数です。問題の大半を解決するタスクが先頭にリストされます。
   - 名前 - タスク名をアルファベット順にリストします。

   修復タスクは「結果リスト」で再ソートされます。

   ソートの順序を逆にする (昇順または降順) には、「結果リスト」の 2 番目の列をクリックします。2 番目の列を再度クリックすると、前のソート順序と逆にすることができます。

優先順位を操作する

このタスクについて

修復タスクのアイコンは、タスクの優先順位を示しています。以下の表でこれらのアイコンについて説明します。

アイコン	意味
	優先順位が高いタスク
	優先順位が中程度のタスク
	優先順位が低いタスク

優先順位は、問題の重大度に基づいて修復タスクに割り当てられます。重大度が「高」であると、優先順位も「高」となります。「中」の重大度であると、優先順位も「中」となります。重大度が「低」および「情報」である場合は、優先順位は「低」になります。

デフォルトの優先順位設定を開始ポイントとして表示することができます。修復タスクに割り当てられている優先順位は変更してもかまいません。優先順位を新しく設定すると、タスク名が同じであるすべての修復に影響があります。

手順

「結果リスト」で、修復タスクを右クリックして 「優先順位」>「高/中/低」を選択します。
「修復タスク」アイコンが新しい優先順位を反映させたものに変わります。

「結果リスト」から修復タスクを削除する

このタスクについて

「結果リスト」からタスクを削除することができます。これにより、選択されたノードと、このノードに含まれるすべてのオブジェクトが削除されます。

手順

1. 「結果リスト」で、ノードを右クリックします。
2. 表示されるメニューで、「削除」をクリックします。

   削除の確認と、テストのデータが永久に削除されることを注意するメッセージが表示されます。
3. 「はい」をクリックします。

   修復タスクは削除されますが、問題には影響がなく、「問題」ビューから変わりなく使用することができます。

修復タスク:詳細ペイン

修復ビューの「詳細ペイン」にはタブが 1 個あります。ここには、「結果リスト」で現在選択されている修復タスクが表示されます。

「詳細」ペインの情報には、タスク名、問題 (このタスクで処理されるスキャン結果のリスト)、および詳細 (1 つ以上の可能な解決策) が含まれます。

第 10 章 レポート

このセクションでは、スキャン結果からレポートを生成する方法について説明します。

関連概念:

206 ページの『スキャン結果をエクスポートする』

レポートの概要

AppScan によるサイトの脆弱性の評価が終了すると、開発者、内部監査員、侵入テスターから管理者や経営陣にまで及ぶ組織内のさまざまな人向けに構成したカスタマイズ・レポートを作成できます。

以下で説明するようにレポートには 5 つの基本タイプがあります。「セキュリティー・レポート」には、レポートを提供する対象者に基づいて、包含または除外できる各種オプションが組み込まれています。

AppScan 内でレポートを開いて表示することができ、レポートをファイルとして保存すれば、Acrobat Reader などのサード・パーティーのアプリケーションで開くことができます。

アイコン	名前	簡略説明
	249 ページの『セキュリティー・レポート』	スキャン中に検出されたセキュリティー問題のレポートセキュリティー情報は非常に広範囲に渡る場合があり、ユーザーの要件に応じてフィルタリングできます。6 つの標準テンプレートが組み込まれていますが、各テンプレートは、必要に応じて情報のカテゴリーを追加または削除するように容易に調整できます。
	253 ページの『業界標準のレポート』	選択した業界団体、またはユーザー独自のカスタム標準チェックリストに対するアプリケーションの準拠 (または非準拠) 状況のレポート。
	255 ページの『コンプライアンス・レポート』	さまざまな法規制、法定基準、またはユーザー独自のカスタム・コンプライアンス・テンプレートに対するアプリケーションの準拠 (または非準拠) 状況のレポート。
	266 ページの『差分分析レポート』	差分分析レポートでは、2 つのスキャン結果セットが比較され、検出された URL またはセキュリティー問題 (あるいはこの両方) の差異が示されます。
	268 ページの『テンプレートに基づくレポート』	ユーザー定義データとユーザー定義文書フォーマット設定を記述した Microsoft Word DOC および DOCX 形式のカスタム・レポート。

レポート・レイアウトの構成

「レポート作成」ダイアログ・ボックスの「レイアウト」タブを使って、レポートの外観をカスタマイズできます (この機能はオプションです。デフォルトのレイアウトを使用してレポートを作成して問題ありません)。

手順

1. 「レポート作成」ダイアログ・ボックスで、「レイアウト」タブをクリックします。
2. 必要なレイアウト・オプションを選択し、適切な値を入力します。

レイアウト・オプション	説明
カバー・ページを含める	レポートにカバー・ページを追加します。選択すると、カバー・ページ・オプションが有効になります。
会社のロゴ	カバー・ページの左上に会社のロゴを出力します (「会社のロゴ」領域で  をクリックし、コンピューター上のロゴ・ファイルを参照します)。AppScan のロゴが、デフォルトのロゴです。
追加のロゴ	カバー・ページの右上に追加のロゴを出力します (「会社のロゴ」領域で  をクリックし、コンピューター上のロゴ・ファイルを参照します)。
レポート・タイプ	カバー・ページの下半分に「レポート・タイプ」(編集可のテキスト) を出力します。
レポート・タイトル	カバー・ページの中央に、メイン・タイトルとして、デフォルトのタイトルまたはユーザー入力のタイトルを出力します。
説明	カバー・ページに説明として、デフォルトの説明かユーザーが入力した説明を出力します。
レポートの日付	レポート内の各ページのフッターに、日付を出力します。
ヘッダー/フッター	各ページ内にヘッダーまたはフッター (あるいはその両方) を追加します。表示するテキストを入力します。
目次	レポートに目次を出力します。
既定のレイアウトとして保存	今後も使用できるように、レイアウト設定およびテキストを保存します。

レポートの表示と保存

レポートの生成、AppScan のレポート・ビューアーでの表示、および各種形式での保存を行うことができます。

手順

1. 必要に応じてレポート・タイプ、テンプレート、フィルターを構成します。
2. レポート・ビューアーでプレビューを表示するには、「プレビュー」をクリックします。
3. レポートを保存するには「レポートの保存」をクリックし、レポート名を入力して形式を選択します。PDF (Adobe Acrobat Reader)、HTML (Web ブラウザー)、RTF (Microsoft Word) または TXT (テキスト・エディター)。

   注: あるフォーマットで以前に保存したレポートを別のフォーマットで保存するときは、別のファイル名で保存する必要があります。例:以前に Report458.pdf という名前でレポートを保存しており、今回は RTF フォーマットで保存する場合、Report458.rtf という名称では保存できず、Report_458.rtf などの名称で保存します。

部分レポートの作成

レポートを作成する URL またはフォルダーを右クリックすることで、スキャン結果のサブセットのセキュリティー・レポートまたはテンプレートに基づくレポートを作成できます。

手順

1. アプリケーション・ツリーで、レポートを作成する URL またはフォルダーを右クリックしてから、以下を選択します。
   - 「このノードのレポート」>「セキュリティー」
   - 「このノードのレポート」>「テンプレートに基づく」

   「レポート作成」ダイアログ・ボックスが開き、選択されたノードのレポート・オプションが表示されます。
2. 通常のレポートと同様に操作を続行します。
   - 『セキュリティー・レポート』
   - 268 ページの『テンプレートに基づくレポート』

前のバージョンのレポート・テンプレート

いくつかの業界標準テンプレートおよびコンプライアンス・テンプレートについては、前のバージョンが「Old Versions」フォルダーに保存されています。

このタスクについて

「レポート」ダイアログ・ボックスには、レポート・テンプレートの最新バージョンがリストされます。ただし、いくつかの業界標準レポートおよびコンプライアンス・レポートについては、前のバージョンが特別なフォルダーに保存されています。フォルダーは[AppScan Standard installation folder]\Regulations\Old Versionsにあります。

手順

1. 「レポート」ダイアログ・ボックスで、「業界標準」または「コンプライアンス」を選択します。
2. 「レポート・タイプ」タブで、「ユーザー定義」を選択します。
3. 「参照...」をクリックし、[AppScan Standard installation folder]\Regulations\Old Versionsに移動します。

   日本語の場合、[AppScan Standard installation folder]\ja-JP\Regulations\Old Versionsにあります。
4. 必要なファイルを選択し、通常のレポート作成の場合と同様に操作を続行します。

セキュリティー・レポート

セキュリティー・レポートには、検出されたセキュリティー問題に関する情報が出力され、ユーザーは必要なコンテンツ・タイプに応じて各種テンプレートから選択することができます。

このタスクについて

スキャン全体をカバーするセキュリティー・レポートを作成できます。また、アプリケーション・ツリー内の特定の URL またはフォルダーに関するレポートも作成できます。

各レポート・テンプレートは、組織内の異なる対象者に対応したコンテンツ・トピックで構成されています。トピックには、各ビュー (セキュリティー問題、修復タスク、アプリケーション・データ) からのスキャン結果が含まれており、結果が意味する内容、結果が適切な理由、およびその修正方法が、印刷に適したフォーマットで、読みやすく、簡単に理解できるように出力されます。

セキュリティー・レポートのオプション

以下の表は、「セキュリティー・レポート」ダイアログ・ボックスのオプションを要約したものです。

オプション	説明
テンプレート	以降の表で示すように、右側ペインのチェック・ボックスを選択/選択解除することで、レポート用のテンプレートのいずれかを選択するか、独自のテンプレートを定義します。 • デフォルト: 概要と問題情報が含まれている中レベルのレポート。バリアントの詳細は含まれていません。 • 概要: Web アプリケーションで検出されたセキュリティー上のリスクの重要部分の概要と、スキャン結果の統計 (表およびチャートの形式)。 • 詳細: 概要に加えて、セキュリティー問題、アドバイザリーと推奨される修正、修復タスク、およびアプリケーション・データが含まれる詳細レポート。 • 修復タスク: スキャンで検出された問題に対応することを意図したアクション。 • 開発者: セキュリティー問題、バリアント、アドバイザリーおよび推奨される修正。「概要」または「修復タスク」のセクションはありません。 • **QA:** セキュリティー問題、アドバイザリーおよび推奨される修正、アプリケーション・データ。バリアントの詳細情報、「概要」、「修復タスク」の各セクションはありません。 • サイト・インベントリー: アプリケーション・データのみ。 • カスタム・テンプレート: このオプションでは、チェック・ボックスを使用して必要なレポートを定義し、「テンプレートとして作成」をクリックしてカスタム・セキュリティー・レポート・テンプレートを作成することができます。テンプレートを保存すると、その後はユーザー・インターフェースとコマンド行インターフェースの両方からテンプレートを使用してレポートを作成できます。 – テンプレートとして保存: 現在のセキュリティー・レポート構成をカスタム・テンプレートとして保存します。 – テンプレートの削除: 現在のカスタム・テンプレートを削除します。
最低重大度	レポートに含める問題の最も低い重大度レベルを選択します。
テスト・タイプ	レポートに含めるテスト結果のタイプを選択します。すべて、アプリケーション、インフラストラクチャまたは サード・パーティー・ウェブ・コンポーネントテスト。
ソート基準	タイプまたは URL ごとに問題をソートするかどうかを選択します。
問題ごとのバリアントの数を制限します	現在の詳細レベルがレポートの受信者に対して有用でないと考えられる場合、問題別にリストされるバリアントの数を制限して、レポートの長さを短くすることができます。
各問題の後に改ページを追加する	この設定は、PDF 出力にのみ適用されます。これにより、レポートが読みやすくなります。
完了時に表示	このチェック・ボックスを選択すると、レポートの生成後にレポートが適切なビューアーで開かれます。 **注:** これは、生成されたレポートを開くことができるプログラムをインストールしている場合にのみ機能します。

いずれかのテンプレートをベースとして選択したら、レポートに出力する情報のフィールドを選択または選択解除することで、各レポートの構成をカスタマイズできます。これを行うと、テンプレート名が「カスタム」に変更されます。

セキュリティー・レポートのセクション

以下の表は、さまざまなセキュリティー・レポートの標準的なコンテンツを要約したものです。すべての場合で実際のコンテンツは、必要に応じて「レポート・コンテンツ」ペインのチェック・ボックスを選択または選択解除することで、変更できます。

注: 詳細レポートは全体で数百ページになることがあるため、レポートの対象者に関係するセクションだけを出力するようにしてください。

レポート・セクション	説明
概要	スキャンに関するいくつかの全般情報を示す短いセクション。検出された問題 (高、中、低、および情報) の全体数や、ログイン設定の詳細などが含まれます。このセクションは、すべてのレポートに含まれます。
要約	スキャン (またはレポートに含まれるスキャンの一部) に関する以下の情報を要約した一連の表: • 問題のタイプ (各タイプについて検出された問題の数や、その重大度など) • 脆弱性のある URL (URL ごとの問題の数やタイプなど) • 推奨される修正 • セキュリティー上のリスク • 原因 • WASC 脅威の分類
セキュリティー問題	アプリケーションで検出された問題 • 基本アクセス以下のいずれのチェック・ボックスも選択しなかった場合、基本情報のみが含まれます。 • 追加:スクリーン・キャプチャーなど、より詳細な情報が含まれます (「問題情報」タブの内容に類似)。 • バリアント:特定のバリアント情報が含まれます。 – 要求/応答 – 差:オリジナルの要求とテスト要求の間の差分 (詳細ペイン >「要求/応答」タブを参照)
アドバイザリーと推奨される修正	検出された問題の技術的な説明と、それを修正するための推奨事項。 **注:** .NET、Java EE、および PHP 環境に固有の推奨される修正を含めるには、「ツール」>「オプション」>「設定」に移動し、必要なオプションを選択します。
修復タスク	検出された問題に基づき、サイト・セキュリティーを改善するための推奨タスク。 1 つのタスクで複数の問題を解決できる場合もあります。
アプリケーション・データ	ユーザーの Web アプリケーションで AppScan が検出したデータのリスト: アプリケーション URL、スクリプト・パラメーター、リンク切れ、コメント、JavaScript、Cookie、およびフィルタリングされた URL。

手順

1. レポートの基本とするスキャン・コンテンツを選択します。
   • スキャン全体に対するレポートを作成するには、「ツール」>「レポート」>「セキュリティー・レポート」をクリックします。

- スキャンに含まれていた特定の URL またはフォルダーのレポートを作成するには、アプリケーション・ツリーでノードを右クリックし、「このノードのレポート」>「セキュリティー」を選択します。

2. 右側ペインのチェック・ボックスを選択/選択解除することで、関連するテンプレートを選択するか、独自のレポート・コンテンツを定義します。
3. 必要なオプションを選択します。
4. 将来の利用のために構成を保存するには、「テンプレートとして保存」をクリックしてテンプレートに一意の名前をつけてください。
5. レポートのレイアウトをカスタマイズするには、「レイアウト」タブをクリックします。詳細については、 247 ページの『レポート・レイアウトの構成』 を参照してください。
6. 必要な出力フォーマットを選択してください:PDF、HTML、TXT、RTF、XML。
7. 「レポートの保存」をクリックします。

セキュリティー・レポートのサイズの制限

大容量のセキュリティー・レポートをより管理しやすいサイズに削減するためのヒントについて説明します。

このタスクについて

セキュリティー・レポートは、非常に大容量になる可能性があります。セキュリティー・レポートの生成時に、ファイルが数百ページの長さになることを示す警告メッセージを受け取った場合、あるいはレポートの作成処理がタイムアウトになった場合は、以下のヒントを試行して、重要な情報を含めたままレポート・サイズを削減することができます。

手順

1. レポート・サイズを減らす 1 つの方法は、レポート対象をアプリケーションの一部に制限することです。これを行うには、アプリケーション・ツリーで関連ノードを選択し、右クリックして「このノードのレポート」>「セキュリティー」を選択します。これにより、選択したノードの下にあるアプリケーションのすべての部分についてのレポートが作成されます。
2. スキャン結果に数千の問題が含まれていることが示された場合は、「概要」のみを生成するか、または「追加の問題情報」のチェック・ボックスをクリアして「デフォルト・レポート」を生成することを検討してください。
3. デフォルトでは、すべての テスト・タイプがレポートに含まれます 。(最も低い重大度 = 情報)「最も低い重大度」設定を引き上げ、重大度が「高」の問題のみ、または重大度が「高」および「中」の問題を含めるようにします。
4. 「最大バリアント」設定が 1 であることを確認し、各問題に対して複数のバリアントが含まれないようにします。
5. 「バリアント」>「要求/応答」、および「アドバイザリーと推奨される修正」を含めると、レポートの容量が大幅に追加されるので注意してください。これらのオプションは、必要な場合にのみ選択してください。

業界標準のレポートおよびコンプライアンス・レポート

業界標準のレポートを使用すると、アプリケーションが、選択した業界の委員会の標準に準拠しているかどうかが分かります。コンプライアンス・レポートを使用すると、アプリケーションが、特定の規制や法定基準に準拠しているかどうかが分かります。

業界標準のレポート

業界標準のレポートを利用すると、ユーザーのアプリケーションが、選択した業界の委員会の標準に準拠しているかどうかが分かります。

このタスクについて

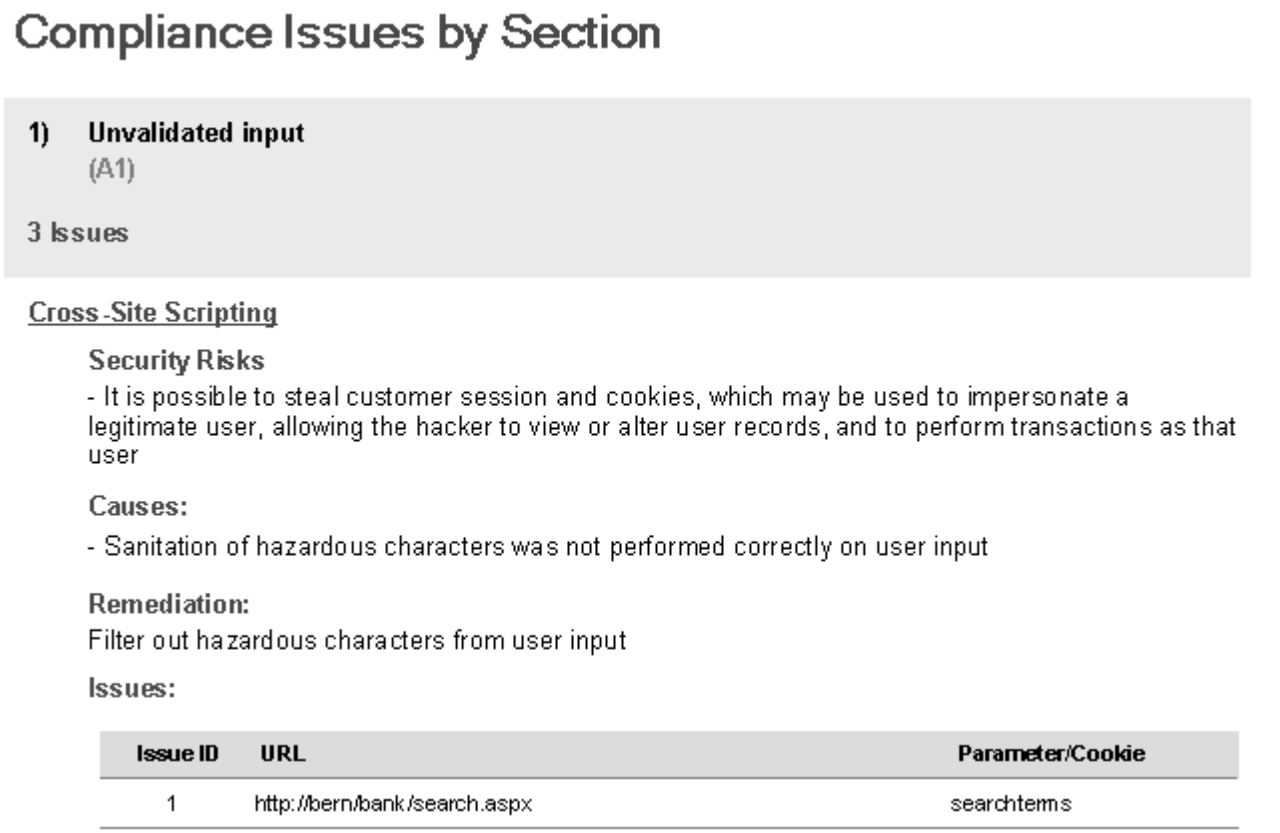
さまざまな業界で新しい標準が作成されているため、選択するテンプレートのリストは IBM が更新し、ご使用の AppScan は定期的に自動で更新されます。

必要な業界標準がリストにない場合は、独自の業界標準のレポート・テンプレートを作成することで対応できます (258 ページの『ユーザー定義レポート』を参照)。

業界標準のレポートは、次のセクションで構成されています。

セクション・タイトル	出力される情報
説明	標準の説明。
コンプライアンスの概要 (Compliance Summary)	標準に準拠していない問題のリストと数。 1 つの問題が複数のセクションで非準拠として出力されることがあります。このため、セクションごとの問題の数を合計すると、実際の問題の数より多くなることがあります。
固有のコンプライアンス問題 (Unique Compliance Issues)	非準拠の URL、関連するパラメーターまたは Cookie、およびテスト名のリスト。 各問題は一度だけ出力されます。
セクション別のコンプライアンス問題 (Compliance Issues by Section)	アプリケーションの非準拠の状況の詳細説明と、問題に対応するための修復方法。

次の図は、業界標準のレポートのサンプル (抜粋) です。



Compliance Issues by Section

1) Unvalidated input
(A1)

3 Issues

Cross-Site Scripting

Security Risks
- It is possible to steal customer session and cookies, which may be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user

Causes:
- Sanitation of hazardous characters was not performed correctly on user input

Remediation:
Filter out hazardous characters from user input

Issues:

Issue ID	URL	Parameter/Cookie
1	http://bern/bank/search.aspx	searchterms

手順

1. 「ツール」>「レポート」>「業界標準」をクリックします。
2. 以下のいずれかを実行します。
   - リストされている「業界標準のレポートのテンプレート」の中から 1 つ選択します。
   - 「ユーザー定義」ラジオ・ボタンを選択し、業界標準のカスタム・テンプレート・ファイル **(*.asreg)** を入力するか、参照します。詳細については、 258 ページの『ユーザー定義レポート』を参照してください。
3. レポートの外観を制御するには、「レイアウト」タブ (247 ページの『レポート・レイアウトの構成』を参照) を開きます。
4. 「プレビュー」をクリックしてレポートを作成し、AppScan で表示するか、「レポートの保存」をクリックしてレポートを作成し、ファイルに保存します。

サポートされるバージョン

サポートされる業界標準およびバージョンのリスト。

以下の業界標準のレポートを生成できます。

業界標準	バージョン
国際規格 - ISO 27001	2013 年 1 月
国際規格 - ISO 27002	2013 年 1 月
NERC CIPC 電子部門セキュリティー・ガイドライン	2013 年 9 月
NIST 特別刊行物 800-53	改訂 4
OWASP Top 10	2013, 2017

業界標準	バージョン
SANS/CWE 上位 25 の最も危険なプログラミング・エラー	1.03
WASC 脅威の分類	2.0

コンプライアンス・レポート

コンプライアンス・レポートを利用すれば、ユーザーのアプリケーションが、規制や法的標準に準拠しているかどうかが分かります。

このタスクについて

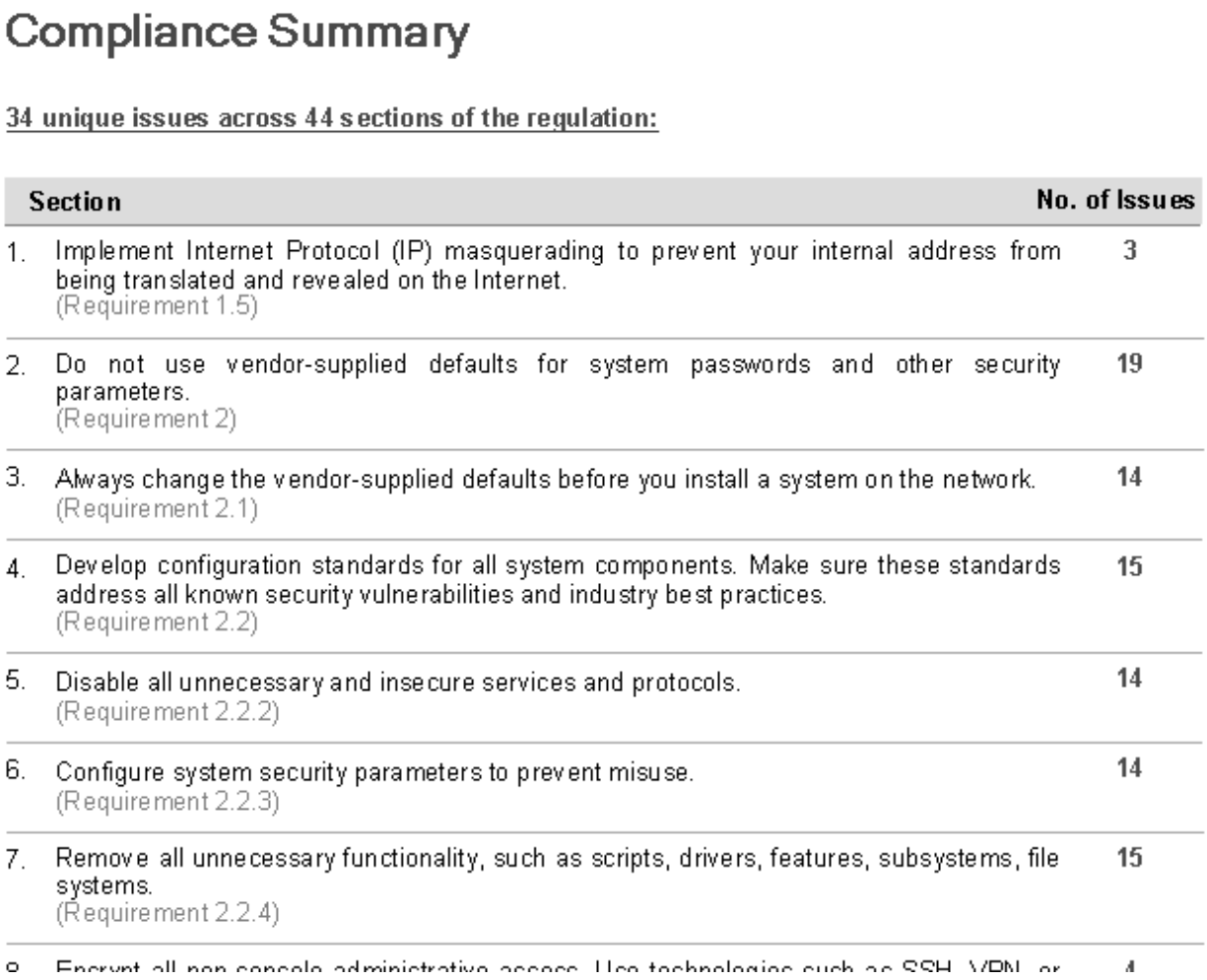
さまざまな国のテンプレートが多数用意されており、そこから選択できます。各テンプレートが、各種規制のコンプライアンス・レポートになります。

必要な規制がリストにない場合は、独自のコンプライアンス・レポート・テンプレートを作成することで対応できます (詳しくは 258 ページの『ユーザー定義レポート』を参照)。

コンプライアンス・レポートは次のセクションで構成されています。

セクション・タイトル	出力される情報
説明	規制の説明。
コンプライアンスの概要 (Compliance Summary)	標準に準拠していない問題のリストと数。 1 つの問題が複数のセクションで非準拠として出力されることがあります。このため、セクションごとの問題の数を合計すると、実際の問題の数より多くなることがあります。
固有のコンプライアンス問題 (Unique Compliance Issues)	非準拠の URL、関連するパラメーターまたは Cookie、およびテスト名のリスト。 各問題は一度だけ出力されます。
セクション別のコンプライアンス問題 (Compliance Issues by Section)	アプリケーションの非準拠の状況の詳細説明と、問題に対応するための修復方法。

次の図は、コンプライアンス・レポートのサンプルです。



Compliance Summary

34 unique issues across 44 sections of the regulation:

	Section	No. of Issues
1.	Implement Internet Protocol (IP) masquerading to prevent your internal address from being translated and revealed on the Internet. (Requirement 1.5)	3
2.	Do not use vendor-supplied defaults for system passwords and other security parameters. (Requirement 2)	19
3.	Always change the vendor-supplied defaults before you install a system on the network. (Requirement 2.1)	14
4.	Develop configuration standards for all system components. Make sure these standards address all known security vulnerabilities and industry best practices. (Requirement 2.2)	15
5.	Disable all unnecessary and insecure services and protocols. (Requirement 2.2.2)	14
6.	Configure system security parameters to prevent misuse. (Requirement 2.2.3)	14
7.	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems. (Requirement 2.2.4)	15
8.	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or	4

手順

1. 「ツール」>「レポート」>「コンプライアンス」をクリックします。
2. 以下のいずれかを実行します。
   - リストされている「コンプライアンス・レポート・テンプレート」の中から 1 つ選択します。
   - 「ユーザー定義」ラジオ・ボタンを選択し、カスタム・コンプライアンス・テンプレート・ファイル (***.asreg**) を入力するか、参照します。詳細については、 258 ページの『ユーザー定義レポート』を参照してください。
3. レポートの外観を制御するには、「レイアウト」タブ (247 ページの『レポート・レイアウトの構成』を参照) を開きます。
4. 「プレビュー」をクリックしてレポートを作成し、AppScan で表示するか、「レポートの保存」をクリックしてレポートを作成し、ファイルに保存します。

サポートされるバージョン

サポートされる規制およびバージョンのリスト。

以下のコンプライアンス・レポートを生成できます。

規制	サポートされるバージョン
[オーストラリア] APRA PPG 234 - Management of Security Risk in Information and Information technology	2012 年 1 月
[カナダ] PIPED 法	2014 年 1 月
[カナダ] 情報の自由とプライバシー保護法 (FIPPA)	2012 年 9 月
[カナダ] Management of Information Security Technology (MITS)	2012 年 9 月
[EU] 欧州指令 1995/46/EC	2012 年 1 月
[EU] 欧州指令 2002/58/EC	2012 年 3 月
[EU] 欧州議会および理事会による 2016/679 規定 (GDPR)	2016 年 4 月
[日本] 個人情報保護法 (JPIPA)	2012 年 1 月
[英国] データ保護法	2014 年 12 月
[米国] カリフォルニア州 Assembly Bill 1950 および Senate Bill 1386	2012 年 3 月
[米国] 児童オンライン・プライバシー保護法 (COPPA)	2014 年 12 月
[米国] DCID 6/3 可用性: 低	2011 年 1 月
[米国] DCID 6/3 可用性: 高	2011 年 1 月
[米国] DCID 6/3 可用性: 中	2011 年 1 月
[米国] DCID 6/3 機密保持要求の保護レベル: レベル 1	2011 年 1 月
[米国] DCID 6/3 機密保持要求の保護レベル: レベル 2	2011 年 1 月
[米国] DCID 6/3 機密保持要求の保護レベル: レベル 3	2011 年 1 月
[米国] DCID 6/3 機密保持要求の保護レベル: レベル 4	2011 年 1 月
[米国] DCID 6/3 機密保持要求の保護レベル: レベル 5	2011 年 1 月
[米国] DCID 6/3 保全性: 低	2011 年 1 月
[米国] DCID 6/3 保全性: 高	2011 年 1 月
[米国] DCID 6/3 保全性: 中	2011 年 1 月
[米国] DCID 6/3 先進テクノロジー IS の保護	2011 年 1 月
[米国] 電子資金決済法 (EFTA)	2013 年 12 月
[米国] 連邦金融機関検査協議会 (FFIEC)、機密保護ハンドブック	2013 年 2 月
[米国] Federal Information Security Management Act (FISMA)	2014 年 9 月
[米国] 米国連邦政府によるリスクおよび認証管理プログラム (FedRAMP)	
[米国] 金融サービス (GLBA)	2013 年 1 月
[米国] 医療保険サービス (HIPAA)	2014 年 12 月
[米国] NERC サイバー・セキュリティー標準	2014 年 9 月
[米国] プライバシー法 (1974 年)	2011 年 1 月
[米国] セーフ・ハーバー	2012 年 11 月
[米国] サーベンス・オクスリー法 (SOX)	2013 年 1 月
[米国] 連邦規制基準タイトル 21	2011 年 11 月

規制	サポートされるバージョン
[米国] 家庭教育の権利とプライバシーに関する法 (FERPA)	2013 年 1 月
[米国] DISA の Application Security and Development STIG	V3 リリース 9
[米国] DoD 指令 8500.1 – サイバーセキュリティー	2014 年 9 月
[米国] DoD 指令 8550.01 - インターネット・サービスとインターネットを使用した機能	2014 年 9 月
[米国] Massachusetts 201 CMR 17.00	2011 年 1 月
Basel II	2012 年 10 月
Payment Application Data Security Standard	3.0
クレジット・カード業界データ・セキュリティー基準 (PCI DSS)	3.2

ユーザー定義レポート

業界標準レポートまたはコンプライアンス・レポート用に、ユーザー定義テンプレートを作成できます。

このタスクについて

AppScan のレポート・テンプレートには、**.asreg** というファイル拡張子が付きます。提供されたテンプレートは、AppScan のインストール・ディレクトリーの \Regulations フォルダーに保管されます。作成したテンプレートは、AppScan のユーザー・ファイルのフォルダーに保管する必要があります。

新しいテンプレートを最初から作成し、拡張子 **.asreg** を付けて保存するか、既存のファイルをコピーして、必要に応じて変更します (以下の手順では、既存のテンプレートをベースにしたテンプレートの作成について説明します)。

手順

1. **[AppScan Standard installation folder]\AppScan\Regulations** フォルダーを開き、既存の **.asreg** ファイルをコピーします。
2. AppScan のユーザー・ファイルのフォルダー内にファイルを貼り付け、新しい名前を付けます。

   注**:** AppScan のユーザー・ファイルのフォルダーは、「ツール」**>**「オプション」**>**「設定」タブ **>**「ファイルの場所」**>**「ユーザー・ファイルのフォルダー」で別の場所を指定していない限り、デフォルトにより \My Documents\AppScan です。
3. ルート・タグは Regulation で、属性は format_version です。

   ```
   <Regulation format_version="2.0">
   ```
4. 次のタグは、作成するテンプレートのタイトルになります。

   ```
   <Title>Our Organization's web Application Requirement Compliance Report
   </Title>
   ```
5. Description タグを使って、規制または標準の説明を入力します。

   ```
   <Description>
    <Subtitle>Sub Section</Subtitle>
    <p>This regulation addresses ...</p>
    <p>It is important because...</p>
    <Subtitle>Sub Section 2</Subtitle>
    <p>This section of the regulation addresses ...</p>
   </Description>
   ```

6. デフォルトで <Disclaimer> タグがあり、レポートの内容に法的な責任を負わないことを明記します。
7. 規制テンプレートの 1 つ以上の要件セクションを (<Section> タグを使用して) 作成し、各セクションにどの AppScan 問題が関連するかを (<Cause>, <Risk>, <ThreatClass>, および <CWE> タグを使用して) 定義します。
   - Section タグの name 属性を使用して、レポートのセクション・タイトルを定義します。
   - Section タグを開いて閉じるまでに、以下の 1 つ以上を追加します。
     - 『原因リスト』から<Cause>。原因は、不完全または不正確な構成、欠落している検証、または類似の状況を示します。
     - 261 ページの『リスク・リスト』から<Risk>。各リスクは、「ワースト・ケース・シナリオ」です。
     - 262 ページの『脅威クラス・リスト』から<ThreatClass>。テストのカテゴリーが脅威クラスです。
     - 番号で<CWE>。

   例:

```
<Section name="My Application login must be secured">
 <Cause>inputLengthNotChecked</Cause>
 <Risk>denialOfService</Risk>
 <Risk>siteDefacement</Risk>
 <CWE>79</CWE>
</Section>
```

8. </Regulation> 終了タグでファイルを閉じます。

原因リスト

原因	説明
hazardousCharactersNotSanitized	ユーザーの入力に対して危険な文字の処理が正しく実行されませんでした。
formatStringsVulnerability	ユーザーの入力が、C/C++ の sprintf および類似の関数の書式制御ストリング入力として直接使用されています。
hiddenParameterUsed	タイプ「非表示」のパラメーターとして、パラメーター値が HTML に「ハードコーディング」されています。
boundsCheckingOnParamValues	適切な境界チェックが着信パラメーター値に対して実行されませんでした。
incorrectDataType	ユーザー入力が想定されるデータ・タイプと一致することを確認する検証が実行されませんでした。
inputLengthNotChecked	ユーザー入力の長さが制限されていないため、バッファー・オーバーフローが起こり得ます。
errorMessagesReturned	機密のデバッグ情報が含まれている可能性がある例外メッセージおよびエラー・メッセージがユーザーに対して表示されています。
debugInfoInHtmlSource	プログラマーが Web ページにデバッグ情報を残しています。
backDoorLeftBehind	プログラマーがバック・ドアまたはデバッグ・オプションを残したままにしています。
clientSideValidation	ユーザー入力の検証がクライアント・サイドで行われるため、バイパスされる可能性があります。
usOfClientSideLogic	Web アプリケーションが Web ページの作成にクライアント・サイドのロジックを使用しています。
cookiesCreatedAtClientSide	クライアント・サイドで Cookie が作成されています。

原因	説明
javaScriptPassWordMechanism	Web アプリケーションがクライアント・サイドのパスワード認証を使用しています。
sqlBuiltByJavaScript	Web アプリケーションが SQL 照会の作成にクライアント・サイドのロジックを使用しています。
dotDotNotSanitized	ユーザー入力に対して「..」文字列のチェックがされていません。
weakTokenUsed	Web アプリケーションが脆弱なトークン・アルゴリズムを使用しています。
missingPatchesForThirdPartyProds	サード・パーティー製品の最新のパッチまたはホット・フィックスがインストールされていません。
tempFilesLeftBehind	実稼働環境に一時ファイルが残されました。
improperFileDirPermissions	ファイル/ディレクトリーに対して不適切なアクセス権/ACL が設定されました。
nimdaWormBackdoor	システム内で Nimda ワームが検出されました。
sampleScriptsFound	Web サイトにデフォルトのサンプル・スクリプトまたはディレクトリーがインストールされました。
insecureThirdPartySoftware	サード・パーティーの脆弱なソフトウェア (既知のパッチが未適用) が Web サイトにインストールされています。
directoryBrowsingEnabled	ディレクトリーの参照が有効になっています。
managementConsoleAccess	Web 管理コンソールが Web 側からアクセス可能になっています。
insecureWebServerConfiguration	Web サーバーまたはアプリケーション・サーバーが非セキュアな方法で構成されています。
frontPageServerUnsecureInstall	FrontPage サーバー・エクステンションが、セキュリティー設定が不適切な状態でインストールされました。
insecureWebAppConfiguration	Web アプリケーションのプログラミングまたは構成が非セキュアです。
vulnSOAPserializer	Web サービス・サーバーが使用する SOAP シリアライザーが SOAP 入力を適切に検証していません。
sensitiveDataNotSSL	ユーザー名、パスワード、クレジット・カード番号などの機密性のある入力フィールドが暗号化されずに受け渡しされています。
nonSecureCookiesSentOverSSL	非セキュアな Cookie を Web アプリケーションが SSL 経由で送信しています。
sessionCookieNotRAM	機密性の高いセッション情報を Web アプリケーションが永続 Cookie (ディスク上) に保存しています。
redirectionFromWithinSite	Web アプリケーションが外部サイトに対してリダイレクトを実行しています。
remoteFileInclusion	Web アプリケーションがリモート・ファイルのインクルードを許可しています。
GETParamOverSSL	クエリー・パラメーターは SSL を介して渡され、重要な情報を含んでいる可能性があります。
SensitiveCache	重要な情報が、お使いのブラウザーにキャッシュされている可能性があります。
InsufficientAuthentication	アプリケーションで不十分な認証方法が使用されていました。
useOfGlobalFlashParamsInPDNFs	潜在的に危険なネイティブ機能でグローバル Flash パラメーターが使用されています。
causeNotAvailable	なし

原因	説明
vulnActiveX	使用されている ActiveX コントロールは、脆弱として分類されています。スキャンされた Web サイトは、マルウェアを配布するためにハッキングされた可能性があります。
compromisedDigiNotarSSLCert	DigiNotar でのセキュリティー・ブリーチが原因で、使用中の SSL 証明書は安全性に問題がある証明書としてフラグが立っています。
paramValManipAllowed	アプリケーション・ロジックによってパラメーター値の操作が許可されました。

リスク・リスト

リスク名	説明
tempScriptDownload	一時スクリプト・ファイルがダウンロード可能になっているため、アプリケーション・ロジックやその他の機密情報 (ユーザー名、パスワードなど) が危険にさらされる可能性があります。
sourceCodeDisclosure	サーバー・サイドのスクリプトのソース・コードが取得可能になっているため、アプリケーション・ロジックやその他の機密情報 (ユーザー名、パスワードなど) が危険にさらされる可能性があります。
pathDisclosure	Web サーバーのインストール済み環境の絶対パスが取得可能になっているため、攻撃者がさらに攻撃を仕掛けたり、Web アプリケーションのファイル・システム構成に関する情報を取得しやすくなる可能性があります。
directoryListing	制限付きファイルが含まれている可能性がある、特定の Web アプリケーションの仮想ディレクトリーのコンテンツが、表示およびダウンロード可能になっています。
envVariablesExposure	サーバーの環境変数が危険にさらされており、Web アプリケーションに対する攻撃者のさらなる攻撃を容易にする可能性があります。
anyFileDownload	(Web サーバー・ユーザーのアクセス権が制限されている) Web サーバー上のファイル (データベース、ユーザー情報、構成ファイルなど) の内容が表示可能になっています。
userImpersonation	ユーザーのセッションと Cookie を盗むことが可能となっているため、正当なユーザーの偽名を使用される可能性があります。このため、ハッカーによるユーザー・レコードの表示または変更や、そのユーザーとしてのトランザクションの実行が可能になります。
remoteCommandExecution	Web サーバー上でリモート・コマンドの実行が可能になっています。通常これは、サーバーとそのコンテンツが全く無防備であることを意味します。
cacheFilesDownload	Web アプリケーションに関する機密情報が含まれている可能性のある、キャッシュ・ファイルの内容が表示可能になっています。
debugErrorInformation	機密性の高いデバッグ情報が収集可能になっています。
eShoplifting	商品やサービスを盗むことが可能になっています (eShoplifting)。
denialOfService	Web アプリケーションによる他のユーザーへのサービスが妨害可能になっています (サービス妨害)。
privilegeEscalation	ユーザー権限のエスカレーションと、Web アプリケーションに対する管理者権限の取得が可能になっています。
genericWorstCase	アプリケーション・ロジックの改ざんが可能になっています。
configurationFile Downloadable	ユーザー名やパスワードなどの重要な情報が登録されている可能性のある構成ファイルの内容が、ダウンロードまたは表示可能になっています。

リスク名	説明
sensitiveInformation	Web アプリケーションに関する機密情報 (ユーザー名、パスワード、マシン名、重要なファイルの場所) が収集可能になっています。
genericWorstCaseJavaScript	JavaScript が悪用される可能性があります。このリスクの範囲は、クライアント・サイドで変更されるページの内容によって異なります。
genericWorstCaseJSCookie	JSCookie のコードが悪用される可能性があります。このリスクの範囲は、クライアント・サイドで作成される Cookie のコンテキストとロールによって異なります。
emailSpoofing	スプーフした電子メール・アドレスを使って、Web アプリケーション経由で電子メールが送信可能になっています。
siteDefacement	Web サーバー上の Web ページ、スクリプト、ファイルのアップロード、変更、削除が可能になっています。
databaseManipulations	データベースのエントリーおよびテーブルの表示、変更、削除が可能になっています (SQL インジェクション)。
authBypass	Web アプリケーションの認証メカニズムがバイパス可能になっています。
siteStructureRevealed	サイトのファイル・システム構造に関する情報が取得可能になっているため、攻撃者による Web サイトのマップが容易になる可能性があります。
publisherInformation Revealed	FrontPage の重要なパブリッシュ情報が取得可能になっています。
dataResourceDownload	機密性の高いデータ・リソースに保管された情報がアクセス可能になっています。
sensitiveNotOverSSL	機密データ (クレジット・カード番号、社会保障番号など) が暗号化されずに送信されており、盗むことが可能になっています。
loginNotOverSSL	ユーザーのログイン情報 (ユーザー名やパスワード) が暗号化されずに送信されており、盗むことが可能になっています。
unsecureCookieInSSL	暗号化セッション中に送信されたユーザー情報およびセッション情報 (Cookie) を盗むことが可能になっています。
sessionCookieNotRAM	永続 Cookie としてディスク上に保管されていたセッション情報 (Cookie) を盗むことが可能になっています。
phishing	経験の浅いユーザーを騙して、機密情報 (ユーザー名、パスワード、クレジット・カード番号、社会保障番号など) を取得することが可能になっています。
cachePoisoning	Web キャッシュを破壊することによって、サイトのコンテンツの外観を破壊することができます。
attackFacilitation	攻撃者が Web サーバーを使用して他のサイトをアタックできるため、攻撃者の匿名性が高まります。
maliciousContent	なし
clientCodeExecution	Web アプリケーションのクライアント上で、任意のコードを実行することが可能です。
siteImpersonation	悪意のある攻撃者が、追加の攻撃ベクトルを使用することで、このサイトになりすます可能性があります。

脅威クラス・リスト

「WASC 脅威の分類」の概要です。これは、Web サイトや Web サイトのデータ、Web サイト・ユーザーのセキュリティー侵害の要因となり得る弱点および攻撃を分類する協調的な取り組みです。

攻撃および脅威の簡略説明を以下の表に示します。WASC 脅威の分類の詳細については、以下の Web サイトを参照してください。

http://projects.webappsec.org/w/page/13246978/Threat%20Classification

攻撃

名前	簡略説明
機能の悪用	Web サイトそのものの機構や機能を使って、アクセス制御メカニズムを消費、籠絡、または迂回する攻撃手法。
ブルート・フォース	個人のユーザー名、パスワード、クレジット・カード番号、暗号鍵の推測に使用する、トライアル・アンド・エラーの自動プロセス。
バッファー・オーバーフロー	割り当てられたバッファー・サイズを超えるデータでメモリーの一部を上書きすることで、アプリケーションの流れを変更する攻撃。
コンテンツ・スプーフィング	Web サイトに表示されているコンテンツが外部ソースに由来するものではない正当なコンテンツであるとユーザーに信じ込ませる攻撃技法。
資格情報/セッション予測	特定のセッションまたはユーザーを識別する固有な値を推定または推測することで、Web サイトのユーザーのコントロールを奪う、またはそのユーザーになりすますメソッド。
クロスサイト・スクリプティング	攻撃者が組み込んだ実行可能コードを Web サイトで強制的にエコー出力させ、ユーザーのブラウザーにロードさせる攻撃手法。
クロスサイト・リクエスト・フォージェリー	被害者としてアクションを実行するために、被害者に対して、被害者の認識や意図なしに HTTP 要求をターゲット宛先に送信するように強制する攻撃。
サービス妨害	Web サイトの通常のユーザー処理の実行を妨害することを意図した攻撃手法。
フィンガー・プリンティング	攻撃者の最も一般的な方法は、ターゲットの Web プレゼンスにまずフットプリントを付け、できるだけ多くの情報を列挙することです。攻撃者はこの情報を使用して、正確な攻撃シナリオを作成できます。このシナリオでは、ターゲット・ホストによって使用されているソフトウェアのタイプ/バージョンにおける脆弱性を効果的に悪用します。
書式文字列	ストリング書式制御ライブラリー機能を使って他のメモリー・スペースにアクセスすることで、アプリケーションの流れを変更する攻撃。
HTTP レスポンス・スマグリング	サーバーから単一の応答を予期 (または許可) している中間 HTTP デバイスを通じて、サーバーからクライアントに 2 つの HTTP 応答を「スマグリング」(密輸) する手法です。
HTTP レスポンス分割	HTTP レスポンス分割の基本は、攻撃者が Web サーバーに出力ストリームを形成させる単一の HTTP 要求を送信し、ターゲットにその出力を 1 つの HTTP 応答ではなく、2 つの HTTP 応答として解釈させることができるということです。
HTTP リクエスト・スマグリング	2 つの HTTP デバイス間の RFC に準拠していない HTTP 要求の構文解析における矛盾を悪用する攻撃手法で、最初のデバイスを通じて 2 番目のデバイスに要求をスマグリングします。
HTTP リクエスト分割	HTTP リクエスト分割は、ブラウザーに任意の HTTP 要求を送信するよう強制することができる攻撃で、XSS に負担をかけ、ブラウザーのキャッシュを汚染します。
整数オーバーフロー	乗算や加算などの算術演算の結果が、保管に使用される整数型の最大サイズを超えている場合に生じる状態。
LDAP 注入	ユーザー入力から LDAP ステートメントを構成する Web サイトを不正に利用するための攻撃技法。

名前	簡略説明
メール・コマンド注入	適切にサニタイズされていないユーザーの入力から IMAP/SMTP ステートメントを組み立てる、メール・サーバーおよび Web メール・アプリケーションを悪用するために使用される攻撃手法。
NULL バイト・インジェクション	URL エンコードされたヌル・バイト文字をユーザー・データに追加することで、Web インフラストラクチャー内の正常性チェック・フィルターを迂回するために使用されるアクティブな悪用技法。
OS コマンド実行	アプリケーションの入力を操作することでオペレーティング・システムのコマンドを実行する攻撃手法で、Web サイトを悪用するために使用。
パス・トラバーサル	Web ドキュメントのルート・ディレクトリー以外に存在する可能性のあるファイル、ディレクトリー、コマンドに強制的にアクセスする手法です。
予測可能なリソースの位置	高度な推測によって、Web サイトの隠されたコンテンツや機能を明らかにするために使用される攻撃手法。
リモート・ファイル・インクルード	Web アプリケーションの「動的ファイルのインクルード」メカニズムを悪用するために使用される攻撃手法で、アプリケーションをだまして悪質なコードを含むリモート・ファイルを組み込ませます。
迂回ルーティング	「中間者」攻撃の 1 タイプで、中間者を注入または「ハイジャック」して、機密メッセージを外部ロケーションにルーティングすることを可能にします。
セッション固定	ユーザーのセッション ID を強制的に明示的な値にする攻撃手法。ユーザーのセッション ID が固定された後、攻撃者はユーザーのログインを待ちます。ユーザーがログインすると、攻撃者は事前定義されたセッション ID の値を使ってユーザーのオンライン・アイデンティティーを装います。
脆弱パスワード・リカバリー検証	Web サイトで別のユーザーのパスワードを攻撃者が不正に取得、変更、またはリカバリーできる場合。
SOAP 配列の悪用	配列を予期している Web サービスは、XML DoS 攻撃のターゲットとなる可能性があります。これは、SOAP サーバーにマシンのメモリー内に大量の配列を作成するよう強制し、メモリーの事前割り振りのためにマシン上の DoS 状態に負担をかけることによって実行されます。
SSI 注入	攻撃者が Web アプリケーションにコードを送信できるようにするサーバー・サイドの攻撃手法。その後、Web サーバーがそのコードをローカルで実行。
SQL 注入	ユーザー入力から SQL ステートメントを組み立てる、Web サイトを不正に利用するための攻撃手法。
URL リダイレクターの悪用	URL リダイレクターは、着信要求を代替リソースに転送するために Web サイトによって使用される一般的な機能であり、フィッシング攻撃で使用される場合があります。
XPath 注入	ユーザー入力から XPath 照会を構成する Web サイトを不正に利用するための攻撃技法。
XML 属性ブローアップ	XML パーサーに対するサービス妨害攻撃。

名前	簡略説明
XML 外部エンティティー	この手法は、処理時に文書を動的にビルドする XML の機能を悪用します。XML メッセージは、データを明示的に提供するか、データが存在する URI を指すことでデータを提供することができます。この攻撃手法では、外部エンティティーがエンティティー値を悪質なデータや代替参照で置換したり、サーバーや XML アプリケーションがアクセス権を持つデータのセキュリティーを危険にさらしたりします。
XML エンティティーの拡張	これは、文書の至るところで使用できる、エンティティーと呼ばれるカスタム・マクロを作成できるようにする XML DTD での機能を悪用します。攻撃者は、文書の上部にある一連のカスタム・エンティティーを再帰的に定義することにより、エンティティーの完全な解決を試行するパーサーに対し、再帰的な定義でほぼ無限に試行を繰り返すように強制して負担をかけます。
XML 注入	XML アプリケーションまたは XML サービスのロジックを操作または危険にさらすために使用される攻撃手法。意図していない XML コンテンツ、XML 構造、またはその両方を XML メッセージに注入することで、アプリケーションの意図されたロジックを変更できます。さらに、XML インジェクションにより、悪質なコンテンツを結果のメッセージや文書に挿入することができます。
XQuery インジェクション	XQuery インジェクションは、XML XQuery 言語に対する従来の SQL インジェクション攻撃のバリアントです。XQuery インジェクションは、不適切に検証されたデータを使用し、それが XQuery コマンドに渡されるようにします。

弱点

名前	簡略説明
誤ったアプリケーション構成	以下の攻撃は、Web アプリケーションに見つかる構成の弱点を悪用します。
ディレクトリー索引付け	自動ディレクトリー・リスト作成/索引作成は Web サーバーの機能で、通常の基本ファイル (index.html/home.html/default.htm) が存在しない場合に、要求したディレクトリー内のすべてのファイルをリストします。ソフトウェアに脆弱性がある状態で特定の Web 要求を実行すると、意図しないディレクトリー・リスト作成が可能になることがあります。
ファイル・システムへの不適切なアクセス許可	Web アプリケーションの機密性、保全性、および可用性への脅威。この問題は、誤ったファイル・システム許可がファイル、フォルダー、およびシンボリック・リンクに対して設定されている場合に生じます。
不適切な入力処理	今日、アプリケーション全般で特定される最も一般的な弱点の 1 つです。不適切に処理された入力は、システムおよびアプリケーションに存在する重大な脆弱性の背後にある主な原因です。
不適切な出力処理	アプリケーションに不適切な出力処理があると、出力データが取り込まれて、脆弱性やアプリケーション開発者が意図しないアクションを引き起す原因となる場合があります。
情報漏えい	アプリケーションが機密データ (Web アプリケーション、環境、およびユーザー固有のデータの技術的詳細など) を漏えいするアプリケーションの弱点。
安全でない索引付け	Web サイトのデータ機密性に対する脅威。本来は公的にアクセスできないファイルにアクセスできるプロセスを介して Web サイトのコンテンツを索引付けすると、そのようなファイルの存在およびそれらの内容について情報が漏えいする恐れがあります。索引付けのプロセスでは、そのような情報が索引付けのプロセスにより収集されて保管されます。この情報は後から、通常は検索エンジンへの一連の照会により、強い意志を持った攻撃者が取得する可能性があります。

名前	簡略説明
Insufficient Anti-automation	手動でのみ実行すべきプロセスを、攻撃者が自動化できるような状態になっている Web サイト。
不適切な認証	適切な認証なしに重要なコンテンツまたは機能に攻撃者がアクセスすることを Web サイトが許可している場合。
不適切な許可	追加のアクセス制御による制限を必要とすべき、重要なコンテンツまたは機能へのアクセスを Web サイトが許可している状態。
不適切なパスワード復元	Web サイトで別のユーザーのパスワードを攻撃者が不正に取得、変更、またはリカバリーできる場合。
不適切なプロセス検証	アプリケーションの本来のフロー制御を攻撃者が迂回または回避できる状態になっている Web サイト。
不適切なセッション有効期限	許可用の古いセッション証明書またはセッション ID を攻撃者が再使用できる状態になっている Web サイト。
不十分なトランスポート層保護	信頼できないサード・パーティーに通信がさらされるのを許します。
誤ったサーバー構成	Web サーバーおよびアプリケーション・サーバーで見つかる構成の弱点を悪用します。

差分分析レポート

「差分分析」レポートでは、2 組のスキャン結果が比較され、URL とそこで発見されたセキュリティー問題の差異が示されます。

このタスクについて

ベース・スキャンおよびターゲット・スキャンを選択すると、AppScan が 2 つの結果を比較し、セキュリティーの状況が 2 つのスキャンの間でどのように改善されたか、あるいはどのように悪化したかを確認できます。

現在ロードしているスキャンと保存してあるスキャンを比較したり、保存してある 2 つのスキャンを比較したりできます。

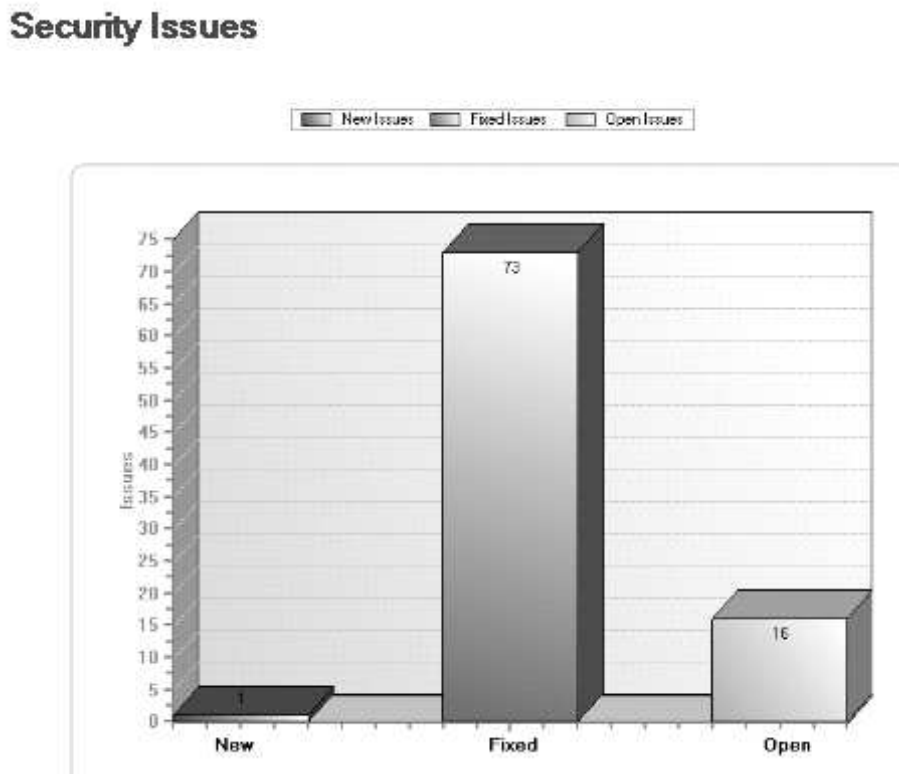
スキャンの比較では、以前のスキャンをベース・スキャンとして使用するのが一般的です。差分分析レポートにより、ターゲット・スキャンの結果とベース・スキャンの結果がどのように違うかが分かります。

差分分析レポートは次のセクションで構成されています。

セクション・タイトル	出力される情報
一般情報	ベース・スキャンおよびターゲット・スキャンの名前と位置をリスト。
説明	スキャンに含まれる情報の説明。
ホストごとの問題	各スキャンで検出された、重大度が高、中、低、情報の各問題数、および合計問題数を表形式で表示。
アプリケーションの URL	(ある場合) 新規/削除済み/残りの URL の数を示す棒グラフと、各タイプの全リスト。

セクション・タイトル	出力される情報
セキュリティー問題	(ある場合) 新規/解決済み/残りのセキュリティー問題の棒グラフ、両スキャンの重大度 (高/中/低/情報) の分布を示す棒グラフ、すべての新規/解決済み/残りの問題の全リスト。

次の図は、差分分析レポートのサンプルです。



手順

1. 「ツール」 > 「レポート」 > 「差分分析」をクリックします。
2. ベース・スキャンを選択します (通常は、比較する 2 つのスキャンのうち古い方)。「ベース・スキャン」エリアで、次のいずれかを実行します。
   - 「**Current**スキャン」ラジオ・ボタンをクリック
   - 「保存済みスキャン」ラジオ・ボタンをクリックし、保存済みのスキャン・ファイルの位置を参照
3. ターゲット・スキャンを選択します (通常は、比較する 2 つのスキャンのうち新しい方)。「ターゲット・スキャン」エリアで、次のいずれかを実行します。
   - 「**Current**スキャン」ラジオ・ボタンをクリック
   - 「保存済みスキャン」ラジオ・ボタンをクリックし、保存済みのスキャン・ファイルの位置を参照
4. 「レポート・コンテンツ」エリアで、レポートで比較する情報のタイプのいずれかまたは両方のチェック・ボックスを選択します。
   - アプリケーションの **URL**
   - セキュリティー問題
5. レポートの外観を制御するには、「レイアウト」タブ (247 ページの『レポート・レイアウトの構成』を参照) を開きます。

6. 「プレビュー」をクリックしてレポートを作成し、AppScan で表示するか、「レポートの保存」をクリックしてレポートを作成し、ファイルに保存します。

テンプレートに基づくレポート

「レポート作成」ダイアログ・ボックスの「テンプレートに基づく」タブでは、ユーザーが必要とするデータのみを指定して、ユーザーが定義する文書フォーマット設定で、Microsoft Word DOC および DOCX 形式のレポートを作成できます。

AppScan には、サンプル・テンプレートがいくつか用意されています。サンプル・テンプレートは以下の用途に使用できます。

- レポートの作成 (編集は不要)
- ユーザー独自のカスタム・レポート・テンプレート作成のベースとして
- ユーザー独自のレポート・テンプレートの作成方法を理解するツールとして

ダイアログ・ボックスには、以下の 2 つのペインがあります。

- 左側のペインに、現在選択可能なテンプレートがリストされます。AppScan が提供するサンプル・テンプレートは文字が斜体で表示され、末尾に「(サンプル)」という文字が付きます。また、ユーザーが作成したテンプレートは、通常の (斜体ではない) 文字で表示されます。
- 右側のペインには、すぐに必要なテンプレートを識別するのに役立つ編集可能な「プレビュー・イメージ」が表示されます (次の表を参照)。

ボタンまたはリンク	クリックで実行される機能
インポート	Word のレポート・テンプレートを、左側のペインのリストにインポートします (ユーザーが以前にカスタマイズしたテンプレートなど)。インポートされたテンプレートは次の場所に保存されます。マイドキュメント **>** **AppScan** **>** レポート・テンプレート **>** **Word** 詳細については、 274 ページの『カスタム・テンプレートのインポート』 を参照してください。
エクスポート	リスト上のテンプレートを別の場所にエクスポートします (編集のためなど)。
削除	テンプレートをリストから削除します。これはテンプレートを削除しませんが、フォルダーに移動します。マイドキュメント **>** **AppScan** **>** レポート・テンプレート **>** **Word** **>** 削除済み
MS Word で編集 (Edit in MS Word)	選択したテンプレートを MS Word で開き、内容とレイアウトを編集します。 詳細については、 270 ページの『カスタム・テンプレートのチュートリアル』 を参照してください。
フィールド参照を表示	Word のレポート・テンプレートの作成に使用する、フィールド参照の HTML リストを開きます。
レポート・プレビュー・イメージの選択	右側のペインでテンプレートを表すイメージを参照し、選択します (左側のペインでテンプレートを選択した場合)。
デフォルト・イメージへの復帰 (Revert to Default Image)	選択したテンプレートのデフォルト・イメージ (ブランク・ページ) を復元します。

ボタンまたはリンク	クリックで実行される機能
プレビュー	テンプレート・ペインで選択したテンプレートを使って、現在のスキャン結果のレポートを生成し、表示します。 MS Word が開くので、必要に応じて内容やレイアウトを編集します。AppScan が作成するのは一時ファイルのみです。保存する必要がある場合は、Word 上で保存してください。
レポートの保存	テンプレート・ペインで選択したテンプレートを使って、(MS Word を開いてレポートの内容を表示せずに) 現在のスキャン結果のレポートを生成し、保存します。 名前とファイルの保存場所を指定するように AppScan が求めてきます。ファイルが保存されると、内容を確認できるよう、そのファイルが開きます。

以下も参照してください。

『カスタム・レポート・テンプレートの作成』

270 ページの『カスタム・テンプレートのチュートリアル』

274 ページの『カスタム・テンプレートのインポート』

248 ページの『部分レポートの作成』

カスタム・レポート・テンプレートの作成

MS Word でフィールド・コードを使用して、独自のカスタム・レポートを定義して生成することができます。

「マージ・フィールド」の概要

AppScan マージ・フィールドは、次の 2 つのカテゴリーに分かれています。

- リピーター **(**またはループ**):** 開始タグと終了タグで構成されています。これそのものはデータを作成しませんが、開始タグと終了タグの間にあるプレーン・フィールドを「ループ」させ、そのグループに対応するデータを取得します。

  例: `<<AS:IssueTypeRepeaterStart>> <<AS:IssueTypeRepeaterEnd>>`

  このリピーターは、スキャン結果内のすべての IssueType をループします。
- プレーン・フィールド**:** 単一のフィールドで構成され、実際のデータを作成します。 (プレーン・フィールドは必ずしもリピーター内に配置する必要はありませんが、別のプレーン・フィールドを「子」として持つことはできません)。

  例: `<<AS:IssueTypeName>>`

  このフィールドは、スキャンで検出されたすべての問題の名前を表しています。

適切なループの開始タグと終了タグの間にプレーン・フィールドを挿入すると、レポートを作成できます。上記の 2 つの例を次のように使用すれば、スキャンで検出されたすべての IssueType のレポートを作成できます。

```
<<AS:IssueTypeRepeaterStart>>  <<AS:IssueTypeName>> <<AS:IssueTypeRepeaterEnd>>
```

これが実際にどう機能するかを理解するために、『カスタム・テンプレートのチュートリアル』下記のを参照してください。

注: 有効なマージ・フィールドの完全なリストは、「ツール」>「レポート」>「テンプレートに基づく」>「フィールド参照を表示」をクリックして開くことができます。

カスタム・テンプレートのチュートリアル

このセクションでは、簡単なカスタム・テンプレートを作成する方法について説明します。

このタスクについて

このセクションでは簡単なカスタム・テンプレートを作成します。このテンプレートは、スキャン中に検出されたすべての問題に対する修復タスクの表を生成するためのものです。テンプレート出力は、以下の項目から構成されます。ただし、当然ながら実際のデータは、レポートの生成時に使用するスキャンによって変わります。

インデックス	名前	件数	優先順位
1/2	RemediationTaskA	4	高
2/2	RemediationTaskB	2	高
1/3	RemediationTaskC	5	中
2/3	RemediationTaskD	2	中
3/3	RemediationTaskE	7	中
2/2	RemediationTaskF	3	低

優先度が「高」のタスクが最初にリストされ、その後に優先度が「中」のタスクと「低」のタスクがリストされます。タスクごとに、タスクの索引 (1/N など)、名前、数 (タスクに適用される問題の数)、および優先度が表に表示されます。

注: 本チュートリアルは、フィールド・コードの基本を理解していることを前提にしています。フィールド・コードについて詳しくは、MS Word の資料を参照してください。

注: 有効なマージ・フィールドの完全なリストは、「ツール」>「レポート」>「テンプレートに基づく」>「フィールド参照を表示」をクリックして開くことができます。

手順

1. 「ツール」>「レポート」>「テンプレートに基づく」>「フィールド参照を表示」をクリックして、有効なマージ・フィールドのリストを開きます。これは、フィールド名をコピーする参照元として必要になります。
2. MS Word 文書を開き、見出し「修復タスク」を入力して保存します。
3. 表見出しの作成: 4 列 × 1 行の表を作成し、見出しに「索引」、「名前」、「数」、および「優先度」を入力します。
4. 次のように、表内に「高」優先度の項目を生成するフィールドを追加します。
   a. 「フィールド参照」表から、コード `AS:RemediationTypeRepeaterStart<Priority=High>` をコピーします。
   b. Word 文書で、ヘッダー・テーブルの後にカーソルを移動します。

c. 文書内にマージ・フィールドをフィールド として貼り付けます(MS Word 2003:「挿入」 > 「フィールド」 > 「マージ・フィールド」 > 「フィールド名」フィールド(MS Word 2010:「挿入」 > 「クイックパーツ」 > 「フィールド」 > 「マージ・フィールド」 > 「フィールド名)。

次の形式で文書内にマージ・フィールドが作成されます。

```
{MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=High>\*  MERGEFORMAT}
```

注: デフォルトで Word は、(長すぎるために) 関連情報を省略した短縮形式でタグを表示します。完全なタグ名を確認するには、**[Alt]** + **[F9]** (フィールド・コードのオン/オフの切り替え) をクリックして、「フィールド・コードを表示」します。

d. 「入力」をクリックし、4 列 × 1 行の別の表を作成します。この表には、後ですべての行に「高」優先度タスクが入ります。

e. 表の後に、マージ・フィールド AS:RemediationTypeRepeaterEnd を追加します。

これは、次のように表示されます。

```
{MERGEFIELD AS:RemediationTypeRepeaterEnd\*  MERGEFORMAT}
```

これで、「高」優先度の修復タスクをリストする文書のセクションの最初と最後のマージ・フィールドが入力されました。この 2 つのフィールドによって「ループ」が形成されます。このループによって、その間に挿入されたフィールドを基にしてリストが作成されます。ここで、上記で追加した表内の 4 つの列のコンテンツ を作成する 4 つのフィールドに入力することができます。

f. 左側の列に、マージ・フィールド AS:RemediationTypeRepeaterIndex を追加します。この操作により、このセクションの各 n タスクに対するカウンター(1/n、2/nといった形式)が作成されます。

g. 2 列目に RemediationTypeName のマージ・フィールドを追加します。

h. 3 列目に RemediationTypeName のマージ・フィールドを追加します。

i. 4 列目に、文字「高」を入力します。

これで、表の「高」優先度セクションが完了しました。これで、スキャン結果で複数行のデータ (「高」優先度の修復タスクごとに 1 行) が生成されます。この時点で、文書は次のように見えるはずです。

Index	Name	Count	Priority
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=High> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	High
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			

5. 優先度が「中」と「低」のタスクについて、ステップ 4 を繰り返します (「優先度」列に、それぞれ「中」と「低」を入力)。表の各行 (「高」、「中」、「低」) について、次の図に示すように、行の前に開始マージ・フィールド、行の後ろに終了マージ・フィールドがあることを確認します。

注: フィールドの 3 つの行の内容は同じであるため、優先度が「高」の行を、優先度が「中」および「低」のタスクの開始タグと終了タグの間にコピー・アンド・ペーストして、単純に「優先度」列のテキストを変更することができます。

注: 「名前」列にはテキスト・ストリングが出力され、「索引」、「数」、「優先度」の各列には数字または短い単語のみが出力されます。そのことを念頭におき、必要に応じて列幅を調整します。

Index	Name	Count	Priority
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=High> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	High
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=Medium> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	Medium
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterStart<Priority=Low> * MERGEFORMAT }			
{ MERGEFIELD AS:RemediationTypeRepeaterIndex * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeName * MERGEFORMAT }	{ MERGEFIELD AS:RemediationTypeCount * MERGEFORMAT }	Low
{ MERGEFIELD AS:RemediationTypeRepeaterEnd * MERGEFORMAT }			

6. 説明文を追加し、必要に応じて文書の残りの部分に書式設定を適用します。
7. ファイルを保存します。
8. このテンプレートを使用してレポートを作成するには、を参照してください。 274 ページの『カスタム・テンプレートのインポート』

タグ階層

AppScan のタグを使ってレポートを作成する際、タグを別のタグの「中」に配置したい場合があります。例えば、各「問題のタイプ」に個別のセクション、各セクション内に問題のリスト、各問題にバリアントのリストが必要になることがあります。これを実現するには、次の図のように、「親」の開始タグと終了タグの間に「子」の開始タグと終了タグを配置します。

```
«AS:IssueTypeRepeaterStart<Severity=High>»
«AS:IssueTypeRepeaterIndex»

    «AS:IssueRepeaterStart»
    «AS:IssueRepeaterIndex»

        «AS:VariantRepeaterStart<Limit=1>»
        «AS:VariantRepeaterIndex»
        «AS:VariantRepeaterEnd»

    «AS:IssueRepeaterEnd»

«AS:IssueTypeRepeaterEnd»
```

次のリピーター (ループ) 階層が可能です。

- 問題のタイプ > 問題 > バリアント
- 修復タイプ > 修復
- 脆弱な URL > 問題のタイプ > 問題 > バリアント
- 修復 > 問題のタイプ > 問題 > バリアント

リピーターは単独、またはこれらの階層のいずれかの中で使用します。これら以外の階層内でリピーターを使用すると、レポートを作成したときにエラーになることがあります。

以下も参照してください。

『リピーターとフィールド』

リピーターとフィールド

各リピーター (ループ) 内にはプレーン・フィールドが 1 つ以上必要です。このフィールドがループへのデータ入力になります 。(例えば、バリアントのループ内に VariantDifference フィールドを配置します。このフィールドは、ループ内のバリアントと各バリアントのオリジナルとの差を表示します)。 各リピーター内には、デフォルトでインデックス・フィールドが追加されます。ただし、このフィールドは削除が可能で、別のフィールドを追加することもできます (チュートリアル参照)。

リピーターとフィールドの例:

```
<<AS:IssueTypeRepeaterStart>>       [Start looping through issue types]

  <<AS:IssueTypeRepeaterIndex>>     [For each type list index (e.g. 3/24) and name]
  <<AS:IssueTypeName>>

  <<AS:IssueRepeaterStart>>         [Start looping through individual issues]

    <<AS:IssueRepeaterIndex>>       [For each issue list index (e.g. 3/24)]

    <<AS:VariantID>>                [For each issue list ID and variants]
    <<AS:VariantTestRequest>>

  <<AS:IssueRepeaterEnd>>           [End issue repeater]

<<AS:IssueTypeRepeaterEnd>>         [End issue type repeater]
```

フィールド・フィルター

このタスクについて

一部のマージ・フィールドには、フィルターが含まれます。例えば、VariantRepeater 制限を使用して、問題ごとに組み込むバリアント数を設定することができます。

注**:** VariantScreenShot フィールドでは、フィルターはパーセント単位 (50%) で目盛り (「Scale=50」) を定義します。この目盛りは、最大 100 (フルサイズ) までのいずれかの整数値に変更できます。

手順

1. フィールドを選択します。

   ```
   <<AS:VariantRepeaterStart<Limit=1> >>
   ```

2. フィールド名全体を表示するには、**[Alt]+F9** をクリックするか、フィールドを右クリックし、メニューから「フィールド・コードの切り替え **(Toggle Field Codes)**」を選択します。

   ```
   {MERGEFIELD AS:VariantRepeaterStart<Limit=1>\*MERGEFORMAT}
   ```

3. 不等号括弧の中のフィルターを更新します。

   ```
   {MERGEFIELD AS:VariantRepeaterStart<Limit=4>\*MERGEFORMAT}
   ```

4. フィールド名を短縮形式で表示するには、**[Alt]+F9** をクリックするか、フィールドを右クリックし、メニューから「フィールド・コードの切り替え **(Toggle Field Codes)**」を選択します。

```
<<AS:VariantRepeaterStart<Limit=4> >>
```

カスタム・テンプレートのインポート

このタスクについて

カスタム・テンプレートを作成して保存したら (270 ページの『カスタム・テンプレートのチュートリアル』を参照)、「テンプレートに基づくレポート (Template Based Reports)」リストに表示されるリストに追加します。

手順

1. 「レポート」ダイアログ・ボックスの「テンプレートに基づく」ビューで、「インポート」をクリックします。
2. カスタム・テンプレート・ファイルを参照し、「開く」をクリックします。

   テンプレートが左側のペインのリストに追加され、カスタム・レポートの生成に使用できるようになります。

第 11 章 ツール

このセクションでは、IBM SecurityAppScan Standard が提供する追加ツールの使用法を説明します。

「オプション」ダイアログ・ボックス

このセクションでは、AppScan をカスタマイズするために、「オプション」ダイアログ・ボックス (「ツール」>「オプション」) から制御できるオプションについて説明します。

このダイアログ・ボックスで行う変更は、すべてのセッションおよびスキャンにわたって AppScan に適用されます。ダイアログ・ボックスには、5 つのタブがあります。

「スキャン・オプション」タブ

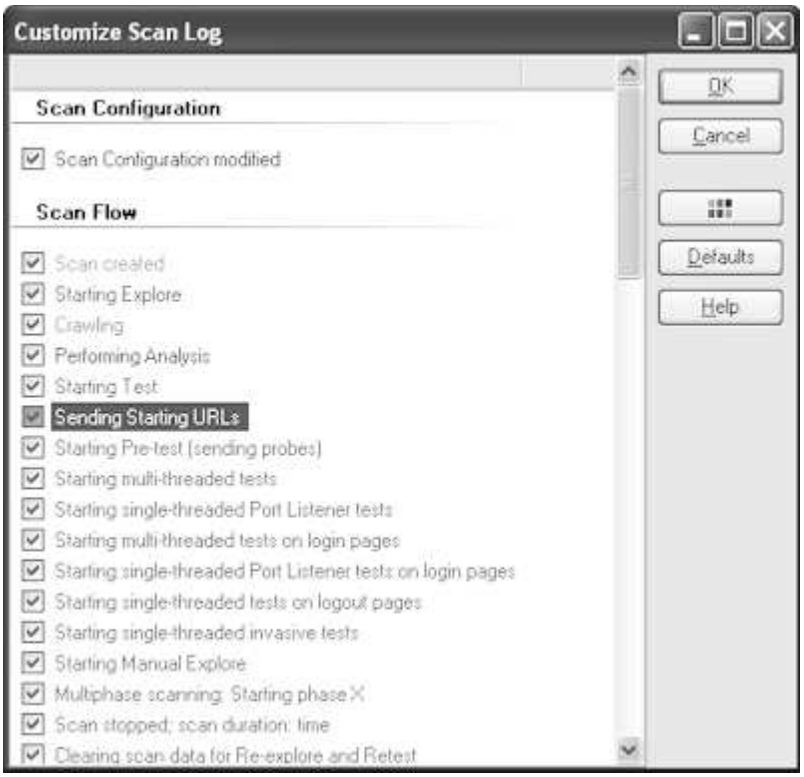
「ツール」 > 「オプション」 > 「スキャン・オプション」タブでは、スキャン中に AppScan がどのように作動するかを制御することができます。

オプション	説明
スキャンの監視:	
スキャン・ログを有効にする	スキャン・ログを有効/無効にしたり、「カスタマイズ」ボタンを使ってログ中に表示する項目やその色を厳密に選択したりできます。 276 ページの『スキャン・ログのカスタマイズ』 を参照してください。
要求/応答のログ記録を有効にする	「要求/応答のログ **(Request/Resonse Log)**」を有効にできます。これは、支援が必要な場合のテクニカル・サポートに役立ちます。ただし、ログをオンにすると、パフォーマンスに影響を与える可能性があります。必要がない限り無効にしてください。
メモリーの消費とディスクの空き領域を監視する	AppScan は、使用可能な仮想および物理メモリーとディスク・スペースを検査し、使用可能なメモリーまたはディスク・スペースが推奨されている量以下になると、警告を送信します。 「メモリーの消費とディスクの空き領域を監視する」チェック・ボックスのチェックを外す (メモリーおよびディスク・スペースのモニターを無効にする) と、AppScan は検査を実行しません。
スキャン未完了の場合に指示	選択すると、スキャンが完了する前に停止した場合に、「結果リスト」の左下隅に `Scan Incomplete` と表示されて、結果が部分的なものに過ぎないことに注意を促します。
スキャン中に自動的に保存	スキャンのファイル (.scan) を、実行中に保存します。 間隔 **(分):**保存する間隔を分数で入力するか、またはスライド・バーを使用して間隔を変更します。
通信:	
TLS/SSL サポート	ご使用のアプリケーションが、クライアントとの通信にセキュア・プロトコルを使用している場合、適切なプロトコルをサポートするように AppScan を構成します。オプションは、TLS 1、1.1、1.2、および SSL 2 です。このオプションを変更した場合、AppScan を再始動する必要があります。
HTTP バージョン	サイトの HTTP バージョンを選択します。1.0 または 1.1

スキャン・ログのカスタマイズ

スキャン・ログに表示される項目とその色を制御できます。

319 ページの『スキャン・ログ』 は、現在のスキャン中に AppScan が実行するアクションをリストします。「スキャン・ログのカスタマイズ」ダイアログ・ボックス (「ツール」> 「オプション」>「スキャン・オプション」タブ >「カスタマイズ」) には、ログに含めることのできるすべての項目を示すスクロールダウン・リスト、現在それが含まれているかどうかを示すチェック・ボックス、およびログの中でそれが表示される色を示す色付きのテキストが含まれています。



- 項目をスキャン・ログから除外するには、その項目の横にあるチェック・ボックスを選択解除し、スキャン・ログに含めるには、チェック・ボックスを選択します。
- スキャン・ログに表示される項目の色を変更するには、次の手順を実行します。項目を選択し、

   をクリックして開いたパレットから色を選び、「**OK**」をクリックします。
- デフォルトの設定値を復元するには、「既定値」をクリックします。

Windows 10 で MS Edge 用のループバックを有効にする

Windows 10 OS で外部ブラウザーとして Edge を使用する場合、特別な構成が必要になることがあります。

MS Windows 10 では、AppScan を介して Edge からアプリケーションに要求が送信されることを防ぐ隔離技術 (「AppContainer」) が使用されています。隔離は必ずしも実施されるとは限りませんが、外部ブラウザーとして構成された Edge を使用してスキャンする前に、ループバックを使用可能にすることをお勧めします。

ループバックを有効にするための方法は、Microsoft のトラブルシューティングのページ で参照可能です。https://msdn.microsoft.com/en-us/library/windows/apps/Hh780593.aspx

- Edge 用にループバックを有効にするには、以下のコマンドを使用します。

  ```
  CheckNetIsolation LoopbackExempt -a -n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
  ```

- Edge 用にループバックを無効にするには、以下のコマンドを使用します。

  ```
  CheckNetIsolation.exe LoopbackExempt –d –n="Microsoft.MicrosoftEdge_8wekyb3d8bbwe"
  ```

注: 詳しくは、を参照してください。 https://blogs.msdn.microsoft.com/fiddler/2011/12/10/revisiting-fiddler-and-win8-immersive-applications/

「設定」タブ

「ツール」 > 「オプション」 > 「設定」タブでは、AppScan ファイル、GUI に表示される推奨される修正、およびようこそ画面に対するさまざまな制御が提供されます。

オプション	説明
起動時に「AppScan へようこそ」画面を表示	AppScan が起動する時に、ようこそ画面が表示されます。この画面からスキャンの構成やロードに、素早くアクセスできます。 ようこそ画面の機能を使うよりも、それを閉じることが多い場合は、このチェック・ボックスのチェックを外して、ようこそ画面が開かないようにできます。
起動時に更新を確認	AppScan の起動時に、更新されたテスト、セキュリティー問題、および修正を確認します。この確認を無効にするには、このチェック・ボックスのチェックを外します。必要であればいつでも、「ヘルプ」 > 「更新の確認」で更新を取得できます。
セキュリティー更新を自動的にインストール	このチェック・ボックスが選択されると、ユーザーの介入なしに、作業中に更新がインストールされます。
誤検出を報告:ファイルを暗号化	この設定は、 235 ページの『誤検出のテスト結果を報告』 に適用されます。AppScan は、選択された zip 済みバリアント情報ファイルを、デフォルトの E メール・クライアントで新規ポストに添付する前に、暗号化します。 送信する E メールの宛先が AppScan サポート・チーム以外であれば、このチェック・ボックスを選択解除してください。
スキャン前にスキャン・エキスパートを実行する	(デフォルトでは選択済み) 選択されると、スキャン・エキスパートはフル・スキャン (探査およびテスト) を実行するたびに自動的に実行されますが、「探査のみ」または「テストのみ」の場合は実行されません。
アドバイザリー研修ビデオを含める	アドバイザリーの中には、アドバイザリーを表示する際に見ることができるように「アドバイザリー」タブに組み込むことのできる、短い研修ビデオが使用可能なものもあります。ファイル・サイズを削減する必要のある場合は選択解除してください。
推奨される修正の設定	ご使用のアプリケーションが、リスト表示されている環境の 1 つ以上を使用しない場合、それらの環境に固有の、推奨される修正を見る必要はありません。 ご使用のアプリケーションに関係のない環境 (.NET/Java EE/PHP) のチェック・ボックスのチェックをすべて外してください。
記録および表示するブラウザー	手動で探査するときに開始 URL の表示および参照に使用するデフォルトのブラウザーを選択します。 2 つのラジオ・ボタンのいずれかを選択した後、ドロップダウン・リストからブラウザーを選択します。 • 組み込みブラウザーの使用: このオプションを選択した場合、組み込みの AppScan IE ブラウザーと AppScan Chromium ブラウザーのいずれかを選択できます。 • 外部ブラウザーの使用: このオプションを選択した場合、お使いのマシンにインストールされているいずれかのサポート対象ブラウザーを選択できます。

「記録プロキシー」タブ

このタブを使用して、AppScan を外部ブラウザーのプロキシーとして機能するように構成したり、リモート・デバイス (携帯電話など) あるいはローカル・アプリケーション (シミュレーターやエミュレーターなど) を使用して非 SOAP Web サービスを手動で探査するために AppScan を構成したりします。

オプション	説明
プロキシー・ポート	AppScan が使用するポートを指定します。AppScan をプロキシー・サーバーとして使用する場合、外部ブラウザーまたはモバイル・デバイスがこのポートを使用するように構成する必要があります。 チェック・ボックスを使用して、AppScan が使用可能なポートを自動的に選択するか、ユーザーがポートを選択するかを選択します。ポートが自動的に選択された場合、そのポートがセッション間で変更され、モバイル・デバイスの再構成が必要になる場合があります。
外部接続	この設定は、外部ドメインが受け入れる接続を決定します。 すべて拒否 (デフォルト) すべての外部 IP から試行された接続が拒否されます。この設定は、AppScan と同じマシン上のアプリケーションを使用して探査を行う場合にのみ使用します。 ホワイトリストのみを受け入れる ホワイトリストに表示された外部 IP からの接続は受け入れられます。その他はすべて拒否されます。 ホワイトリストを受け入れ、その他の場合はプロンプトを表示する ホワイトリストに表示された外部 IP からの接続は自動的に受け入れられます。その他の場合は、AppScan ユーザーにプロンプトが表示され、ホワイトリストに新規 IP を追加するオプションが示されます。プロンプトは、外部トラフィック・レコーダーが開いている場合にのみ表示されるので、注意してください。
ホワイトリスト	ここにリストされた IP からの接続は自動的に受け入れられます。 リストに新規 IP を追加するには、  をクリックし、オプションを選択します。 • リストに 1 つの IP を追加するには、IP および任意でその説明を入力します。 **ヒント:** リモート・デバイスを使用するが、その IP アドレスが不明である場合、あるいは IP アドレスが頻繁に変更される場合は、「ホワイトリストおよびその他の場合はプロンプト」を選択します。デバイスが新規 IP を使用して初めて接続したときに、ポップアップが表示され、その IP をホワイトリストに追加するためのオプションが提示されます。 • IP アドレスの範囲 を追加するには、IPv4 アドレスとサブネット・マスク、または IPv6 アドレスとサブネット接頭部の長さ、および任意でその説明を追加します。

オプション	説明
AppScan SSL 証明書	サーバーが HTTPS を使用する場合、Web サービスとマニュアル探査に使用するデバイスの間のトラフィックを記録するためには AppScan がプロキシーとして機能する必要があるため、Web サービスの証明書ではなく SSL 証明書がデバイスに送信されます。ブラウザーが認識できない証明書を受信すると、通常、ユーザーに対してポップアップで警告が発行されますが、モバイル・デバイスの場合、通常は要求が無視されるだけです。そのため、要求を送信するデバイスで AppScan 証明書が受け入れられない限り、アプリケーションを探査することはできません。 追加　AppScan SSL 証明書をこのマシン上のルート証明書に追加します。 Web サービスへの要求の送信を許可するには、これを行う必要があります。AppScan 証明書がルート証明書に追加され、Web サービスからシミュレーターへの要求は拒否されません。 **注:** 証明書を追加した後、ボタンは「削除」に変わります。このボタンを使用して、AppScan マシンから証明書を削除することができます。 エクスポート このマシンに現在インストールされている AppScan SSL 証明書を Zip ファイルとして保存し、別のデバイスのルート証明書にその SSL 証明書を手動で追加できるようにします。ほとんどの場合、デバイスから証明書を直接インポートすることができるため、通常はこれを実行する必要はありません。 1. AppScan で「スキャン」 > 「マニュアル探査」 > 「外部デバイスの使用」をクリックします。 外部トラフィック・レコーダーが開き、状況「着信接続を待機中」が表示されます。 **重要:** これを開いたまま次のサブステップに進みます。 2. モバイル・デバイスで `http://appscan` をブラウズします。 3. AppScan でご使用のデバイスからの着信接続の許可を求めるプロンプトが表示された場合は、「**OK**」をクリックします。 デバイスがそのプロキシーとして AppScan に正常に接続されると、デバイス上で接続、IP、およびポートを確認するメッセージが表示されます。AppScan マシンに証明書がインストールされている場合、その証明書をデバイスにインストールするためのボタンも表示されます。 **注:** ボタンがグレー表示されている場合、証明書は AppScan マシンにインストールされていません。 **注:** デバイスのドメインおよび要求は、外付けトラフィック・レコーダーのリストに表示されます。 4. モバイル・デバイス上で、「**AppScan SSL** 証明書のインストール」をタップします。 証明書がインストールされます。 **注:** この手順の後、テストを行っているアプリケーションにデバイスがアクセスできない場合、証明書を (リモート・デバイスまたはアプリケーションに) 手動でインストールする必要があります。 a. AppScan で「ツール」 > 「オプション」 > 「記録プロキシー」を開きます。 b. 「エクスポート」をクリックし、証明書を Zip ファイルとして保存します。 c. デバイスまたはアプリケーションにルート証明書として証明書をインストールします。 5. 完了したら、外部トラフィック・レコーダーで「キャンセル」をクリックして閉じます。 **注:** このオプションは、証明書がこの マシンのルート証明書に既に追加されてい

詳細については、 157 ページの『記録プロキシーとして AppScan を使用』を参照してください。

「全般」タブ

「ツール」 > 「オプション」 > 「全般」タブでは、AppScan がどのように問題に優先順位を付け、更新を取得し、ダイアログ・ボックスを表示するかを制御するためのオプションが提供されます。

オプション	説明	
ファイルの場所	AppScan は、使用中にさまざまなファイルをディスクに書き込みます。ファイル・タイプの右にある「参照」ボタンをクリックして別の場所を参照することによって、これらのファイルが保存される場所を変更できます。	
	ユーザー・ファイル	*.scan (スキャン)、*.exd (探査データ)、*.xml (レポート、エクスポート)、*.scant (スキャン・テンプレート)、*.asreg (レポート・テンプレート)、*.aspol (テスト・ポリシー) ....\My Documents\AppScan
	ログ・ファイル	*.log (ログ)、*.lic (ライセンス)、*.dmp (メモリー・ダンプ)、*.css (サポート情報パッケージ) [AppScan Standard インストール・フォルダー]\Logs
	カスタム・アドバイザリー	*.xml (ユーザー作成のアドバイザリー・ファイル) ...\My Documents\AppScan\Advisories
	ノイズ分類ファイル	*.xml [AppScan Standard インストール・フォルダー]\IssueManagement (詳しくは、 221 ページの『問題の状態:「オープン」または「ノイズ」』を参照してください。) [-] ボタンをクリックすると、ノイズ分類ファイルが削除され、デフォルトのノイズ分類を復元します。
ログ・ファイルのサイズ	ログ・ファイルの最大サイズを MB 単位で設定します。 この制限に達すると、ファイルはバックアップとして保存され、新規ログ・ファイルが開きます。(次回バックアップが保存されると、以前のバックアップは削除されます。) ハード・ディスクのスペースに制限がある場合、AppScan ログ・ファイルのサイズに制限を設けることもできます。	
オペレーティング・システム優先度レベル	デフォルトでは、AppScan は、実行中のアプリケーションに共通して **Normal** Priority となっています。他のアプリケーションで、ご使用のコンピューターのリソースをさらに必要とする場合、AppScan の値をより優先度の低い**Idle** に変更することができます。これにより、他のアプリケーションがリソースを必要としない場合にのみ、実行するようにできます。 注意: オペレーティング・システムの優先順位を変更すると、同じシステムで現在実行されている他のアプリケーションのパフォーマンスに大きな影響を与える恐れがあります。	

オプション	説明
ダイアログ抑制の解除	AppScan 警告で「このメッセージを再び表示しない」チェック・ボックスを選択した場合は、「ダイアログ抑制の解除」ボタンをクリックすることにより、メッセージを再び表示するようにリセットすることができます。
履歴を消去	クリックして、すべての履歴リスト (URL 履歴、最近実行したスキャンの履歴、最近使用したテンプレートの履歴、最近検索したストリングの履歴、および最近ユーザーが定義したポリシー) を消去します。
言語の選択	ワークステーション上で、AppScan が複数言語で作動可能な場合、ここでインターフェース言語を選択できます。この設定を変更した後で、変更を反映させるために AppScan を終了して、再オープンするよう 要求されることがあります。

「詳細」タブ

「ツール」 > 「オプション」 > 「詳細」タブでは、詳細設定のデフォルト値を表示および変更することができます。

「詳細」タブには、多数の設定のタイプ (ストリング、DWord、またはブール値) および現行値がリストされており、それらを変更することができます。設定をクリックして選択すると、その設定の簡略説明およびその使用方法がリストの下部に表示されます。

- 特定の設定名を見つけるには、ダイアログの上部にあるフィルター・フィールドにワードまたはフラグメントを入力します。ドリルダウン矢印を使用して、「大文字と小文字を区別」および/または「すべての語に一致」を選択します。
- 設定を変更するには、「値」フィールドをクリックして、新しい値を選択するか入力します。

  デフォルト値から変更されている設定は、太字で表示されます。

  注: 無効な値を入力しようとすると、警告が表示され、その値は受け入れられません。
- 単一の 設定のデフォルト値を復元するには、その設定を右クリックし、「デフォルトの復元」を選択します。
- すべての 設定をデフォルト値に復元するには、ダイアログの下部にある「デフォルトの復元」ボタンをクリックします。

Web サービス構成ウィザード

この拡張機能では、Open API 記述ファイルを使用してスキャンできます。この拡張機能は「ツール」 > 「エクステンション」 > 「Web サービス・ウィザード (オープン API)」から利用でき、デフォルトで有効になっています。

AppScan の拡張機能は、Open API (v2 および v3) 記述ファイル (JSON または YAML) に基づく Web サービスのスキャンをサポートします。以下のステップで、ウィザードのワークフローを示します。ステップ名をクリックすると、そのステップの詳細が表示されます。

注: この拡張機能では、Web サービスのみを探査します。他のリンクは無視されます。

注: API キーを HTTP 照会パラメーターとして使用することはサポートされていません。

表 9. *Web* サービス構成ワークフロー

ステップ	ステップ名	説明
1	記述ファイル	Web サービスを定義する 1 つ以上の Open API 記述ファイルを追加します。
2	ドメイン	記述ファイルで検出されたドメインが、スキャン可能なドメインのリストに追加されます。このステップでは、スキャンしないドメインを削除できます。
3	ログイン管理	Web サービスのログイン手順を定義します。
4	283 ページの『シーケンス』	記述ファイルで作成された要求とそのパラメーターをレビューし、特定の順序で送信する必要のある要求の「シーケンス」を作成します。 **重要:** AppScan が別のオブジェクトの以前の作成に依存するオブジェクトを作成できるようにするには、要求のシーケンスが正しく作成されていることが不可欠です。
5	パラメーター	要求で検出されたすべてのパラメーターをレビューします。追跡するパラメーターと追跡しないパラメーターを選択し、その値を編集できます。
6	完了	構成が完了したら、スキャンを今開始するか、後から開始するかを決定します。

追加タスク:

ウィザードの構成の完了後、可能な追加タスク (サービスによって異なります) が AppScan のメイン「構成」ダイアログ・ボックスでカスタム・ヘッダーを構成する可能性があります。詳しくは、 105 ページの『シーケンス変数』を参照してください。

記述ファイル

Web サービスを定義する 1 つ以上の Open API 記述ファイルを追加します。

ローカル・ファイルを追加することはできません。URL のみです。必要な場合は、記述ファイルを Web サーバーにアップロードして、URL を提供します。

記述ファイルのリストを作成するには:

1. 「URL」フィールドに Open API リンクを入力して、「追加」をクリックします。URL が検証され、リストに追加されます。
2. 必要に応じて、さらに URL を追加します。
3. リストが完成したら、「次へ」をクリックします。リンクが再検証され、次のステップが開きます。

次のステップ: 『ドメイン』

ドメイン

記述ファイルで検出されたすべてのドメインが、スキャン可能なドメインのリストに追加されます。このステップでは、スキャンしないドメインを削除できます。

右ペイン (「含まれたドメイン」) にリストされたドメインがスキャンされます。スキャンしないドメインは左ペイン (「除外されたドメイン」) に移動させる必要があります。

ドメインをスキャンから除外するには:

- ドメインを選択して、左矢印をクリックします。選択されたドメインが「除外されたドメイン」ペインに移動します。

次のステップ**:** 『ログイン管理』

ログイン管理

Web サービスのログイン手順を構成します。

ログインが必要な場合、AppScan がサービスにログインできるように構成する必要があります。

Limitation: API キーを HTTP 照会パラメーターとして使用することはサポートされていません。

以下のいずれかのログイン・ラジオ・ボタンを選択します。

下部でログインを構成
: このオプションを選択すると、ダイアログ・ボックスの下部がアクティブになり、以下を入力できます。

  1. ログイン要求**:** 記述ファイルからの要求のドロップダウン・リストから、ログイン要求を選択します。

     注**:** Web サービスが API キーを使用する許可の制御を実装する場合、ログイン要求は不要であるため、ドロップダウン・リストから「なし」を選択します。
  2. ログイン資格情報**:** ログイン資格情報の値をレビューし、必要に応じて編集します。
  3. カスタム・ヘッダー**:** サービスがカスタム・ヘッダーを使用する場合 (許可ヘッダーでのベアラー認証など)、「編集」をクリックして「カスタム・ヘッダーの追加」ダイアログ・ボックスを開きます。詳しくは、 91 ページの『「カスタム・ヘッダー」タブ』を参照してください。
  4. セッション内検出要求**:** ドロップダウン・リストからセッション内要求を選択します。これは、テスト時にログインしていることを確認するために AppScan によって使用されます。

既存のログイン構成の使用
: スキャン構成に、既に使用可能な有効なログイン・シーケンスが含まれる場合に選択します。

AppScan 構成のログイン・シーケンスの記録 **>** ログイン管理
: 記述ファイルにログイン要求が含まれない場合に選択します。AppScan のメイン「構成」ダイアログ・ボックスを使用し、AppScan の組み込みブラウザーまたは外部デバイスを使用してログインを記録できます。これは主に、ユーザーがユーザー・インターフェースを介してログインしたり、ログイン・プロセスに JavaScript が使用されるような場合です。詳しくは、 52 ページの『「ログイン管理」ビュー』を参照してください。

なし　サービスがログインを必要としない場合に選択します。

次のステップ**:** 『シーケンス』

シーケンス

記述ファイルで作成された要求 (とそのパラメーター) をレビューし、特定の順序で送信する必要のある要求の「シーケンス」を定義します (最初に作成された他のオブジェクトに依存するオブジェクト)。

要求

「要求」タブの左ペインには、定義ファイルから作成されたすべての要求のリストが、それぞれメソッドおよびパスとともに表示されます。表示する要求を選択します。

- 右上のペイン:要求内のパラメーターのリストと、その名前、タイプ、場所、値。「編集」アイコンをクリックして、説明を表示し、値を編集することもできます。パラメーターを追跡し、値の変更を類似するすべてのパラメーターに適用します。

- 右下のペイン:ヘッダーなどを含む未加工の HTTP 要求 (送信されるとおりに)。「送信」ボタンをクリックして要求を送信し、同じペインの下部で応答を確認することができます。
- 右クリック > 「要求を除外する」で、要求をスキャンから除外します。要求は、取り消し線が付けられて表示されます。再び含めるには、もう一度右クリックして、右クリック > 「要求を含める」を使用します。

シーケンス

オブジェクト間の依存関係を表す、適切に作成されたシーケンスは、Web サービスを徹底的にスキャンするための重要なツールです。特定オブジェクトの作成要求が、以前に作成された他のオブジェクトに依存する場合、正しい要求シーケンスを構成する必要があります。

シーケンスを構成するには:

1. 「要求」タブで、シーケンスの最初の要求をクリックして選択します。
2. **Control** キーを押しながら、残りの要求を正しい順序で選択します。その後、Control キーを離します。シーケンスのすべての要求が選択された状態で表示されます。
3. 「名前」フィールドにシーケンスの名前を入力して、「シーケンスの作成」をクリックします。
4. 「シーケンス」タブをクリックすると、以下が表示されます。
   - 左ペイン:構成されたすべてのシーケンス。「有効」チェック・ボックスを選択またはクリアして、各シーケンスをスキャンに対して有効にするか、他のスキャンに取っておくために無効にします。
   - 右上のペイン:選択したシーケンスで記録された URL。上/下の矢印を使用して要求の順序を変更し、「マイナス」ボタンで要求をシーケンスから削除することができます。
   - 右下のペイン:選択したシーケンスで検出された変数のリスト。変数を右クリックして、ダイナミック値を設定できます。詳しくは、 105 ページの『シーケンス変数』を参照してください。

次のステップ: 『パラメーター』

パラメーター

要求で検出されたすべてのパラメーターをレビューします。追跡するパラメーターと追跡しないパラメーターを選択し、その値を編集できます。

このステージでは、アプリケーションの要求で検出されたすべてのパラメーターが 1 つのリストとして表示されるため、複数のパラメーターの値を追跡または変更する際に特に便利です。以下のことが可能です。

- パラメーターをクリックして、個々のパラメーターの値を編集し、ステータスを追跡します。
- デフォルトの一般的な値、ユーザー名およびパスワードを変更します。

  注: 記述ファイルでデフォルトが定義されている場合、ここで変更しない限り、デフォルトが使用されます。フォーム入力構成に定義がある場合、それが記述ファイルで定義されていないパラメーターに使用されます。
- 変更を加えた後、デフォルト値を復元します。

次のステップ: 『完全』

完全

構成が完了したら、スキャンを今開始するか、後から開始するかを決定します。

構成が完了したので、以下を実行できます。

- 自動フル・スキャンを開始
- 自動探査のみを開始 (テスト・ステージに進む前に探査結果をレビューできます)
- 後でスキャンを開始

構成でデフォルト以外のテスト・ポリシーが指定されている場合を除き、デフォルトでは、ウィザードは Web サービス・テスト・ポリシーを適用します。これは、チェック・ボックスを選択またはクリアして変更できます。

スキャン・スケジューラー

スキャンがスケジュールに従って自動的に開始するように設定できます。スキャンのスケジュールは、1 回限りでもルーチンの予定でも構いません。スケジュール済みのスキャンの時刻になると、AppScan は自動的に開かれてスキャンを実行します。

新規スキャンをスケジュールに入れる

このタスクについて

現在のスキャンまたは保存済みスキャンの構成を使用して、スキャンをスケジュールすることができます。スケジュールされたスキャンの名前は、ソース・スキャンの名前に日時が付加されたものになり、ソース・スキャンと同じフォルダーに保存されます。

手順

1. 「ツール」メニューで、「スキャン・スケジューラー」をクリックします。

   「スキャン・スケジューラー」ダイアログ・ボックスが現れ、その時点でスケジュールに入れられているすべてのスキャンがリスト表示されます。
2. 「新規」をクリックします。

   「スケジュール設定」ダイアログ・ボックスが現れます。
3. スケジュールの名前を入力してください。
4. 現在のスキャンをスケジュールに入れるか、保存したスキャン (***.scan** ファイル) のロードをスケジュールに入れるかを決定します。

   現在のスキャンを選択した場合、現在のスキャンが保存されていなければ、スケジューラーがロードできるようにそのスキャンをスキャン・ファイルとして保存することを、AppScan が求めてきます。
5. 繰り返しスケジュール (毎日、毎週、毎月)、または指定した日時に一度だけを選択してください。
6. 最初のスキャンが開始する日時を選択します。
7. オプションとして、スキャンの制限時間を設定できます。「スキャン時間の制限」チェック・ボックスを選択し、分数でスキャンの最大所要時間を入力してください。
8. ドメイン・ネーム、ユーザー名、およびパスワードを入力します。

   これらの認証値によって、そのタスクは指定されたユーザーによって開始されたかのように実行できます。この情報がないと、タスクはまったく実行できません。
9. 「**OK**」をクリックします。

   「スキャン・スケジューラー」ダイアログ・ボックスにスケジュール名が表示されます。

スケジュール済みスキャン構成の編集

手順

1. 「スキャン・スケジューラー」ダイアログ・ボックス (「ツール」 | 「スキャン・スケジューラー」) で、スケジュール済みのスキャンを選択します。
2. 「編集」をクリックします。

   「スケジュール設定」ダイアログ・ボックスが現れます。
3. 必要に応じて詳細を編集します。
4. 「**OK**」をクリックします。

スケジュール済みのスキャンの削除

手順

1. 「スキャン・スケジューラー」ダイアログ・ボックス (「ツール」 > 「スキャン・スケジューラー」) で、スケジュール済みのスキャンを選択します。
2. 「削除」をクリックします。

テスト・ステージのみをスケジュールに入れる

このタスクについて

フル・スキャンは 2 つのステージ (探査およびテスト) から構成されます。探査ステージを毎回実行する必要がなければ、スケジュール済みのスキャンがテスト・ステージのみを実行するように構成できます。これを行うには、*Windows*「コントロール パネル」の「タスク」を使用します。

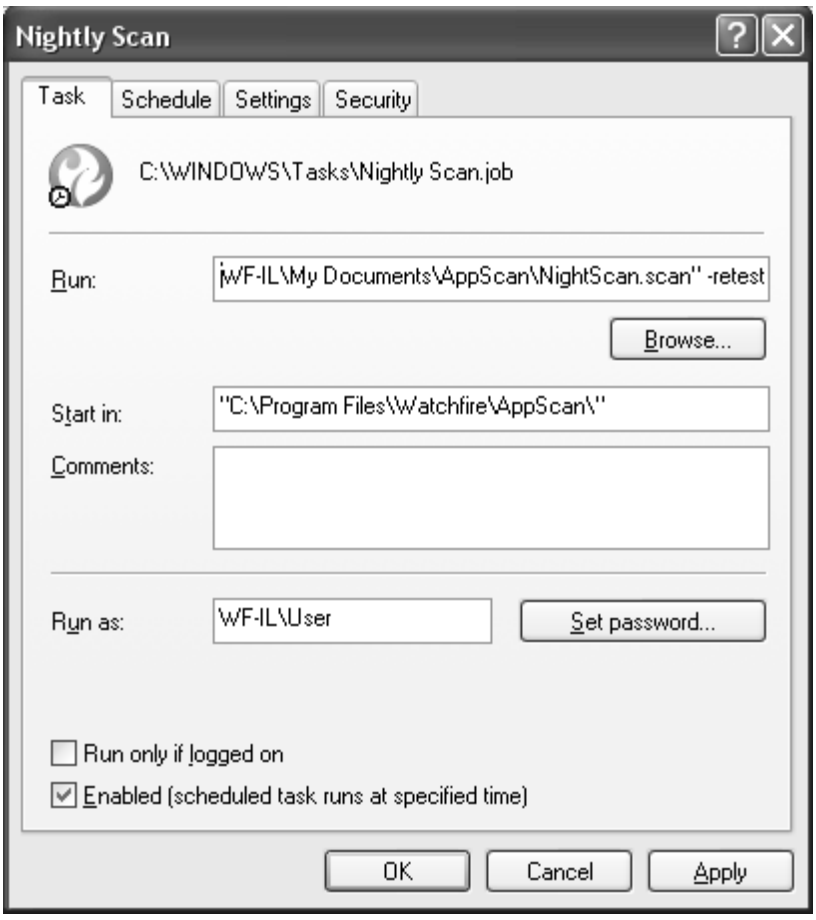
手順

1. AppScan で、 285 ページの『新規スキャンをスケジュールに入れる』 (「ツール」>「スキャン・スケジューラー」>「新規」)。
2. Windows の「スタート」メニューで、「コントロール パネル」>「タスク」をクリックします。

   注**:** *Windows*「コントロール パネル」に「タスク」オプションが表示されない場合、「カテゴリの表示」になっているため一部のオプションが表示されていない可能性があります。必要に応じて、「クラシック表示」に切り替えてください。

   Windows の「タスク」ダイアログ・ボックスが開き、AppScan で作成したタスクがタスクのリストに表示されます。
3. AppScan のスケジュール済みのスキャンを右クリックして、ポップアップ・メニューから「プロパティ」を選択します。

   「スケジュールされたタスクのプロパティ」ダイアログ・ボックスが開きます。



4. 「実行するファイル名」フィールドで、テキスト・ストリングの最後 (最後の引用符の後) に、**[**スペース**][**ハイフン**]retest** と入力します。
5. 「**OK**」をクリックします。

スケジュールされた時刻になると、テスト・ステージのみが実行されます。

スキャンを分割してスケジュールに入れる

このタスクについて

スキャンを実行するための「時間枠」が限られていて (例えば 1 日に、午前 1 時から 4 時までの 3 時間のみ)、スキャンを完了するのにこれより多くの時間がかかる場合、スケジュール済みのスキャンを分割して実行するように構成できます。これを行うには、AppScan に対して、以下のように指示する必要があります。

- 元のファイル名を付けて (名前の一部としてのタイム・スタンプは除く) スキャンを保存する
- 次回のスケジュール済みのスキャンを、前回のスキャンを終えた場所から続行する

*Windows*の「コントロール パネル」の「タスク」を通じてコマンド行パラメーターを追加することで、そのようにできます。

手順

1. AppScan で、 285 ページの『新規スキャンをスケジュールに入れる』 (「ツール」>「スキャン・スケジューラー」>「新規」)。

2. Windows スタート・メニューの「実行」フィールドで、Task Schedulerを入力します。

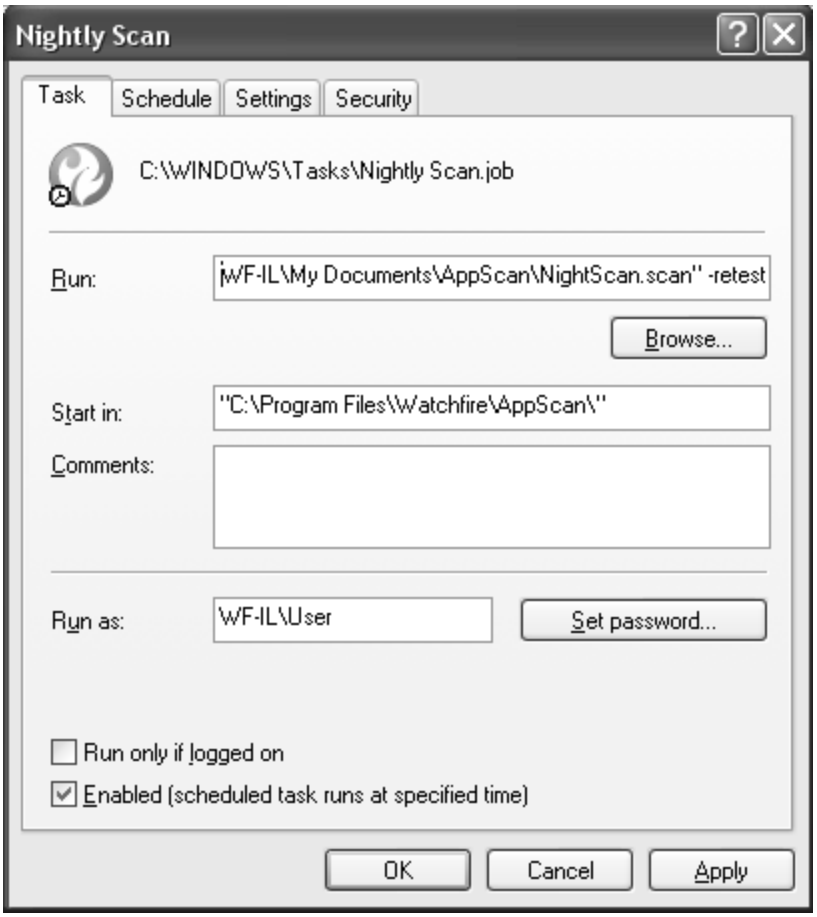
   Windows の「タスク」ダイアログ・ボックスが開き、AppScan で作成したタスクがタスクのリストに表示されます。
3. スケジュールされたスキャンを右クリックし、「プロパティ」を選択します。

   「スケジュールされたタスクのプロパティ」ダイアログ・ボックスが開きます。
4. 「トリガー」タブで、必要に応じてタスクを構成します。詳しくは、Microsoft Windows の資料を参照してください。

スケジュールされたタスクのコマンド行パラメーター

次の表には、*Windows*「コントロール パネル」の「タスク」ダイアログ・ボックスで使用する、使用可能なコマンド行パラメーターが示されています。

パラメーターは「タスク」タブの「実行するファイル名 (Run)」フィールドの主なストリングの後に追加されます。



コマンド行パラメーター	機能
[スペース][数値]	この数値はスケジュール済みのスキャンに対するタイムアウトの分数です。

コマンド行パラメーター	機能
[スペース][ハイフン]retest	スケジュール済みのスキャンが、探査ステージを省いてテスト・ステージから開始するように構成します。 これは、既にそのサイトを探査してあるソース・スキャンを使用して、間隔を置いてサイトを再テストするのに便利です。
[スペース][ハイフン]continue	スケジュール済みのスキャンを、新しく開始せずに、終えた場所から続行するように構成します。 これは、既にそのサイトを探査したソース・スキャンを使用し、間隔を置いてサイトを再テストするのに便利です。 このオプションを使用して分割で スキャンを行う場合、スケジュール済みのスキャンが実行されるたびに元のスキャンを上書きするように、*saveName* スイッチも使用する必要があることに注意してください。 (287 ページの『スキャンを分割してスケジュールに入れる』 を参照してください。)
[スペース][ハイフン]saveName[filename]	スケジュール済みのスキャンを保存するためのファイル名を定義します。*saveName* が定義されていない場合、AppScan はソースのファイル名の後にタイム・スタンプを付けてスケジュール済みのスキャンを保存します。

ユーザー定義テスト

AppScan は、何千ものテストのデータベースを提供しています。ただし、ご使用の Web アプリケーションが固有の問題を抱えている場合や、問題を解決するための独自のアドバイザリーを書き込みたい場合、独自のテストを作成できます。それらのテストは、AppScan のテストのデータベースに保存され、組み込まれます。

各テストは、1 つの特定の問題を対象とします。例えば、あるテストは要求のパスを変更し、別のテストはユーザーの入力を変更して無効であるべき文字を組み込みます。各テストでは、以下の 3 つに関して複数の条件を定義できます。

- フィルター**:** テストを実行するために満たす必要がある条件。
- 修正**:** 要求に対して行われる変更の内容。
- 検証**:** テスト結果が有効な検出であると判定されるために満たす必要がある条件。

ユーザー定義テストを作成および管理するには、以下のようにします。

- 「ツール」**>**「ユーザー定義テスト」をクリックします。

  「ユーザー定義テスト」ダイアログ・ボックスが表示され、定義済みのテストとそのタイプがリストされます。各テストの隣にあるチェック・ボックスは、そのテストが現在スキャンで使用可能かどうかを示します。

オプション	説明
「使用可能」チェック・ボックス	選択/クリアして、現在のスキャンへのテストの組み込み/スキャンからの除外を行います。

オプション	説明
	クリックすると、ユーザー定義テスト、およびそれらの使用可能/クリア状況が UDT ファイルとして、すべてのテストがエクスポートまたは選択されたテストがエクスポートされます。この UDT ファイルは、インポートして別のスキャンで使用することができます。
	クリックすると、以前に保存された UDT ファイルがインポートされます。インポートされたファイル内のテストは、現在のテストのリストに追加されます。
	テスト行 (そのチェック・ボックスではない) を選択し、「編集」 をクリックすると、選択されたテストを編集するためのユーザー定義テスト・ウィザードが開きます。
	クリックすると、選択したテストが削除されます。
	クリックすると、「ユーザー定義テスト」ウィザードが開き、新規テストを作成します。

ユーザー定義テスト・ウィザード

ユーザー定義テスト・ウィザードによって、AppScan が自動的に作成するテストに加えて、AppScan がスキャン時に使用するユーザー定義テストを作成できます。

ようこそ画面で基本的なテスト属性を定義します。

テスト属性

名前	割り当てた名前は、スキャン結果とレポートに表示されます。
説明	この説明は、AppScan 内のユーザー定義テスト・リストにのみ表示されます。
作成者	この属性は、同じ名前のユーザー定義テストを区別してその競合をユーザーに通知するために AppScan によって内部的に使用されます。
重大度	問題に「高」、「中」、「低」、または「通知」の重大度レベルを割り当てます。

終了したら、「次へ」をクリックして、次のステップに進みます。

テスト・タイプ

このステップでは、作成するテストの種類を定義します。この定義は、表示されるウィザード・ステップに影響します。

以降のウィザード・ステップは、選択したテスト・タイプによって異なります。

パスの修正 (インフラストラクチャー)	スキャン中に特定の URL に接続を試みるテストを作成します。
パラメーターおよび Cookie の修正	1 つ以上の Cookie またはパラメーター (あるいはその両方) の値を変更するテストを作成します。
完全要求の修正	以下によって元の要求のパスを変更するテストを作成します。 • 「ファイル名」セクションの設定、前に付加、または追加 • Cookie またはパラメーターの追加、削除、または変更 • 要求本文の上書き

パターン検索 (修正なし)	アプリケーションからのフィルター済みの探査ステージ応答すべて (フィルターを定義することも、すべての 応答を組み込むことも可能) において、検証の条件を検索するテストを作成します。
グローバル検証 (すべての AppScan テストに対して)	アプリケーションからのテスト・ステージ応答すべてにおいて、検証の条件を検索するテストを作成します。 検出された結果は、このユーザー定義のテストに対して脆弱であるとしてリストされます。

終了したら、「次へ」をクリックして、次のステップに進みます。

フィルター

このステップでは、このテストを実行するために満たす必要がある条件を定義します。条件を満たす要求のみがテストされます。

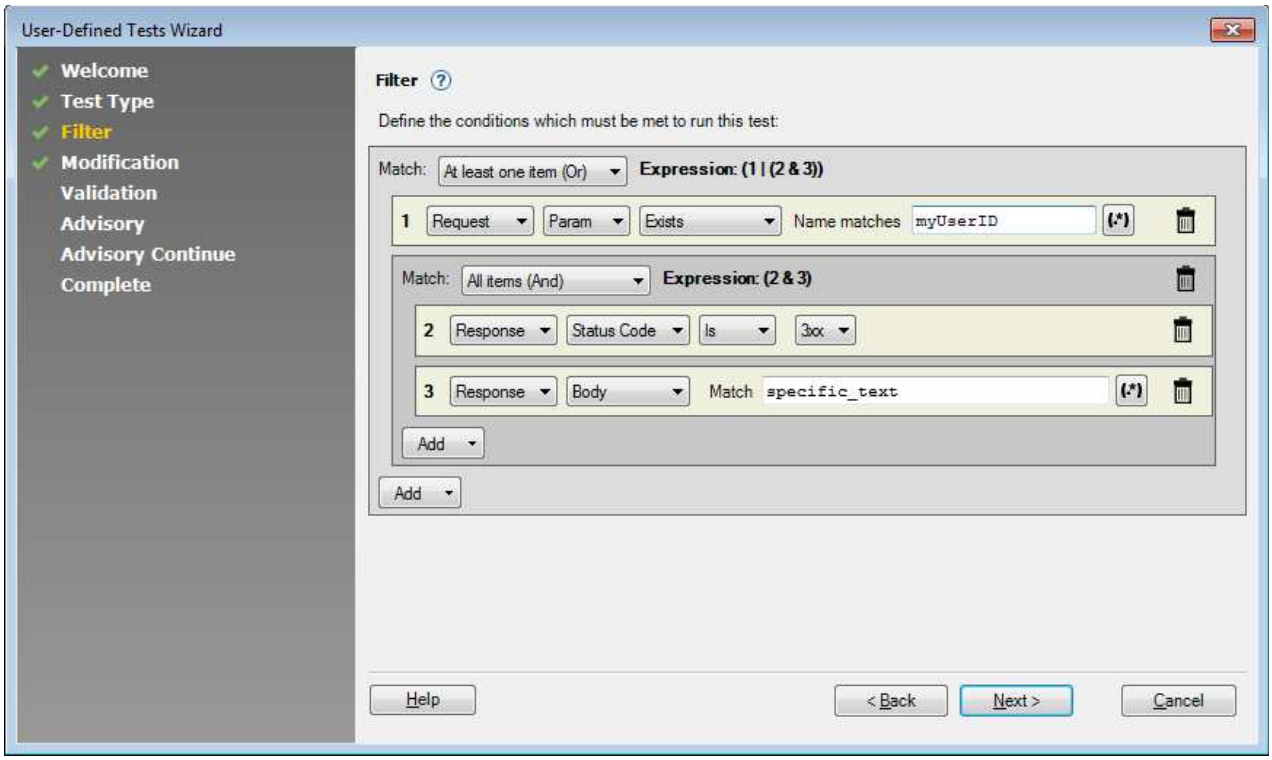
関連する要求に対してのみ にテストを行うように制限するフィルターを定義すると、効率性を大幅に向上できます。

- 「追加」をクリックして、別の「単一」フィルターまたは「グループ」フィルターを追加します。
- 複数の項目を追加する場合、その項目間の論理関係を指定する必要があります(「すべて」、「任意」または「なし」) 。以下の例を参照してください。

終了したら、「次へ」をクリックして、次のステップに進みます。

例

この例では 3 つの条件が追加されています。 新規テストは、条件 1 (myUserID パラメーターを含む要求)、または 条件 2 と 3 の両方 (応答状況コードが 3xx であり、かつ 応答本文に specific_text が含まれている) のいずれかを満たした場合のみ、応答に対して実行されます。



式として表すと、次のようになります。

```
( 1 | (2 & 3 )
```

修正

このステップでは、テスト要求を作成するために、元の要求に加えられる変更を定義します。

元の要求に適用する 1 つ以上の変更を追加して修正を定義し、テスト要求を作成します。

- 「追加」をクリックして、変更を追加します。
- 複数の変更を追加した場合、それらはまとめて 1 つの修正として適用されます。 個別に変更を適用する場合、個別のテストを作成する必要があります。
- 変更にダイナミック値を組み込みたい場合、「値」フィールドの隣の「マクロ・エディター」アイコンをクリックします。

終了したら、「次へ」をクリックして、次のステップに進みます。

マクロ・エディター

マクロ・エディターを使用してダイナミック値 (マクロ) をユーザー定義テストの修正に追加します。

1 つ以上のマクロを含む修正値を追加するには、以下のようにします。

1. 「値」フィールドの隣の「マクロ・エディター」アイコンをクリックします。
2. 必要なプレーン・テキストをテキスト・フィールドに入力します。
3. カーソルを希望する挿入ポイントに移動します。
4. 下のリストからマクロを選択します。
5. 「挿入」をクリックします。

検証

このステップでは、テストが成功したことを示す条件を定義します。

- 「追加」をクリックして、別の「単一」フィルターまたは「グループ」フィルターを追加します。
- 複数の項目を追加する場合、その項目間の論理関係を指定する必要があります(「すべて」、「任意」、または「なし」)。
- ほとんどの場合、テスト要求に対する応答に対して検証が適用されます。それがデフォルトの動作です。 ただし、特定の脆弱性 (格納されたクロスサイト・スクリプティングなど) の場合、別の 要求に対する応答に対して、検証を行う必要があります。その場合、2 番目のラジオ・ボタン (「以下の要求に対する応答でこの検証を実行します」) を選択し、要求を定義します。

  ヒント: 本文を上書きする必要がある場合、または GET や POST を指定する場合など、URL 定義をより細かく制御するには、「要求の編集」をクリックしてください。

終了したら、「次へ」をクリックして、次のステップに進みます。

例

例として、 291 ページの『フィルター』 ステップを参照してください。

アドバイザリー

「アドバイザリー」ステップと「アドバイザリーの続き」ステップでは、スキャン結果とレポートに表示されるアドバイザリーのテキスト・コンテンツを入力します。 すべてのフィールドはオプションです。

技術的な説明	この問題の技術的な説明。
影響を受ける製品	この問題がサード・パーティー製品に影響を及ぼすのであれば、その製品をこちらにリストします。
修復タスク	問題に対処するために必要な一般タスクを記述します。
推奨される修正	この問題の解決策または回避策を指定します。
参考資料と関連リンク	この問題について、詳細情報を提供する参考資料や外部リンクがあればリストします。

終了したら、「次へ」をクリックして、次のステップに進みます。

ウィザードの終了

新規テストの定義が完了したら、「終了」をクリックしてそのテストをリストに加えます。

パワー・ツール

AppScan は 5 つのユーティリティー (パワー・ツール) にアクセスします。各パワー・ツールは、アプリケーションのセキュリティーを管理したり、 AppScan を使用する際に役立つ特定の機能を提供します。

パワー・ツールは within AppScan (**Tools > PowerTools**) または Windows スタート・メニューから個別に開くことができます。

Authentication Tester

Authentication Tester パワー・ツールは、「ブルート・フォース」技法を使用して、Web アプリケーションへのアクセス権を取得するために使用される可能性のあるユーザー名とパスワードの脆弱な組み合わせを見つけるテスト・ユーティリティーです。(ブルート・フォース攻撃は、認証資格情報の推測に使用される自動化された試行錯誤プロセスで、不正ユーザーを正当なユーザーとしてサーバーに認識させる原因になります。)

悪質なユーザーはブルート・フォース技法を使用して、認証された領域へのアクセス権を可能にする資格情報を偶然見つけ出すまで、組み合わせを循環させます。悪質なユーザーはブルート・フォース用のアプリケーションを使用することで、辞書ファイルを使用したり、さらには受け入れ可能な文字セットのあらゆる組み合わせを単純に試行したりすることができます (組み合わせは、サイトで受け入れ可能なユーザー名およびパスワードのフォーマットに依存します)。このような攻撃では、アクセス権の取得に成功するまでに数千から数百万もの間違った組み合わせを生成することがあり、通常は数時間から数週間、またはそれ以上の期間を要します。

Web アプリケーションにおいて破られにくいパスワードを強制的に使用させることで、ブルート・フォース攻撃の実現可能性をかなり低くすることができます。

- Authentication Tester は AppScan から実行できます。これを行うには、「ツール」 > 「パワー・ツール」 > 「**Authentication Tester**」をクリックします。
- Authentication Tester は単独で実行できます。これを行うには Windows の「スタート」メニューで、「すべてのプログラム」 > **[AppScan Standard** がインストールされているフォルダー**]** > 「パワー・ツール」> 「**Authentication Tester**」をクリックします。

認証方式

Authentication Tester のメインウィンドウでは、Web アプリケーションで使用する認証方式を選択します。オプションは以下のとおりです。

- フォーム認証**:** (認証はカスタムの Web ページによって実行されます。)

  『フォーム認証』
- **HTTP** 認証**:** (認証はプロトコルで定義されます。)

  296 ページの『HTTP 認証』

選択した方式によって、利用可能なスキャン・オプションが変わります。

注**:** アプリケーションで両方の タイプの認証を使用する (つまり、通常は HTTP 認証を使用し、特定の管理者向けページではフォーム認証を使用する) 場合、HTTP 認証用の実際のユーザー名およびパスワードを Authentication Tester に提示して、該当するページでフォーム認証をテストできるようにしておく必要があります。(詳細については、 297 ページの『HTTP 認証よりフォーム認証を優先』を参照してください。)

フォーム認証

このタスクについて

「フォーム認証」ラジオ・ボタンを選択した場合、以下の手順を実行します。

手順

1. 『標準ログインの提示』.
2. 295 ページの『アプリケーションのログイン応答の記述』.

標準ログインの提示**:**
このタスクについて

メインウィンドウの「認証方式」セクションで「フォーム認証」を選択した場合、「設定」ボタンが表示されます。これを使用して、Authentication Tester に正しいログイン手順を構成します。

手順

1. 「設定」をクリックします。

   Authentication Tester ブラウザーが開きます。
2. Web アプリケーションのログイン・ページまでブラウズします。
3. 次の資格情報を使用してログイン手順を実行します (ブラウザー・ウィンドウの上部にある資格情報をカット・アンド・ペーストできます)。

ユーザー名:	BruteUsername
パスワード:	BrutePassword

Authentication Tester では、これらの値を使用してサイトへのログイン手順をモデル化する必要があります。テスト段階において、Authentication Tester が「ブルート・フォース」技法によってサイトにアクセスしようとすると、これらのストリングは候補となるユーザー名とパスワードの組み合わせで置換されます。ログイン手順を完成しても、Authentication Tester はこれらの資格情報を使用して実際にログインを試行するのではなく、単にログイン要求を検査するにすぎません。

注意:
「**BruteUsername**」および「**BrutePassword**」というストリングがクライアント側の検査で許可されない場合、**Authentication Tester** で検査するログイン要求は全く作成されません。このような場合、ユーザー名およびパスワードのプレースホルダーにあるストリング値を変更する必要があります。 **299** ページの『「フォーム認証」タブ』を参照してください。

ログイン・プロセスが完了すると、Authentication Tester はログイン要求の「取り込み」を行い、確認メッセージが表示されます。

4. 確認メッセージの「**OK**」をクリックします。

ブラウザーが閉じて、「正常なログインの検出」ウィンドウが開きます。これはログイン応答の記述に使用されます。『アプリケーションのログイン応答の記述』 を参照してください。

アプリケーションのログイン応答の記述:
このタスクについて

「正常なログインの検出」ウィンドウでは、ログイン要求が成功か失敗かを Authentication Tester で認識できるようにします。この情報は、いつ Web アプリケーションが資格情報を有効なものとして受け入れたかを知るために必要です。

正常な応答の一部はデフォルトでリストに表示されますが、使用するアプリケーションに固有の応答をすべて含むにはリストを編集する必要があります。

手順

1. 記述する応答のタイプを以下から選択します。
   - 成功応答: 有効なログイン試行への応答です。
   - エラー応答: 無効なログイン試行への応答です。
2. テキスト・ストリングを入力するか、応答ページの一部のコンテンツに一致する正規表現 (regexp) を入力します。(変数ではなく、静的コンテンツのみに一致させてください。)

   例えば、無効な資格情報によって 「`Username and password do not match`」 という応答を受け取ることが多い場合、この応答を使用して、Authentication Tester にテスト結果を通知することができます。

   ストリングの代わりに正規表現を使用すると、Web アプリケーションの開発段階において、複数の実行に対して Authentication Tester の構成を 1 回で済ませることができます。

   例えば、ログイン成功ページのデザインを、ページ全体に大きく「`Welcome!`」と表記するか、またはホーム・ページの上部に小さい文字列で「`welcome`」と表記するかがまだ最終決定していない場合、「`(?i)welcome`」と入力して、検索語が大/小文字を区別しないように指示することができます。

   ヒント: 正規表現について、およびリテラル・ストリングより多くの意味を示すのに使用できるメタキャラクターについて詳しくは、 296 ページの『メタキャラクターについて』を参照してください。 Authentication Tester で正規表現を使用する前にテストするには、Expression Test PowerTool を試行してください。
3. 「追加」をクリックします。

   正規表現が応答リストに追加されます。

正規表現はいくつでも追加できます。Authentication Tester ではこれらを OR 演算子と一緒に使用します。つまり、1 つ以上の正規表現がサイトのページのコンテンツに一致した場合、そのページは結果ページ (選択した応答タイプに応じて、ログイン成功ページまたはエラー・ページのいずれか) として認識されます。

4. 不要な正規表現をリストから除去するには、正規表現を選択して「削除」をクリックします。
5. 「**OK**」をクリックします。

「正常なログインの検出」ウィンドウが閉じて、メインウィンドウに戻ります。これで、現在の構成を使用してブルート・フォース・テストを実行できます (298 ページの『認証テストの実行』を参照)。

メタキャラクターについて:

メタキャラクターとは、正規表現のコンテキストで非リテラルの特殊な意味を持つ 1 つ以上の文字です。例えば、曲折アクセント記号 (^) は「先頭を検索」を意味するメタキャラクターです。メタキャラクター・パターンではない曲折アクセント記号文字を検索する場合、この文字を「\^」のように円記号で保護 (つまり、エスケープ) する必要があります。

以下の表は、一般的な正規表現のメタキャラクターの例をリストしたものです。

	メタキャラクターの説明	例
\	次の文字を保護します (メタキャラクターとしてではなく文字通りに解釈します)。	\! は感嘆符 (!) を検索します。 \. は文字ではなくピリオド (.) を検索します。
^	文字列の先頭を検索します。	^H は **Home** を検出しますが、**home** または **PHP** は検出しません。
.	改行を除く任意の文字 (文字、数値、記号、空白文字) を検索します。	(.*) は任意の段落を検出します。
( )	パターン・グループを検索します。	(word) は 「In this **word**」を検索します。 ^(Word) は「**Word**s in this line」を検索します。 Welcome ((back)|(home)) は「**Welcome back**」および「**Welcome home**」を検出します。
[ ]	パターンの範囲を検索します。	[a-z] は任意の小文字の英字を検出します。
*	ゼロ回以上出現するパターンを検出します。	<(.*)> は、すべての HTML タグおよびそのコンテンツを検出します。
+	1 回以上出現するパターンを検出します。	(<.l>)+ は **<UL><OL>** を検索します。
?	ゼロ回または 1 回出現するパターンを検出します。	log(.?)in は **login** および **log in** を検出します。
(?i)	大/小文字を区別しないで次の文字を検索します。	(?i)word は、**word**、**Word**、**woRd**、**WORD** を検出します。

HTTP 認証

このタスクについて

「認証方式」セクションで「**HTTP** 認証」ラジオ・ボタンを選択した場合、「**URL** アドレス」フィールドおよび「ドメイン」フィールドが表示されます。

手順

1. ログイン・ページの URL を「**URL** アドレス」テキスト・ボックスに入力します。
2. この URL が正しいことをテストするには、「表示」をクリックします。

   ブラウザーが開きます。
   - 標準の HTTP ログイン・ウィンドウがブラウザー前面にポップアップ表示される場合、これは正しい URL です。
   - ページが表示されても HTTP ログイン・ウィンドウが表示されない場合、この URL は正しくありません。URL を訂正してください。
3. ブラウザーを閉じます。
4. HTTP ログイン・ウィンドウでドメインが必要な場合、「ドメイン」フィールドに正しいドメイン・ネームを入力します。

   これで、現在の構成を使用してブルート・フォース・テストを実行できます (298 ページの『認証テストの実行』を参照)。

HTTP 認証よりフォーム認証を優先

このタスクについて

アプリケーションによっては、両方の タイプの認証を使用することが必要な場合があります。すべてのページについて通常は HTTP 認証を使用し、特定の管理者領域を保護するにはフォーム認証を使用します。このような場合はおそらく、両方のタイプのテストを実行することが必要になります。

HTTP 認証: これは既に説明した方法でテストされます (296 ページの『HTTP 認証』を参照)。

フォーム認証**:** このテストを行うには、HTTP 認証用の実際のユーザー名およびパスワードを Authentication Tester に提示する必要があります。こうすることで HTTP 認証は「合格」となり、該当するページでフォーム認証がテストされます。

手順

1. Authentication Tester のメインウィンドウで、「フォーム認証」ラジオ・ボタンを選択します。
2. フォーム認証を構成します (294 ページの『フォーム認証』を参照)。
3. 「詳細」をクリックします。

   「詳細構成」ダイアログ・ボックスが開きます (「全般」タブが最前面に表示されます)。
4. 「**HTTP** 認証よりフォーム認証を優先」領域で、「有効にする」チェック・ボックスを選択します。

   「ユーザー名」、「パスワード」、および「ドメイン」のフィールドがアクティブになります。
5. フォーム認証ページをテストするときに Authentication Tester で使用される有効な HTTP 認証の資格情報を入力します。
6. HTTP ログイン・ウィンドウでドメインが必要な場合、「ドメイン」フィールドに正しいドメイン・ネームを入力します。
7. 「**OK**」をクリックして、ダイアログ・ボックスを閉じます。

   これで、現在の構成を使用してブルート・フォース・テストを実行できます (298 ページの『認証テストの実行』を参照)。

認証テストの実行

認証方式を選択して基本テストを構成した後、「開始」をクリックして Authentication Tester のスキャンを開始することができます。

メインウィンドウの進行状況表示バーに以下の情報が表示されます。

- 試行するユーザー名とパスワードのペア数のうち、テスト済みのペア数。
- Authentication Tester がこのスキャンで使用しているスレッド数。
- スキャンが進行中でない場合のスキャンの状況 (一時停止、再開、停止、終了)。

スキャンを一時停止して Authentication Tester を開いたままにした (終了しない) 場合、後で「再開」をクリックするとスキャンを再開できます。一時停止の後で Authentication Tester を終了すると、スキャンは削除されます。

スキャンを停止すると、それまでに収集されたデータは削除されます。

スキャン結果

テストが完了すると、ログインに成功したユーザー名とパスワードのペアが「正常なログイン」の表にリストされます。

結果は XML ファイル形式でエクスポートすることで保存できます。この機能は、修正の実施後に Authentication Tester の結果を比較できるため、開発中での認証テストに便利です。

「結果のエクスポート」をクリックして、エクスポート・ファイルの名前を入力します。アクセス権の取得に成功した資格情報をリストした XML ファイルが作成されます。

詳細構成

「詳細構成」ダイアログ・ボックスでは、使用中のローカル・ネットワークおよびテスト対象のアプリケーションに合わせて Authentication Tester の動作をカスタマイズすることができます。

ヒント: フォーム認証および HTTP 認証の両方をテストする場合、すべての情報を一度に入力できます。現在実行中のテストのタイプ (フォームまたは HTTP) に関連した情報のみが使用されます。

メインウィンドウで「詳細」をクリックすると、「詳細構成」ダイアログ・ボックスが開きます。以下の 4 つのタブがあります。

- 『「全般」タブ』
- 299 ページの『「フォーム認証」タブ』
- 299 ページの『「プロキシー」タブ』
- 300 ページの『「証明書生成」タブ』

「全般」タブ:

「詳細構成」ウィンドウの「一般」タブでは、ネットワーク構成を変更できます。

オプション	説明
スレッドの数	Authentication Tester が同時にテストする接続スレッドの最大数を設定します。デフォルト値は 12 です。スレッドが多くなると、スキャンが高速になります。Authentication Tester によってネットワークに過負荷が生じることがわかった場合、スレッド数を減らすことができます。

オプション	説明
要求のタイムアウト (ミリ秒単位)	Authentication Tester が Web アプリケーション・サーバーに到達するために与えられた、接続タイムアウトまでの時間を設定します。
内部プロキシー・ポート	使用可能なポートが、自動的に内部プロキシーに割り当てられます。必要に応じて、別のポートを割り当てることができます。選択したポートが使用できない場合は、警告を受け取ります。
HTTP 認証よりフォーム認証を優先	Web アプリケーションで HTTP 認証よりフォーム認証を優先して使用する場合、フォーム認証をテストするには、「有効にする」を選択して、HTTP 認証のユーザー名、パスワード、およびドメインの有効な値を入力する必要があります。こうすることで、Authentication Tester は Web アプリケーション・サーバーにアクセスして、フォーム認証のメカニズムでブルート・フォース・テストを実行することができます。 これらの値は HTTP 認証テストには影響せず、「フォーム認証」方式を選択した場合にのみ適用されます。

「フォーム認証」タブ**:**

このタブには、受け入れられたユーザー名およびパスワードに応答して送信されるページを記述するために入力する、正常なログインの正規表現が保持されます。(ここに入力する情報は、フォーム認証をテストする場合にのみ適用されます。)

オプション	説明
正常なログインの検出	
正常な応答	これを選択すると、現在構成されている正常な応答が下のペインに表示されます。
エラー応答	これを選択すると、現在構成されているエラー応答が下のペインに表示されます。
追加/削除	応答をリストに追加するには、 295 ページの『アプリケーションのログイン応答の記述』を参照してください。また、正規表現の記述について詳しくは、 296 ページの『メタキャラクターについて』を参照してください。
デフォルトの偽の証明書	
ユーザー名/パスワード	これらのフィールドは、フォーム認証を構成するためのログイン要求を作成するときに入力を求められるストリングを表します (294 ページの『フォーム認証』を参照)。これらはサイトへの実際のログインには使用されないため、有効な 資格情報でなくても構いません。これらは単に、ログイン要求での資格情報の場所を Authentication Tester に識別させるために使用されます (ログイン要求はサイトのブルート・フォース・テストに使用します)。 デフォルト値は `BruteUsername` および `BrutePassword` です。クライアント側のロジックによって、サイトへのログイン要求でこれらの値が使用できない場合 (例えば、アプリケーションではユーザー名に E メールを使用する必要があり、ログイン要求を作成するときにクライアント側のロジックでこの規則が強制適用される場合)、これらの値を有効なフォーマットに変更してください。 デフォルトの偽の証明書を変更するときは、一方の値が他方の値のサブストリングとならないようにしてください。例えば、ユーザー名に user@email.com と入力した場合、パスワードに user は使用できません。

「プロキシー」タブ**:**

Web アプリケーションで Web プロキシー接続が必要な場合、「プロキシー」タブの「有効にする」チェック・ボックスを選択して、サーバーおよびポートを入力します。プロキシーの認証が必要な場合は、ユーザー名およびパスワード、さらに必要に応じてドメインも入力します。

「証明書生成」タブ:

このタブのオプションでは、Authentication Tester がスキャン中に試行するユーザー名およびパスワードの構成を選ぶことができます。

以下の 2 つの領域があります。

- モード: 『証明書生成:「モード」領域』
- 構成: 『証明書生成:「構成」領域』

証明書生成:「モード」領域:
手順

Authentication Tester を実行するモードを以下から選択します。

- マトリックス: リスト内の各ユーザー名は、リスト内のすべてのパスワードとペアにして試されます。このモードは、より包括的なスキャンを行う場合に選択します。
- 並列:ユーザー名およびパスワードは、索引番号によってペアにされます。このモードは、高速スキャンを行う場合に選択します。

証明書生成:「構成」領域:
このタスクについて

この領域では、テスト対象となるユーザー名またはパスワードの一方または両方を生成するために Authentication Tester で使用されるオプションを構成します。

手順

1. ユーザー名またはパスワードをカスタマイズする、いずれかのラジオ・ボタンを選択します。

   「構成」領域に表示されるすべてのフィールドおよびデータは、選択した項目にすぐに適用されます。項目ごとに、ドロップダウン・リストを使用して、作成されて攻撃に使用されるユーザー名/パスワードの構造を構成します。
2. 「要素タイプ」ドロップダウン・リストで、攻撃に含める要素タイプを選択して、その下のフィールドに、 301 ページの『リスト・タイプ』の説明に従って要素の値を入力します。
3. 「追加」をクリックして、「構成」ペインのリストに新しい定義を追加します。
4. 必要に応じて繰り返し、要素を追加します。
5. 要素のタイプを調整して (「上」および「下 」を使用)、試行されるユーザー名またはパスワードがそれぞれ、リストされた順に各タイプで構築されるようにします。

リスト・タイプ*:*

要素	説明	サンプル値
辞書	攻撃用のユーザー名/パスワードの生成に使用する「1 行に値が 1 つ」のファイル。 ユーザー名およびパスワードの両方についてデフォルトのファイルが用意されていますが、「参照」ボタンを使用して別の適切なファイルを参照することができます。データ・フォルダーにはさらに大きなパスワード辞書ファイル (passwords_long.txt) も含まれており、デフォルトのファイルの代わりに使用できます。	「1 行に値が 1 つ」の辞書ファイルへのパス名
数値	生成されるユーザー名/パスワードに含まれる数値の範囲。	0 から 999999999
定数	生成されるすべてのユーザー名/パスワードに含めるストリング。	任意のストリング
文字の範囲	生成されるユーザー名/パスワードに含まれる文字についての、文字の範囲およびストリングの長さ。	(スペースから波形記号) -~ およびストリングの長さ

注**:** スペースから波形記号の範囲には、a から z、A から Z、0 から 9、および ASCII 入力記号が含まれます。「文字の範囲」として「 **-~**」と入力すると、Authentication Tester では含まれるすべての文字を正規表現リストに自動的に挿入します。

長さフィールドの有効な値は範囲に依存します。例えば、範囲が 0 から 9 で長さが 10 の場合、範囲は有効です (0000000000、0000000001、...9999999999)。しかし、範囲が a から z の場合、長さが 10 だと、組み合わせの数によって過度の時間およびリソースが消費されるため、Authentication Tester では有効な長さとして受け入れられません。

注**:** ダッシュを範囲を示すのでなく文字として使用するには、円記号を前に付けてください (**-**)。

証明書生成の構成例*:*

証明書生成	得られる証明書
辞書:辞書: C:\web tests\data\users.txt 定数値: _ 数値の範囲: 0 から 9	user_0 user_1 user_2 ... user_9
定数値: passwd 文字の範囲: a-zA-Z0-9、長さ:3	passwdaaa passwdaab ... passwd999
定数値: iamgod 文字の範囲: -~; 長さ: 1 数値の範囲: 1900 から 3000	iamgod 1900 iamgod!1900 ... iamgod~3000

要素の削除*:*
手順

下のペインで不要な要素をクリックして選択してから、「削除」をクリックします。

接続テスト

この 接続テスト パワー・ツールを使用すると、多くのファイアウォールでブロックされてしまう Ping プロトコルを使用せずに Web サイトを ping することができます。

- 接続テスト は AppScan から実行でき、これを行うには「ツール」 > 「パワー・ツール」 > 「接続テスト」の順にクリックします。
- Windows の「スタート」メニューから「すべてのプログラム」 > **[AppScan Standard** インストール・フォルダー**]** > 「パワー・ツール」>「接続テスト」の順にクリックして、接続テスト を単独で実行することもできます。

接続テスト の使用

手順

1. 「**Web** サイト」テキスト・ボックスに URL を入力または貼り付けます。
2. 「サイトの **ping**」をクリックします。

   Ping 結果リストには 接続テスト が対象 URL と正常に通信できたかどうか、および成功した場合は対象 URL との通信にかかった時間 (ミリ秒) が表示されます。

次のタスク

- Ping 結果リストを消去するには、「消去」をクリックします。

HTTP メソッド**:**

「**HTTP** メソッド」ドロップダウン・メニューには 2 つの HTTP 要求メソッドがあります。

- **HEAD:** HTTP ヘッダーのみを取得する場合に選択します。早いのはこちらのメソッドです。
- **GET:** ページ全体を取得する場合に選択します。一部のサイトではHEAD メソッドを使用した HTTP 要求が許可されません。その場合には、GET メソッドを試してください。

ポート**:**

「ポート」テキスト・ボックスには、Web サーバーの listen ポートを指定します。

ほとんどの非セキュアな URL のデフォルトのポートは **80** です。必要に応じて特定の URL のポートを変更できます。

SSL (Secure Sockets Layer) を使用するには、「セキュア」を選択します。デフォルトのポートは **443** に変更されます。

間隔の数**:**

「間隔の数」テキスト・ボックスに 接続テスト が対象の URL に ping する 回数を指定します。

- 対象の URL に通信可能かどうかのみテストする場合は、小さな値 (3 から 5 など) を指定します。
- サーバーの破損をモニターする必要がある場合は、大きな値 (100 から 1000 など) にします。接続テスト はユーザーが他のタスクを行っている間にバックグラウンドで動作するので、間隔の数の値は好きなだけ大きくできます。

接続テスト は次の ping の前であれば「停止」をクリックしていつでも停止できます。

待機間隔**:**

「待機間隔」テキスト・ボックスに接続テスト が待機する ping 間隔をミリ秒数で指定します。

- 対象の URL に通信可能かどうかをテストする場合は、値を 0 (ゼロ) にします。
- サーバーの破損をモニターする必要がある場合、値を大きく (2000 (2 秒) など) します。

Server ヘッダーを表示**:**

「**Server** ヘッダーを表示」チェック・ボックスを選択し、 ping されている Web server のタイプを参照します。この情報は最後の間隔が到達した後に表示されます。

Server ヘッダーの例:

- www.ibm.com - `Microsoft-IIS/6.0`
- www.cnn.com - `Apache`
- www.sky-news.co.uk - `Microsoft-IIS/5.0`
- www.sourceforge.org - `Apache/1.3.31 (Unix) PHP/4.3.11 mod_ssl/2.8.19 OpenSSL/0.9.7a`

Encode/Decode

Encode/Decode PowerTool は指定されたストリングに、指定されたフォーマットのエンコードおよびデコードを行います。

- Encode/Decode は AppScan から実行でき、これを行うには「ツール」 **>** 「パワー・ツール」 **>** 「**Encode/Decode**」の順にクリックします。
- Windows の「スタート」メニューから「すべてのプログラム」 **> [AppScan Standard** インストール・フォルダー**] >** 「パワー・ツール」**>**「**Encode/Decode**」の順にクリックして、Encode/Decode を単独で実行することもできます。

Encode/Decode の使用

手順

1. 「入力」テキスト・ボックスにテキストを入力または貼り付けます。
2. 「方式」ドロップダウン・メニューからエンコード/デコードの方式を選択します。 (『方式』 を参照してください。)

   3DES 方式を選択した場合、「暗号鍵」テキスト・ボックスに適切な暗号鍵を入力または貼り付けてください。
3. 「エンコード」または「デコード」をクリックします。

   エンコード化テストまたはデコード化テストの結果が「出力」ボックスに表示されます。

エンコード**/**デコードの階層化**:** 「戻す」をクリックすると、出力を入力として戻し、再度エンコードまたはデコードすることができます。

これは、以下を実施する場合に役立ちます。

- エンコードがデコードと 1 対 1 対応になっていることを確認する
- ストリングに複数のエンコードを行う
- 多重に暗号化されたストリングをデコードする

方式**:**

方法	機能	変換
URL	エンコード + デコード	テキスト <-> URL エンコード
Base64	エンコード + デコード	テキスト <-> Base64 エンコード

方法	機能	変換
Overlong UTF-8	エンコード + デコード	テキスト <-> オーバーロング UTF-8 (2 バイト)
UU	エンコード + デコード	テキスト <-> UU エンコード
HTML	エンコード + デコード	テキスト <-> HTML エンティティー
MD5	エンコード	テキスト <-> デジタル署名
SHA1	エンコード	テキスト <-> デジタル署名
SHA256	エンコード	テキスト <-> デジタル署名
SHA384	エンコード	テキスト <-> デジタル署名
SHA512	エンコード	テキスト <-> デジタル署名
3DES (192 ビット・キー)	エンコード + デコード	読み取り可能なテキスト <-> 暗号化されたテキスト (指定のキーを使用)

Expression Test

正確な正規表現を記述することは面倒な試行錯誤のプロセスです。この Expression Test パワー・ツールを使用すると、プロセスを加速させることができます。

- Expression Test は AppScan から実行でき、これを行うには「ツール」 > 「パワー・ツール」 > 「**Expression Test**」の順にクリックします。
- Windows の「スタート」メニューから「すべてのプログラム」 > **[AppScan Standard** インストール・フォルダー**]** > 「パワー・ツール」>「**Expression Test**」の順にクリックして、Expression Test を単独で実行することもできます。

Expression Test の使用

手順

1. 「テキスト」フィールドに正規表現で検索するテキストを入力または貼り付けます。
2. 「正規表現」フィールドに対象のテキストを検索すると思われる 正規表現を入力します。
3. 「テスト」をクリックします。

タスクの結果

パターンと一致するテキスト・ボックスのテキストが赤で強調表示されます。

テキストの置換

特定のパターンと一致するテキストを置換します。

このタスクについて

特定のパターンと一致するテキストの置換のために正規表現を使用する場合、 Expression Test を使用して、置換が正しく行われるかをテストすることができます。

手順

1. 「正規表現」フィールドに正規表現を入力します。
2. 「置換」ボックスに正規表現のパターンと一致するテキストと置き換えるテキストを 入力します。
3. 「テキスト」ボックスに試すテキストを入力または貼り付けます。
4. 「テスト」 をクリックし、予測したテキストが正規表現によってマッチングされていることを確認します。
5. 「置換」をクリックします。

タスクの結果

正規表現パターンと一致するテキスト (赤で強調表示) は、「置換」ボックスのテキストに置き換えられます。

パターン・グループ

正規表現を文字グループまたはメタキャラクター・グループに適用します。

正規表現を文字グループまたはメタキャラクター・グループに適用することが必要な場合がよくあります。

1 つのセットにグループ化するには文字を括弧 ( ) で囲みます。

グループには「グループを照合」ボックスで番号が付けられ、マッチング・テキストがその隣に表示されます。

一致するものがある場合、「グループを照合」ボックスでどのテキストがどのグループに一致しているかを参照できます。

例えば、テキストに `<UL>first` という HTML コードあるとします。

正規表現として `(<.L>)([a-z ]*)` と入力します。

「テキスト」フィールドの `<UL>first` が赤で強調表示されます。

「グループを照合」では、グループが以下のように分割されます。

- グループ 1 `<UL>`
- グループ 2 `first`

メタキャラクター

メタキャラクターに関する一般情報。

正規表現で単一文字 (文字、数字、または記号) は、メタキャラクターである場合を除いて、文字通りそれ自身と一致します。メタキャラクターは、1 つ以上の文字で構成され、固有の意味を持っています。また、正規表現マッチングで文字通りには使用されません。

例えば、曲折アクセント記号 (^) は「先頭を検索」を意味するメタキャラクターです。

この文字をメタキャラクター・パターンとして使用するのではなく、検索する場合、文字の前に円記号 ( ) を付けます。

例えば、曲折アクセント記号をテキスト文字として検索するには、正規表現は次のようにする必要があります。\^

正規表現	説明	例
\	次の文字を文字として検索し、メタキャラクター・パターンとして使用しないようにします。	\. は、テキスト内のピリオド (.) を検索します。 . は、最初の文字 (任意の文字) を検索します。
^	文字列の先頭を検索します。	^1 は、「**1**.Click Save.」を検索しますが、「in the 2**1**0th line」は検索しません。
.	任意の文字を検索します (改行文字は除く)。	a、A、1、<、.、=、など、すべての先頭文字を検索します。
()	パターン・グループを検索します。	(word) は 「In this **word**」を検索します。 ^(Word) は「**Word**s in this line」を検索します。
[]	パターンの範囲を検索します。	[a-z] は 文字を検索しますが、数値は検索しません。
*	直前のパターンの 0 回以上の繰り返しを検索します。	.* はすべての文字を検索します。<(.*)> はすべての HTML タグを検索します。
+	直前のパターンの 1 回以上の繰り返しを検索します。	(<.l>)+ は **<UL><OL>** を検索します。
?	直前のパターンの 0 または 1 回の繰り返しを検索します。	(<.l>)? は **<UL>** を検索します。
(?i)	大/小文字を区別しないで次の文字を検索します。	(?i)word は、**word** および **Word**を検索します。

HTTP Request Editor

HTTP Request Editor パワー・ツールによって、十分に制御された HTTP 要求をサイトに送信できるため、さまざまな種類の HTTP 要求にサイトがどのように応答するかをテストできます。

- HTTP Request Editor は AppScan から実行でき、これを行うには「ツール」 > 「パワー・ツール」 > 「**HTTP Request Editor**」の順にクリックします。
- Windows の「スタート」メニューから「すべてのプログラム」 > [AppScan Standard インストール・フォルダー] > 「パワー・ツール」>「HTTP Request Editor」の順にクリックして、HTTP Request Editor を単独で実行することもできます。

HTTP Request Editor の使用

手順

1. 「要求」タブで、関連するフィールドを入力します。
2. 「送信」をクリックします。
3. 「応答」タブを開いて、ホストが要求をどのように処理したかを確認します。

「要求」タブ

ビュー・オプション**:** 「要求」タブの「ビュー」オプションでは、以下のさまざまな方法で HTTP 要求を作成できます。

- 未加工**:** テキストを入力するか貼り付けて要求を作成します。
- 解析済み**:** フォームに入力して要求を作成します。

「解析済み」ビューで入力した未加工の HTTP 要求の詳細を更新するには、「未加工」タブの「解析結果から更新」をクリックします。

解析済みのフォームに入力してセットアップした要求が、未加工のフォームに表示されます。

要求設定**:**

設定	説明
ホスト	Web サイトの IP アドレスまたはホスト名を入力します。
ポート	Web サーバーが listen する TCP ポートを入力します。 デフォルトは 80 です。
方法	方法をドロップダウン・メニューから選択するか、方法要求パラメーターの値を入力します。デフォルトのドロップダウン・メニューには以下のものがあります。 GET:Request-URI によって識別されるすべての情報を取得します。 POST:発信元サーバーに対して、要求に含まれるエンティティーを、Request-Line の Request-URI によって識別されるリソースの新しい従属として受け入れることを要求します。この方法によって実行される実際の機能はサーバーによって判断され、多くの場合は Request-URI に依存します。 HEAD:Request-URI によって識別される情報を取得しますが、サーバーは応答でメッセージ・ボディを戻しません。HEAD 要求に応答して受け取る HTTP ヘッダー内のメタ情報は、GET 要求に応答して受け取るものと同じです。ボディ全体を転送せずに情報を取得するときに使用され、ハイパーテキスト・リンクの妥当性、アクセス可能性、および変更をテストするために多く使用されます。
セキュア	HTTPS を使用して要求を送信する場合にチェックします。
URL	URL を入力するか、貼り付けます。 最新の応答から抽出されたリンクのリストは、「応答」タブで確認できます。
HTTP バージョン	要求で使用する HTTP プロトコルのバージョン番号を入力します。 デフォルトは 1.1 です。
自動的にコンテンツ長を計算	チェックされた場合、HTTP Request Editor はコンテンツ長ヘッダーおよびその正しい値を自動的に計算して追加します。

メッセージの詳細**:** 要求に含めるパラメーター、ヘッダー、Cookie、およびこれらの値を作成するか、または変更します。

パラメーター**:**

パラメーターの追加**:**
手順

1. 「追加」をクリックします。

   「パラメーターの追加」ダイアログ・ボックスが開きます。
2. パラメーターの名前を入力して、値を入力します。
3. 以下からタイプを選択します。

- 本文: パラメーターを要求のボディに入れて送信します。
- 照会: パラメーターを要求のクエリー部分に入れて送信します。

4. 「**OK**」をクリックします。

   パラメーターが要求に追加されます。

   「解析済み」ビューの「パラメーター」表に、入力した名前、値、および場所が表示されます。

   「未加工」ビューでは、パラメーターは選択した場所によって表示方法が異なり、以下のようになります。

   - ボディ: name=valueの組は要求のボディに表示されます。
   - クエリー: name=value の組は要求のクエリー部分 (? 記号の後) に表示されます

   どちらの場合も、name=value の組が複数存在するときは & で連結されます。

パラメーターの編集:
手順

以下のいずれかを実行します。

- 「解析済み」ビューで、パラメーターを選択して「編集」をクリックします。
- 「未加工」ビューで、テキストを編集します。

パラメーターの削除:
このタスクについて

パラメーターを HTTP Request Editor から削除せずに要求から削除できます。

手順

「解析済み」ビューで、パラメーター名のチェック・マークを外します。

パラメーターの削除:
手順

以下のいずれかを実行します。

- 「解析済み」ビューで、パラメーターを選択して「削除」をクリックします。
- 「未加工」ビューで、テキストを削除します。

ヘッダー:

ヘッダーの追加:
手順

1. 「追加」をクリックします。

   「ヘッダーの追加」ダイアログ・ボックスが開きます。

2. 新しい HTTP ヘッダーの名前および値を入力します。
3. 「**OK**」をクリックします。

   ヘッダーが要求に追加されます。

   - 「解析済み」ビューの「ヘッダー」表に、新しい HTTP ヘッダーの名前および値が表示されます。

- 「未加工」ビューでは、ヘッダーが次のように表示されます。**ヘッダー名:ヘッダー値**

ヘッダーの編集*:*
手順

以下のいずれかを実行します。
- 「解析済み」ビューで、ヘッダー名を選択して「編集」をクリックします。
- 「未加工」ビューで、編集するヘッダーを見つけ、テキストを変更します。

ヘッダーの削除*:*
このタスクについて

ヘッダーを HTTP Request Editor から削除せずに要求から削除できます。

手順

「解析済み」ビューで、ヘッダー名の横にあるチェック・ボックスをクリアします。
HTTP Request Editor によって、いくつかのデフォルトのヘッダー (Accept、Host、User Agent) を持つ要求が生成されます。これらのヘッダーは他のヘッダーと同じように削除または編集できます。

ヘッダーの削除*:*
手順

以下のいずれかを実行します。
- 「解析済み」ビューで、ヘッダー名を選択して「削除」をクリックします。
- 「未加工」ビューで、削除する HTTP ヘッダーを見つけ、テキストを要求から削除します。

Cookie:

Cookie の追加*:*
手順
1. 「追加」をクリックします。

   「Cookie の追加 (Add Cookie)」ダイアログ・ボックスが開きます。
2. Cookie の名前を入力して、値を入力します。
3. 「**OK**」をクリックします。

   Cookie が要求に追加されます。
   - 「解析済み」ビューの「Cookies」表に、入力した名前および値が表示されます。
   - 「未加工」ビューでは、Cookie が次のようにヘッダーに表示されます。`Cookie: name=value`

Cookie の編集*:*
手順

以下のいずれかを実行します。
- 「解析済み」ビューで、Cookie を選択して「編集」をクリックします。
- 「未加工」ビューで、変更する Cookie ヘッダーを見つけ、テキストを編集します。

Cookie の削除*:*

このタスクについて

Cookie を HTTP Request Editor から削除せずに要求から削除できます。

手順

「解析済み」ビューで、Cookie 名のチェック・ボックスをクリアします。

Cookie の削除*:*
手順

以下のいずれかを実行します。

- 「解析済み」ビューで、Cookie を選択して「削除」をクリックします。
- 「未加工」ビューで、削除する Cookie ヘッダーを見つけ、テキストを削除します。

応答タブ

「要求」タブで「送信」をクリックすると、Web サーバーから応答を受け取ります。

応答を表示する方法は以下の 3 つです。

- 未加工**:** 応答は未加工のテキストで表示されます。
- 解析済み**:** 応答の HTML から抽出されたリンクのリストと、SSL 情報が表示されます。
- ブラウザー**:** 応答は Web ブラウザーに表示されます。

  注**:**

  Web サーバーによって送信された実際の応答のみがブラウザーに表示されます。リダイレクト、画像、および CSS は自動的に要求されません。

未加工ビューには、応答のテキストを検索するオプションがあります。ウィンドウ下部のテキスト・ボックスに正規表現を入力して (例えば E メールを検索するときは「[a-z0-9]@」と入力)、「検索」をクリックします。

大文字と小文字の両方の文字でパターン・マッチングを行うときは、「大文字と小文字を区別しない」にチェック・マークを付けます。

Generic Service Client (GSC)

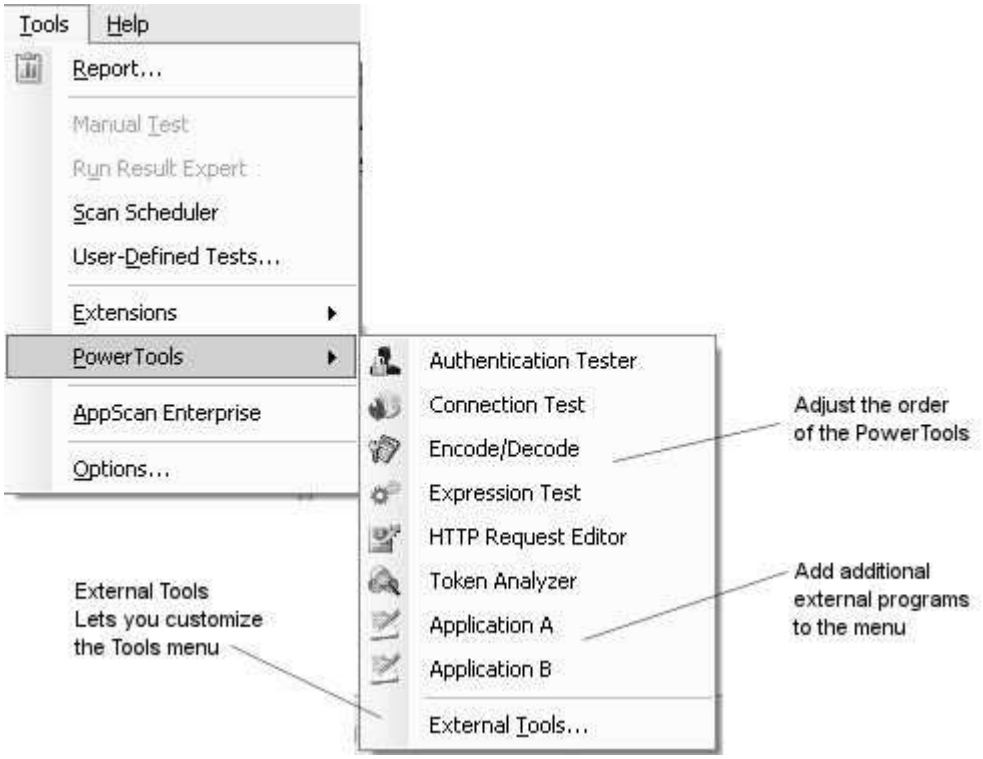
Generic Service Client (GSC) は、使用可能なサービスを表示し、パラメーターを入力したり、結果を表示したりできる単純なインターフェースを提供します。これを使用して SOAP Web サービスを手動で探査することで、AppScan がユーザーの入力を使用して適切なテストを作成することが可能になります。

参照先: 161 ページの『GSC の使用』

「ツール」メニューのカスタマイズ

以下のことを行うために、「ツール」メニューをカスタマイズすることができます。

- 『パワー・ツールの順序の調整』
- 『「ツール」メニューへのプログラムの追加』



パワー・ツールの順序の調整

手順

1. 「ツール」>「パワー・ツール」>「外部ツール」をクリックします。

   「外部ツール」ダイアログ・ボックスが開きます。
2. リストからメニュー項目を選択し、必要に応じて「上へ移動」または「下へ移動」をクリックします。

「ツール」メニューへのプログラムの追加

このタスクについて

AppScan を実行する際に頻繁に使用する特定の外部プログラムに対するリンクを追加できます。「ツール」メニューにリンクを追加して、AppScan 内から開けるようにできます。

手順

1. 「ツール」>「パワー・ツール」>「外部ツール」をクリックします。

   「外部ツール」ダイアログ・ボックスが開きます。
2. 「追加」をクリックします。

   「新規外部ツールの作成」ダイアログ・ボックスが開きます。

3. 「タイトル」フィールドに、「ツール」メニューで表示する名前を入力します。
4. 「参照」ボタン (...) をクリックし、プログラムの EXE ファイルを見つけて「開く」をクリックします。
5. 「**OK**」をクリックします。

   その EXE ファイルのタイトルとパスが、「外部ツール」リストに追加されます。
6. メニューの中での位置を調整するには、その新規項目を選択し、必要に応じて「上へ移動」または「下へ移動」をクリックします。

拡張子

AppScan を使えば、エクステンションの作成や組み込みが容易になります。エクステンションは、AppScan に機能を追加するアドオンです。エクステンションとしては、小さな E メール通知ユーティリティーから、非常に大きい脆弱性悪用ツールまで、さまざまなものが可能です。ユーザーは、エクステンションを使って AppScan を自分の必要に合わせてカスタマイズできます。エクステンションは、AppScan の SDK およびエクステンション・フレームワークを使用して作成されます。

AppScan と共にエクステンションを使用する方法、およびエクステンションをダウンロード/ホストする場所については、http://www.ibm.com/developerworks/rational/downloads/08/appscan_ext_framework/ をご利用ください。

SDK オンライン・ヘルプ・ファイルの **AppScanSDK.chm** は、AppScan ドキュメンテーションのメイン・フォルダーにあります。

AppScan には、Pyscan エクステンションとその他のエクステンションが組み込まれています。エクステンション・マネージャーを使用すると、追加のエクステンションを容易に組み込んだり管理したりできます。

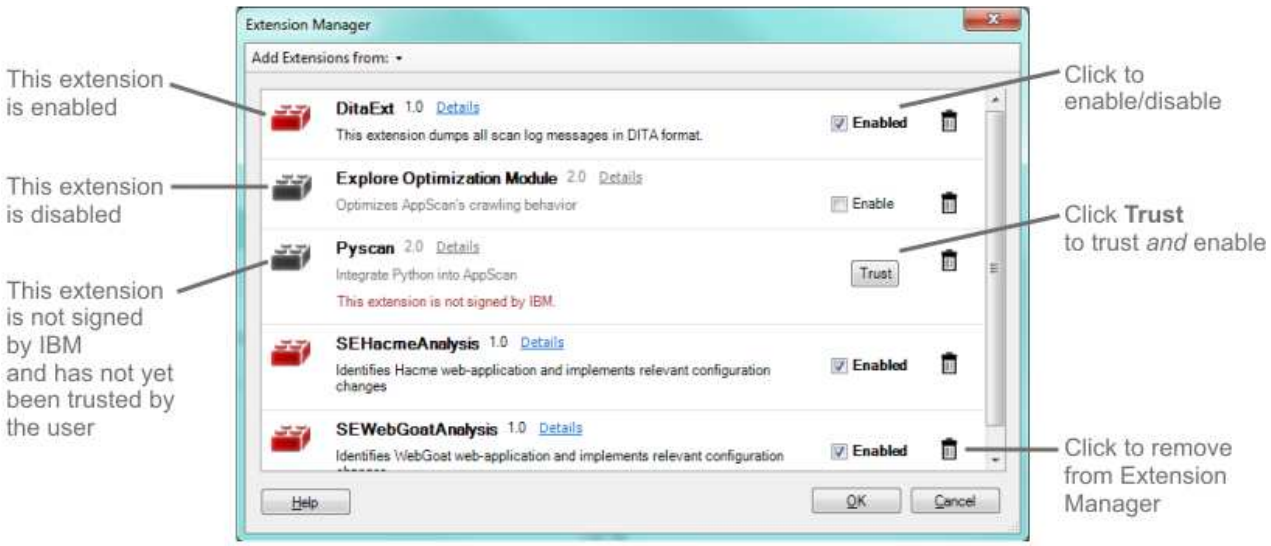
エクステンション・マネージャー

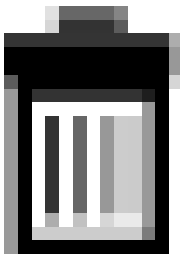
エクステンション・マネージャーによって、 で使用するエクステンションを追加/削除、有効化/無効かすることができます。 AppScan

エクステンション・マネージャー (「ツール」 > 「エクステンション」 > 「エクステンション・マネージャー」) は、追加されたすべてのエクステンションをリストします。

- IBM Security から入手可能なエクステンションを追加することも、独自のエクステンションを追加することもできます。
- 追加されたエクステンションは有効にしたり無効にしたりできます。
- 署名されていないエクステンションを信頼するよう選択することができます (例えば、お客様自身が作成したエクステンションなど)。

エクステンションが追加されたものの、信頼されず有効化できない場合は、左側にあるアイコンがグレー表示されます。



オプション	説明
エクステンションの追加元:	新規エクステンションを追加するには、以下のソースをクリックして選択します。 • 「このコンピューター」、または • 「**AppScan eXtensions Framework** ページ」
「有効」チェック・ボックス	エクステンションを有効/無効にするためにチェック・ボックスを選択/選択解除します。この変更は、次に AppScan を開いたときから有効になります。 新規エクステンションが追加されると、AppScan がこれを実行できない理由 (バージョンが非互換など) がない限り、それは自動的に有効となります (このチェック・ボックスも選択されます)。あるいは、このエクステンションは署名されません。
「信頼する」ボタン	エクステンションをインストールしたが、署名されていない場合、AppScan はエクステンションをロードしませんが、横に「信頼する」ボタンが表示されます。AppScan を開くと、無効な署名されていないエクステンションが存在することを警告するポップアップが示されます。 そのエクステンションを信頼できる場合 (例えば、お客様自身がそれを作成した場合など) は、「信頼する」ボタンをクリックすると、それ以降信頼され、有効になります。 **ヒント:** 以前のバージョンの AppScan で使用した署名なし IBM エクステンションがある場合は、それを信頼するよう選択することも、「他のエクステンションを取得」をクリックして、代わりとなる署名済みバージョンがあるかどうか確認することもできます (366 ページの『署名なしエクステンションの置換』 を参照)。
	エクステンションを削除する場合にクリックします。

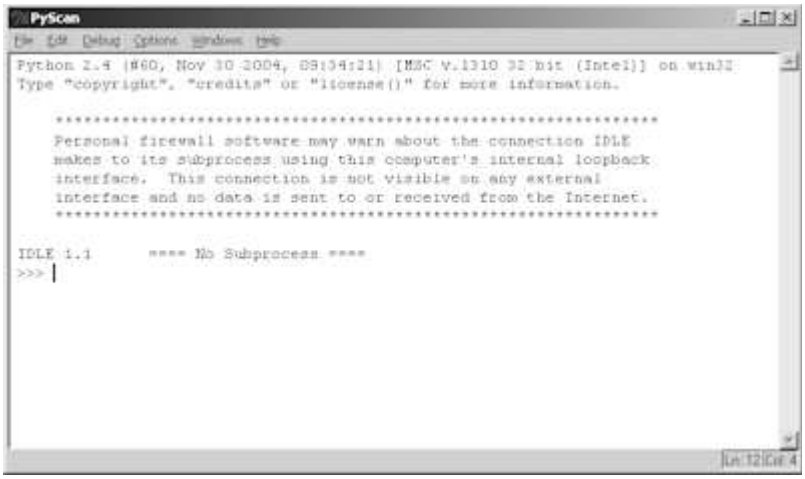
Pyscan

このタスクについて

Pyscan は、Python インターフェースを使用して AppScan を制御できるようにする Python エクステンションです。Pyscan は、標準の AppScan インストールの際にインストールされ有効にされます。

手順

「ツール」ツールバーで、「エクステンション」>「**Pyscan**」をクリックします。
Pyscan インターフェースが開きます。



探査の最適化モジュール

この拡張機能は、探査結果から不要な URL を除去することにより、スキャン効率を高めるのに役立ちます。

この拡張機能は、サイトによって URL 再書き込みが使用されており、組み込みパラメーターの違いのみが原因で別個と見なされる重複 URL のためにスキャンの探査ステージが膨張する場合に、特にパフォーマンスを向上させることができます。

探査の最適化モジュールは、パラメーターを組み込むために再書き込みされる URL を識別します。例えば、以下のような URL が何度も出現する場合、AppScan はそれぞれについてフォルダーを作成します。しかし、これらは実際は、便宜上 URL に再書き込みされたパラメーターです。

```
http://mysite.com/2010/10/01/
http://mysite.com/2010/10/02/
http://mysite.com/2010/11/01/
http://mysite.com/2010/11/02/
http://mysite.com/2010/12/01/
http://mysite.com/2010/12/02/
```

このようなケースでは、不要な URL が何千も作成されたり、探査ステージに長時間かかったりする可能性があります。

関連性があると思われる URL を多数検出すると、モジュールはそれらを分析します。モジュールは次にカスタム・パラメーター (この場合は `/[year]/[month]/[day]`) を作成し、探査結果を消去して、新規探査ステージを実行します。これにより、テスト・ステージでテスト対象となる URL が大いに削減される可能性があります。これによりパフォーマンスを大幅に向上させることができます。

注: スキャン効率を最大化するのに役立つ、このモジュールの追加機能は、「ナビゲーション・パラメーター検出の実行」(詳しくは、 317 ページの『探査の最適化の構成』を参照) です。

モジュールの自動実行

探査ステージで検出されたリンクの数 (アクセスされていないリンクを含む) が構成済みのしきい値に到達した場合は必ず、スキャン時にこのモジュールを実行することが推奨されます。このしきい値 (「モジュールを開始する最小リンク数」) は、通常、少なくとも 1,000 です。

注: コマンド行インターフェース (CLI) からスキャンを開始した場合、探査の最適化は、構成されている場合でも自動的には実行されません。

注: スキャン構成にマニュアル探査データまたはマルチステップ操作が含まれている場合、探査の最適化は構成されている場合でも自動的には実行されません が、手動で実行することはできます (「ツール」 > 「エクステンション」 > 「探査の最適化モジュール」 > 「実行」)。

構成を変更するには、次のようにします。

1. 「ツール」>「エクステンション」>「探査の最適化モジュール:構成」をクリックします。

   「探査の最適化モジュールの構成」ダイアログ・ボックスが開きます。
2. 「スキャン中に探査最適化プログラムを自動的に実行」チェック・ボックスを選択します。
3. 「**OK**」をクリックします。

モジュールの手動実行

検出された URL の数が構成済みのしきい値 (「モジュールを開始する最小リンク数」) より少ない 場合も含め、どのような探査結果に対しても、このモジュールを手動で実行することができます。ただし、モジュールが最も役に立つのは、URL の数が少なくとも数百以上の場合です。

探査の最適化を手動で実行するには、以下の手順を実行します。

- 「ツール」>「エクステンション」>「探査の最適化モジュール: を実行します。

  構成済みの「開始 URL」からモジュールが探査を開始します。探査ステージが完了すると、モジュールは結果を分析します。最適化が検出されると、最初の結果セットを保存するかどうかをユーザーに確認してから、結果セットを消去して再探査を行います。

以下も参照してください。

85 ページの『冗長性調整』

87 ページの『冗長性調整のデフォルト』

探査の最適化の処理

このセクションでは、探査の最適化がアクティブな状態でのスキャンの実行について説明します。

このタスクについて

サイトがその URL にパラメーターを再書き込みする場合、あるいは、探査の最適化が無効になった状態でサイトの最初の探査試行を行った結果、非常に多くの URL が作成されたり、スキャンが終了しなかったりした場合は、探査の最適化モジュールによって、スキャンを扱いやすい大きさまで縮小することができ

ます。さらに、「ナビゲーション・パラメーター検出の実行」オプションをアクティブ化することが役立つ場合があります。

手順

1. 通常のスキャンと同様に、開始 URL およびその他の必要な設定を構成します。
2. 「ツール」>「エクステンション」>「探査の最適化モジュール**:** を構成し、「スキャン中に探査最適化プログラムを自動的に実行」チェック・ボックスを選択します。

   注**:** スキャン構成にマニュアル探査データまたはマルチステップ操作が含まれている場合、探査の最適化は構成されている場合でも自動的には実行されません が、手動で実行することはできます (「ツール」 > 「エクステンション」 > 「探査の最適化モジュール」 > 「実行」)。
3. スキャン構成エリアで、オプションで「ナビゲーション・パラメーター検出の実行」設定を「**True**」に変更します。
4. 「**OK**」をクリックします。
5. スキャンを開始します (「スキャン」>「フルスキャン」)。

   探査ステージで検出された URL の数 (探査されない URL を含む) が「モジュールを開始する最小リンク数」(デフォルト: 1000) で定義されたしきい値に到達した場合は、探査ステージが一時停止し、探査の最適化モジュールが次の 2 つの (メイン) ステージから構成されるフェーズ を開始します。

   ナビゲーション・パラメーターの識別 **(**構成されている場合**)**

   モジュールは、定義された名前および値 (「ツール」「エクステンション」「探査の最適化モジュール: 構成」) を使用して、ナビゲーション・パラメーターを検索します。ナビゲーション・パラメーターの識別に成功した場合、モジュールは以下の処理を行います。

   a. それらのパラメーターをパラメーターのリスト (「スキャン構成」>「パラメーターおよび Cookie」> メイン・タブ) に定義します
   b. それらの冗長性調整を最も厳しいレベルに設定します
   c. デフォルト の冗長性調整 (非ナビゲーション・パラメーター用) を、より低いレベルに下げます (87 ページの『冗長性調整のデフォルト』を参照)

   URL 再書き込みの識別

   モジュールは URL に書き込まれたパラメーターを検索します。そのようなパラメーターを検出した場合は、それらをカスタム・パラメーターのリスト (「スキャン構成」>「パラメーターおよび Cookie」>「詳細: カスタム・パラメーター」タブ) に定義します。
6. 探査の最適化のこのフェーズ の最後に、以下の処理が行われます。
   - 構成変更が行われた場合は、既存の探査データが消去され、新規探査ステージが実行されます。 (モジュールを手動で開始した場合は、新規探査ステージが実行される前に、現行データの保存についてのオプションが提示されます。)
   - 構成変更が行われなかった場合は、探査の最適化の新規フェーズ が実行されます。その際、パラメーターを識別するための十分なデータを収集し、探査データを適度なサイズに縮小するために、より高いしきい値 (ユーザー設定不可) が使用されます。
7. モジュールが (1 つ以上のフェーズ、および 1 つ以上の再探査ステージにより) 正常に実行された後に、スキャンが再開し、終了します。
8. スキャンが完了したら、その結果を調べて、スキャンが成功したことを示す以下の事項について確認してください。
   - 画面左下のステータス・バーには、作成されたテスト数および送信されたテスト数が示されます。すべてのテストが送信されている必要があります。

- アプリケーション・ツリーが完成していて、サイトのすべての重要パーツがアクセスされたことを示している必要があります。
- 追加されたナビゲーション・パラメーターを調べて、すべての重要パラメーターが完全に追跡されたことを確認します。
- 追加されたカスタム・パラメーターを調べて、サイトがパラメーターをその URL に書き込む方法をこれらのカスタム・パラメーターが正しく表していることを確認します。

探査の最適化の構成

このダイアログ・ボックスは、探査の最適化モジュールをアクティブ化および構成するために使用します。

モジュールのアクティブ化を除き、ほとんどの場合、その他の構成を変更する必要はありません。以下に示すように、サポートからの指示がない限り決して変更してはならないものもあります。

このダイアログ・ボックスは、「ツール」 > 「エクステンション」 > 「探査の最適化モジュール: 構成」から開きます。

注: これらの設定に変更を加えて、新規スキャンを作成すると、そのチェック・ボックスの設定を除くすべての設定がそれぞれのデフォルトに戻ります。

名前	説明
チェック・ボックス	
スキャン中に探査最適化プログラムを自動的に実行	これを選択すると、「探査のみ」または「フル・スキャン」のいずれかを実行するときに、「開始する最小リンク数」の制限 (下限) に到達している場合は必ず、モジュールが自動的に実行されます。 **重要:** この設定は、すべての スキャンに適用されます。このダイアログ・ボックス内のその他の設定は、現在のスキャンにのみ適用されます。 デフォルト:消去済み **注:** コマンド行インターフェース (CLI) からスキャンを開始した場合、探査の最適化は、構成されている場合でも自動的には実行されません。 **注:** スキャン構成にマニュアル探査データまたはマルチステップ操作が含まれている場合、探査の最適化は構成されている場合でも自動的には実行されません が、手動で実行することはできます (「ツール」 > 「エクステンション」 > 「探査の最適化モジュール」 > 「実行」)。
スキャン構成	

名前	説明

再書き込みルールを右側にアンカー	以下のような URL を考えます。
	`http://...php/1/index`
	`http://...php/2/index`
	`http://...php/3/index`
	
	モジュールがカスタム・パラメーターを作成するときに、
	
	これが False に設定されている場合、作成されるパラメーターは次のようになります。
	
	`php/([^/.]+)`
	
	これが True に設定されている場合、作成されるパラメーターは次のようになります。
	
	`php/([^/.]+)/index`
	
	デフォルト:False

信頼性マージン (%)	これは、サポートからの指示があった場合にのみ変更してください。
URL 再書き込みで使用される区切り文字	アプリケーションで使用される任意のカスタム区切り文字を追加します。
行ペア開始の最大深度	これは、サポートからの指示があった場合にのみ変更してください。
最大フェーズ時間 (分)	探査の最適化フェーズの最大実行時間です。
再書き込みルールを左側にマージ	これは、サポートからの指示があった場合にのみ変更してください。
モジュールを開始する最小リンク数	「スキャン中に探査最適化プログラムを自動的に実行」チェック・ボックスが選択されている場合に、探査の最適化モジュールを自動的に開始するために必要な、探査ステージ・データ内の最小リンク数 (アクセスされていない URL を含む)。 **注:** この設定を変更した場合も、探査ステージでリンク数が 1,000 に到達すると、モジュールをアクティブ化することを推奨する通知が表示されます。 デフォルト:1,000
名前/値ペアの区切り文字	アプリケーションで使用するすべてのカスタム区切り文字を指定します。
ナビゲーション・パラメーター名	ナビゲーション・パラメーター名の部分一致。シングル・スペースで区切ります。
ナビゲーション・パラメーター値	ナビゲーション・パラメーター値のパターンの部分一致。シングル・スペースで区切ります。
未使用の区切り文字の削除	これは、サポートからの指示があった場合にのみ変更してください。 デフォルト:True

名前	説明
ナビゲーション・パラメーターの検出を実行	「True」の場合、モジュールは、ナビゲーション・パラメーターを名前または値で識別しようと試みます。モジュールは、これらのパラメーターの冗長性調整の構成を最も制限されたレベルに設定し、その他のすべてのパラメーターに適用されるデフォルト設定を削減します。 これにより AppScan は、ナビゲーション・パラメーターをこれまでより徹底的に テストすることが可能になり、その一方で、すべての非ナビゲーション・パラメーターの処理の徹底度を低めつつ 安全に処理することが可能になります。 この値を「True」に設定することで、正確度とパフォーマンスの両方を大幅に向上させることができますが、結果を慎重に確認して、スキャン範囲が影響を受けていないことを確認する必要があります。 デフォルト:False
切り替えの複雑性の制限	あるフォルダーにこの制限よりも多くのサブフォルダーが含まれている場合、AppScan は、これらのサブフォルダーは動的パラメーター値であり、個別にスキャンする必要はないと見なします。 **注:** ここで入力する値は、探査の最適化を手動で実行するためのしきい値としても使用されます。ここで入力した数より少ないリンクが発見された場合、モジュールは実行されません。 デフォルト:20

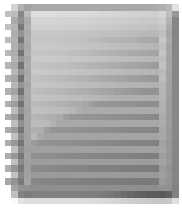
ログ

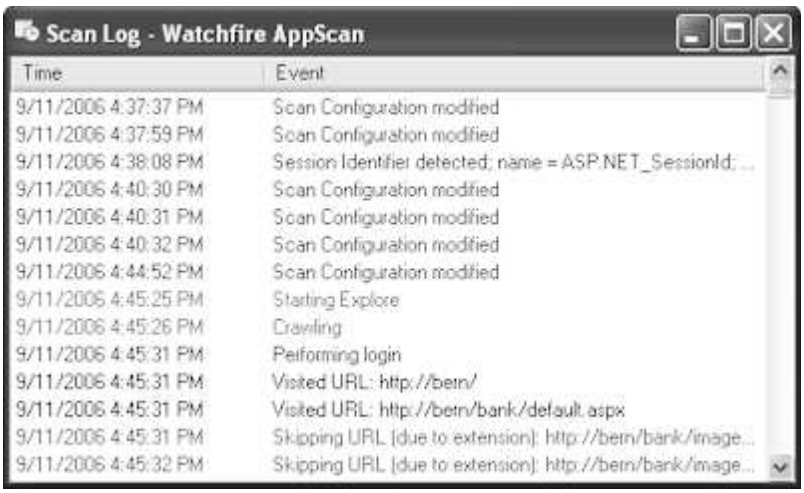
ログは、トラブルシューティングに役立ちます。

スキャン・ログ

このログは、現在のスキャン中に AppScan が実行するアクションをリストします。

スキャンの実行中、スキャン・ログはライブで更新されるので、任意の時点の AppScan が実行している内容を確認できます。

- ツールバーで「スキャン・ログ」アイコン  をクリックします



スキャン・ログはスキャンの一部として保存されます。保存されたスキャンがロードされると、既存のスキャン・ログもロードされ、スキャンが継続している間、そこにデータが追加されます。

注: スキャン・ログ・ウィンドウには、スキャン・ログに保存されていた以前のデータは表示されません。このデータは、実際のログ・ファイルでのみ確認できます。確認するには、圧縮ファイルを開くプログラムを使用してスキャン・ファイル (.SCAN) を開き、ScanLog.log を見つけて、このファイルをテキスト・ビューアーを使用して開きます。

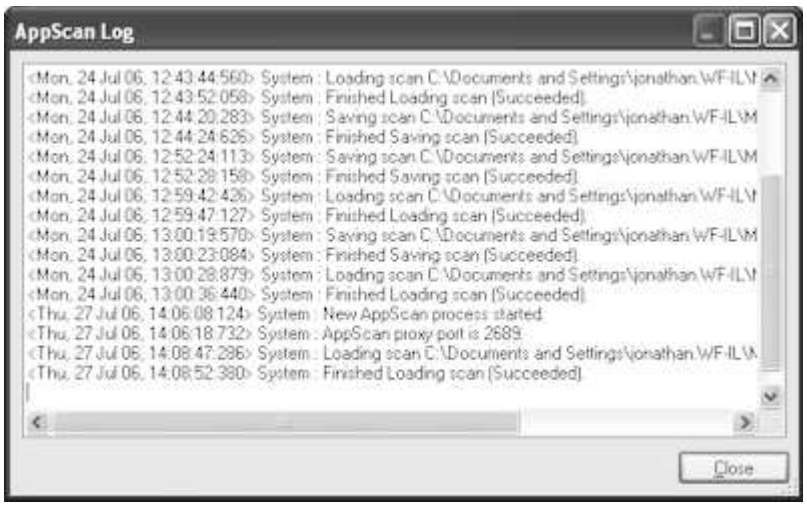
厳密にどの項目をスキャン・ログに含めるかを定義してスキャン・ログをカスタマイズしたり、スキャン・ログ・ウィンドウでの項目の色を制御したりすることができます (275 ページの『「スキャン・オプション」タブ』 を参照)。

関連がある場合は、メッセージの説明および推奨されるユーザー応答が 367 ページの『スキャン・ログ・メッセージ』 で説明されています。

AppScan ログ

このログには、エラー、接続、および AppScan システム・メッセージ (一般アプリケーション・イベントおよび警告) がリストされます。

- AppScan 内で AppScan ログを表示するには、「ヘルプ」 > 「**AppScan** ログ」をクリックします。



- このログの保存先を確認するには、「ツール」 > 「オプション」 > 「全般」タブ > 「ログ・ファイル」フォルダーをクリックします。

  Windows 7 では、デフォルトの場所は次のとおりです。

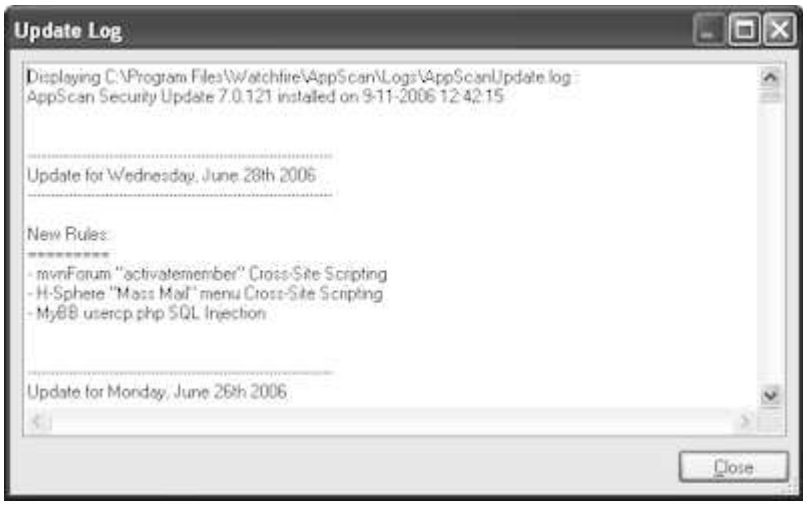
  ```
  ...\AppData\Roaming\IBM\AppScan Standard\Logs
  ```

関連がある場合は、メッセージの説明および推奨されるユーザー応答が 378 ページの『AppScanログ・メッセージ』 で説明されています。

更新ログ

このログには、インストール後のプログラムに対するすべての更新がリストされます。

- 更新ログを表示するには、「ヘルプ」 > 「ログの更新」をクリックします。



- このログの保存先を確認するには、「ツール」 > 「オプション」 > 「全般」タブ > 「ログ・ファイル」フォルダーをクリックします。

  Windows 7 では、デフォルトの場所は次のとおりです。

  ```
  ...\AppData\Roaming\IBM\AppScan Standard\Logs
  ```

以下も参照してください。

13 ページの『更新』

トラフィック・ログ

このログは、スキャン中の AppScan とサイトとの間の要求および応答をリストしているため、トラブルシューティング時に役立ちます。

トラフィック・ログには、スキャン中のアプリケーションのすべての要求および応答がリストされています。 AppScan はデフォルトでトラフィック・ログを保存しませんが、必要であれば、サポートに役立てるために有効にすることができます。

ログをオンにするとパフォーマンスに影響が及ぶ場合があるため、必要な場合にのみ有効にしてください。

- ログ・トラフィックを有効にするには、「ツール」 > 「オプション」をクリックして、「要求/応答のログ記録を有効にする」を選択します。
- このログの保存先を確認するには、「ツール」 > 「オプション」 > 「全般」タブ > 「ログ・ファイル」フォルダーをクリックします。

  Windows 7 では、デフォルトの場所は次のとおりです。

  ```
  ...\AppData\Roaming\IBM\AppScan Standard\Logs
  ```

検索結果

すべてのビューで特定のデータについて「結果リスト」をフィルタリングすることができます。

手順

1. ツールバーで「検索」をクリックするか、**Ctrl + F** を押します。

   「検索」バーは、画面の下部に表示されます。
2. 「アプリケーション・ツリー」でノードを選択します。
   - 「マイ・アプリケーション」ノードを選択すると、すべての結果について検索が行われます。
   - ツリー内のいずれかのノードを選択すると、選択したノードとそのサブノードについて検索が行われます。
3. 「検索」バーの「検索」テキスト・ボックスに、ストリングまたはストリングの一部を入力します。
4. 「表示」リストで、データ・タイプをクリックします。
5. 「ただちに検索」をクリックするか、**Enter** キーを押します。

   「結果リスト」に結果が表示されます。もともと表示されていたリストは上書きされます。カウンターが更新され、各カテゴリーの項目数が新しく表示されます。結果のないタブはグレー表示されます。

   別の「検索」ストリングを入力して「ただちに検索」を再度クリックすると、新規検索は、表示されている直前の検索結果についてではなく、「アプリケーション・ツリー」で選択されているノードについて実行されます。

   注**:** 全データが表示された、フィルタリングされていない「結果リスト」に戻すには、「消去」をクリックします。

第 12 章 統合

このセクションでは、その他のアプリケーションと AppScan Standard との統合について説明します。

AppScan Enterprise

このセクションでは、AppScan Standard 版と Enterprise 版の相互作用について説明します。

AppScan Enterprise 版は、集約化されたスキャン制御とユーザー・アクセス制御、修復機能、管理用ダッシュボード、コンプライアンス・レポート、および AppScan Standard とのシームレスな統合を提供します。組織で AppScan Enterprise を使用している場合、以下のことが可能です。

- ローカルの AppScan Standard ライセンスで使用できる許可だけでなく、AppScan Enterprise ユーザーの許可をインポートして使用する。
- AppScan Enterprise で作業するために、AppScan Standard のスキャン結果をエクスポート (「パブリッシュ」) する。
- AppScan Enterprise ジョブを作成する。

AppScan Enterprise ライセンス許可のインポート

AppScan Enterprise ライセンスによって許可されるサイトをスキャンするように AppScan Standard を構成します。

このタスクについて

自分が所属する組織が、ローカルの AppScan Standard ライセンスで許可されているユーザーに対して追加のサイトのスキャンを許可する AppScan Enterprise ライセンスを持っている場合、これらの許可をローカルのマシンにインポートして、既存のライセンスと共に使用することができます。これで、一方または両方のライセンスによって許可されるどの URL でもスキャンできるようになります。

注: このオプションは、AppScan Standard のフル・ライセンス (デモ・ライセンスではなく) がロードされる場合のみ使用可能です。

手順

1. 「ヘルプ」>「ライセンス」とクリックします。

   「ライセンス」ダイアログ・ボックスが開きます。
2. 「**AppScan Enterprise** ライセンスの追加」をクリックします。

   「AppScan Enterprise」ダイアログ・ボックスが開きます。
3. 「**AppScan Enterprise**」チェック・ボックスを選択します。

   フィールドが有効になります。
4. このチェック・ボックスを選択して、AppScan Enterprise サーバーのユーザー名、パスワード、ドメイン、および URL を入力します。
5. (オプション) ネットワークに接続済みであることを確認し、「設定の確認」ボタンをクリックします。

AppScan は AppScan Enterprise サーバーとの接続を確立し、組織のライセンスが下のペインに表示されます。

注: ローカル・クライアントが Enterprise サーバーと接続できなかった場合には、スキャンはローカル・ライセンスによって許可された IP に限定されるという通知を受け取ります。

6. 「**OK**」をクリックします。

独自の許可に加えて、AppScan Enterprise 許可が AppScan ライセンスにロードされます。

AppScan Enterprise へのパブリッシュ

AppScan Standard の結果を AppScan Enterprise にパブリッシュして、そこで処理することができます。

手順

1. 結果をエクスポートするスキャンを開きます。
2. 「ファイル」>「エクスポート」>「**AppScan Enterprise** にパブリッシュする **(Publish to AppScan Enterprise)**」をクリックします。

「ログイン」ダイアログ・ボックスが開きます。

3. AppScan Enterprise サインイン情報の構成:

ユーザー **ID** とパスワードでのサインイン:

a. 「ユーザー **ID** とパスワードでログイン」を選択します。
b. URL フィールドには、以下のように入力します。
   - **AppScan Enterprise 9.0.3.1** 以上: AppScan Enterprise サーバーのサービス URL を入力します。

     形式: `https://[AppScan Enterprise Server]:[Server port]/ase`
   - **AppScan Enterprise 9.0.3** 以下: AppScan Enterprise サーバーの SOAP サービス URL を入力します。

     形式: `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
c. 有効なユーザー ID (形式 `[domain name]\[username]` を使用) とパスワードを入力します。
d. 「ログイン」をクリックします。

クライアント側の証明書またはスマート・カードを使用してサインインするには、次のようにします。

a. 「クライアント側の証明書 / スマート・カードを使用してログイン」を選択します。
b. URL フィールドには、以下のように入力します。
   - **AppScan Enterprise 9.0.3.1** 以上: AppScan Enterprise サーバーのサービス URL を入力します。

     形式: `https://[AppScan Enterprise Server]:[Server port]/ase`
   - **AppScan Enterprise 9.0.3** 以下: AppScan Enterprise サーバーの SOAP サービス URL を入力します。

     形式: `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`
c. 必要な証明書のチェック・ボックスを選択します。

d. 「ログイン」をクリックします。

注: スマート・カードの PIN コードがログインに必要な場合は、ダイアログ・ボックスが表示されるので、入力してください。

「結果のパブリッシュ (Publish Results)」ダイアログ・ボックスが開きます。

4. ジョブ名と、オプションで AppScan Enterprise のフォルダーとアプリケーションを定義します。

注:

- フォルダー選択は SOAP にのみ適用され、AppScan Enterprise バージョン 8.7 からサポートされています。 フォルダーを選択しない場合、デフォルトの AppScan Enterprise フォルダーが使用されます。 REST サービス・フォルダーの場合、選択は適用されず、結果は選択したアプリケーションに保存されます。
- アプリケーション選択は、AppScan Enterprise バージョン 9.0 からサポートされています。
- 「アプリケーションの選択」ダイアログ・ボックスには、「サーバー上で新規アプリケーションを作成」オプションが含まれます (ユーザー権限で許可されている場合)。

5. 「発行」をクリックします。

プロセスが完了すると、ダイアログ・ボックスに緑色の成功メッセージが表示されます。これで、ジョブを AppScan Enterprise 内で開いて処理できるようになりました。

AppScan Enterprise でのジョブの作成

AppScan Standard 構成を使用して、AppScan Enterprise ジョブを作成することができます。

このタスクについて

スキャン構成を新規ジョブとして AppScan Enterprise にエクスポートし、AppScan Enterprise で処理することができます。

注: Security AppScan Enterprise Version 9.0 以降が必要です。

手順

1. 構成を使用したいスキャンを開きます。
2. 「ファイル」>「エクスポート」>「**AppScan Enterprise** でジョブを作成」をクリックします。

「ログイン」ダイアログ・ボックスが開きます。

3. AppScan Enterprise サインイン情報の構成:

ユーザー **ID** とパスワードでのサインイン:

a. 「ユーザー **ID** とパスワードでログイン」を選択します。

b. URL フィールドには、以下のように入力します。

- **AppScan Enterprise 9.0.3.1** 以上: AppScan Enterprise サーバーのサービス URL を入力します。

  形式: `https://[AppScan Enterprise Server]:[Server port]/ase`

- **AppScan Enterprise 9.0.3** 以下: AppScan Enterprise サーバーの SOAP サービス URL を入力します。

  形式: `http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx`

c. 有効なユーザー ID (形式 [domain name]\[username] を使用) とパスワードを入力します。
d. 「ログイン」をクリックします。

クライアント側の証明書またはスマート・カードを使用してサインインするには、次のようにします。
a. 「クライアント側の証明書 / スマート・カードを使用してログイン」を選択します。
b. URL フィールドには、以下のように入力します。
   - **AppScan Enterprise 9.0.3.1** 以上**:** AppScan Enterprise サーバーのサービス URL を入力します。

     形式: https://[AppScan Enterprise Server]:[Server port]/ase
   - **AppScan Enterprise 9.0.3** 以下**:** AppScan Enterprise サーバーの SOAP サービス URL を入力します。

     形式: http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx
c. 必要な証明書のチェック・ボックスを選択します。
d. 「ログイン」をクリックします。

   注**:** スマート・カードの PIN コードがログインに必要な場合は、ダイアログ・ボックスが表示されるので、入力してください。

「ジョブの作成」ダイアログ・ボックスが開きます。

4. ジョブ名と、オプションで AppScan Enterprise のフォルダーとアプリケーションを定義します。

   注**:** フォルダー選択は、AppScan Enterprise バージョン 8.7 からサポートされており、アプリケーション選択は AppScan Enterprise バージョン 9.0 からサポートされています。スキャン・テンプレート・フォルダーは表示されません。 フォルダーを選択しない場合、デフォルトの AppScan Enterprise フォルダーが使用されます。

   注**:** 「アプリケーションの選択」ダイアログ・ボックスには、「サーバー上で新規アプリケーションを作成」オプションが含まれます (ユーザー権限で許可されている場合)。
5. 構成にマニュアル探査データが含まれている場合、以下のオプションがあります。
   - フルスキャンを継続**:** AppScan は自動探査ステージを実行してから、すべての探査データをテストします(マニュアルと自動の両方)
   - テストのみ**:** 既存のマニュアル探査データのみテストされます。
6. 「作成」をクリックします。

   プロセスが完了すると、ダイアログ・ボックスに緑色の成功メッセージが表示されます。これで、結果を AppScan Enterprise 内で開いて処理できるようになりました。

AppScan Enterprise でのスキャン・テンプレートの作成

AppScan Standard 構成を使用して、AppScan Enterprise テンプレートを作成することができます。

このタスクについて

スキャン構成をテンプレートとして AppScan Enterprise にエクスポートし、AppScan Enterprise で処理することができます。

注**:** Security AppScan Enterprise Version 9.0 以降が必要です。

手順

1. 構成を使用したいスキャンを開きます。
2. 「ファイル」>「エクスポート」>「**AppScan Enterprise** でスキャン・テンプレートを作成」をクリックします。

   「テンプレートの作成」ダイアログ・ボックスが開きます。
3. AppScan Enterprise サインイン情報の構成:
   a. 有効なユーザー ID (形式 `[domain name]\[username]` を使用) とパスワードを入力します。
   b. URL フィールドに、AppScan Enterprise サーバーの URL を次のフォーマットで入力します。

      ```
      http://[AppScan Enterprise Server]/ase/desktop/permissions.asmx
      ```
   c. 「設定の確認」をクリックします。

   「ジョブの作成」ダイアログ・ボックスが開きます。
4. テンプレート名を定義し、AppScan Enterprise のフォルダーとアプリケーションを選択します。

   注**:** フォルダー選択は、AppScan Enterprise バージョン 8.7 からサポートされており、アプリケーション選択は AppScan Enterprise バージョン 9.0 からサポートされています。テンプレート・フォルダーのみが表示されます。 フォルダーを選択しない場合、デフォルトの AppScan Enterprise フォルダーが使用されます。

   注**:** 「アプリケーションの選択」ダイアログ・ボックスには、「サーバー上で新規アプリケーションを作成」オプションが含まれます (ユーザー権限で許可されている場合)。
5. 「作成」をクリックします。

   プロセスが完了すると、ダイアログ・ボックスに緑色の成功メッセージが表示されます。これで、テンプレートを AppScan Enterprise 内で開いて処理できるようになりました。

自動化フレームワーク

QA 自動化フレームワーク (Selenium など) のために記述されたスクリプトを使用して、AppScan スキャンでマニュアル探査記録を作成することができます。

QA 担当員が Web アプリケーションで機能テストを実行する際に自動化フレームワークを使用する場合、すでに作成済みのスクリプトを使用して、それぞれに適したスキャンを作成できます。自動化フレームワークからアプリケーションへの要求は、プロキシーとして AppScan を使用して送信されるので、AppScan では独自のスキャンの探査ステージとしてそれらのアクションを記録できます。 次に AppScan はその探査ステージをベースにしてサイトをテストします。 これは AppScan CLI を使用して行われます。

原則として、以下のバッチ・コマンドを作成して実行します。

1. AppScan を開いて以下を構成します:
   a. 開始 URL
   b. ユーザー資格情報
   c. テストのみ
   d. 特定の listen ポートで AppScan のプロキシーを開く。
2. 同じポートを使用して自動化フレームワーク・スクリプトを実行する。
3. スクリプトの終了時、AppScan のプロキシーを閉じると、テスト・ステージが開始する。

4. スキャン結果を保存し、オプションでレポートを作成して保存する。

以降のセクションでは Selenium を使用して AppScan デモ・テスト・サイトをテストする方法を説明しますが、この処理は、どのようなサイトおよび自動化フレームワークに対しても簡単に適用できます。

バッチ・コマンドの作成

この例は、探査ステージで Selenium スクリプトを使用してスキャンを実行します。 同じ原則をその他の自動化フレームワークに対しても適用できます。

このタスクについて

Selenium スクリプトを使用し、ポート 56232 が Selenium と AppScan Standard 間の通信に使用されるものとします。当然、これは必要に応じて変更できます。

注: 各コード・サンプルでは、そのステップに追加されたコードが太字で強調表示されています。

このサンプルをご自分で使用する場合には、ここで使用するファイルが含まれるフォルダーが以下の場所にあります。

```
[AppScan Standard installation folder]\Docs\Selenium Example
```

注: AppScan フォルダーのパスが異なる場合、JAR ファイル内の該当するパスを変更する必要があります。

手順

1. TXT ファイルを作成して、テキスト・エディターで開きます。
2. AppScan コマンドを入力して AppScan を開き、開始 URL、ログイン資格情報、「テストのみ」オプション、オープン・プロキシー、プロキシー listen ポートを定義します。

   ```
   START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
   /starting_url "https://demo.testfire.net"
   /credentials "jsmith:demo1234"
   /test_only
   /opr
   /lp "53262"
   ```

   ヒント: 特定のテスト・ポリシーを定義するコマンドやレポートを作成するコマンドなど、必要に応じてコマンドを追加できます (詳細は、 387 ページの『第 15 章 CLI』を参照)。
3. AppScan が開くための時間を確保する 15 秒のタイムアウトのバッチを追加します。

   ```
   START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
   /starting_url "https://demo.testfire.net"
   /credentials "jsmith:demo1234" /test_only /opr /lp "53262"

   timeout /t 15
   ```
4. Selenium スクリプトを追加します。

   ```
   START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
   /starting_url "https://demo.testfire.net"
   /credentials "jsmith:demo1234" /test_only /opr /lp "53262"

   timeout /t 15

   java -jar selenium-server-standalone-2.52.0.jar -trustAllSSLCertificates -htmlSuite "*firefox" "https://demo.testfire.n
   ```

   重要: Selenium の開始 URL は、AppScan テンプレートの開始 URL と同一でなければなりません。

5. Selenium がその要求を送信する AppScan プロキシーのポートとホストを Selenium スクリプトに挿入します。

```
START "" "[AppScan Standard installation folder]\AppScanCMD.exe"
/starting_url "https://demo.testfire.net"
/credentials "jsmith:demo1234" /test_only /opr /lp "53262"

timeout /t 15

java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=56232 -Dhttps.proxyHost=localhost -Dhttps.proxyPort=56232 -jar selen
-htmlSuite "*firefox" "https://demo.testfire.net" "mytestsuite.html" "results.html"
```

6. 最後の個所に、AppScan プロキシーを閉じてテスト・ステージを開始するためのコマンドを追加します。

```
START "" "[AppScan Standard installation folder]\AppScanCMD.exe" /scan_template
" C:\Users\<username>\Documents\AppScan\QA Automation Demo Template.scant " /test_only /opr /lp
"56232"

timeout /t 15

java -Dhttp.proxyHost=localhost -Dhttp.proxyPort=64345 -Dhttps.proxyHost=localhost
-Dhttps.proxyPort=56232 -jar selenium-server-standalone-2.52.0.jar -trustAllSSLCertificates
-htmlSuite "*firefox" "https://demo.testfire.net" "mytestsuite.html" "results.html"

"[AppScan Standard installation folder]\AppScanCMD.exe" cpr
```

7. このファイルを保存し、コマンド・ラインを使用して実行します。

タスクの結果

Selenium が開いてサイトを探査します。その後 AppScan がテストを開始します。 スキャンの完了時に AppScan は、そのスキャンをバッチ・ファイルと同じフォルダーに保存します。

重要: 何らかの理由でプロセスが完了しなかった場合、または完了前にプロセスを停止した場合には、Internet Explorer や Chrome ブラウザーのプロキシー設定が変更される場合があります。その場合、変更は手動で元に戻す必要があります。

Application Security on Cloud

このセクションでは、クラウド上のアプリケーションをスキャンするために、AppScan Standard が IBM と対話する方法について説明します。

この機能を使用するには、Application Security on Cloud アカウントが必要で、1 つ以上のアプリケーションが作成されている必要があります。

ご使用のサイトにインターネットからアクセスできない場合、Application Security on Cloud が接続に使用できる、サイトおよびインターネットにアクセス可能な AppScan Presence が作成されている必要があります。

詳しくは、Application Security on Cloud 資料を参照してください。

へのアップロード Application Security on Cloud

AppScan Standard スキャンやテンプレート・ファイル (SCAN または SCANT) をIBM Application Security on Cloud をアップロードし、クラウド上で新規スキャンを実行することができます。

手順

1. アップロードするスキャンあるいはテンプレートを開きます。

2. 「ファイル」>「エクスポート」>「**Application Security on Cloud** へのスキャンのアップロード」をクリックします。
3. キー ID およびキーの秘密を使用してログインします。
4. 「アプリケーションの選択」をクリックし、リストから既存のアプリケーションを選択して、「選択」をクリックします。

   「スキャンの実行」ダイアログ・ボックスが開きます。
5. 「スキャンの設定」 エリア:オプションでスキャン名を変更し、スキャンの完了時に通知されるようにチェック・ボックスを選択することができます。
6. プライベート・サイトのスキャンエリア:サイトがインターネット上で使用できない 場合のみチェック・ボックスを選択し、リストからご使用の AppScan Presence を選択します。
7. テスト・オプションエリア:以下の 2 つのラジオ・ボタンのいずれかを選択します。

   テストのみ
   : AppScan Standard で既に探査済みのサイトの部分をテストします。このオプションは、AppScan Standard に記録したマルチステップ操作またはマニュアル探査のみをテストしたい場合に使用します。テスト・ステージは、アップロードするファイルの既存の探査データに対して実行されます。

   フル・スキャン
   : 探査ステージを続行 (データをファイルに保存された既存の探査データに追加) し、テスト・ステージを実行します。アップロードしたファイルに含まれている探査データのデータが使用されていたり、探査データにデータが追加された場合に、そのデータを無視するには、「テストのみ」を選択する必要があるので注意してください。
8. 「アップロードおよび実行」をクリックします。

   通知により、アップロードが正常に完了したことが確認されます。スキャンは即時に開始されますが、スキャン状態は Application Security on Cloud からしか確認できません。

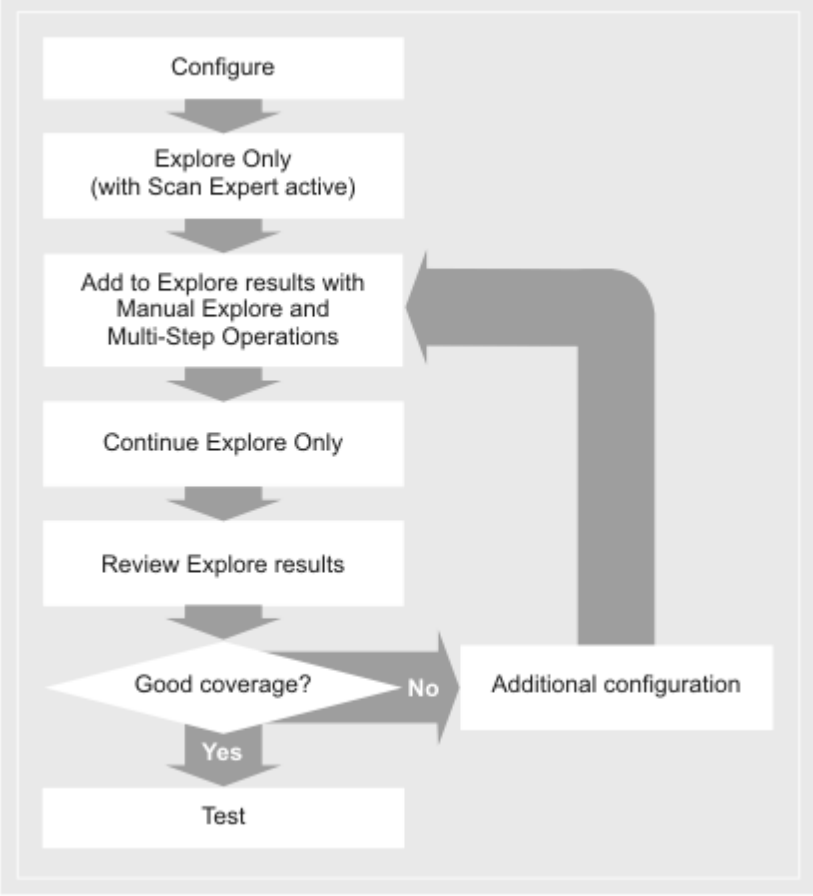
第 13 章 ベスト・プラクティスおよび FAQ

このセクションでは、上級ユーザー向けのベスト・プラクティスおよびユース・ケースと、よくある質問について説明します。

上級ユーザー用のワークフロー

このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

テスト・ステージと、それに伴ってスキャン自体が成功するかどうかは、探査ステージで設定する範囲によって決まります。探査ステージでアプリケーション・ロジックの重要な部分を見落とすと、存在する可能性のある重要な脆弱性をテスト・ステージで検出することはできません。以下のワークフローに従って操作することで、探査ステージで設定する範囲を改善することができます。



タスク	説明
1.初期構成	ウィザードまたは「スキャン構成」ダイアログ・ボックスを使用して、以下の操作を行います。 1. 開始 URL を定義します。 2. ログイン手順を記録します。 3. セッション内パターンを検証し、必要に応じて新規パターンを選択します。 4. サイトがアカウントのロックアウト機能を備えている場合は、この機能を無効にするか、ログイン・ページをテストしないように AppScan を構成します。これを行わないと、テスト・ステージの途中で AppScan がサイトからロックアウトされ、以降の手順に進むことができなくなります。 このステップについて詳しくは、 333 ページの『初期構成』 を参照してください。
2.探査のみ	以下の手順に従って、初期の自動探査を実行します。 1. ツールバーで、  > 「探査のみ」 をクリックし、新しい探査ステージを完了させます。AppScan はサイトを探査しますが、テストは行いません。探査ステージの開始時にスキャン・エキスパートが実行されます。このとき、構成の変更がいくつか表示される場合があります。デフォルト設定では、自動的に適用可能な変更だけが、スキャン・エキスパートによって行われます。 **注:** サイトが URL の再書き込みを使用する場合、探査の最適化 (「ツール」 > 「エクステンション」 > 「探査の最適化モジュール:実行) を実行し、エクステンションによって推奨される場合は Automatic Explore ステージを再度実行します (「スキャン」 > 「再探査」)。 2. AppScan がセッション外になったことが原因で探査が途中で終了した場合は、セッション内検出とセッション ID 追跡に特に注意して、ログイン手順の再記録と再構成を行ってください。 このステップについて詳しくは、 334 ページの『初期自動探査』 を参照してください。
3.ブラウザーを使用したサイト範囲の手動による改善	以下の手順に従って、自動探査で検出されなかった URL を追加します。 1. マニュアル探査: 「マニュアル探査」を使用して、個別のページ (特定の入力が必要なページなど) を追加します。 **注:** 標準装備のブラウザーでアプリケーションを参照できない場合がまれにありますが、その場合は、別のブラウザーを使用するように AppScan を構成することができます。 2. マルチステップ操作: サイトの一部にアクセスする際に特定の順序でリンクをクリックする必要がある場合は、 1 つ以上のマルチステップ操作を記録します。 このステップについて詳しくは、 335 ページの『手動によるサイト範囲の改善』 を参照してください。
4.探査のみを継続	多くの場合、マニュアル探査で入力した新しいデータにより、自動探査でさらに詳細にアプリケーションを探査できるようになります。 **注:**  > 「自動探査の継続」 (または 「スキャン」 > 「探査のみ」) をクリックして、初期探査結果とマニュアル探査データを保存します。「再スキャン」>「再探査」はクリックしないでください。これをクリックすると、既存のデータが削除されます。
5.探査結果の評価	これまでの結果を検討して、これまでに実行した探査でアプリケーション・ロジックが十分にカバーされているかどうかを確認します。 **注:** 構成を変更した場合は、自動探査を再度実行する必要があります (「スキャン」>「再探査」)。 このステップについて詳しくは、 337 ページの『探査結果の評価』 を参照してください。

タスク	説明
6.(必要な場合) 追加の構成	これまでに設定したアプリケーションの範囲が十分でない場合は、いくつかの追加の構成オプションを検討する必要があります。 このステップについて詳しくは、 339 ページの『追加の構成』 を参照してください。
7.テスト・ステージ (Test stage)	「テストのみ」をクリックしてテスト・ステージへ進み、スキャンを完了します。

初期構成

このタスクについて

手動か自動かを問わず、サイトの探査を開始する前に、以下の基本構成ステップを実行してください。

手順

1. スキャンの開始 **URL** を定義して確認します。
   a. 「ファイル」>「新規」をクリックし、ウィザードを使用して新規 Web アプリケーション・スキャンを作成します (または、構成ダイアログ・ボックスを使用して、「スキャン構成」>「**URL** およびサーバー」ビューで構成します)。
   b. スキャンの開始 URL を入力します。
   c. アプリケーションが大文字と小文字を区別する場合は、「大文字と小文字を区別するパス」チェック・ボックスが選択されていることを確認します。

      一般的に、Linux ベースのオペレーティング・システムで実行されるアプリケーションは大文字と小文字を区別する傾向にありますが、Microsoft Windows で実行されるアプリケーションは大文字と小文字を区別しません。 Java ベースのアプリケーションは例外で、どのオペレーティング・システムでも大文字と小文字を区別する傾向にあります。
   d. 「URL」フィールドの隣にある「ブラウザーで表示」アイコンをクリックして、必要なページが AppScan ブラウザーに表示されることを確認します。
2. ログイン手順を記録します。 これにより、スキャンを開始するため、およびスキャン中にログアウトされるたびに、AppScan がアプリケーションにログインできるようになります。
   a. ウィザードのステップ 2 で (または「スキャン構成」>「ログイン管理」ビューで)、 

をクリックして、アクションの記録を開始します。ブラウザーが開き、上記で定義した開始 URL が表示されます。
   b. アプリケーションにログインするためにユーザーが実行する必要があるすべてのステップを実行します。
   c. ページ上で、ログインしたユーザーにのみ表示される「ようこそ [ユーザー名]」や「ログアウト」リンクなど、正常にログインしたことを確認できる表示を探します。
   d. ブラウザーを閉じて緑色の鍵アイコン  を探し、セッション内パターンが特定されたことを確認します。

      赤い  アイコンが表示されている場合、セッション内パターンは検出されていないため、手動で定義する必要があります (「 63 ページの『「検出パターン」ダイアログ・ボックスを選択します。』」を参照してください)。

注: 一般に、応答にセッション内パターンが含まれる最初の URL は「セッション内 URL」であり、これは自動的に選択されている URL ですが、状況によっては、後で URL を選択することでパフォーマンスが向上する場合があります (64 ページの『セッション内検出の最適化』を参照してください)。

3. セッション内パターンを確認します。 セッション内パターンは、ログインの成功後にユーザーに表示される、ページ上のパターンまたはストリング (「ようこそ [ユーザー名]」や「ログアウト」リンクなど) に一致する正規表現です。緑のアイコンが表示されている場合でも、このパターンを確認してください。
   a. ウィザードのステップ 2 で「セッション内検出オプションを構成します」を選択してから、「次へ」をクリックします (または「スキャン構成」>「ログイン管理」>「詳細」ビューに移動します)。

      ログイン手順が表示されます。
   b. 「セッション内」とマークが付けられたページ上をダブルクリックして、ブラウザーで開きます。
   c. ブラウザーで「要求/応答」タブをクリックしてソース・コードを表示し、選択されたパターンが実際にセッション内状態を示していることを確認します。

      注: ページ・コンテンツが JavaScript または CSS の場合は、どのような場合でもセッション内ページとして適切ではないため、別のページを選択する必要があります。

   緑の鍵アイコンが表示されているが、選択されたパターンがセッション内パターンではない 場合は、359 ページの『要求ベースのログインのトラブルシューティング』を参照してください。
4. ロックアウト構成を設定します。 テスト・ステージで、AppScan は多数の無効なログイン試行を行います。無効なパスワードが一定回数入力されるとユーザーをロックアウトするアカウント・ロックアウト機能をサイトが備えている場合、AppScan はロックアウトされ、スキャンを完了できなくなります。
   - アカウント・ロックアウトを無効にします。無効にするのが難しい場合は、以下の処理を行います。
   - ログイン・ページとログアウト・ページをテストしないように AppScan を構成します (「スキャン構成」>「テスト・オプション」で、「ログイン・ページとログアウト・ページに関するテストを送信する」を選択解除します)。

関連概念:

331 ページの『上級ユーザー用のワークフロー』
このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

初期自動探査

基本構成を行った後に初期自動探査を実行して、AppScan がこの段階でサイトをどの程度カバーしているかを確認できます。

このタスクについて

フル・スキャンは探査とテストの両ステージから構成されていますが、ここでは、探査ステージのみを実行します。

初期構成に基づいたサイト範囲は不完全な場合がありますが、サイトのどの部分が検出されてどの部分が検出されないのかを確認することで、構成を改善することができます。

手順

1. 「スキャン」>「探査のみ」をクリックします。

   スキャン・エキスパートが、探査ステージの前に自動的に実行されるように構成されます。
2. スキャン・エキスパートが構成の変更を推奨した場合は、その推奨に従います。

   注: 自動的に実装できる変更もありますが、ユーザーの入力を必要とする変更もあります。
3. 停止するまで AppScan にサイトを探査させます。スキャン中に、サイトがクロールされていくにしたがって、アプリケーション・ツリーとデータ設定されていくのを確認することができます。
4. 探査ステージが正常に終了し、AppScan がセッション外になったことが原因で途中で終了することがなかったことを確認します。

   注: AppScan がセッション外になったことが原因で途中で終了した場合は、セッション内検出とセッション ID 追跡に特に注意して、ログイン手順の再記録と再構成を行ってください。
5. (URL 再書き込みを使用するサイト:) サイトで URL 再書き込みを使用している場合は、このステージで探査結果から不要な URL を取り除くことで、探査の最適化モジュールによってスキャンの効率を改善することができます。
   a. 「ツール」>「エクステンション」>「探査の最適化モジュール: 実行
   b. プロセスの最後にモジュールによって推奨された場合は、「スキャン」>「再探査」をクリックします。

   重要: サイトが URL 再書き込みを使用していることが確実でない場合は、このステップは実行しないでください。

関連概念:

331 ページの『上級ユーザー用のワークフロー』
このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

手動によるサイト範囲の改善

初期自動探査ステージで見逃した URL (特定の入力を必要とするフォームによってアクセスされる URL などの個別 URL と、買い物かごなど、順序付けられた URL シーケンスの両方) を追加できます。

このタスクについて

いくつかの理由により、最初にユーザーからの入力がない限り、AppScan はサイトの特定の部分を自動的にクロールすることはできません。

- 特定の入力を必要とするフォームをアプリケーションが持っている場合は、マニュアル探査機能を使用して当該ページにナビゲートして、必要なデータを入力することができます。このデータは自動フォーム入力で記録され、スキャン時に使用されます。
- アプリケーションで Javascript、Java アプレット、または Flash を使用していて、特定の状態シーケンスの後の特定の状態でのみ表示されるリンクがある場合、自動探査はこうしたリンクを見逃してしまう可能性があります。マニュアル探査を使用してこうしたリンクにアクセスすると、AppScan でそのリンクをテストし、リンク先のリンクもテストすることができます。
- リンクを示す Java アプレットをアプリケーションで使用している場合は、ユーザーが手動で探査しない限り、AppScan はこうしたリンクをテストしません。

- 特定の順序 でリンクをクリックしない限りサイトの特定の部分に到達できない場合は (買い物かごなど)、マルチステップ操作を記録する必要があります (「スキャン構成」「マルチステップ操作」ビュー)。

手順

1. マニュアル探査機能を実行します。 この機能は、自動探査中に検出されず、特定のコンテキストなしでアクセスできる URL を追加する場合に使用します。
   a. ツールバーで「マニュアル探査」をクリックします。

      AppScan 組み込みブラウザーが開きます。

      注**:** アプリケーションがブラウザーに正しく表示されない場合は、アプリケーションが AppScan 組み込みブラウザー用に最適化されていない可能性があります。その場合は、別のブラウザーを使用するように AppScan を構成することができます。 355 ページの『デフォルト・ブラウザーの変更』を参照してください。
   b. テストするリンクをクリックし、データを入力し、できる限り多くの機能をカバーすることにより、アプリケーションをブラウズします。
   c. 終了したら、(タイトル・バーの X ボタンをクリックして) ウィンドウを閉じます。

      「マニュアル探査」ウィンドウが開きます。
   d. 「エクスポート」をクリックして保存することにより、今後のスキャン用にデータを保存します。
   e. データを現在のスキャンに追加するには、「すべて追加」を選択して「**OK**」をクリックします。
   f. 新規ページがロードされたら、ツールバーで「スキャン」**>**「探査のみを継続」をクリックします。

      AppScan これで、 は、マニュアル探査で検出された新規リンクを探査します。
   g. 探査が終了したら、アプリケーション・データを確認して、必要な範囲が探査によってカバーされていることを確認します。
2. マルチステップ操作を実行します。 この機能は、特定の順序でアクセスする必要がある URL シーケンスを記録する場合に使用します。
   a. 「スキャン構成」**>**「マルチステップ操作」ビューを開きます。
   b. 赤い「記録の開始」ボタンをクリックし、「ログインして記録」を選択します。
   c. アプリケーションにログインして、記録したいプロセス (買い物かごへのアイテムの追加やチェックアウトなど) を実行します。

      注**:** 記録したくないリンクをクリックする必要がある場合は、「一時停止」をクリックします。記録を再開する場合は、もう一度「一時停止」をクリックします。
   d. ブラウザー・ウィンドウを閉じます。
   e. シーケンス内のパラメーターの一部で固有値が必要な場合は、 105 ページの『シーケンス変数』または技術情報

      『Using Variables in Multi-Step Operations』を参照してください。

関連概念:

331 ページの『上級ユーザー用のワークフロー』
このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

149 ページの『AppScan の使用』
マニュアル探査を使用すると、実行中にフィールドおよびフォームを入力しながらアプリケーションの特定の部分を探査することができます。 この方法を使用することで、サイトの特定のエリアが確実にカバーされ、AppScan では、すべてのフォームへの正しい入力に必要な情報を得ることができます。

関連資料:

98 ページの『「マルチステップ操作」ビュー』
「構成」ダイアログ・ボックスの「マルチステップ操作」ビューは、リンクを特定の順序でクリックすることによってのみ到達できるサイトの部分をテストするためのビューです。

探査結果の評価

テスト・ステージに進む前に、探査結果を確認します。これは、探査ステージでサイトの重要な領域が見逃された場合、テスト・ステージではそれらの領域がテストされないためです。

このタスクについて

探査ステージの結果は、3 つのデータ・ビュー・ペインに表示されます。探査ステージでの処理が正常に実行され、アプリケーションの十分な範囲がカバーされているかどうかを評価するためのいくつかのヒントを以下に示します。

注**:** このステージで構成変更を行った場合は、テスト・ステージを開始する前にアプリケーションを再探査する必要があります。

手順

1. スキャン・ログ機能を実行します。この機能は、AppScan が頻繁にセッション外になっていないかどうかを確認する場合に使用します。
   a. 「表示」>「スキャン・ログ」をクリックします。
   b. ログ項目をスクロールダウンして、AppScan が頻繁にセッション外になっていないかどうかを確認します。

   AppScan が 5 分間に数回を超えてセッション外になっている場合は、セッション内検出構成に特に注意して、記録されたログインの再記録と再構成を行うことをお勧めします。
2. アプリケーション・ツリーを使用します。これは、検出および探査された、サイトのすべての領域を示すグラフィカル表現です。サイトがどの程度カバーされているかを確認するために使用します。
   a. アプリケーション・ツリーは、アプリケーションの階層構造とメインページを正確に示していますか?
   b. ツリー内にログイン URL はありますか? (存在しない場合、ログインは送信されていません)
   c. 認識された URL の総数 (左下隅に表示) は、把握している実際のサイト・サイズに一致していますか?
   d. テスト・ステージで送信するための妥当な数のテストが作成されていますか? (URL の数の 5 倍以上のテストが必要です)
3. 送信された要求を確認します。探査ステージで送信された要求の確認と検証を行います。
   a. データ・ペインで「要求」ビューを選択して、送信されたすべての要求を表示します。
   b. このリストにログイン URL が表示されていることを確認します (特に、セッション内要求と、ユーザー資格情報が含まれたログイン要求)。
   c. ログイン手順で、ログイン要求の後に表示されている要求のいくつかを確認します。応答にエラーが含まれていないことを確認します。これを行うには、詳細ペインの検索フィールドに単語

「error」を入力してから、上部パネルで URL を 1 つずつ選択します。特定の応答に単語「error」が含まれている場合は、検索フィールドの色が赤 (「見つからない」) から緑 (「見つかった」) に変わり、応答本文で単語「error」が強調表示されます。

d. これらの要求にエラー・ストリングが含まれている場合は、ユーザーがセッション外になったため、ログイン手順が正しく記録されなかったことを示しています。その場合は、ログイン手順をもう一度記録します。

4. 「アプリケーション・データ」ビューを使用します。これはテスト・ステージのデフォルト・ビューで、ペインの上部に並んだフィルターをクリックすると、各種ビューが表示されます。
   a. F2 をクリックするか、ツールバーの右側にあるデータ・アイコンをクリックして、このビューを開きます。
   b. データ・ペインの上部でフィルターを選択して情報を表示します。
   c. データ・ペイン内の項目をクリックして、その項目の詳細を詳細ペインに表示します。
5. カスタム・エラー・ページを使用します。4xx 応答は、エラー・ページとして自動的に識別されます。サイトがカスタム・エラー・ページを使用して 2xx 応答を返す場合は、この応答を認識するように AppScan を構成する必要があります。この情報は、テストの成功を判断する上で必要不可欠な情報です。カスタム・エラー・ページを構成しないと、誤検出と検出漏れの両方が発生し、結果が不正確なものになります。そのため、応答に単語「エラー」が含まれているにもかかわらず、エラー・ページとして分類されなかったページが前のステップで見つかった場合は、そのページをここで構成します。
   a. 詳細ペインで「ブラウザーで表示」をクリックして、対象のページが実際にエラー・ページであることを確認します。
   b. 「エラー・ページとして設定」をクリックします。

      注**:** 「スキャン構成」**>**「エラー・ページ」でエラー・ページを定義することもできます。その場合、正符号 (+) アイコンをクリックし、ストリング、正規表現、URL、またはページを定義します。
6. フィルタリングされた **URL** を確認します。送信されなかった 要求のリストを確認して、送信する必要があった 要求が含まれていないことを確認します。
   a. データ・ペインで「フィルタリングされた **URL**」ビューを選択して、フィルタリングされた URL が実際にフィルタリングする必要がある URL であることを確認し、正しく分類されていることを確認します。
   b. ドメインが原因で URL が間違って除外されている場合は (「未テストの Web サーバー」)、そのドメインをスキャンに追加します (「構成」**>**「**URL** およびサーバー」**>**「追加のサーバーおよびドメイン」**>**「**+**」)。
   c. 「パスの制限」に到達したことが原因で URL が間違って除外されている場合は、以下の構成変更のいずれかを行うことをお勧めします。

      - 冗長なパスの制限を増やす (「構成」**>**「探査オプション」**>**「冗長なパスの制限」)

      - デフォルトの冗長性調整を調節する (「パラメーターおよび **Cookie**」**>**「冗長性調整のデフォルト」)

      - 個別パラメーターの冗長性調整を調節する
7. パラメーター・ベースの移動を行います。 サイトのすべてまたは一部で単一の URL を送信するが、異なるパラメーターでコンテンツと構造を制御する場合は、 340 ページの『パラメーター・ベースの移動を使用するサイト』を参照してください。

8. パラメーターを確認します。データ・ペインで、探査ステージで検出されたパラメーターを確認します。
   a. データ・ペインで「パラメーター」ビューを選択して、探査ステージで検出されたすべてのパラメーターを表示します。
   b. 必要に応じて、定義を更新します (「構成」>「パラメーターおよび **Cookie**」)。
9. 失敗した要求。 これは、応答状態が 4xx (「エラー」) の要求です。このリストを確認して、適切な要求が予期せずエラー応答を受け取っていないかどうかを確認します。
   a. 「データ」ペインで「失敗した要求」ビューを選択します。
   b. **404 Not Found:** 「ブラウザーで表示」をクリックして、URL が存在しないことを確認します。
   c. **Timeout** または **Connection Failed:** スキャンのタイムアウト (「構成」>「通信およびプロキシー」>「タイムアウト」) を長くする必要があるのか、サイトのサーバーまたは環境を改善する必要があるのか、接続の問題の原因が要求が同時に送信されていることにあるのか (「構成」>「通信およびプロキシー」>「スレッドの数」を選択して、設定を「1」に減らす)、あるいは、一定時間に送信される要求が多すぎることにあるのか (「構成」>「通信およびプロキシー」>「要求率の制限」) を判断します。
   d. **401** または **407 Authentication Required:** これは、HTTP 認証を必要とするアプリケーション領域が存在することを意味します (「構成」>「プラットフォーム認証」で設定)。
   e. その他の **4xx** 状態**:** ユーザーがログインしていなかったことが原因でサイトがエラーを返したのかどうかを確認します。必要に応じて、ログイン手順を再度記録します (「構成」>「ログイン管理」)。
10. 初期探査結果の確認後にその範囲が不十分であると感じた場合は、考えられる構成変更について次のセクションを参照してください。『追加の構成』を参照してください。

関連概念:

331 ページの『上級ユーザー用のワークフロー』
このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

340 ページの『パラメーター・ベースの移動を使用するサイト』
単一の URL を使用してすべてのページにアクセスできるサイトでは、特定のスキャン構成が必要です。

関連タスク:

『追加の構成』
初期探査ステージでのサイト範囲が不十分であった場合に検討すべきいくつかの構成変更を以下に示します。

追加の構成

初期探査ステージでのサイト範囲が不十分であった場合に検討すべきいくつかの構成変更を以下に示します。

このタスクについて

初期探査ステージでのサイト範囲が不十分であったか、30 分を超える時間がかかった場合は、パラメーターと Cookie 定義に対して、以下の考えられる構成変更の一部またはすべてを行うことをお勧めします。

手順

1. 「構成」>「パラメーターおよび **Cookie**」ビューをクリックします。

2. 追跡の設定を確認します。 サイトで Cookie (ユーザーがログインするたびに更新されるセッション ID など) を追跡している場合は、Cookie が正しく定義されていることを確認する必要があります。
   a. サイトの Cookie とパラメーターが識別されていて、メインの「パラメーターおよび Cookie」タブにリストされており、「追跡対象」として設定されていることを確認します。
   b. 必要であれば、  アイコンをクリックして、追加のパラメーターと Cookie を定義します。詳細については、 80 ページの『パラメーター定義』を参照してください。
3. 冗長性調整を行います。 冗長性調整を注意深く行うことで、スキャンの範囲と正確性を一切損なうことなく、スキャン時間を大幅に短縮することができます。冗長性調整を確認して、不要な重複要求は送信せず、必要な要求だけを送信するようにします。詳細については、 85 ページの『冗長性調整』を参照してください。
   a. 構成したい Cookie またはパラメーターがリストされていない場合は、  アイコンをクリックして定義します。
   b. 各 Cookie または各パラメーターの設定が適切であることを確認します。
4. セッション **ID** の検証を行います。 正確なセッション ID 定義は、AppScan が探査ステージで適切な要求を作成するために重要です。
   a. すべてのセッション ID の追跡設定が「ログイン値」として正しく定義されていることを確認します。
   b. 「ログイン値」として設定されたすべてのパラメーターがセッション ID であることを確認します。
5. 「パラメーターおよび Cookie」の定義を変更した場合は、アプリケーションを再探査します。マニュアル探査とマルチステップ操作の再記録が必要になる場合もあります。

78 ページの『「パラメーターおよび Cookie」ビュー』
「構成」ダイアログ・ボックスの「パラメーターおよび Cookie」ビューです。

80 ページの『パラメーター定義』

83 ページの『セッション ID』

85 ページの『冗長性調整』
冗長性調整を慎重に行うことで、スキャン時間を大幅に短縮できます。

331 ページの『上級ユーザー用のワークフロー』
このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

パラメーター・ベースの移動を使用するサイト

単一の URL を使用してすべてのページにアクセスできるサイトでは、特定のスキャン構成が必要です。

「パラメーター・ベース」の移動を使用するサイトは、1 つの URL (コントローラー) のみが送信されるサイトですが、URL にさまざまなパラメーターを指定すると、さまざまなコンテンツおよび構成が返されます。(このようなサイトのことを、サポート・チームが「メガスクリプト」サイトと呼ぶことがあります。)

- 以下の例のように、一部のサイトでは、すべての「ページ」について URL が実質的には同じままである場合があります。

```
http://site.com/content.aspx?PageName=page1
```

```
http://site.com/content.aspx?PageName=page2
```

- 他のサイトでは、すべてのリンクが、GET パラメーターを使用する単一のプロキシー・ページによってダイレクトされます。以下に例を示します。

  ```
  http://site.com?default.aspx/redirect=page1
  ```

  以下にリダイレクトされます。

  ```
  http://site.com/page1.aspx
  ```

  同じ URL が毎回送信されるため、前の場合と同じ問題が AppScan で発生します。
- ASP.NET 2.0 ポストバック・リンクの場合、各リンクは、そのリンクが張られているページへの POST 要求を生成します。

  この場合も、AppScan で同じ問題が発生します。

いずれの場合も、すべての「ページ」の要求が同じ URL に送信されます。デフォルトの構成ではスキャンが不完全になるため、AppScan から特殊な処理を行う必要があります。

パラメーター・ベースの移動を使用するサイトをスキャンするには、以下のようにします。

1. スキャンの作成時に、「標準的なスキャン」テンプレートではなく、「パラメーター・ベースの移動」テンプレートを選択します。
2. サイトのナビゲーション・パラメーターが正しく定義されていることを確認するために、「スキャン」>「スキャン構成」>「パラメーターおよび **Cookie**」を選択して、リスト内の最後のパラメーターを定義する正規表現にサイトのナビゲーション・パラメーターが含まれていることを確認します。必要な場合は、正規表現を編集します。(78 ページの『「パラメーターおよび Cookie」ビュー』 を参照してください。)
3. (オプションおよび詳細:) AppScan が意味のあるアプリケーション・ツリーを提示できるように、「スキャン構成」ダイアログ・ボックスの「コンテンツ・ベースの結果」タブを構成します。 (106 ページの『「コンテンツ・ベースの結果」ビュー』 を参照してください。)
4. 他の必要な構成変更を行い、標準的なスキャンを継続します。
5. (オプション) アプリケーション・ツリーでスキャン結果を表示する場合は、デフォルトの URL ベースのビューではなく、コンテンツ・ベースのビューを選択します。(22 ページの『アプリケーション・ツリー』 を参照してください。)

以下も参照してください。

145 ページの『パラメーター・ベースの移動テンプレート』

『パラメーター・ベースの移動を使用するサイトでの課題』

パラメーター・ベースの移動を使用するサイトでの課題

ナビゲーションがパラメーター・ベースであるサイトをスキャンするために必要な構成変更について説明します。

デフォルトで、AppScan の冗長なパスの制限は 5 です (要求を同じ URL に送信できる最大回数。 72 ページの『「探査オプション」ビュー』を参照)。通常のサイトでは、これにより不必要なテストが繰り返し行われることがなくなります。ただし、サイトのナビゲーションがパラメーター・ベースの場合、この低い

制限では、AppScan はサイトを十分にスキャンすることができず、「標準的なスキャン」テンプレートを使用して実行されるスキャンは、ほとんどのどのサイトもディスカバーしてテストすることができません。

「冗長なパスの制限」を増やすか、完全に無効にするだけでは、この問題は解決しません。このようにしても、AppScan が無限ループに入るか、あまりに多くのテストを持つスキャンが作成されて、AppScan でメモリー不足が発生します。これには、以下のような 2 つの理由があります。

1. 探査ステージ中の要求のハッシュ時に、AppScan は、要求内で検出したすべてのパラメーターおよび Cookie を組み込みます。冗長なパスの制限を無効にすると、これらの値のすべての組み合わせが考慮されてしまいます。

   例えば、サイトのセクションの各ページに、販売可能な商品についての情報をデータベースから取得するスクリプトへの何百ものリンクが含まれているとします。これらのリンクには、item_id というパラメーターが含まれていますが、これは新しいページを生成する際に重要でなく、項目に関する情報を取り出すためにのみ使用されます。その結果、AppScan は、item_id をハッシュから除外できる場合を除き、この項目情報ページの数千ものインスタンスを要求します。
2. テスト・ステージでは、この問題はより深刻になります。例えば、要求に par1 と par2 の 2 つのパラメーターがあり、AppScan がこれらのパラメーターを含む以下の 4 つのリンクを検出するとします。

   ```
   http: // site.com/content.aspx?par1=a&par2=c
   http: // site.com/content.aspx?par1=a&par2=d
   http: // site.com/content.aspx?par1=b&par2=c
   http: // site.com/content.aspx?par1=b&par2=d
   ```

   各パラメーターに 400 のテストを適用可能な場合、AppScan は合計で 1,600 のテストを送信します (par2=c と par2=d のとき par1 で 800、par1=a と par1=b のとき par2 で 800)。したがって、これらのパラメーターを探査ハッシュから除外することに加えて、各パラメーターを 1 回のみテストするように AppScan に通知する必要があります (par1 で 400 回のテスト、par2 で 400 回のテスト)。

上記から導き出される、パラメーター・ベースの移動を使用するサイトをスキャンするための原理は、以下のとおりです。

1. 探査ステージ: ナビゲーション・パラメーター以外は、すべてのパラメーターの値を無視する。
2. テスト・ステージ: パラメーターの値が変更されても、新しいテストを作成しない (ナビゲーション・パラメーターは除く)。

以下も参照してください。

340 ページの『パラメーター・ベースの移動を使用するサイト』

145 ページの『パラメーター・ベースの移動テンプレート』

ライブ実稼働環境のスキャン

AppScan を使用してライブ・サイトをスキャンする前に、以下のリスクと提案について考慮してください。

稼働中のサイトをスキャンする際、定義済みの実動サイト・テンプレートを使用できます。このテンプレートには、特別に選択された実動サイト・テスト・ポリシーのほか、稼働中のサイトに損害を与えたり、実際のユーザーに対するサービス妨害が発生したりするリスクを最小限に抑えるよう設計された構成設定が入っています。

独自の構成またはテスト・ポリシーを使用する場合、以下のセクションは、スキャンを効果的に構成する上で役立ちます。

スキャン中に送信される人工的な情報でデータベースがいっぱいになる可能性

以下の予防措置を取ることによって、この影響を緩和することができます。

- フォームの自動入力を無効にします (「スキャン構成」>「フォームの自動入力」> 最初のチェック・ボックス)。

  これにより、 AppScan が、自動的にフォームに入力して、データベース、掲示板、またはオンライン・フォーラム・システムをフラッディングする可能性のあるデータを送信したり、管理者アカウントまたはモデレーター・アカウントに不必要な電子メールを送信したりすることがなくなります。ただし、これにより、AppScan Standard は、フォームを送信することによってアクセスできるサイトの領域にアクセスできなくなることにご注意ください。この操作モードでは、AppScan は、(パラメーターの指定にかかわらず) リンクをたどることによってアクセスできるサイトの領域のみをスキャンします。
- AppScan が使用するテスト・アカウントを作成します。

  テスト・アカウントを使用すると、データベースの変更の追跡が簡単になり (例えば、サービスが実際に注文されないようにするなど)、サイト管理者がスキャン後にサイトをクリーンアップしやすくなります。

  アカウントの作成時に、以下の提案を考慮してください。
  - 変更されたレコードを復元できるように、データベースのアクセスをテスト・レコードのみに制限する。
  - テスト・アカウントによって作成される新規レコードが削除されるようにする。
  - テスト・アカウントからの注文書 (または他のトランザクション) が無視されるようにする。
  - トランザクションによって影響が生じる場合 (例えば、株を処理する場合) は、アカウントのアクセスをテスト・レコードに対してのみ許可する。
  - サイトにフォーラムがある場合は、テスト・ステージ中に作成されたテストが実際の顧客に表示されないように、テスト・アカウントのアクセスをテスト・フォーラムに対してのみ許可する。
  - サイトにさまざまなアカウント用のさまざまな特権がある場合は、さまざまな特権を持つ複数のテスト・アカウントを設定する。これにより、サイトをより包括的にスキャンできるようになります。
  - 管理者レベルのアクセス権限を持つテスト・アカウントを作成しない。

電子メール・フラッディングのリスク

電子メール通知を使用するページをテストする場合、AppScan が多くの要求を生成して、サイトの電子メール・サーバーが過負荷の状態に陥る可能性があります。

以下の 1 つ以上の提案は、これに対処するのに役立ちます。

- 電子メールが無効な電子メール・アドレスに送信されるよう、テスト対象のページ上の電子メール・アドレスを一時的に変更する。
- 適切であれば、このようなページを実動スキャンから除外するよう AppScan を構成する。
- 一度に 1 つの Web サーバーのみをスキャンし、スキャン中に SMTP サーバーに接続しないようにする。
- 「フォームの自動入力」を有効のままにする場合は、電子メールのフィールドに固有な値が挿入されるように構成して、受信者が AppScan によって生成された電子メールを簡単に識別できるようにする。

プロキシーによるスキャン

可能であれば、プロキシーによるスキャンは避けてください。これはサポートされていますが、プロキシーが原因で結果が不明確になる場合があります。

スキャンがアプリケーションからロックアウトされるリスク

間違ったログイン試行が特定の回数に達した後にユーザーをロックするように構成されているアプリケーションもあります。スキャン中にこれが発生すると、AppScan は間違いなくスキャンを完了できなくなります。

これを回避するには、以下のようにします。

- 「ログインおよびログアウト・ページに関するテストを送信します」を無効にする (「スキャン構成」> 「テスト・オプション」)。

アプリケーション障害を引き起こすリスク

AppScan がライブ・アプリケーションの障害を引き起こすリスクを回避するために、安全でないテストをテスト・ポリシーで非アクティブにすることができます。これにより、サービス妨害、バッファー・オーバーフロー、またはアプリケーションか Web サーバーの障害を引き起こす可能性のある他のテストが送信されなくなります。

重要**:** 多くの場合、Web アプリケーションには、安全でないテストによってのみ発見できる脆弱性が含まれています。安全でないテストをまったく省略してしまうことは推奨されていません。Web サイトの所有者または管理者と連携して、例えば、アプリケーションがアイドル状態になっていると予想されるオフピーク時にスキャンをスケジュールすることによって、このような脆弱性に対してアプリケーションをテストしてください。

現在のテスト・ポリシーで安全でないテストを無効にするには、以下のようにします。

1. 「構成」>「テスト・ポリシー」を開きます。
2. 「安全でないテスト」列をクリックして、すべての安全でないテストを 1 つのグループにまとめます。
3. 安全でないテスト (「安全でないテスト」値が「安全でない」になっているテスト) をスクロールダウンして、現在選択されているテストがあれば選択解除し、そのテストをスキャンから実行できるようにします。

テストの最適化の理解

このセクションでは、テストの最適化の動作と、テストの最適化を開発ライフサイクルに組み込むための最善の方法について説明します。

動作説明

通常の AppScan Standard の全体スキャンでは、一般的に数千ものテストを送信し、完了までに数時間、場合によっては数日かかることがあります。開発の初期段階で、または製品の現在のセキュリティ体制の全体をすばやく評価するために、テストの最適化を使用して、より短い時間フレームで必要な結果を入手できます。

当社のインテリジェントなテスト・フィルターは、統計分析に基づき、特定のテストや、特定のテストのバリアントもフィルタリングによって除外し、より一般的な脆弱性、より重大な脆弱性、またはより重要な脆

弱性のみを識別する短いスキャンを生成します。AppScan のフィックスパックと iFix により、最適化フィルターが最新の状態に保たれます。テストの最適化を使用することで、徹底的で詳細なスキャンよりも迅速な結果を優先する場合に、全体のスキャン時間を大幅に短縮することができます。

テストの最適化はスキャン用に選択したテンプレートに適用され、最新の統計分析の結果が使用されます。

開発の初期段階や自動化でテストの最適化を使用することを推奨しますが、サイトのセキュリティー体制を完全に把握できるように、時間がある場合にはフル・スキャンも実行することを推奨します。

テストの最適化は、構成ウィザードおよびメインの「構成」ダイアログ・ボックスの両方から活動化できます。

FAQ

Q:テストの最適化はすべてのテスト・ポリシーに適用されますか**?**

A: はい。テストの最適化は、定期的に更新されるテスト結果の統計分析に基づいてテスト・ポリシーをフィルタリングします。

Q:テストの最適化はテスト全体をフィルタリングによって除外しますか**?**

A: そうとは限りません。特定のテストのバリアントのみをフィルタリングによって除外することもあります。

Q:選択したテスト・ポリシーからフィルタリングによって除外されたテストまたはバリアントを正確に把握する方法はありますか**?**

A: 現在は不可能です。

Q:テストの最適化は他の構成設定を変更しますか**?** また、「構成」ダイアログ・ボックスでその変更を確認できますか**?**

A: 現在のところ、構成は変更されません。今後の AppScan リリースでは変更されるようになる可能性がありますが、その場合は加えられた変更が示されるようになります。

Q:スキャンが高速化するのであれば、常にテストの最適化を使用するべきではないですか**?**

A: テストの最適化は、より速く結果を出す必要がある場合には優れていますが、フル・スキャンほど徹底的ではありません。速さが重要な場合には最適化されたスキャンを推奨しますが、定期的にフル・スキャンで補完することも推奨します。

Q:同じサイトでは、**2** つの最適化されたスキャンの結果は同一になりますか**?**

A: 当社のチームは絶えず設定の分析と更新を行っているため、AppScan が更新されるたびに最適化の設定が改善されています。そのため、サイトが変更されていなくても結果が同一にならない可能性があります。ただし、前のスキャンで問題を明らかにしたテストが、後のスキャンでフィルタリングによって除外されることはほとんどありません。

Flash コンテンツ

このセクションでは、Adobe Flash コンテンツのスキャンに関するアドバイスを紹介します。

AppScan は、Adobe ActionScript 1.0、2.0 および 3.0 と、Adobe Flex フレームワーク 2.0 および 3.0 を探査してテストします。Flash の解析および実行は、「スキャン構成」ダイアログ・ボックスの「探査オプション」ビューでアクティブにできます。

システム要件

スキャン中に AppScan が Adobe Flash コンテンツを実行できるようにするため、サポートされているバージョンの Adobe Flash Player for Internet Explorer がインストールされている必要があります。バージョン 9.0.124.0 から 14.0.0.125 までがサポートされています。

注**:** Flash Player は、ブラウザー固有の ActiveX プラグインとして提供されます。AppScan には、Adobe Flash Player for Internet Explorer が必要です。

- ご使用のバージョンが古い場合は、最新の Flash Player を からダウンロードできます。 http://get.adobe.com/flashplayer/
- Adobe Flash Player バージョン 10.1 以降がインストールされている場合は、AppScan で使用するためには構成が必要であるというメッセージが表示されることがあります。 8 ページの『Flash Player の構成』 を参照してください。

注**:** いずれの場合も (サポートされている Flash Player がインストールされていない場合も、Flash Player が構成されていない場合も)、「構成」ダイアログ・ボックスに警告が表示されます。また、スキャン中に *Flash* は実行されません。

Flash スキャンに関する制約

Flash スキャンには以下の制約があることに注意してください。

- AppScan はプロキシーを介して Flash コンテンツをスキャンするため、localhost の URL はスキャンされません。
- 検出された問題は、ご使用のマシンにインストールされている Adobe Flash Browser for Internet Explorer のバージョンに固有のものです。以下のような場合が考えられます。
  - ご使用の再生プログラムには報告された問題に対する脆弱性が存在するが、別のブラウザー用の再生プログラムまたは新しいバージョンの再生プログラムにはその脆弱性が存在しない
  - ある問題に対する脆弱性は、ご使用の Internet Explorer 用の再生プログラムには存在せず、したがって AppScan で報告されないが、他のブラウザー用の再生プログラムや古いバージョンの再生プログラムには存在する

URL が完全に網羅されていない

スキャンを実行してその結果を確認したときに、Flash コンテンツからの URL が AppScan で識別されていないように思われる場合のアドバイスを、以下に紹介します。

AppScan で、**Flash** コンテンツの一部の **URL** は識別されるが、検出されない **URL** もあるのはなぜか

いくつかの原因が考えられます。

- Flash ムービーのバージョンがサポートされていることを確認します。(サポートされていないバージョンは、「アプリケーション・データ」ビューの「フィルタリングされた URL」の下にリストされます)
- スキャンを実行したマシンで Internet Explorer ブラウザーを使用してムービーを再生し、正しく再生されることを確認します。

- JavaScript の実行 (デフォルトで有効) が無効になっていないことを確認します。(「スキャン構成」 > 「探査オプション」 > 「**URL** およびダイナミック・コンテンツを見つけるために **JavaScript** を実行する」)

Flash コンテンツの一部が対象範囲に含まれていない

いくつかの原因が考えられます。

1. フォームの自動入力で入力される情報が完全であることを確認します (「スキャン構成」 > 「フォームの自動入力」)。
2. 「スキャン構成」 > 「探査オプション」 > 「**Flash**」 > 「クリック制限」の設定値を増やしてみます。
3. 「スキャン構成」 > 「詳細」 > 「**Flash:** サンプル間の最大時間」設定をデフォルト値である 160 ms よりも増やしてみます。
4. 「スキャン構成」 > 「詳細」 > 「**Flash:** 範囲」設定を 1 から 2 へ増やしてみます。
5. Internet Explorer でムービーを再生してみて、予期したとおりに再生されることを確認します。
6. ムービーが再生されない場合は、Flash Browser の「デバッグ・レベル」を「トレース 3」(再スキャン) に設定し、ブラウザー・ログ ([AppScan Standard インストール・フォルダー]\Logs\AppScanFlashBrowser.log) をサポート・プロバイダーに送信します。

脆弱性が検出されない

AppScan が URL を検出してそれらをアプリケーション・ツリーに追加したが、それらの URL の脆弱性が検出されなかった場合は、以下のようにすることをお勧めします。

検出された **Flash URL** の脆弱性が **AppScan** で検出されない

考えられる原因は、以下のとおりです。

- 疑わしいパラメーターがムービーに含まれていない。「アプリケーション・データ」 > 「スクリプト・パラメーター」で、検出された Flash パラメーターを調べてください。
- すべての Flash テスト (ActionScript 2 および ActionScript 3) が有効になっていることを確認します 「スキャン構成」 > 「テスト・ポリシー」を開いて「ActionScript」を探し、すべてのテストが選択されていることを確認します)。
- ムービーに脆弱性が存在しない。

他にできること

それでもなお、Flash の脆弱性が見逃されている疑いがある場合は、拡張サポート・モードを有効にして、スキャンを再び実行し、結果をサポート・プロバイダーに送信してください。 353 ページの『拡張サポート・モード』 を参照してください。

よくある質問

このトピックでは、一般的なアプリケーションについての質問を扱います。

Web サービスをスキャンする各種方法

サイトのスキャンは、最初に探査が行われ、次に収集されたデータに基づくテストが行われて実施されます。「探査データ」は、1 つ以上の探査方法を使用して収集することができます。どのケースでも、探査データが収集されると、AppScan を使用してテストが作成され、テスト・ステージ中にサイトに送信されます。

Web アプリケーションの探査 **(**ユーザー・インターフェースのあるサイト**)**

- Web サービスなしのアプリケーション (サイト) の場合は、AppScan がサイトをテストできるようにするために、開始 URL とログイン認証の資格情報を提供するだけで十分なことが多くあります。
- 必要な場合は、特定のユーザー入力によってのみ到達可能な領域にアクセスできるようにするために、 を介して*AppScan* サイトを手動で探査することができます。
- 特定の順序でページにアクセスすることでのみ到達可能なページの場合、AppScan のマルチステップ操作を記録して使用することができます。
- 構成ウィザードではいくつかの手順でスキャンを構成して開始できますが、複雑なサイトの場合は、「構成」ダイアログ・ボックスでさらに多くの設定を微調整およびカスタマイズできます。

Web サービスの探査

- サービスの探査に使用するデバイス (携帯電話やシミュレーターなど) の記録プロキシーとして AppScan を設定できます。そうすることで、AppScan は収集された探査データを分析し、適切なテストを送信することができます。AppScan を使用して、Web サービス機能テスターなどの外部ツールでトラフィックを記録することもできます。 157 ページの『記録プロキシーとして AppScan を使用』を参照してください。
- Web サービス用の Open API 記述ファイル (JSON または YAML) がある場合、 Web サービス・ウィザードの拡張機能を使用してスキャン、およびサービスの使用に必要なマルチステップ・シーケンスを構成できます。AppScan は、サービスを自動的にスキャンします。
- 最初の 2 つの方法を使用できず、Web サービス (SOAP Web サービスなど) 用の WSDL ファイルがある場合、AppScan のインストールには、ユーザーが Web サービスに組み込まれた各種メソッドの表示、入力データの操作、サービスからのフィードバックの確認を行うことができる個別のツールがオプションで組み込まれます。まず、AppScan にサービスの URL を提供する必要があります。組み込まれている「Generic Service Client (GSC)」では、WSDL ファイルを使用して、ツリー形式で個々のメソッドが表示され、要求をサービスに送信するための使いやすい GUI が作成されます。このインターフェースから、パラメーターを入力して結果を確認できます。この処理は、AppScan によって「記録」され、AppScan によるサイトのスキャン時に、サービスに対するテストを作成するために使用されます。GSC は REST 要求のクライアントとしても使用できます (WSDL ファイルの解析なしの、単純な HTTP クライアントとして)。 161 ページの『GSC の使用』を参照してください。

マニュアル探査とマルチステップ操作の差異

マニュアル探査

マニュアル探査は、AppScan がサイトをテストするときに自動探査ステージが行われていない可能性があるアプリケーションまたはサービスの一部が確実にカバーされるようにするために、ユーザーがサイトを探査して AppScanが使用できるデータを収集する場合に行います。これは、特定のユーザー入力が必要である、またはサイトが別のタイプのツールやデバイスに対してのみ応答するなどの理由で行われます。マニュアル探査は、AppScan を使用するか、AppScan を記録プロキシーとして使用するか、あるいは Generic Service Client (GSC) を使用して行うことができます。

149 ページの『第 5 章 マニュアル探査』 を参照してください。

マルチステップ操作

ユーザーが品目をカートに追加し、まだ支払いを行っていないオンライン・ショップなど、リンクを特定の順序で クリックすることによってのみ到達できるサイトの部分を探査するには、マルチステップ操作が必要です。以下の 3 つのページについて考えます。

1. ユーザーがショッピング・カートに 1 つ以上の品物を追加します
2. ユーザーが支払いと配送方法の詳細を入力します
3. ユーザーが、この注文が完了した確認を受け取ります

ページ 2 にはページ 1 を経由してのみ到達できます。ページ 3 にはページ 1、ページ 2 を経由してのみ到達できます。これがシーケンスです。ページ 2 とページ 3 をテストできるようにするには、AppScan が各テストの前に HTTP 要求の正しいシーケンスを送信する必要があります。

98 ページの『「マルチステップ操作」ビュー』 を参照してください。

アクション・ベースの再生と要求ベースの再生の差異

ログイン操作やマルチステップ操作で使用するために手順を記録する場合、以下の 2 つの再生方法が使用可能です。

要求ベースの再生
: 生の HTTP 要求を記録から送信します。一般的に早いのはこちらの方法です。

アクション・ベースの再生
: ユーザーのクリックおよびキー・ストロークを再生します。この方法を選択するのは、サイトに大量の JavaScript が含まれている場合や、要求ベースの再生に含まれている要求を検証した際に、その一部に赤色の X でマークが付けられた場合などです。この方法では、スキャン時間が長くなる可能性があります。

「構成」 > 「探査」 > 「 56 ページの『レビューと検証タブ』」、および「構成」 > 「 98 ページの『「マルチステップ操作」ビュー』」を参照してください。

第 14 章 トラブルシューティング

このセクションは、ユーザー処置によるトラブルシューティングに関する提案を紹介します。

トラブルシューティング機能

AppScan は、問題をより効率的に特定および解決するための、さまざまな情報を提供しています。

- **AppScan** ログ - AppScan 機能に関する情報を表示します。これにはそのプロキシーへの接続方法、および各再始動後にプロキシーが listen するポートが含まれます。
- トラフィック・ログ - 使用可能になっている場合、AppScan はこのログに、Web サイトとの間で送受信されたすべてのトラフィックを書き込みます。

  注: トラフィック・ログを使用可能にすると、アプリケーションの実行は遅くなり、ディスク・スペースの使用量は増えます。
- ダンプ・ファイル - 異常終了の場合に、AppScan はメモリー・ダンプ・ファイルを作成し、そのパスとファイル名の通知を出します。このファイルは、異常終了の原因となったユース・ケースに関する入手可能なすべての情報が含まれ、詳細に調査するために AppScan Standard サポートに送信する必要があります。
- サポート・モード - 問題を複製し、データ・ファイルをパックし、テクニカル・サポートに送信できます。
- パック・ファイル - AppScan は、テクニカル・サポートに送信するためのデータ・ファイルのアーカイブを自動的に作成します。これらのファイルには、スキャン・ファイル (*.scan) 、AppScanDbg.log、AppScanSys.log、および AppScanTraffic.log が含まれます。
- 誤検出を報告- 特定のテスト、特にお使いのアプリケーションで誤検出であると疑われる結果を含むテストについて、IBM Security AppScan Standard へフィードバックを送信できます。AppScan は選択したバリアントから情報を zip し、デフォルトの E メール・クライアントで開かれる新しい E メール・メッセージに zip ファイルを添付します。

ライセンスのトラブルシューティング

このタスクについて

サイトのスキャンに IBM Security AppScan Standard を使用するには、有効なライセンスを持っている必要があります。ライセンスは有効であるが、AppScan がそのライセンスを受け入れない場合は、以下の手順を試行してください。

手順

1. AppScan を使用するサーバーがライセンス・サーバーとネットワーク接続していることを確認します。

   注: AppScan Standard Edition ライセンスは IBM Rational License Key Server にインストールされます。このライセンス・サーバーは、AppScan が稼働するサーバーと同じではない可能性があります。AppScan が機能するためには、インストール先のサーバーがライセンス・キー・サーバーとネットワーク接続する必要があります。ユーザーが AppScan を開くたびにライセンスがチェックアウトされ、AppScan を閉じるたびにライセンスが再びチェックインされます。

2. ライセンスをテキスト・エディター (Microsoft メモ帳など) で開きます。

   重要**:** ライセンス・ファイルは変更しないでください。
3. ライセンスの有効期限が切れていないことを確認します。
4. スキャンするサイトが (IP とホスト名の両方が) ライセンス制限内にあることを確認します。
5. ライセンスの MAC アドレスとディスク・シリアル番号がマシンのものと同じであることを確認します。

次のタスク

この手順でも問題が解決しない場合は、以下に示す文書を参照してください。AppScan Standard ライセンスの取得および適用方法またはAppScan サポートに連絡してください。

ディスクの空き容量が不足しています

このタスクについて

AppScan スキャンの処理時に作成される一時ファイルのサイズは、スキャン自体のサイズにまで到達することがあるので、一時フォルダーには必ずその容量 (スキャンのサイズ) が必要です。 スキャンのサイズは、スキャンされているサイト、テンプレート、構成、見つかった問題に応じて異なります。

- デフォルトでは AppScan は一時ファイルを `C:\ProgramData` に保管します。
- AppScan のサード・パーティー・コンポーネントは、TEMP および TMP の Windows ユーザー環境変数で定義されたパスにデータを保管します。

手順

1. 3 つのパスのディスク・スペースを解放できるかどうかを確認します。
2. 必要な場合は、パスを変更します。
   - AppScan の一時パスを変更するには、新規パスを次のように定義します。

     「ツール」>「オプション」> 「詳細」>「**TempFilesDir**」

     注**:** このパスは、ローカルであること、ASCII 文字のみを使用することが必要です。
   - サード・パーティーの一時パスを変更するには、Windows ユーザー環境変数の TEMP 値と TMP 値を変更します。

デジタル署名のトラブルシューティング

このタスクについて

AppScan を開くたびに、そのセキュリティー・ルールのデジタル署名 (DLL ファイル) が検証されます。検証は、以下の原因で失敗することがあります。

- DLL ファイルが破損している
- DLL ファイルが (おそらくハッカーにより) 改ざんされている
- 以下の証明書 (Windows インストールの一環としてデフォルトでインストールされる) が、Windows ストアの「信頼されたルート証明機関」証明書のリストから欠落している。

  `VeriSign Class 3 Public Primary Certification Authority - G5`

手順

1. 以下のルート証明書がインストールされていることを確認します。

   ```
   VeriSign Class 3 Public Primary Certification Authority - G5
   ```

2. AppScan をアンインストールしてから再インストールします。
3. この手順で問題が解決しない場合は、サポートに連絡してください。

   注: システムの情報が漏えいしていないことが確かな場合は、警告メッセージによって続行するためのオプションが提示されます。

レガシー・スキャン・テンプレートのインポート

8.6 より前のバージョンの AppScan に保存されているスキャンからスキャン・テンプレートをインポートする方法。

AppScan バージョン 8.6 でスキャン・ファイルのフォーマットが再設計されたので、旧バージョンで保存されているスキャンを現行バージョンで開くことはできません。必要に応じて、新規スキャンで使用するためにテンプレートをインポートできます。

スキャン・テンプレートをインポートするには、以下のようにします。

1. スキャン・ファイルの拡張子を SCAN から ZIP に変更します
2. ZIP ファイルを開き、`templateconfig.xml` を見つけて抽出します
3. その拡張子を XML から SCANT に変更します
4. AppScan で開きます。

誤検出結果の報告

特定の AppScan の結果が誤っている (誤検出) と感じる場合には、AppScan から送信された要求、およびご使用の Web アプリケーションの応答を、IBM Security AppScan Standard サポートに E メールで送信することができます。 235 ページの『誤検出のテスト結果を報告』を参照してください。

「誤検出を報告」機能のトラブルシューティング

以下で提供するヒントは、「誤検出を報告」機能を使用して、AppScan サポート・チームにバリアント情報を添付したフィードバックを送信する際に問題が生じた場合に役立ちます。

問題	原因	解決方法
受信者が添付ファイルを読み取れない	E メールが暗号化されて送信された。 他の受信者が、E メールを読むために必要な秘密鍵を持っていない。	暗号化をオフにするには、「ツール」メニュー > 「オプション」コマンド > 「全般」タブ > 「誤検出を報告」オプションで、「添付ファイルの暗号化」チェック・ボックスをクリアします。

拡張サポート・モード

拡張サポート・モードでは、AppScan のすべてのアクティビティーがログに記録されます。問題のある手順のトラブルシューティングのため、それらのログをパッキングしてサポート・プロバイダーに送信することができます。

このタスクについて

問題のある手順のトラブルシューティングについて支援が必要な場合、AppScan を拡張サポート・モードで実行してすべてのアクティビティーをログに記録し、そのデータを 1 つのファイルにパックするようにサポート・プロバイダーから求められることがあります。

重要**:** 権限があるサポート担当員により指示されたのでない限り、拡張サポート・モードはオンにしないでください。このモードは、AppScan のパフォーマンスに影響を与えます。

手順

1. 拡張サポート・モードをアクティブにする。「ヘルプ」>「サポート」>「拡張サポート・モード」

   メッセージが表示され、拡張サポート・モードが有効であり、すべてのアクションがログに記録されることが示されます。
2. 「**OK**」をクリックします。

   ステータス・バーのインディケーターに、AppScan が拡張サポート・モードで実行されていることが示されます。 

3. 問題のある手順を再現します。
4. 完了したら、拡張サポート・モードを無効にします。「ヘルプ」>「サポート」>「拡張サポート・モード」

   または

   手順を実行した結果、AppScan が機能停止状態になった場合は、AppScan を再び開き、引き続き拡張サポート・モードを有効にするかどうかたずねられたら、「無効」を選択します。
5. 必要なオプションを選択します。

オプション	説明
暗号化	保存されるすべてのサポート・データ (スキャン・ファイルが対象の場合はこれも含む) が暗号化されます。 **重要:** パッケージを AppScan サポートに送信する場合以外では、暗号化を選択しないでください。暗号化されたファイルを開くことができるのは、サポートのみです。
スキャン・ファイルを含める	現在のスキャン、または関連する別の保存済みスキャンをサポート・ファイルに含めることができます。

6. 以下をクリックします。

オプション	説明
保存	既存のサポート・データを .SUPPORT ファイルとして保存します (構成内容に応じて、暗号化や、スキャン・ファイルの組み込みも行われます)。サポート・データは AppScan インターフェースから消去され、AppScan は通常のモードに戻ります。 デフォルト・パスは以下のとおりです。 `...\My Documents\AppScan\Support\`

オプション	説明
保存しない	サポート・データは AppScan インターフェースから消去され、AppScan は通常のモードに戻ります。
キャンセル	サポート・データは AppScan インターフェースから消去されず、AppScan は拡張サポート・モードのままになります。

デフォルト・ブラウザーの変更

標準装備のブラウザー以外のブラウザーを使用するように AppScan を構成することができます。

このタスクについて

デフォルトの場合、ログイン手順やマルチステップ操作を記録したり、「ブラウザーで表示」ボタンをクリックすると、AppScan は標準装備のブラウザーを起動します。

標準装備のブラウザーではサイトの一部にアクセスできない場合や、サイトが標準装備のブラウザー用に最適化されていない場合は、代わりにマシンにインストール済みの別のブラウザーを使用するように AppScan を構成することができます。

手順

1. 「ツール」>「オプション」をクリックし、「外部ブラウザーの使用」を選択します。
2. ご使用のマシンにインストールされた サポート対象ブラウザーのドロップダウン・リストからブラウザーを選択します。サポートされているブラウザーは次のとおりです。
   - MS Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - MS Edge
3. 以下に示す 2 つの構成オプションのいずれかが変更された場合、新しく選択されたブラウザーのヘッダー値ではなく、定義済みのヘッダー値が使用されます。デフォルト値は、必要に応じて復元することができます。
   - 「構成」>「詳細構成」>「通信: **Accept-Language** 要求ヘッダー値
   - 「構成」>「探査オプション」>「ユーザー・エージェントのヘッダー値」

   これらの設定がユーザーによって 変更される可能性があるのは、以下の場合です。
   - ブラウザーを起動し、ログイン手順またはマルチステップ操作を記録した場合、または「ブラウザーで表示」をクリックした場合。
   - これらの設定を手動で変更した場合。
   - 保存されたスキャンをロードした場合。

   これら 2 つの設定値を新しく定義されたブラウザーの設定値に設定するには、単純にこれらの値を削除してから、必要に応じてログイン手順またはマルチステップ操作をもう一度記録します。この操作により、新しく定義されたブラウザーのヘッダー値が AppScan で自動的に使用されるようになります。

   注: 新しく定義されたブラウザーには、以下の制約が適用されます。
   - 選択したブラウザーがプロキシー構成ファイルを使用するように構成されている場合、この選択は無視され、標準装備のブラウザーが開きます。

- 「ログインして記録」オプションを使用してマルチステップ操作を記録する場合、標準装備のブラウザーが開きます。
- AppScan の別のインスタンスが開いている状態で外部ブラウザーを開こうとすると、標準装備のブラウザーが開きます。
- 「ログイン管理」>「詳細」タブで、URL を選択して「ブラウザーで表示」または「選択」をクリックした場合、標準装備のブラウザーが開きます。
- Firefox を選択すると、「AppScan」という名前のプロファイルが自動的に作成されます (この名前のプロファイルが存在しない場合)。この操作の実行後に Firefox が起動された場合、変更内容を反映するために Firefox を閉じる必要があります。

関連概念:

331 ページの『上級ユーザー用のワークフロー』
このワークフローは、Web セキュリティー分野の経験を持つユーザーが、さらに詳細なスキャンを実行する場合に役立ちます。

関連タスク:

335 ページの『手動によるサイト範囲の改善』
初期自動探査ステージで見逃した URL (特定の入力を必要とするフォームによってアクセスされる URL などの個別 URL と、買い物かごなど、順序付けられた URL シーケンスの両方) を追加できます。

関連資料:

124 ページの『「詳細構成」ビュー』
「スキャン構成」ダイアログ・ボックスの「詳細」タブ (「スキャン」>「スキャン構成」>「詳細」タブ) は、特定のスキャンに影響を与える詳細レジストリー設定を変更するために使用します。このタブは、経験を積んだ AppScan ユーザーである場合にのみ、または、問題をトラブルシューティングするためにサポート・チームから指示された場合にのみ、使用してください。

72 ページの『「探査オプション」ビュー』
「構成」ダイアログ・ボックスの「探査オプション」ビューです。

ログインのトラブルシューティング

「スキャン構成」 > 「ログイン管理」ビューでのセッション検出の問題のトラブルシューティングのヒント。

ログイン手順の記録後にブラウザーを閉じると、緑色の鍵アイコン  が表示されます。これは、スキャン中にセッション内状況を検証するために使用できるパターンが AppScan によって検出されたことを示します。代わりに別のアイコンが表示された場合は、AppScan がスキャン中にサイトにログインするための情報が不足していた可能性があります。

「スキャン構成」 > 「ログイン管理」 > 「詳細」は、ログイン手順を 2 つの方法 (「アクション」および「要求」) で記録します。これらの 2 つの方法のうち *1* つ でも成功していれば、AppScan はサイトにログインすることができます。以下の表は、両方の方法が失敗した場合のトラブルシューティングに役立ちます。

以下の表は、メッセージおよび考えられるユーザーのトラブルシューティング・アクションの要約を示しています。

アイコン	メッセージ	考えられるユーザー・アクション
	アクション・ベースのログインの使用 アクション・ベースのログイン:成功 要求ベースのログイン:成功	アクションは不要です。アクション・ベースのログインが使用され、要求ベースのログインはフォールバック方法として使用可能です。
	アクション・ベースのログインの使用 アクション・ベースのログイン:成功 要求ベースのログイン:失敗	アクションは不要です。アクション・ベースのログインが使用されます。 要求ベースの手順をトラブルシューティングするには、を参照してください。 359 ページの『要求ベースのログインのトラブルシューティング』
	要求ベースのログインの使用 アクション・ベースのログイン:失敗 要求ベースのログイン:成功	アクションは不要です。アクション・ベースのログインが優先方式ですが、要求ベースのログインが成功したため、こちらが使用されます。 アクション・ベースの手順をトラブルシューティングするには、を参照してください。 359 ページの『アクション・ベースのログインのトラブルシューティング』 **注:** 非常に遅いログイン・ページがある場合は、要求ベースのログインを使用するのが実用的な場合があります。これは、通常、多くのログインがスキャン中に必要になるためです。
	ログインはまだ記録されていません	 をクリックしてログインを記録するか、あるいはログインが不要な場合は、「ログイン/ログアウト」タブ > 「ログイン方法」で「なし」を選択してセッション検出を無効にします。
	ログインはまだ検証されていません	いずれかの手順を変更した場合は、「検証」ボタンをクリックして新規のログイン手順を検証する必要があります。
	セッション内検出パターンが未定義	まず、ログインの記録を再試行します。ただし今回は、ログイン後、ログイン・レコーダーを閉じる前に追加リンクをクリックします。 追加リンクは、ユーザーがセッション内にあるときのみ使用可能なデータやリンクが応答に含まれるページにリンクするものでなければなりません。 これにより、AppScan は自動的に有効なパターンを特定できます。 これが機能しない場合は、セッション内パターンを自分で定義してください。詳しくは、 63 ページの『「検出パターン」ダイアログ・ボックスを選択します。』 を参照してください。

アイコン	メッセージ	考えられるユーザー・アクション
	セッション要求がログイン要求と同じです	通常、ログイン手順は AppScan がアプリケーションにログインした直後に終了します。ただし、まれにセッション内要求にログイン要求 (ユーザー名とパスワードを使用) も含まれている場合があります。そのような場合、AppScan が (ログインしていることを確認するために) セッション内要求を再生するたびに実際にログインが行われるため、いつログアウトしたかを検出することができません。 解決策として、ログイン手順を記録し、ログインしている間はそのページ上の別のリンクをクリックします。これで、ログイン手順に追加の手順が記録されます。この新規要求に資格情報が含まれていない限り、AppScan はこの手順を使用して、いつログアウトされたかを確認することができ、鍵アイコンの色は緑に変わります。
	セッション・ページがリダイレクトされます	最初のセッション内ページとして選択されたページが別のページにリダイレクトされた場合、AppScan によって選択されたセッション内パターンが誤っている可能性があります。 • 現在のセッション内検出パターンがセッション内状況を示していることを確認します。 • 不明確な場合は、要求ベースのログイン手順でページのリダイレクトを追加ステップとして追加することを試してください。
	セッション・ページが識別されていません	「要求」タブで、ログイン手順の最終ページを開き、(「ブラウザー」タブまたは「要求/応答」タブで) ログイン済みのユーザーに固有の パターン (「ログアウト」リンクなど) を探し、それをセッション内パターンとして選択します。 • アクション・ベースの手順をトラブルシューティングするには、を参照してください。 359 ページの『アクション・ベースのログインのトラブルシューティング』 • 要求ベースの手順をトラブルシューティングするには、を参照してください。 359 ページの『要求ベースのログインのトラブルシューティング』 • 詳細なトラブルシューティングのワークフローについては、を参照してください。 360 ページの『詳細なログイン・トラブルシューティング・ワークフロー』
	セッション検出は無効です	アクションは不要です。 セッション検出は、3 つのログイン方法 (「記録済み」、「プロンプト」、または「自動」) のいずれかを選択することで有効にできます。

アクション・ベースのログインのトラブルシューティング

以下のステップを使用して、アクション・ベースのログインのトラブルシューティングを行います。

手順

1. 「ログイン管理」>「詳細」>「アクション」で、ユーザー名 (uid) とパスワード (passw) が正しいことを確認し (入力されている値を表示するには、パスワード値をダブルクリックします)、必要な場合は手動で修正します。
2.  をクリックし、プレイヤーで手順を再生します。これは、どこで手順が失敗したのかを確認するのに役立ちます。

   注: 非常に遅いログイン・ページがある場合は、要求ベースのログインを使用するのが実用的な場合があります。これは、通常、多くのログインがスキャン中に必要になるためです。
3.  をクリックし、手順を再度記録します。ただし、今回は次のようにします。
   a. テキスト・エディターでユーザー名とパスワードを入力し、それらを Web ページにコピー・アンド・ペーストします。
   b. Web サイトの「実行依頼」ボタンをクリックせずに、キーボードの **Enter** キーを押します。

   これらのステップをすべて実行しても問題が解決しない場合は、要求ベースの手順の使用を試みてください。

要求ベースのログインのトラブルシューティング

「詳細」タブに表示されている「セッション内検出パターン」がセッション内状況を正しく識別していない場合、要求シーケンスを使用する別のパターンを選択することができます。

手順

1. 「ログイン管理」>「詳細」>「要求」で、「セッション内」とマークされている (緑色で強調表示) URL を選択し、ダイアログ・ボックスの下部にある「選択」ボタンをクリックして別のパターンを選択します。

   ブラウザーが開き、ブラウザー内または応答本体タブで新規パターンを選択することができます。その後、ブラウザーを閉じて「検証」をクリックします。
2. 最終ページでセッション内パターンを識別できない場合は、次のようにします。
   a. 直前に調査した要求の上にある 要求を選択します。
   b. それをダブルクリックし、ログイン資格情報が含まれていないことを確認します。
   c. 含まれていない場合、「選択」をクリックし、別のパターンの識別を試行します。
3. セッション内パターンが見つからない場合は、その 1 つ上の要求に対して上記のステップを繰り返します。ログイン資格情報が含まれる要求が見つかるまで、必要に応じてこのステップを繰り返すことができます。
4. これらのどのページでもセッション内パターンを識別できず、セッション内ページの後に 1 つ以上の URL がリストされている場合は、その ページで同じ手順を使用してセッション内パターンを探します。
5. 追加の URL がない 場合は、ログイン手順の記録を再試行してください。ただし、ログイン後に 1 つの追加リンク (できれば個別設定) をクリックし、そのページでセッション内パターンを探します。
6. これが失敗した場合は、次のように、セッション無効パターンの選択を試行してください。

a. 元からセッション内要求としてマークされていた URL を選択します。
b. ブラウザーを (AppScan 外部で) 開き、この要求を (残りのログイン手順を行わずに) そのまま送信します。
c. 2 つの応答を比較し、ステップ B からの応答の本文にセッション内ページには存在しない記述 (「ログインしていません」など) がないかを識別します。

   注: 要求が別のページにリダイレクトした場合、ブラウザーで表示される応答を使用することはできず、実際の要求に対する応答を使用する必要があります (これは、スニファーを使用して実行できます)。
d. 「詳細」タブの下部にある「セッション内」ドロップダウン・ボタンをクリックして「セッション無効」を選択し、識別したパターンを「検出パターン」フィールドに貼り付けます。

次のタスク

この手順でも問題が解決しない場合は、以下に示すオンライン技術情報を参照してください。

http://www.ibm.com/support/docview.wss?&rs=3378&uid=swg21283302#Overview%20of%20In-Session%20Detection

詳細なログイン・トラブルシューティング・ワークフロー

上級ユーザーがログインの問題をトラブルシューティングする際に役に立つステップ。

このタスクについて

以下のステップは、ログインの問題をシステマティックに特定して解決できるように設計されています。ワークフロー内の各推奨ステップが完了するたびに、再スキャンを実行して、問題が解決されたかどうかを確認してください。

手順

1. アクション・ベースのブラウザーを表示するように設定

   「ツール」>「オプション」>「詳細」>「**SessionManagement.ShowActionBasedPlayerWindow**」で、設定を 「**True**」 に変更すると、ブラウザー・アクションを確認できます。
2. サイトが稼働中であり、資格情報が正しいことを確認

   通常のブラウザーで開始 URL を開き、指定した資格情報で手動でログインできることを確認します。
3. 「詳細構成」の調整 「構成」>「**URL** およびサーバー」ビューで、「ブラウザーで表示」をクリックし、AppScan ブラウザーにログインできることを確認します。
   - スクリプト・エラーのポップアップが表示された場合、以下を (個別にまたはすべてまとめて) 試してください:
     - 「構成」>「詳細構成」>「通信: **Accept-Encoding** ヘッダーの削除」で、設定を「**False**」に変更し、「適用」をクリックします。
     - 「構成」>「詳細構成」>「全般: プロキシー・ファイル拡張子フィルター」で、「値」フィールドのコンテンツをすべて削除し、「適用」をクリックします。
     - 「詳細構成」>「セッション管理:手順のコンテンツ・タイプフィルター」で、「値」フィールドのコンテンツをすべて削除し、「適用」をクリックします。
   - サイトの AppScan ブラウザーでの動作が、通常のブラウザーでの動作と異なる場合、以下を試してください。

– 「構成」>「探査オプション」>「ユーザー・エージェント」で、「編集」アイコンをクリックし、すべてのコンテンツを削除してから「適用」をクリックします。

4. **HTTP** 認証を使用するサイト

   サイトが HTTP 認証を使用する場合 (認証が必要なポップアップが表示された場合)、以下を実行します。

   a. 「構成」>「ログイン管理」ビューで、「ログイン方法」を「なし」に設定します。

   b. 「構成」>「**HTTP** 認証」ビューで、ユーザー名とパスワードを指定し、必要な場合はドメインも指定します。

      注**:** ユーザー名にスラッシュ (/) が含まれている場合、その前のコンテンツはドメイン、その後がユーザー名です。 その他の場合はドメイン・フィールドを空のままにしてください。

5. 自動ログイン

   自動ログインを使用している場合、次を試してください。

   a. 「構成」>「ログイン管理」>「ログイン**/**ログアウト」タブで、ログイン方法が「自動」に設定されていることを確認します。

   b. ユーザー名とパスワードに値を入力します。

   c. 「構成」>「ログイン管理」>「詳細」タブで、「セッション内構成の自動検出」をクリックします。

      AppScan がサイトへのログインを自動的に試行している場合、発生する可能性がある問題は以下の 3 タイプです。

      - AppScan によるログイン・フィールドへの入力が失敗した場合、AppScan でのユーザー名やパスワードの識別が不可能な場合があります。
        1) 通常のブラウザーで開始 URL を開きます。
        2) 「ユーザー名」フィールドで右クリックし、「検査」を選択します。
        3) 開いた HTML ソース・コード・ペインで、「ユーザー名」フィールドの ID 値を見つけ、それをクリップボードにコピーします。
        4) AppScan で、「構成」>「フォームの自動入力」に移動し、ID 値を「ユーザー名パラメーター」フィールドに貼り付けます。
        5) 「パスワード ID」値に対しても、ステップ 2 から 4 を繰り返します。
      - AppScan で正しくないボタンがクリックされた場合、「ログインを記録」に切り替えます。
      - AppScan によるセッション内パターンの識別が失敗した場合は、 を参照してください 63 ページの『「検出パターン」ダイアログ・ボックスを選択します。』

6. 記録されたログイン

   「ログインを記録」を使用している場合は以下を試行してください。

   a. 「構成」>「ログイン管理」>「ログイン**/**ログアウト」タブで、ログイン方法が「記録」に設定されていることを確認します。

   b. ログイン・シーケンスを記録します。

   c. 「詳細」タブ >「アクション」リストを開き、「再生」ボタンをクリックします。

      AppScan がサイトへのログインを試みます。 以下の問題が発生する可能性があります。

- AppScan によるログインとパスワードのパラメーターの入力速度が速すぎた場合、「ログイン管理」>「詳細」>「アクション」リストに進み、アクション間の「待機」期間を長くします。
- AppScan により、いくつかのアクションが誤って抜かされた場合、「Tab」/「Enter」をマウス・クリックに変更してみるか、その逆を試してください。

d. 「詳細」タブ >「アクション」リストで、「検証」をクリックします。

AppScan はシーケンスを再生し、セッション内パターンを識別しようと試みます。 セッション内パターンが見つからない場合、ログイン・ステップの後に、より詳しい情報 (AppScan がセッション内パターンとして使用できる "Welcome [username]" または "[userID]" など) が記載されたページにアクセスするために、シーケンスへのステップの追加を試してください。

7. 要求ベース・ログインへの切り替え

上記作業が該当しない場合、外部ブラウザーを使用した要求ベースのログインを使用してみてください。

a. 「ツール」>「オプション」>「スキャン・オプション」で、「外部ブラウザーの使用」チェック・ボックスをクリックし、ブラウザーを選択します。
b. 「構成」>「ログイン管理」で、「ログイン方法」を「記録」に設定します。
c. 「記録を開始」>「外部ブラウザーの使用」をクリックします。
d. サイトにログインし、ブラウザーを閉じます。

探査ステージが長い、または終了しない

ある種類のサイトでは、探査ステージに長い時間がかかったり、探査ステージが終了しないことがあります。

この問題の原因としては、サイトがパラメーターを URL に再書き込みするため、本質的に同じページであるものに対して何十 (または何百) もの「動的」URL が作成されることが考えられます。

例:

```
http://...php/1/index
http://...php/2/index
...
http://...php/100/index
```

これらの URL は、異なる 100 個のノードとしてアプリケーション・ツリーに表示され、それぞれのノード用にテストが作成されますが、それらすべてを別々にテストする必要はおそらくないでしょう。

探査の最適化モジュールは、このパターンを識別して、AppScan がこれらすべての URL を 1 つの URL として処理できるようにするカスタム・パラメーターを作成することができます。

314 ページの『探査の最適化モジュール』 を参照してください。

Flash ムービーのトラブルシューティング

このセクションでは、Flash スキャン機能のトラブルシューティングに関する提案を示します。

問題	アクション
AppScan の新規バージョンをインストールした後で、AppScan を開くたびに以下のエラー・メッセージが繰り返し表示される。 `FlashBrowser has encountered a problem and needs to close.`	1. AppScan を閉じる。 2. 以下のタイプのフォルダー内の **user.config** という名前のすべてのファイルを削除する (Windows 7)。 `C:\Users\<USER_NAME>\AppData\Local\IBM_Corporation\FlashBrowser.exe_Url_<CODE>` 3. AppScan を再始動する。
AppScan がムービー内で URL をまったく検出しなかった。	1. ご使用のシステムがシステム要件を満たしていることを確認する。 2. 「潜在的な脆弱性を発見するために Flash ファイルを実行」(「スキャン構成」 > 「探査オプション」) が選択されていることを確認する。
AppScan が一部の Flash ムービー内では URL を識別したが、他のムービー内では識別しなかった。	1. Flash ムービーのバージョンがサポートされていることを確認する。(サポートされていないムービーは、「アプリケーション・データ」ビューの「フィルタリングされた URL」の下にリストされます。) 2. スキャンを実行したマシンで、Internet Explorer を使用して問題のあるムービーを再生する。Internet Explorer がムービーを正しく再生できること、およびムービーの終了時に IE ステータス・バーに'「完了」'が表示されることを確認します。 3. 「スキャン構成」 > 「探査オプション」で JavaScript 実行が有効であることを確認する。
スキャンの範囲が不完全である。	1. 「スキャン構成」 > 「フォームの自動入力」情報が完全であることを確認する。 2. 「詳細構成」で、「Flash: サンプル間の時間」を大きくする。 3. 「詳細構成」で、「Flash: 範囲」を 2 に設定する。 4. 「拡張オプション」>「**ShowDebugFlashExecution**」を True に設定し、AppScan を再始動し、開かれる"「プレイヤー・コンテナー」"内でムービーが正しく再生されることを確認する。
AppScan が Flash ムービー内で脆弱性をまったく検出しない。	1. 「テスト・ポリシー」で、すべての ActionScript 2 および 3 テストが有効であることを確認する。 2. 「アプリケーション・データ」ビュー > 「スクリプト・パラメーター」で、Flash パラメーターが欠落していないことを確認する。 3. この特定のムービーに脆弱性が存在しない。
AppScan を使用して Flash ムービーを探査した後で、スタンドアロン Flash ムービーのパフォーマンスに変化が認められる。	AppScan は、Flash Player バージョン 10.1 以降に対して復元可能な構成変更を行います。詳細、および変更を取り消すための手順については、 365 ページの『Adobe Flash Player 設定の復元』を参照してください。

問題	アクション
Flash ログのロケーションを知りたい。	385 ページの『Flash ログ・メッセージ』 を参照してください。
サポートに連絡する場合に、どのような情報を送信する必要があるかを知りたい。	1. 拡張サポート・モードをアクティブにする。 2. ムービーを再スキャンする。 3. AppScan ログ・ディレクトリーから AppScanFlashBrowser.log ファイルを送信する。

一部の Flash ムービーがスキャンされない

Flash の実行は使用可能になっているが、AppScan はスキャン中に特定の Flash ムービーのロードに失敗します。

原因

Adobe Flash Player が Flash ムービー実行時に使用する初期化シーケンスと、Flash ムービー内の組み込み Flash SWF ファイルの初期化シーケンスには違いがあります。

動作 **1:Flash** ムービー

Flash ムービーの場合、Adobe Flash Player は以下のアクションを実行します。

1. Flash Stage オブジェクトの初期化
2. Flash ムービー自体 (Sprite オブジェクトまたは Movie Clip オブジェクト) のコンストラクターの呼び出し

動作 **2:**組み込み **SWF** ファイル

Flash ムービーに組み込まれた SWF ファイルの場合、Adobe Flash Player は以下のアクションを実行します。

1. Flash ムービー自体 (Sprite オブジェクトまたは Movie Clip オブジェクト) のコンストラクターの呼び出し
2. Flash Stage オブジェクトの初期化

したがって、組み込み Flash ムービーがそのコンストラクター内で Stage オブジェクトを参照する場合は、その時点で Stage が初期化されていないため、「NULL ポインター例外」が発生することになります。

スキャン中に SWF ファイルをクロールする目的で、AppScan Standard はこれらのファイルを独自の Flash コンテナーにロードします。この処理が Flash ファイルの動作に影響を及ぼすべきではありませんが、上記の不整合があるため、ムービーが AppScan Standard コンテナーにロードされる場合、Adobe Flash Player は (期待される動作 1 ではなく) デフォルトで動作 2 を実行します。ムービーのコンストラクター内に Stage オブジェクトへの参照が含まれている場合、AppScan Standard は NULL ポインターを検出し、ムービーのロードができなくなります。

回避策

現行の Adobe Flash Player 機能を前提とした場合、この問題の唯一の回避策は、スキャンされるサイトの SWF ファイルに小さな変更を加えることです。この変更が、Flash ムービーの機能に影響を及ぼすことはなく、問題の SWF ファイルに対するセキュリティー・リスクを招くこともありません。

コード例:

問題のある SWF ファイルの典型的な構造:

```
package {

 import flash.display.*;
 import flash.events.*;

 public class TestSample extends MovieClip {

  public function TestSample(){

   // Begin initialization tasks
   // There may be one or more references to the Stage object here

   // For example: stage.addEventListener(MouseEvent.CLICK,MouseClicked);

   // End of initialization tasks

  }
  // other functions – no change required

 }

}
```

解決策は、初期化タスクを以下のようにコピーすることです。

```
package {

 import flash.display.*;
 import flash.events.*;

 public class TestSample extends MovieClip {

  public function TestSample(){
   this.addEventListener(Event.ADDED_TO_STAGE, solutionToFlashProblem);
  }

  private function solutionToFlashProblem(e:Event):void
  {

   // Begin initialization tasks
   // There may be one or more references to the Stage object here
   // For example: stage.addEventListener(MouseEvent.CLICK,MouseClicked);

   // End of initialization tasks

  }
  // other functions – no change required
 }
}
```

ここで行ったのは、現在のクラスが Stage オブジェクトに追加されるときに呼び出されるコールバック関数に、コンストラクターの内容をコピーすることだけです。そのようにした場合、Stage オブジェクトは初期化され、その結果、Flash Player は動作 1 を実行します。

Adobe Flash Player 設定の復元

このタスクについて

Flash の実行をアクティブにした状態でスキャンを実行すると、Flash Player 10.1 以降の機能がわずかに影響を受けるため、次に示す機能において Flash 10.0 と同じような動作になります。それは、Flash

Player のウィンドウがアクティブなウィンドウではない場合に Flash Player の実行が停止するというバージョン 10.1 の機能です (この機能は、10.0 にはありません)。この機能は、スキャンを実行すると無効になります。

スキャンが終了したら、変更内容を元に戻すことができます。ただし、Flash の実行をアクティブな状態にして次回にスキャンを実行すると、設定が再度変更されることに注意してください。

手順

1. Flash Player フォルダーを開きます。デフォルトの場合、通常は以下のフォルダーです。

   ```
   C:\WINDOWS\system32\Macromed\Flash
   ```

2. `mms.cfg` ファイルを探し、Microsoft メモ帳などのテキスト・エディターでこのファイルを開きます。
3. 以下の行を探します。

   ```
   FullFramerateWhenInvisible=True
   ```

4. この行を削除します (または、この行の値を False に設定します)。
5. ファイルを保存します。
6. ブラウザーを再始動して、変更内容を有効にします。

マルチステップ操作のトラブルシューティング

アクション・ベースのマルチステップ操作のトラブルシューティングに関するいくつかの提案。

AppScan がアクション・ベースのマルチステップ記録のスキャンに失敗した場合、以下のトラブルシューティングのステップを試してください。

1. 「構成」 > 「マルチステップ操作」 で、シーケンスを選択し、「検証」をクリックします。ブラウザーが開き、シーケンスを再生します。 必要なすべてのステップをブラウザーが実行したことを確認します。記録されたアクションが、サイトの現行バージョンに対応していない場合、シーケンスを再度記録します。
2. ブラウザーが閉じたら、シーケンスの各アクションの隣に緑色のチェック・マークが表示されていることを確認してください。 アクションのいずれかに赤色の X が付いていた場合、シーケンスの次のステップを実行するために、そのアクションが必要があるかどうかを確認してください (再生時に表示されないポップアップのクリックなど)。 そのアクションが必要ない場合、アクションを選択し、 をクリックして削除します。
3. AppScan はシーケンスの各ステップの後に所要時間 0 秒の WAIT アクションを挿入します。 失敗したアクションの前では、WAIT アクションの所要時間を増やしてみてください。
4. テスト要求のすべてのパラメーターと Cookie に対する冗長性調整オプションと追跡オプションの値が正しいことを確認してください。 正しくない場合、それらを修正するか「構成」 > 「パラメーター**/Cookie**」メイン・タブのリストから削除してください。
5. 「構成」 > 「詳細構成」 > 「アクション・ベース**:** マルチステップ再生、非相互作用タイムアウト」 > の非相互作用タイムアウトの値を増やしてください。

署名なしエクステンションの置換

以前のバージョンの AppScan で使用した署名なしエクステンションを使用する場合は、それを信頼するよう選択することも、それの代わりとなる署名済みバージョンがあるか確認することもできます。

このタスクについて

AppScan が開くときに、有効にされているエクステンションが署名済みまたはユーザーによっ動で信頼されているかが検証されます。手動で信頼されていない、署名なしエクステンションはロードされません。

以前のバージョンの AppScan で使用した署名なし IBM エクステンションがある場合は、以下に示すように、横にある「信頼する」ボタンをクリックしてそれを信頼するよう選択することも、代わりとなる署名済みバージョンがあるか確認することもできます。

手順

1. エクステンション・マネージャー (「ツール」>「エクステンション」>「エクステンション・マネージャー」) を開きます。

   ユーザーによって有効にされている (チェック・ボックスが選択されている) が、署名のないエクステンションには、その横に「信頼する」ボタンが表示されます。

   注**:** そのエクステンションを置換することなく信頼するには、「信頼する」ボタンをクリックします。それ以降、このエクステンションは信頼されます。
2. ダイアログ・ボックスの上部にある「他のエクステンションを取得」リンクをクリックします。
3. 開いたページで、「エクステンション」タブをクリックし、そのエクステンションの署名済みバージョンがあるか確認します。
4. エクステンションをご使用のマシンに保存します。
5. エクステンション・マネージャーで、署名なしバージョンを選択 (強調表示) し、「削除」をクリックします。
6. 「インストール」をクリックし、新規エクステンションを選択して、「開く」をクリックします。

   新規エクステンションがインストールされ、有効になります。変更を有効にするには、AppScan を再始動する必要があります。

関連資料:

312 ページの『エクステンション・マネージャー』
エクステンション・マネージャーによって、 で使用するエクステンションを追加/削除、有効化/無効かすることができます。 AppScan

スキャン・ログ・メッセージ

以下のセクションでは、スキャン・ログ・メッセージ (「表示」 > 「スキャン・ログ」) について説明します。

このセクションでは、すべてのスキャン・ ログ・メッセージについて説明します。関連がある場合は、説明および推奨されるユーザー処置を示します。

CRWAD0201I スキャンが作成された

説明**:** 新規スキャンが作成されました。事前に開いているスキャン・データはすべて破棄されます。

ユーザーの処置**:** なし

CRWAD0202I 探査を開始中

説明**:** スキャンの探査ステージを開始しています。

ユーザーの処置**:** なし

CRWAD0203I クローリング

説明**:** 探査ステージの一環としてアプリケーションをクロールしています。

ユーザーの処置**:** なし

CRWAD0204I 探査結果の分析中

説明: テストを作成するために、探査結果を分析しています。

ユーザーの処置: なし

CRWAD0205I テストを開始中

説明: スキャンのテスト・ステージを開始しています。

ユーザーの処置: なし

CRWAD0206I 開始 **URL** の送信中

説明: 開始 URL、および記録されたマルチステップ操作を送信しています。

ユーザーの処置: なし

CRWAD0214I マニュアル探査を開始中

説明: なし

ユーザーの処置: なし

CRWAD0215I マルチフェーズ・スキャン:開始フェーズ **<#>**

説明: なし

ユーザーの処置: なし

CRWAD0216I スキャン停止; スキャン時間: **<time>**

説明: なし

ユーザーの処置: なし

CRWAD0217I 探査データおよびテスト・データが消去されました

説明: なし

ユーザーの処置: なし

CRWAD0218I テスト・データが消去されました

説明: なし

ユーザーの処置: なし

CRWAD0219I 時間制限に達しました。スキャンを停止中です...

説明: スキャン・エキスパートの探査ステージに設定された時間制限に達したため、スキャンが停止し、スキャン・エキスパートは評価ステージに進みました。(AppScan が変更内容を自動的に適用してからメイン・スキャンに進むように構成されている場合は、そのように動作します。「スキャンの停止」とは、スキャン・エキスパートの探査ステージのみを指します。)

ユーザーの処置: 時間制限を変更するには、「スキャン構成」 > 「スキャン・エキスパート」に移動します。

CRWAD0220I **Flash** の実行を開始中

説明: なし

ユーザーの処置: なし

CRWAD0221I サポートされている **Flash Player (Internet Explorer** 用バージョン **9.0.124.0** 以降**)** がインストールされていません。**Flash** は実行されません。**(Flash Execution will not run.)**

説明: Flash ファイルを実行するようにスキャンが構成されていますが、サポートされているバージョンの Adobe Flash Player がこのマシンにインストールされていないため、Flash ファイルは実行されません。

ユーザーの処置: AppScan でスキャン中に Flash ファイルが実行されるようにする場合は、サポートされているバージョンをインストールする必要があります。

最新の Adobe Flash Player は、http://get.adobe.com/flashplayer/ からダウンロードできます。

CRWAD0222I **Flash Player** が構成されていません。**(Flash Player not configured.)Flash** は実行されません。 **(Flash Execution will not run.)**

説明: Flash ファイルを実行するようにスキャンが構成されていますが、AppScan で使用できるように Adobe Flash Player が構成されていないため、スキャン中に Flash ファイルは実行されません。

ユーザーの処置: AppScan でスキャン中に Flash ファイルが実行されるようにする場合は、管理者が Flash Browser を構成する必要があります。 8 ページの『Flash Player の構成』 を参照してください。

CRWAD0301I 認識された **URL: <URL>**

説明: なし

ユーザーの処置: なし

CRWAD0302I URL <URL> の動的なコンテンツによりリンク <URL> を抽出

説明: JavaScript または Flash コンテンツからテスト用の URL が抽出されました。

ユーザーの処置: なし

CRWAD0303I URL をスキップ (拡張子のため): <URL>

説明: この拡張子を持つファイルを除外するようにスキャンが構成されているため、この URL はスキップされます。

ユーザーの処置: これは、「構成」|「除外するパスおよびファイル」で変更できます。

CRWAD0304I URL をスキップ (除外のため): <URL>

説明: スキャンはこの URL を除外するように構成されています。

ユーザーの処置: これは、「構成」|「除外するパスおよびファイル」で変更できます。

CRWAD0305I URL をスキップ (ホストがスキャンに含まれていない): <URL>

説明: スキャンはこのホストを含むように構成されていません。

ユーザーの処置: これは、「構成」|「URL およびサーバー」で変更できます。

CRWAD0306I URL をスキップ (パスの制限を超えました): <URL>

説明: なし

ユーザーの処置: パスの制限は、「構成」|「探査オプション」で変更できます。

CRWAD0307I URL をスキップ (深さ制限を越えました): <URL>

説明: なし

ユーザーの処置: 深さ制限は、「構成」|「探査オプション」で変更できます。

CRWAD0308I URL をスキップ (リンクの制限を超えました): <URL>

説明: なし

ユーザーの処置: リンク制限は、「構成」|「探査オプション」で変更できます。

CRWAD0309I 次の URL 用にテスト <ID> <Issue Type Name> を作成: <URL> <param>

説明: なし

ユーザーの処置: なし

CRWAD0310I アクセスされたページ: [URL]

説明: なし

ユーザーの処置: なし

CRWAD0311I アクセスしたページ: <URL>

説明: なし

ユーザーの処置: なし

CRWAD0312I ドメイン <Host> のデコード・サービスが見つかりませんでした

説明: なし

ユーザーの処置: なし

CRWAD0313I WebSphere Portal デコード・サービス URL <URL> が見つかりました。

説明: なし

ユーザーの処置: なし

CRWAD0401I ログイン要求検出: <URL>

説明: なし

ユーザーの処置: なし

CRWAD0402I ログアウト要求を検出: <URL>

説明: なし

ユーザーの処置: なし

CRWAD0403I 次のセッション識別子が検出されました; 名前 = <name>; 値 = <value>

説明: なし

ユーザーの処置: なし

CRWAD0404I 次のセッション識別子の値が更新されました; 名前 = <name>; 値 = <value>

説明: なし

ユーザーの処置: なし

CRWAD0405I セッションの有効期限切れ

説明: なし

ユーザーの処置: なし

CRWAD0406I ログイン実行中

説明: なし

ユーザーの処置: なし

CRWAD0407I セッション内パターンが検出されませんでした

説明: なし

ユーザーの処置: セッション内パターンは、「構成」|「ログイン管理」|「詳細」で定義されます。

CRWAD0408I 操作がタイムアウトになりました

説明: なし

ユーザーの処置: なし

CRWAD0409I 通信エラー

説明: なし

ユーザーの処置: なし

CRWAD0410I 不要な要求が削除されました: **[URL]**

説明: なし

ユーザーの処置: なし

CRWAD0411I 記録されたログインでの **JavaScript** の実行が有効

説明: なし

ユーザーの処置: なし

CRWAD0412I ログイン時にパラメーター **[name]** を追跡する必要がありますが、このパラメーターは追跡対象外として事前に定義されています。

説明: このパラメーターはログイン手順で出現します。AppScan はこのパラメーターをパラメーターおよび Cookie のリスト (「スキャン構成」 > 「パラメーターおよび **Cookie**」) に追加して、それを「追跡対象」(スキャン時に追跡する) に設定することになっていました。しかし、このパラメーターは既にリストに含まれており、「追跡しない」として構成されているため、AppScan はその構成を変更しませんでした。

ユーザーの処置: 手動でこのパラメーターの状態を「追跡対象」に変更できます。

CRWAD0413I ログイン時に **Cookie [name]** を追跡する必要がありますが、この **Cookie** は追跡対象外として事前に定義されています。

説明: この Cookie はログイン手順で出現します。AppScan はこのパラメーターをパラメーターおよび Cookie のリスト (「スキャン構成」 > 「パラメーターおよび **Cookie**」) に追加して、それを「追跡対象」(スキャン時に追跡する) に設定することになっていました。しかし、このパラメーターは既にリストに含まれており、「追跡しない」として構成されているため、AppScan はその構成を変更しませんでした。

ユーザーの処置: 手動でこの Cookie の状態を「追跡対象」に変更できます。

CRWAD0414I 新しい追跡パラメーター **[name]** が追加されました:

説明: 表記のパラメーターは、パラメーターおよび Cookie のリスト (「スキャン構成」>「パラメーターおよび **Cookie**」) に追加され、「追跡対象」として定義されたため、スキャン時に追跡されます。

ユーザーの処置: なし

CRWAD0415I 新しい追跡 **Cookie [name]** が追加されました:

説明: 表記の Cookie は、パラメーターおよび Cookie のリスト (「スキャン構成」 > 「パラメーターおよび **Cookie**」) に追加され、「追跡対象」として定義されたため、スキャン時に追跡されます。

ユーザーの処置: なし

CRWAD0416I セッション内検出の形式が **[pattern format]** に設定されました

説明: セッション内かどうかを確認するために AppScan が検索するパターンの形式 (「スキャン構成」 > 「ログイン管理」 > 「詳細」を参照) が変更されました。

ユーザーの処置: なし

CRWAD0417I セッション内検出パターンが **[pattern]** に設定されました

説明: なし

ユーザーの処置: なし

CRWAD0418I セッション内 **URL** が **[URL]** に設定されました

説明: ログインしているかどうかを確認するために AppScan が使用するログイン手順の URL が、この URL に設定されました (「スキャン構成」 > 「ログイン管理」 > 「詳細」を参照)。

ユーザーの処置: なし

CRWAD0419I 次のようにログイン・ユーザー名が設定されました: **'<name>' = '<value>'**

説明: なし

ユーザーの処置: なし

CRWAD0420I 次のようにログイン・パスワードが設定されました: **'name' = 'value'**

説明: なし

ユーザーの処置: なし

CRWAD0421I 次のログアウト・ページ検出パターンが設定されました: **'pattern'**

説明: なし

ユーザーの処置: なし

CRWAD0501I テスト **<ID> (<name>)** に成功: **<URL> <param>**

説明: なし

ユーザーの処置: なし

CRWAD0502I テスト **<ID> (<name>)** に失敗: **<URL> <param>**

説明: なし

ユーザーの処置: なし

CRWAD0503I 通信エラーのため、テスト要求 **<URL>** が失敗しました: **<**エラーの説明**>**

説明: 発生する可能性がある 5 つのエラー・メッセージの考えられる理由は、以下のとおりです。

- 接続できない
  - リモート・ホストがアクティブに接続を拒否している
  - リモート・ホストがダウンしている
  - ネットワークが使用不可である
- 接続がタイムアウトになった
  - 制限時間内にサーバーからの応答を受信しなかった
- 接続が閉じている (リモート側)
  - アプリケーションが既にタイムアウトになった接続に対してキープアライブを設定しようとした
  - リモート・ピアによって接続がリセットされた
- 接続が閉じている (ローカル側)
  - 基礎となるソケット・プロバイダーによって接続が異常終了した
  - ソケットが閉じているために、重複した操作が異常終了した
  - 基礎となるソケット・プロバイダーで開いているソケットが多すぎる
- 不明
  - その他のすべての原因

ユーザーの処置: なし

CRWAD0504I テスト応答内で次の **URL** が検出されました: **<URL>;** 認識されていない **URL** に追加しています

説明: 新規 URL は、スキャンに次のフェーズがある場合は、そのフェーズで探査されます。フェーズの限度に達した場合、その新規 URL は、認識されていない URL として結果に表示されます。

ユーザーの処置: なし

CRWAD0505I **<URL>** のテスト **<ID> (<name>)** は、最適化テストによってフィルタリングされました。

説明: なし

ユーザーの処置: 最適化テストのフィルタリングは、「構成」|「テスト・オプション」で変更できます。

CRWAD0506I テスト **<ID> (<name>)** を送信中: **<URL> <param>**

説明: なし

ユーザーの処置: なし

CRWAD0507I ページ分析が **[URL]** で開始されました

説明: なし

ユーザーの処置: なし

CRWAD0508I ページ分析が **[URL]** で完了しました

説明: なし

ユーザーの処置: なし

CRWAD0509I ページ分析が **[URL]** で失敗しました: **(**エラー**)**

説明: なし

ユーザーの処置: なし

CRWAD0510I マルウェア・テスト **<URL>** 結果:脆弱ではない **(<**簡略説明**>)**

説明: なし

ユーザーの処置: なし

CRWAD0601I ホストに接続できません: **<server name>**

説明: なし

ユーザーの処置: なし

CRWAD0602I ホスト **<server name>** との接続が確立されました

説明: なし

ユーザーの処置: なし

CRWAD0603I 必要なホストが応答しなくなったので、スキャンを停止しています

説明: なし

ユーザーの処置: なし

CRWAD0604I セッションが無効になっていることが検出されたため、スキャンを停止しています

説明: AppScan は、「構成」|「ログイン管理」|「詳細」で定義されたパターンに基づいて、セッションが無効になっていることを検出したため、ログインできませんでした。そのため、スキャンを停止しています。

ユーザーの処置: なし

CRWAD0605I **AppScan** により、セッションが無効になっていることが検出されました。

説明: AppScan は、「構成」|「ログイン管理」|「詳細」で定義されたパターンに基づいて、セッションが無効になっていることを検出しました。

ユーザーの処置: なし

CRWAD0606I **AppScan Enterprise** に接続できません

説明: なし

ユーザーの処置: なし

CRWAD0607I **SSL** 構成がホスト **{1}** と一致しません。デフォルトの **SSL** プロトコル **{0}** が使用されます。

説明: ユーザーが選択した最もセキュアな SSL プロトコルを使用して AppScan がホストに接続できない場合、AppScanは、次にセキュアなオプションから順に別の選択済みプロトコルの使用を試みます。このメッセージは、一致が見つかったことを示します。この問題は、AppScan およびホストがサポートしている SSL プロトコルをオペレーティング・システムがサポートしていない場合に発生する可能性があります。

ユーザーの処置: Service Pack をインストールするか、別のオペレーティング・システムを使用することで、この不一致問題が解決される可能性があります。

CRWAD0701I マニュアル・テストを開始中

説明: なし

ユーザーの処置: なし

CRWAD0702I マニュアル・テストで追加されたセキュリティー問題

説明: なし

ユーザーの処置: なし

CRWAD0801I スキャン保存済み: **<full path>**

説明: なし

ユーザーの処置: なし

CRWAD0802I ユーザーによって削除されたセキュリティー問題 **<Issue Type Name>**

説明: ユーザーがこの問題を選択し、右クリックして、「削除」を選択したため、この問題は削除されました。

ユーザーの処置: なし

CRWAD0803I セキュリティー問題 **<Issue Type Name>** の再テスト中

説明: なし

ユーザーの処置: なし

CRWAD0804I テスト **<ID> [<name>]** では再テストはサポートされていません

説明: 再テスト機能ではブラック・ボックス・テストのみがサポートされます。

ユーザーの処置: このテストを再送するには、適切なモジュール (例えば JSA や、マルウェアのテストなど) を再実行する必要があります。

CRWAD0805I ファイル **[full path]** からスキャンをロードしています。スキャンが作成されました。バージョン**: [version]**、ビルド**: [build number]**

説明: なし

ユーザーの処置: なし

CRWAD0806I ユーザーによって脆弱として設定されたセキュリティー問題 **<Issue Type Name>**

説明: なし

ユーザーの処置: なし

CRWAD0807I ユーザーによって脆弱ではないと設定されたセキュリティー問題 **<Issue Type Name>**

説明: なし

ユーザーの処置: なし

CRWAD1001I Scan Expert の開始中

説明: なし

ユーザーの処置: なし

CRWAD1002I Scan Expert が終了しました

説明: なし

ユーザーの処置: なし

CRWAD1003I Scan Expert の評価の開始中

説明: なし

ユーザーの処置: なし

CRWAD1004I Scan Expert の評価が終了しました

説明: なし

ユーザーの処置: なし

CRWAD1005I Scan Expert テスト結果の自動適用中

説明: スキャン・エキスパートのテスト結果に基づいて、スキャン構成を自動的に更新しています。

ユーザーの処置: なし

CRWAD1006I Scan Expert テスト結果の適用が終了しました

説明: スキャン・エキスパートのテスト結果に基づくスキャン構成の自動更新が終了しました。

ユーザーの処置: なし

CRWAD1007I Scan Expert 分析で評価しました**: <name>**

説明: なし

ユーザーの処置: なし

CRWAD1008I Scan Expert 分析で評価に失敗しました**: <name>**

説明: なし

ユーザーの処置: なし

CRWAD1009I スキャン・エキスパート推奨の適用中**: <name>**

説明: なし

ユーザーの処置: なし

CRWAD1010I スキャン・エキスパート**:**探査の最適化**:** 分析のためにスキャンを一時停止中**...**

説明: なし

ユーザーの処置: なし

CRWAD1011I スキャン・エキスパート**:**探査の最適化**:** 自動で開始

説明: 探査の最適化モジュールは、スキャン実行時に自動的に開始するように構成されています。

ユーザーの処置: この設定は、「ツール」 **>** 「探査の最適化**:** 構成」から変更できます。

CRWAD1012I スキャン・エキスパート**:**探査の最適化**:** 手動で開始

説明: なし

ユーザーの処置: なし

CRWAD1013I スキャン・エキスパート:探査の最適化: 反復ごとの最大繰り返し数に達しました。さらに **URL** を収集するためにスキャンを再開します

説明: なし

ユーザーの処置: なし

CRWAD1014I スキャン・エキスパート:探査の最適化: このフェーズに対してハイパフォーマンス・モードをアクティブ化

説明: なし

ユーザーの処置: なし

CRWAD1015I スキャン・エキスパート:探査の最適化: フェーズ完了。次のフェーズのために、**URL** の制限を **{0}** に設定します

説明: なし

ユーザーの処置: なし

CRWAD1016I スキャン・エキスパート:探査の最適化: スキャンの再始動中**...**

説明: 探査の最適化モジュールによって構成変更が行われた後に、既存の探査データを削除して探査ステージをもう一度開始する必要がありました。

ユーザーの処置: なし

CRWAD1017I スキャン・エキスパート:探査の最適化: スキャンを再開中**...**

説明: 続行前に既存データの消去が必要となる構成変更は行われませんでした。スキャンは、中止された位置から再開しています。

ユーザーの処置: なし

CRWAD1018I スキャン・エキスパート:探査の最適化**:URL** が不足しています **({0}** を超えている必要があります**)**

説明: 「切り替えの複雑性」設定は、探査の最適化モジュールが再書き込みセグメントをパラメーターとして定義し、探査ステージを再実行するためには、いくつの URL 内に同じ再書き込みセグメントが含まれていなければならないかを定義します。このしきい値に到達しませんでした。

ユーザーの処置: 「ツール」|「エクステンション」|「探査の最適化: 構成」で、「切り替えの複雑性」設定値を下げることをお勧めします。

CRWAD1019I スキャン・エキスパート:探査の最適化: 中断しています**...**

説明: ユーザーによって探査の最適化が中止されました。

ユーザーの処置: なし

CRWAD1020I スキャン・エキスパート:探査の最適化: ステップ**1**、ナビゲーション・パラメーターを識別しています**...**

説明: 探査の最適化モジュールはナビゲーション・パラメーターを識別しようとしています。識別した場合、それらの冗長性調整は最も厳しい設定値に設定されます。

ユーザーの処置: なし

CRWAD1021I スキャン・エキスパート:探査の最適化**:{0}** 固有 **URL** の分析

説明: なし

ユーザーの処置: なし

CRWAD1022I スキャン・エキスパート:探査の最適化: 分析の許容時間を超過しました

説明: 探査の最適化の実行に許可されている時間を超過しました。

ユーザーの処置: この設定は、「ツール」|「エクステンション」|「探査の最適化モジュール: 構成」で変更できます。

CRWAD1023I スキャン・エキスパート:探査の最適化: 分析が完了しました。

説明: なし

ユーザーの処置: なし

CRWAD1024I スキャン・エキスパート:探査の最適化: 分析は失敗しました。

説明: なし

ユーザーの処置: なし

CRWAD1025I スキャン・エキスパート:探査の最適化: 構成変更を適用中**...**

説明: なし

ユーザーの処置: なし

CRWAD1026I スキャン・エキスパート:探査の最適化: 最適化が見つかりません

説明: なし

ユーザーの処置: なし

CRWAD1027I スキャン・エキスパート:探査の最適化: 冗長性調整のデフォルト設定が変更されました

説明: なし

ユーザーの処置: なし

CRWAD1028I スキャン・エキスパート:探査の最適化: 見つかった再書き込みルール: **{0}**

説明: なし

ユーザーの処置: なし

CRWAD1029I スキャン・エキスパート:探査の最適化: 見つかったナビゲーション・パラメーター **'{0}'**

説明: 探査の最適化モジュールはナビゲーション・パラメーターを検出しました。このパラメーターはパラメーターおよび Cookie のリストに追加され、その冗長性調整は最も厳しい設定値に上げられます。

ユーザーの処置: なし

CRWAD1030I スキャン・エキスパート:探査の最適化: ステップ **2**、**URL** 再書き込みの識別中**...**

説明: 探査の最適化モジュールは URL 再書き込みを識別しようとしています。識別した場合は、適切なカスタム・パラメーターが作成され (「スキャン構成」 | 「パラメーターおよび **Cookie**」 | 「詳細」 タブ)、新規探査ステージが実行されます。

ユーザーの処置: なし

CRWAD1101I **<**エクステンション・ログ・メッセージ **>**

説明: このメッセージは、エクステンションによってログに書き込まれました。

ユーザーの処置: エクステンションは、「ツール」 | 「エクステンション (Extensions)」 | 「エクステンション・マネージャー」で管理されます。

CRWAD1201I マルチステップ操作シーケンスの探査を開始しています

説明: なし

ユーザーの処置: マルチステップ操作は、「構成」 | 「マルチステップ操作」で管理されます。

CRWAD1202I マルチステップ操作シーケンスの探査が終了しました

説明: なし

ユーザーの処置: なし

CRWAD1203I マルチステップ操作シーケンスの探査中**: <name>**

説明: なし

ユーザーの処置: なし

CRWAD1204I マルチステップ操作シーケンスのテストを開始しています

説明: なし

ユーザーの処置: なし

CRWAD1205I マルチステップ操作シーケンスのテストが終了しました

説明: なし

ユーザーの処置: なし

CRWAD1206I マルチステップ操作シーケンスのテスト中**: <name>**

説明: なし

ユーザーの処置: なし

CRWAD1207I シーケンス **[name]** の最適化が見つかりました:要求 **[n]** をテストする前に、要求 **[#1]** ～ **[#2]** を再生する必要があります

説明: AppScan は、要求 n をテストするために、シーケンスで指定されたステップが再生されると判定しました。この要求をテストするとき、シーケンス内の ([#1] 以前の) ステップはすべて省略されます。

ユーザーの処置: 必要な場合は、「スキャン構成」 **>** 「マルチステップ操作」でシーケンスを確認および編集することができます。

CRWAD1208I シーケンス **[name]** の最適化が見つかりました:要求 **[n]** のテスト前に再生は不要です

説明: AppScan は、要求 [n] をテストする前にマルチステップ再生は必要ないと判定しました。したがって、この要求をテストする場合、シーケンス内の前のすべてのステップが省略されます。

ユーザーの処置: 必要な場合は、「スキャン構成」 > 「マルチステップ操作」でシーケンスを確認および編集することができます。

CRWAD1209I シーケンス内の要求 **[n]** を最適化できません: **[name]**

説明: 要求 [n] を送信する試行はすべて失敗しました (複数ステップのシーケンスで以前の要求がある場合もない場合も)。最適化の試行が失敗したので、この要求はテストされません。

ユーザーの処置: AppScan がこの要求を無視するのは適切ではない場合は、「構成」 > 「マルチステップ操作」の「再生最適化を許可する」チェック・ボックスを無効にします。

CRWAD1301I 問題情報の生成中

説明: なし

ユーザーの処置: 「構成」 > 「問題情報」ビューで、どの問題情報モジュールが自動的に実行されるかを制御できます。

CRWAD1302I 問題情報の生成完了

説明: なし

ユーザーの処置: なし

CRWAD1303I 問題情報モジュールの開始中: **<name>**

説明: なし

ユーザーの処置: なし

CRWAD1304I 問題情報モジュールが終了しました: **<name>**

説明: なし

ユーザーの処置: なし

CRWAD1305I 問題情報モジュールが失敗しました: **<name>**

説明: なし

ユーザーの処置: なし

CRWAD1401I **<#>** 件の **Web** サービス要求が探査されました

説明: なし

ユーザーの処置: なし

CRWAD1601I **Glass Box** は、**[URL]** にパラメーター **[parameter name]** を検出しました

説明: なし

ユーザーの処置: なし

CRWAD1602I **Glass Box** は、新規 **URL [URL]** を追加しました

説明: なし

ユーザーの処置: なし

CRWAD1603I **Glass Box** サーバーに接続できません: **[server name]**

説明: なし

ユーザーの処置: なし

CRWAD1604I **Glass Box** テスト **<ID> (<name>)** に成功: **<URL> <param>**

説明: なし

ユーザーの処置: なし

CRWAD1605I **Glass Box** テスト **<ID> (<name>)** に失敗: **<URL> <param>**

説明: なし

ユーザーの処置: なし

CRWAD1606I 通信エラーのため、**Glass box** テスト要求 **<URL>** に失敗しました: <エラーの説明>

説明: 発生する可能性がある 5 つのエラー・メッセージの考えられる理由は、以下のとおりです。

- 接続できない
  - リモート・ホストがアクティブに接続を拒否している

  - リモート・ホストがダウンしている
  - ネットワークが使用不可である
- 接続がタイムアウトになった
  - 制限時間内にサーバーからの応答を受信しなかった
- 接続が閉じている (リモート側)
  - アプリケーションが既にタイムアウトになった接続に対してキープアライブを設定しようとした
  - リモート・ピアによって接続がリセットされた
- 接続が閉じている (ローカル側)
  - 基礎となるソケット・プロバイダーによって接続が異常終了した
  - ソケットが閉じているために、重複した操作が異常終了した
  - 基礎となるソケット・プロバイダーで開いているソケットが多すぎる
- 不明
  - その他のすべての原因

ユーザーの処置: なし

CRWAD1607I Glass Box テスト **<ID> (<name>)** を送信中: **<URL> <param>**

説明: なし

ユーザーの処置: なし

CRWAD1608I Glass Box シンク結果の取り出し

説明: なし

ユーザーの処置: なし

CRWAD1609I Glass Box 未参照パラメーター結果の取り出し

説明: なし

ユーザーの処置: なし

CRWAD1610I Glass Box:未参照パラメーターの監視を開始しました。

説明: なし

ユーザーの処置: なし

CRWAD1611I Glass Box:未参照パラメーターの監視を停止しました。

説明: なし

ユーザーの処置: なし

CRWAD1612I Glass Box:シンクの監視を開始しました。

説明: なし

ユーザーの処置: なし

CRWAD1613I Glass Box:シンクの監視を停止しました。

説明: なし

ユーザーの処置: なし

CRWAD1614I Glass Box エージェント・ホストのオペレーティング・システム、オペレーティング・システム・バージョン、または **Web** サーバーが検出されました。

説明: AppScan が、Glass Box エージェント・ホストに関する情報を検出したことを示す通知メッセージです。

ユーザーの処置: なし

CRWAD1615I アクション・ベースのプレイヤーが開始されました。

説明: なし

ユーザーの処置: なし

CRWAD1616I アクション・ベースのプレイヤーが終了しました **[**成功**]**

説明: なし

ユーザーの処置: なし

CRWAD1617I アクション・ベースのプレイヤーが終了しました **[**失敗**]**

説明: なし

ユーザーの処置: なし

CRWAD1618I アクション・ベースのプレイヤーは、ログインに失敗し、要求ベースのログインにロールバックしています。

説明: AppScan はアクション・ベースのログイン記録に失敗し、今後は要求ベースのログインを使用します。

ユーザーの処置: アクション・ベースのログイン手順の再表示または再記録を試行して問題を解決してください。

AppScanログ・メッセージ

以下のセクションでは、AppScan ログ・メッセージについて説明します。(「ヘルプ」 > 「AppScan ログ」)

このセクションでは、重要度が高い AppScan ログ・メッセージについてのみ取り上げます。関連がある場合は、説明および推奨されるユーザー処置を示します。

CRWAD3000E 不正な **AppScan** レジストリー項目 **<key name>** です。

説明: なし

ユーザーの処置: なし

CRWAD3002I 詳細構成オプションが設定されました **(Advanced Configuration option set)。ID: <ID> =** 値 **<value>**。

説明: なし

ユーザーの処置: なし

CRWAD3003E エラーのため、詳細構成オプションが設定されませんでした **(Advanced Configuration option not set due to error)。ID: <#>**、値 **<value>**。

説明: 指定された ID と値の形式が正しくないため、AppScan は、ユーザーによる詳細構成の変更内容を適用することができませんでした。

ユーザーの処置: ID を設定し、値を修正して、詳細構成の設定を検索してください。

CRWAD3010I AppScan バージョン**: <#> (**ビルド番号**: <#>**、セキュリティー・ルールのバージョン**: <#>)**

説明: なし

ユーザーの処置: なし

CRWAD3100I 新規 **AppScan** プロセスが開始しました。

説明: なし

ユーザーの処置: なし

CRWAD3101I AppScan が終了しました。

説明: なし

ユーザーの処置: なし

CRWAD3102I AppScan プロキシー・ポートは **<port number>** です。

説明: なし

ユーザーの処置: なし

CRWAD3103I AppScan Flash プロキシー・ポートは **<port number>** です。

説明: なし

ユーザーの処置: なし

CRWAD3104I 次のホストで探査ステージを開始しています**: <host(s)>**。

説明: なし

ユーザーの処置: なし

CRWAD3105I 探査ステージを再開しています。 **(Resuming Explore stage.)**

説明: なし

ユーザーの処置: なし

CRWAD3106I ユーザーによって探査ステージが停止されました。**(Explore stage stopped by user.)**

説明: なし

ユーザーの処置: なし

CRWAD3107I 探査ステージが完了しました。**(Explore stage completed.)**

説明: なし

ユーザーの処置: なし

CRWAD3108I 探査ステージとテスト・ステージのデータを消去しています **(Clearing Explore and Test stage data)**。

説明: なし

ユーザーの処置: なし

CRWAD3109I 新規スキャンの作成中です。**(Creating a new scan.)**

説明: なし

ユーザーの処置: なし

CRWAD3200I 次のホストでテスト・ステージを開始しています: **<host(s)>**。

説明: なし

ユーザーの処置: なし

CRWAD3201I テスト・ステージを再開しています。**(Resuming Test stage.)**

説明: なし

ユーザーの処置: なし

CRWAD3202I ユーザーによってテスト・ステージが停止されました。**(Test stage stopped by user.)**

説明: なし

ユーザーの処置: なし

CRWAD3203I テスト・ステージが完了しました。**(Test stage completed.)**

説明: なし

ユーザーの処置: なし

CRWAD3204I テスト・ステージのデータを消去中です。**(Clearing Test stage data.)**

説明: なし

ユーザーの処置: なし

CRWAD3205I **<path>** から探査データをインポートしています。

説明: なし

ユーザーの処置: なし

CRWAD3300W ファイル **<file path>** からの探査データのインポートに失敗しました。

説明: なし

ユーザーの処置: なし

CRWAD3407E ライセンスの確認に失敗しました。**RCL** エラー・メッセージ **(**使用可能な場合**) : <message>**

説明: 考えられる原因:1) ライセンスの有効期限が切れている、2) 使用可能なフローティング・ライセンスがない、3) 3 日間以上、ライセンス・キー・サーバーに接続できない、の 3 つが考えられます。RCL (Rational Common Licensing) メッセージには、この問題の原因についてさらに詳細な内容が記述されている可能性があります。

注: RCL メッセージは使用できない場合があります。

ユーザーの処置: なし

CRWAD3409W **<host>** のライセンスがありません。

説明: なし

ユーザーの処置: 表記のホストが含まれるようにライセンスを更新します (「ヘルプ」 > 「ライセンス」)。あるいは、追加ホストのリストからこのホストを削除します (「スキャン構成」 > 「URL およびサーバー」 > 「追加のサーバーおよびドメイン」)。

CRWAD3410W ライセンス・サーバーが使用できません **(License server unavailable)**。切断モードでの実行は、最長で **3** 日間許可されています。**RCL** メッセージ**: <message>**

説明: AppScan からライセンス・キー・サーバーに接続してフローティング・ライセンスの妥当性を検証できない場合でも、最長で 3 日間、切断モードで引き続き稼働することができます。この期間の経過後も、サーバーに接続してライセンスを検証できない場合は、demo.testfire.com 以外のすべてのサイトについてスキャンが無効になります。RCL (Rational Common Licensing) メッセージには、この問題の原因についてさらに詳細な内容が記述されている可能性があります。

ユーザーの処置: なし

CRWAD3411I ライセンスが正常にチェックアウトされました **(License successfully checked out)**。

説明: なし

ユーザーの処置: なし

CRWAD3500E **AppScan**内部エラーが発生しました。ダンプ・ファイルが **<file path>** に作成されました。 サポートに連絡してください。

説明: 重大な内部エラーが発生したため、AppScan が終了しました。この問題の原因を特定するのにメモリー・ダンプ・ファイルが役立つ可能性があります。

ユーザーの処置: サポートに連絡して、ダンプ・ファイルやその他の関連情報を提供してください。

CRWAD3501E **AppScan**内部エラーが発生しました。スキャンを保存しようとしています。

説明: 重大な内部エラーが発生しました。AppScan は、スキャンを閉じる前に保存しようとしました。この保存が正常に完了した場合は、保存されたスキャンのパスがログの後の方に出現します。

ユーザーの処置: なし

CRWAD3502E 自動リカバリー保存が成功しました。**(Auto-Recover save succeeded.)** リカバリーされたスキャンは **<file path>** に保存されました。

説明: AppScan は、クリティカル・エラーが発生した後のスキャンの保存に成功しました。スキャンは、表記のパスに存在します。

ユーザーの処置: 保存されたスキャン・ファイルをロードして、スキャンを続行してください。

CRWAD3503E 強制終了する前にスキャンを保存しようとしましたが、失敗しました。**(Attept to save the scan before terminating failed.)**

説明: AppScan は、強制終了前に自動リカバリー・スキャン・ファイルを保存できませんでした。

ユーザーの処置: サポートに連絡してください。

CRWAD3600E ルール・ファイルが破損しています。**(Rules file is corrupted.)**

説明: AppScan テストを定義するセキュリティー・ルール・ファイルが破損しています。

ユーザーの処置: サポートに連絡してください。

CRWAD3601E ユーザー定義のルール・ファイルが破損しています。**(User-Defined rules file is corrupted.)**

説明: ユーザー定義テストを定義するセキュリティー・ルール・ファイルが破損しています。

ユーザーの処置: サポートに連絡してください。

CRWAD3602W ルールが欠落しているため、ロードされたスキャンのセキュリティー問題は一部削除されました。

説明: なし

ユーザーの処置: なし

CRWAD3707I サーバー **<name>** が応答していません。

説明: なし

ユーザーの処置: なし

CRWAD3708I サーバー **<name>** が再び応答しています。

説明: なし

ユーザーの処置: なし

CRWAD3709I プロキシー **<name>** が応答していません。

説明: なし

ユーザーの処置: なし

CRWAD3703E 以下の理由でサーバー **{0}** に接続できません。**SSL** 証明書が無効です。

説明: AppScan は、無効な SSL 証明書を持つサーバーへの接続をリジェクトするようにユーザーによって構成されています。アプリケーション・サーバーの SSL 証明書は無効であるため、接続を行うことができません。

ユーザーの処置: 介入者アタックまたはその他のアタックが行われている心配がない場合は、この構成変更を取り消すことができます。「ツール」 > 「オプション」 > 「詳細」タブに進み、HttpsIgnoreCertErrors の項目を見つけて、値を「False」に変更してください。

CRWAD3710I プロキシー **<name>** が再び応答しています。

説明: なし

ユーザーの処置: なし

CRWAD3800E 致命的なエラー: スキャン・ファイル **<file path>** が破損しています。

説明: スキャン・ファイルをロードできません。

ユーザーの処置: サポートに連絡してください。

CRWAD3801E **AppScan** はセッションをロードできませんでした。セッション・ファイルが破損しているか、無効である可能性があります。**(The session file may be corrupt or invalid.)**

説明: スキャン・ファイルは正常に開きましたが、AppScan はスキャン・ファイルからセッションをロードできませんでした。

ユーザーの処置: サポートに連絡してください。

CRWAD3806I スキャンをファイル **<full path>** に保存しています

説明: なし

ユーザーの処置: なし

CRWAD3807I ファイル **<full path>** へのスキャンの保存が終了しました

説明: なし

ユーザーの処置: なし

CRWAD3808I ファイル **<full path>** からスキャンをロードしています。

説明: なし

ユーザーの処置: なし

CRWAD3809I ファイル **<full path>** からのスキャンのロードが終了しました

説明: なし

ユーザーの処置: なし

CRWAD3810I バージョン **<original version>** のスキャンをロードし、現行バージョン **<current version>** に更新しています。

説明: なし

ユーザーの処置: なし

CRWAD3811E バージョン **{0}** のスキャンをロードしていますが、これは現行バージョン **{1}** よりも新しいバージョンです

説明: ロード中のスキャンは、現行バージョン (メッセージに記載) よりも新しいバージョン (メッセージに記載) で作成されています。このスキャンは、ロードに失敗する可能性があります。

ユーザーの処置: なし

CRWAD3813E ディスク容量不足のため、スキャン **<file path>** の保存に失敗しました。

説明: AppScan スキャンの処理時に作成される一時ファイルのサイズは、スキャン自体のサイズにまで到達することがあるので、一時フォルダーには必ずその容量 (スキャンのサイズ) が必要です。 スキャンのサイズは、スキャンされているサイト、テンプレート、構成、見つかった問題に応じて異なります。

ユーザーの処置: 参照: 352 ページの『ディスクの空き容量が不足しています』

CRWAD3814E スキャン・ファイルは読み取り専用ファイルであるため、スキャン **<file path>** を保存できません。

説明: なし

ユーザーの処置: なし

CRWAD3816E ディスク容量不足のため、**AppScan** はスキャンをロードできませんでした。ドライブ **<drive letter>** 上の **<#> MB** を解放して、再試行してください。

説明: AppScan スキャンの処理時に作成される一時ファイルのサイズは、スキャン自体のサイズにまで到達することがあるので、一時フォルダーには必ずその容量 (スキャンのサイズ) が必要です。 スキャンのサイズは、スキャンされているサイト、テンプレート、構成、見つかった問題に応じて異なります。

ユーザーの処置: 参照: 352 ページの『ディスクの空き容量が不足しています』

CRWAD3817W SDK 結果データベースをエンジン・データベースから再ビルドしています **(Rebuilding SDK result database from engine database)**。

説明: SDK 結果データベースが見つかりませんでした。AppScan は、このデータベースをエンジン・データベースから再ビルドしています。

ユーザーの処置: なし

CRWAD3818E DB バージョンが **{n}** のスキャンをロード中。このバージョンはサポートされていません。

説明: このスキャンは、サポートされない AppScan データベース・バージョンを使用して保存されているため、現行の AppScan バージョンではロードできません。

ユーザーの処置: なし

CRWAD4105E クリティカル・スレッド **(<thread name>、tid: <thread id>)** が不自然に消滅しました。

説明: 重大な内部エラーが発生しました。

ユーザーの処置: サポートに連絡してください。

CRWAD4106E 非クリティカル・スレッド **(<thread name>、tid: <thread id>)** が不自然に消滅しました。

説明: 重大な内部エラーが発生しました。

ユーザーの処置: サポートに連絡してください。

CRWAD4300I AppScan 拡張サポート・モードを開始しています。

説明: なし

ユーザーの処置: なし

CRWAD4301I AppScan 拡張サポート・モードは既に **<On/Off>** になっています。

説明: なし

ユーザーの処置: なし

CRWAD4302I AppScan 拡張サポート・モードが停止しました。

説明: なし

ユーザーの処置: なし

CRWAD4303I 拡張サポート情報をファイル **<full path>** に圧縮できませんでした。

説明: なし

ユーザーの処置: なし

CRWAD4500E ディスク容量不足のため、**AppScan** は停止しました。**[** 解放**: <#>M**、必須**: <#>M]**

説明: AppScan スキャンの処理時に作成される一時ファイルのサイズは、スキャン自体のサイズにまで到達することがあるので、一時フォルダーには必ずその容量 (スキャンのサイズ) が必要です。 スキャンのサイズは、スキャンされているサイト、テンプレート、構成、見つかった問題に応じて異なります。

ユーザーの処置: 参照: 352 ページの『ディスクの空き容量が不足しています』

CRWAD4501E メモリー使用量が事前定義された制限に達したため、**AppScan** は停止しました。**[MemUsage: <#>K**、**MaxMemUsage: <#>K]**

説明: なし

ユーザーの処置: メモリー制限 (「ツール」 > 「拡張オプション 」) の値を大きくするか、サポートに連絡してください。

CRWAD4502E システムの仮想メモリーが不足しているため、**AppScan** は停止しました。**[VM: <#>K , AvailableVM: <#>K]**

説明: なし

ユーザーの処置: メモリーを解放するため、他のアプリケーションを閉じてみてください。

CRWAD4503E システム・メモリー不足 **- AppScan** を正常に続行できません。 **[MemUsage: <#>K 、TotalPhysicalMem: <#>K]**

説明: なし

ユーザーの処置: メモリーを解放するため、他のアプリケーションを閉じてみてください。

CRWAD5002E XML 構成のインポートが失敗しました。**(Importing XML Configuration failed.)** 解析エラー **(**有効な場合**): %s (Parse error (if available): %s)**

説明: 構成をエンジンに送信できませんでした。スキャンを続行できません。

ユーザーの処置: サポートに連絡してください。

CRWAD5003I 更新されたスキャン構成をエンジンに適用しています **(Applying updated scan configuration to engine)**。

説明: なし

ユーザーの処置: なし

CRWAD5004E **XML** 構成の解析が失敗しました。**(Parsing XML configuration failed.)**

説明: 構成をエンジンに送信できませんでした。スキャンを続行できません。

ユーザーの処置: サポートに連絡してください。

CRWAD5100E **AppScan** 重大なエラー**: %s**

説明: なし

ユーザーの処置: なし

CRWAD5101E ソフトウェア例外が発生しました**: <message>** 呼び出しスタック**: <stack>**

説明: なし

ユーザーの処置: なし

CRWAD5400I **Glass Box** サーバー **<URL>** バージョン**:**エージェント・バージョン**: <#> ; GBootStrap** バージョン**: <#> ;** エージェント・ルール・バージョン**: <#>**

説明: なし

ユーザーの処置: なし

CRWAD5401E **Glass Box** サーバー **{0}** に接続できません。理由**:**エージェントがインストールされているサーバー、またはエージェント・アプリケーション **URL** にアクセスできません。

説明: AppScan は、リストされているいずれかの理由により、Glass Box サーバーに接続できませんでした。エージェント URL が誤っているか、GBootStrap が実行されていないか、サーバーが停止している可能性があります。

ユーザーの処置: サーバーが実行されており、入力したエージェント URL が正しいことを確認してください。Web ブラウザーを使用してエージェント URL を開くことで、GBootStrap が正しく実行されていることを検証できます。この手順で問題を特定できない場合は、サポートに連絡してください。

CRWAD5402E **Glass Box** サーバー **{0}** に接続できません。理由**:Glass Box** エージェントに接続するための資格情報が指定されていないか、誤っています。

説明: Glass Box エージェントにアクセスするための資格情報が指定されていないか、誤っています。

ユーザーの処置: Glass Box エージェントのインストール時に定義した正しいユーザー名およびパスワードを指定してください。

CRWAD5403E **Glass Box** サーバー **{0}** に接続できません。理由**:**指定された **Glass Box** エージェント **URL** に **Glass Box** エージェントがインストールされていません。

説明: この URL は、Glass Box の GBootStrap ルートでないサイトにつながります。

ユーザーの処置: URL を確認してください。デフォルトでは、次の形式です。

```
http://<server_name>:<port_number>/GBootStrap/
```

CRWAD5404E **Glass Box** サーバー **{0}** に接続できません。理由**:Glass Box** エージェント・インスツルメンテーションが実行されていません。

説明: Glass Box エージェントが指定したサーバーで機能化されていません。

ユーザーの処置:

1. エージェントをインストールしたときにデスクトップ・ショートカットが作成された場合は、サーバーを停止し、デスクトップ・ショートカットを使用して再始動します。
2. Glass Box エージェントを手動で再インストールします (175 ページの『Glass Box エージェントのインストール』を参照)。

CRWAD5405E **Glass Box** サーバー **{0}** に接続できません。理由**:**クライアント・バージョン **{1}** は、**Glass Box** エージェントのファイル・バージョン **{2}** または **Glass Box** エージェントのアプリケーション・バージョン **{3}** より古いバージョンです。

説明: ローカル・マシン上の AppScan のバージョンが最新ではありません。

ユーザーの処置: AppScan の最新バージョンをインストールします。

CRWAD5406E Glass Box サーバー {0} に接続できません。理由:Glass Box エージェントのファイル・バージョン {1} および Glass Box エージェント・アプリケーション・バージョン {2} は、Glass Box クライアント・バージョン {3} より古いバージョンです。

説明: Glass Box エージェントのバージョンが最新ではありません。

ユーザーの処置: Glass Box エージェントの最新バージョンをサーバー・マシンにインストールしてください。

CRWAD5407E Glass Box サーバー {0} に接続できません。理由:Glass box エージェント・アプリケーションのバージョン {1} は Glass box クライアント・バージョン {2} より古いバージョンです。

説明: Glass Box エージェントを手動でインストールする際に、GBootStrap.war をデプロイしなかった可能性があります。

ユーザーの処置: 特定のサーバーに Glass Box エージェントを手動でインストールする際の手順どおりに作業してください。 175 ページの『Glass Box エージェントのインストール』 を参照してください。

CRWAD5408E Glass Box サーバー {0} に接続できません。理由:Glass box エージェント・ファイルのバージョン {1} は Glass box クライアント・バージョン {2} より古いバージョンです。

説明: Glass Box エージェントの JAR ファイル・バージョンが、AppScan のバージョンより古いです。

ユーザーの処置: エージェントのインストール後に、単にサーバーを再始動しなかった可能性があります。サーバーを再始動してみてください。これで解決しない場合は、Glass Box エージェントを再インストールしてください。

CRWAD5409E Glass Box サーバー {0} に接続できません。理由:Glass box エージェント・ルールのバージョン {1} は Glass box クライアント・ルールのバージョン {2} より古いバージョンです。

説明: Glass Box ルールが最新ではありません。

ユーザーの処置:

1. 「**AppScan**」 > 「ヘルプ」 > 「更新の確認」に移動します。
   - ダウンロードが使用可能な場合は、マシンに自動的にダウンロードおよびインストールされます。
   - ダウンロードを利用できない場合、Fix Central で最新バージョンを確認し、インストールしてください。
2. サーバー上のエージェント・ルールを更新するには、「ツール」 > 「**Glass Box** エージェント管理」を開き、目的のサーバーをダブルクリックして、開かれたダイアログ・ボックスで「ルールの更新」をクリックします。
3. アプリケーション・サーバーを再始動して、変更内容を有効にします。

CRWAD5410E Glass Box サーバー {0} に接続できません。理由:Glass Box エージェント・ルールが更新されましたが、更新プロセスを完了するには再始動が必要です。

説明: Glass Box エージェント・ルールが更新されました。新規インスツルメンテーション・ルールをロードするには、サーバーを再始動する必要があります。

ユーザーの処置: サーバーを再始動します。

CRWAD5411E Glass Box サーバー {0} に接続できません。理由:Glass box クライアント・ルールのバージョン {1} が Glass box エージェント・ルールのバージョン {2} より古いです。

説明: Glass Box エージェント・ルールが更新されました。新規インスツルメンテーション・ルールをロードするには、サーバーを再始動する必要があります。

ユーザーの処置:

1. 「**AppScan**」 > 「ヘルプ」 > 「更新の確認」に移動します。
   - ダウンロードが使用可能な場合は、マシンに自動的にダウンロードおよびインストールされます。
   - 自動ダウンロードを利用できない場合、Fix Central (http://www.ibm.com/support/fixcentral/) で最新バージョンを確認し、インストールしてください。
2. アプリケーション・サーバーを再始動して、変更内容を有効にします。

CRWAD5412E Glass Box サーバー {0} に接続できません。理由:SSL 証明書が無効です。

説明: AppScan は、無効な SSL 証明書を持つサーバーへの接続をリジェクトするようにユーザーによって構成されています。Glass Box サーバーの SSL 証明書は無効であるため、接続を行うことができません。

ユーザーの処置: 介入者アタックまたはその他のアタックが行われている心配がない場合は、この構成変更を取り消すことができます。「ツール」 > 「オプション」 > 「詳細」タブに進み、HttpsIgnoreCertErrors の項目を見つけて、値を「False」に変更してください。

Flash ログ・メッセージ

以下の表では、Flash ログを使用したトラブルシューティングについて説明します。

Flash ログには、トラブルシューティングに利用できるメッセージが含まれています。このログは以下に配置されています。

```
...[AppScan Standard installation folder]\Logs\AppScanFlashBrowser.log
```

エラー・メッセージ

エラー・メッセージ	考えられるユーザーの対応
Explore Failed: Couldn't reach initial state!	「構成」 > 「詳細構成」 > 「ムービーのロード待ち時間」の設定値を大きくします。
Movie (NAME) load failed! (TIME) miliseconds timeout, (COUNT) try(s).	「構成」 > 「詳細構成」 > 「ムービーのロード待ち時間」の設定値を大きくします。
current state failed, since Movie is not ready!	「構成」 > 「詳細構成」 > 「ムービーのロード待ち時間」の設定値を大きくします。
Exception while sending status! (MESSAGE). Microsoft .NET framework Hotfix required! Contact IBM Support. Hotfix reference http://support.microsoft.com/kb/971521	この修正プログラムを入手するには、サポートに連絡してください。
Movie(NAME) version (NUMBER) not supported!	ムービーをバージョン 7 以降に再コンパイルします。
Exception in Document Completed at URL(URL)! (MESSAGE)	mshtml.dll の正しいバージョンを入手するには、サポートに連絡してください。
Flash Player not Found!	7 ページの『Flash Player のアップグレード』 を参照してください。
Flash Player version not Supported!	7 ページの『Flash Player のアップグレード』 を参照してください。
Flash Player not configured!	8 ページの『Flash Player の構成』 を参照してください。
Exception while trying to load SWF file!	364 ページの『一部の Flash ムービーがスキャンされない』 を参照してください。

警告メッセージ

警告メッセージ	考えられるユーザーの対応
Explore movie (NAME) stopped! Click limit (VALUE) reached.	「スキャン構成」 > 「探査オプション」 > 「クリック制限」の設定値を大きくします。
Explore movie (NAME) Stopped! Screen limit (VALUE) reached.	「スキャン構成」 > 「探査オプション」 > 「画面制限」の設定値を大きくします。

警告メッセージ	考えられるユーザーの対応
Exception while loading unsupported Flash Movie! (MESSAGE)	ムービーを Flash バージョン 7 以降でリパブリッシュします。
Parsing data from bridge failed due to unsupported movie(NAME)!	ムービーを Flash バージョン 7 以降でリパブリッシュします。
Exception while parsing data from bridge in unsupported movie(NAME)!	ムービーを Flash バージョン 7 以降でリパブリッシュします。
Movie (NAME) not supported!	ムービーを Flash バージョン 7 以降でリパブリッシュします。
Document Complete event not received from Browser!	ムービーを Internet Explorer のスタンドアロン・バージョンで再生します。ステータス・バーの左側に「完了」メッセージが表示されない場合は、SWF ファイルの HTML ページ内でのリンク切れの可能性があります。
Movie (NAME) failed to load in (TIME) miliseconds for (NUMBER) try(s)! Reloading...	「構成」 > 「詳細構成」 > 「ムービーのロード待ち時間」の設定値を大きくします。
No Browse Dialog found!	指定のストリングを「詳細構成」 > 「**Flash:**ファイル・アップロード・ストリング」または「**Flash:**ファイル・ダウンロード・ストリング」で再確認してください。アップロードまたはダウンロード用のボタンを識別しないストリングを削除します。
Exception while trying to create file for upload! (MESSAGE)	アップロード用のファイルが構成されていません。「詳細構成」 > 「**Flash:** ファイル・アップロード・パス」で構成してください。

Glass Box のトラブルシューティング

Glass box エージェント・メッセージおよびその他のトラブルシューティングのヒントをリストした Web ページを開きます。

http://www.ibm.com/support/docview.wss?uid=swg21567723

第 15 章 CLI

このセクションでは、コマンド行インターフェースを使って使用できる構文およびオプションを説明しています。

一部の AppScan 機能は、コマンド行インターフェースを使用して実行できます (つまり、グラフィカル・ユーザー・インターフェースを使用するのではなく、コマンド・プロンプトでコマンドを入力します)。これは特に、スクリプトまたはバッチ・ファイル内から AppScan を自動的に制御する必要がある場合に役立ちます。

重要: CLI を使用するには、管理者権限が必要です。

コマンドの構造

AppScan CLI コマンドは、以下の 3 つの部分で構成されます。

1. ユーティリティー・コマンド: `AppScanCMD`
2. 実行する特定のコマンド。例: `exec`
3. 選択したコマンドの必須指定オプション。例:

```
/base_scan <full path>/d <full path>
```

上記の例では、コマンド全体は以下のようになります。

```
AppScanCMD exec /base_scan <full path> /d <full path>
```

(このコマンドは、選択したベース・スキャンの構成を使用して新規スキャンを実行し、結果を指定された場所に保存します。)

注: コマンドは、接頭部なし (`exec` など)、負符号付き (`-exec` など)、またはスラッシュ付き (`/exec` など) で入力できます。簡潔にするために、このセクションのすべての例では接頭部は使用していません。

注: コマンド・オプションには、負符号 (`-base_scan` など) またはスラッシュ (`/base_scan` など) のどちらかの 接頭部を付ける必要があります。簡潔にするために、以下の例ではすべてスラッシュの接頭部を付けています。

コマンド

このセクションでは、CLI を使用して実行できるアプリケーション固有のコマンドを説明しています。

exec コマンド

`exec` コマンドは、(`/starting_url`、`/base_scan`、または `/scan_template`で) 指定された開始 URL を持つ新規スキャンを作成、実行、および保存します。さらにこのコマンドはオプションで、スキャンのレポートを生成および保存するために使用できます。

`exec` コマンドを実行するには、コマンド・プロンプトで `exec`、`ex`、または `e` と入力し、それに続いて必須コマンド・オプションを入力します。これについては以下に説明します。

注: コマンドが指定されない場合は、exec コマンドがデフォルトで実行されます。

パラメーター

exec コマンドには、以下のパラメーターを含めることができます。

パラメーター	説明
/starting_url | /surl | /su <full_path>	スキャンの開始 URL を設定します。開始 URL がスキャン・テンプレートまたはベース・スキャンで定義されている場合は、ここで定義する必要はありません。
/credentials | /cred | /cr <username:password>	「自動ログイン」を指定し、ユーザー名とパスワードを設定します。 この設定は、SCANT ファイル (使用されている場合) に構成されているログイン情報をオーバーライドします。
/base_scan | /base | /b <full_path>	ソース・スキャンを指定します (絶対パスを含める必要があります)。このスキャンの構成が新規スキャンで使用されます。
/dest_scan | /dest | /d <full_path>	新規スキャンを保存する宛先を指定します (絶対パスを含める必要があります)。パスが指定されない場合、スキャンは一時フォルダーに保存され、AppScanCMD はその正確なロケーションおよびファイル名を通知します。
/scan_template | /stemplate | /st <full_path>	スキャン・テンプレート・ファイルを指定します。
/old_host | /ohost | /oh <full_path> /new_host | /nhost | /nh <full_path>	これらの 2 つのパラメーターを使用して、ベース・スキャン内で 1 つのホストを検索し、別のホストに置き換えることができます。
/login_file | /lfile | /lf <full_path>	保存されたログイン手順をインポートします。
/multi_step_file | /mstepfile | /mf <full_path>	マルチステップ操作ファイルをインポートします。
/manual_explore_file | /mexplorefile | /mef <full_path>	マニュアル探査 (EXD、HAR、DAST.CONFIG、または CONFIG) ファイルをインポートします。 **注:** AppScan Standard バージョン 9.0.1 以降は、EXD ファイルに応答データが含まれています。このデータをインポートするには、フラグ /ir を追加します。フラグが追加されていない 場合、応答データはインポートされず、代わりに探査ステージが実行され (保存された要求が送信されます)、新規の 応答を収集してテストのために分析します。
/policy_file | /pfile | /pf <full_path>	テスト・ポリシー・ファイルをインポートします。
/additional_domains | /adomains | /ad <domain>	スキャンに含める開始 URL のドメイン以外のドメインを定義します。複数の追加ドメインがある場合は、コンマで区切るか、パラメーターの複数インスタンスを追加してください。
/report_file | /rf <full_path>	生成されるレポートの宛先と名前を指定します (絶対パスを含める必要があります)。 このフィールドはオプションです。設定されていない場合、レポートは生成されません。 /rt が rc_ase として定義されている場合、出力は AppScan Enterprise にパブリッシュされるため、レポート・ファイルは必要ありません。

パラメーター	説明
/report_template | /rtemplate| /rtm <CliDefault | GuiDefault | Summary | DetailedReport | Developer | QA | SiteInventory>	レポートに含める情報のタイプを指定します (詳細は 249 ページの『セキュリティー・レポート』 を参照)。 デフォルトのテンプレート (何も指定されていない場合): CliDefault。 これは、「レポート」ダイアログ・ボックスのデフォルト・テンプレートと同一ではありません。そのテンプレートを使用するには、GuiDefault を指定します。
/report_type | /rt <xml|pdf|rtf|txt|html|rc_ase>	レポート・フォーマットを指定します。デフォルトは XML です。 rc_ase は AppScan Enterprise レポートを意味し、出力は既存の設定を使用して AppScan Enterprise にパブリッシュされます (設定を表示するには、「ファイル」 > 「エクスポート」 > 「**AppScan Enterprise** にパブリッシュする **(Publish to AppScan Enterprise)**」 > 「接続設定」をクリックします)。
/ase_application_name | /aan <AppScan Enterprise application name>	レポートのパブリッシュ先の AppScan Enterprise アプリケーションを指定します。 /report_type rc_ase でのみ使用されます。
/min_severity | /ms <low|medium|high|informational>	レポートに含める最小の結果重大度を指定します (非 xml レポートのみ)。 デフォルトは「low」です。
/test_type|/tt <All | Application | Infrastructure | ThirdParty>	レポートに含めるテストのタイプを指定します。デフォルトは「すべて」です。

フラグ

exec コマンドには、以下のフラグを含めることができます。フラグを含めると、フラグの設定を False から True に変更するのと同等の効果が得られます。

フラグ	説明
/continue | /c	スキャンを続行します。
/explore_only | /eo	探査ステージのみを実行します。
/include_responses | /ir	応答データを含むマニュアル探査データ (EXD ファイル) をインポートする際に、応答を組み込みます (/mef と一緒に使用)。 **注:** AppScan Standard バージョン 9.0.1 以降は、EXD ファイルに応答データが含まれています。このフラグを追加し、ファイルに応答データが含まれる場合は、テストのための分析時に使用されます。ファイルに応答データが含まれていない 場合、探査ステージが実行され (保存された要求が送信されます)、新規の 応答を収集してテストのために分析します。
/merge_manual_explore_requests | /mmer	「探査ステージの冗長性調整」設定をマニュアル探査データに適用し、重複する要求を回避します (/mef と一緒に使用)。
/multi-step | /mstep	マルチステップ操作のみをテストします。

フラグ	説明
/open_proxy | /oprxy| /opr /listening_port|/lport|/lp <port number> /save_only|/saveo|/so	AppScan 記録プロキシーを開きます。 デフォルトでは、「ツール」 > 「オプション」 > 「記録プロキシー」タブで設定されたポートが使用されます。 別のポートを設定する場合は、/listening_port <port number> を使用します。 スキャンを実行せずに SCAN ファイルとして保存するには、/save_only|/saveo|/so を使用します。 SCAN ファイルはいくつかのコンポーネント・ファイルを含む Zip ファイルです。コンポーネント・ファイルには、個別の Manual_Explore_#.exd ファイル (ここで "#" は連番) として保存されているマニュアル探査シーケンスなどがあります。 EXD ファイルは別のスキャンにインポートできます。
/scan_log | /sl	スキャン中にスキャン・ログを表示します。
/test_only | /to	テスト・ステージのみを実行します。
/verbose | /v	出力に進行状況行を含めます。

以下に完全なコマンドの例をいくつか示します。

例 **1**

このコマンドは、「標準的なスキャン」テンプレートを使用して、指定された開始 URL を持つスキャンを開始します。

```
appscancmd e /su http://demo.testfire.net.scan
```

例 **2**

このコマンドは、「標準的なスキャン」テンプレートを使用して、指定された開始 URL を持つ探査ステージのみを開始します。

```
appscancmd e /su http://demo.testfire.net.scan /eo
```

例 **3**

このスキャンには、マニュアル探査、マルチステップ操作、記録されたログイン、およびテスト・ポリシーが含まれます。

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/mf D:\MyMultistepOperation.seq
/lf D:\LoginSequence.login
/pf D:\MyTestPolicy.policy
```

例 **4:**追加ドメイン

2 つ以上の追加ドメインをコンマで区切って、単一の -additional_domains パラメーターとして定義できます。または、複数のパラメーターとして定義することもできます。

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/ad demo.testfire.net1,demo.testfire.net2,demo.testfire.net3
/sl
```

または

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/ad demo.testfire.net1
/ad demo.testfire.net2
/ad demo.testfire.net3
/sl
```

例 **5:**ホストおよびポートの変更

スキャン・テンプレートまたはベース・スキャンのホストおよびポートの両方を変更できます。

```
appscancmd e
/st D:\demo.testfire.net.scant
/d D:\demo.testfire.net.scan
/mef D:\ManualExplore.exd
/oh http://demo.testfire.net:80
/nh http://demo.testfire.net2:8090
```

report コマンド

report コマンドは、指定されたスキャンをロードし、セキュリティー・レポートを生成します (詳細は、249 ページの『セキュリティー・レポート』 を参照)。

このコマンドを実行するには、コマンド・プロンプトで report、rep、または r と入力し、それに続いて必須コマンド・オプションを入力します。これについては以下に説明します。(ベース・スキャンおよび宛先パラメーターは必須です。他のパラメーターはオプションです)。

コマンド	説明
/base_scan | /base | /b <full_path>	レポートの作成元のソース・スキャンを指定します (絶対パスを含める必要があります)。
/report_file | /rf <full_path>	生成されるレポートの宛先と名前を指定します (絶対パスを含める必要があります)。 **ヒント:** /rt が rc_ase として定義されている場合、出力は AppScan Enterprise にパブリッシュされるため、レポート・ファイルは必要ありません。

コマンド	説明
/report_template | /rtemplate| /rtm <CliDefault | GuiDefault | Summary | DetailedReport | Developer | QA | SiteInventory | CustomTemplateName>	レポートに含める情報のタイプを指定します。 デフォルトのテンプレート (何も指定されていない場合): CliDefault。 これは、「レポート」ダイアログ・ボックスのデフォルト・テンプレートと同一ではありません。そのテンプレートを使用するには、GuiDefault を指定します。 カスタム・テンプレートを保存してある場合には、それらを指定することもできます。 詳しくは、 249 ページの『セキュリティー・レポート』 を参照してください。
/report_type | /rt <xml|xml_report|pdf|rtf|txt|html|rc_ase>	結果をレポートに保存するための形式を指定します。 **xml** XML ファイルとして保存されている完全なスキャン結果 (レポートではありません) **xml_report** XML ファイルとして保存されている完全に構造化されたレポート **pdf|rtf|txt|html** PDF、RTF、TXT、または HTML ファイルとして保存されている完全に構造化されたレポート **rc_ase** 「ファイル」 **>** 「エクスポート」 **>** 「**AppScan Enterprise** にパブリッシュする **(Publish to AppScan Enterprise)**」 **>** 「接続設定」で定義されている設定を使用して、出力を AppScan Enterprise にパブリッシュします。
/ase_application_name | /aan <AppScan Enterprise application name>	レポートのパブリッシュ先の AppScan Enterprise アプリケーションを指定します。 /report_type rc_ase でのみ使用されます。
/min_severity | /ms <low|medium|high|informational>	レポートに含める最小の結果重大度を指定します (非 xml レポートのみ)。デフォルトは「情報」です。これは、すべての重大度をレポートに含めることを意味します。
/test_type|/tt <All | Application | Infrastructure | ThirdParty>	レポートに含めるテストのタイプを指定します。デフォルトは「すべて」です。

フラグ

report コマンドには、以下のフラグを含めることができます。

フラグ	説明
/verbose | /v	出力に進行状況行を含めます。

例 **1**

このコマンドは、指定されたベース・スキャンの結果を AppScan Enterprise にパブリッシュします。

```
report
-base_scan  "D:\demo.testfire.net.scan"
-report_type rc_ase
```

例 **2**

このコマンドは、「標準的なスキャン」テンプレートを使用して、指定された開始 URL を持つスキャンを開始します。

```
report
-base_scan  "D:\demo.testfire.net.scan"
-report_file D:\SecurityReport.pdf
-report_type pdf
-Scan_Log
-min_severity "informational"
```

delta analysis report コマンド

delta analysis report コマンドは、スキャン結果の 2 つのセットを比較します (詳細は 266 ページの『差分分析レポート』 を参照)。

このコマンドを実行するには、コマンド・プロンプトで delta_analysis_report、delta_report、または dar と入力し、それに続いて必須コマンド・オプションを入力します。これについては以下に説明します。

コマンド	説明
/base_scan | /base | /b <full_path>	レポートの作成元のソース・スキャンを指定します (絶対パスを含める必要があります)。
/target_scan | /target | /ts <full_path>	ベース・スキャンが比較されるターゲット・スキャンを指定します (絶対パスを組み込む必要があります)。
/report_file | /rf <full_path>	生成されるレポートの宛先と名前を指定します (絶対パスを含める必要があります)。
/report_type | /rt <xml|pdf|rtf|txt|html>	レポートを保存するための形式を指定します。

フラグ

report コマンドには、以下のフラグを含めることができます。

フラグ	説明
/verbose | /v	出力に進行状況行を含めます。

このコマンドは、2 つの指定したスキャンの結果を比較する XML レポートを生成します。

```
das
-b  "D:\demo.testfire.net_1.scan"
-ts  "D:\demo.testfire.net_2.scan"
-rf D:\DeltaAnalysisReport.xml
-rt xml_report
```

その他のコマンド

Close Proxy コマンド

close_proxy コマンドは、AppScan 記録プロキシーを閉じます (以前に開かれていた場合)。

close_proxy コマンドを実行するには、コマンド・プロンプトで close_proxy、cprxy、または cpr と入力します。

help コマンド

help コマンドは、このセクションで説明するコマンドの使用法を出力します。

help コマンドを実行するには、コマンド・プロンプトで help または h と入力します。

終了状況コード

AppScanがスクリプトまたはバッチ・ファイル内で実行されると、終了状況コードは操作が正常に実行されたかどうかを示します。

コード	意味
0	正常に終了
1	AppScan は起動に失敗
2	コマンド行エラー
3	ライセンスが無効
4	ロードが失敗
5	スキャンが失敗
6	レポートが失敗
7	保存が失敗
8	一般エラー

コマンド行からの AppScan の起動

手順

コマンド行で以下を入力します。AppScan.exe [<filename>]

- このコマンドは AppScan 実行可能プログラムを実行して GUI を起動します。オプション・パラメーターを追加して、**.scan** ファイルまたは **scant** ファイルを呼び出すこともできます。
- コマンドにファイル名を含める場合、アプリケーションが開始するとすぐに、指定したスキャンまたはスキャン・テンプレートがロードされます。

第 16 章 メニュー、ツールバー、およびキーボード・ショートカット

このセクションでは、メインメニューおよびツールバーの要約を示します。

「ファイル」メニュー

スキャンの作成、オープン、保存などに使用します。

コマンド	クリックで実行される機能
新規	新規スキャンを作成します。
オープン	保存済みスキャン (.scan) またはスキャン・テンプレート (.scant) を開きます。 **ヒント:** フォルダーから AppScan にドラッグ・アンド・ドロップすることで、これらのファイルを開くことも可能です。
保存	現在のスキャンまたはスキャン・テンプレートを保存します。
名前を付けて保存	現在のスキャンまたはスキャン・テンプレートを新しい名前を付けて保存します。
「エクスポート」 > 「XML 形式のスキャン結果」	完了したスキャン結果を、AppScan Enterprise で使用するために XML ファイルとしてエクスポートします。使用している AppScan Enterprise のバージョンによって 2 つのオプションがあります。 • ASE 9.0.3.1 以降 • それより前のバージョン (レガシー)
「エクスポート」 > 「DB 形式のスキャン結果」	完了したスキャン結果をリレーショナル・データベースとしてエクスポートします。データベース・オプションでは、結果が Firebird データベース構造にエクスポートされます。これはオープン・ソースで、ODBC および JDBC 標準に準拠します。
「エクスポート」 > 「クロス・スキャン・データ」	特定の問題を「ノイズ」(誤検出) と定義した場合、この情報を、他のワークステーション上で実行されるスキャンで使用するためにエクスポートできます。(ユーザー自身のワークステーションでこれを実行する必要はありません。この情報は自動的に保存されてその後のスキャンに適用されます。)
「エクスポート」 > 「AppScan Enterprise に結果をパブリッシュ」	AppScan Standard スキャンの結果を AppScan Enterprise にエクスポートし、その結果に対してテスト・ステージを実行し、結果をレポートにまとめます。
「エクスポート」 > 「AppScan Enterprise でジョブを作成」	AppScan Standard のスキャンを AppScan Enterprise にエクスポートします。 AppScan Enterprise バージョン 9.0 以降が必要です。
「エクスポート」 > 「AppScan Enterprise でスキャン・テンプレートを作成」	AppScan Standard の構成を AppScan Enterprise にテンプレートとしてエクスポートします。 AppScan Enterprise バージョン 9.0 以降が必要です。
「エクスポート」 > 「Application Security on Cloud へのスキャンのアップロード」	AppScan Standard 構成ファイル (SCAN または SCANT) を IBM Application Security on Cloud にアップロードします。この構成を使用してフルスキャンを実行することも、ファイルに保存された既存の探査ステージ結果を使用して「テストのみ」を実行することもできます。

コマンド	クリックで実行される機能
「インポート」 > 「探査データ」	マニュアル探査ファイルを読み込みます。サポートされている形式は、EXD、HAR、DAST.CONFIG、および CONFIG です。**注:** 外部で生成された HAR (HTTP Archive) ファイル v1 および v2 がサポートされます。
「インポート」 > 「クロス・スキャン・データ」	特定の問題が、別のワークステーション上で「ノイズ」(誤検出) と定義されてエクスポートされた場合、この情報を、ご使用のワークステーションで実行されるスキャンで使用するためにインポートして、これらの問題がスキャン結果内に含まれないようにできます。
ページ設定	「印刷」コマンド用の用紙サイズ、ソース、用紙の向き、および余白を定義します。
印刷プレビュー	「プレビュー」ウィンドウを開き、アプリケーション・ツリーまたは(現在のカーソル位置に基づく)「結果リスト」を、「印刷」コマンドを使用して印刷した時のイメージで表示します。
印刷	アプリケーション・ツリーおよび 結果リストの現在の内容を印刷します。(アプリケーション・ツリーおよび結果リストをスクロールアップまたはスクロールダウンして表示できるすべてのノードが組み込まれますが、画面上で閉じているノードは印刷出力でも閉じた状態で表示されます。)
ファイル名 (Filenames)	最近使用されたファイル。
終了	AppScan を終了します。

「編集」メニュー

スキャン結果のカスタマイズに使用します。

コマンド	クリックで実行される機能
削除	選択した問題または修復を削除します。
重大度	(「問題」ビューのみ) 選択した問題の重大度レベルをカスタマイズします。
状態	(「問題」ビューのみ) 選択した問題を「ノイズ」として指定します (AppScan では問題として分類されましたが、ご使用のアプリケーションのコンテキストではそれが問題ではないことを意味します。)。 「ノイズ」と指定された問題は、結果から完全に削除するか、または取り消し線付きで表示する (「表示」メニュー >「ノイズとしてマークされた問題を表示」) ことができます。
優先順位	(「修復」ビューのみ) 修復の優先順位を変更します。
検索	現在のスキャン結果内にあるストリング、ID、HTTP コードなどを検索します。(オプションは、3 つのビューのいずれが現在選択されているかによって決まります。)

注: 「重大度」と「優先度」は相互に排他的です。つまり、選択しているビューによって、常にいずれか 1 つだけしか表示されません。

「表示」メニュー

メイン・ウィンドウの表示方法、および表示されるデータを決定するために使用します。

コマンド	クリックで実行される機能
セキュリティー問題	「セキュリティー問題」ビューを表示します。
修復タスク	「修復タスク」ビューを表示します。

コマンド	クリックで実行される機能
アプリケーション・データ	「アプリケーション・データ」ビュー (失敗した要求、認識された URL、スクリプト・パラメーターなど) を表示します。
「表示順」 >	「結果リスト」のソート方法を選択します (重大度/結果/名前)。 「逆順」を選択すると、結果が昇順ではなく降順でリストされます。
レイアウト >	メイン・ウィンドウ・ペインの「水平」または「垂直」レイアウトを選択します。
ようこそ画面	AppScan ようこそ画面を開きます
ノイズとしてマークされた問題を表示	AppScan により検出された問題で、ご使用のアプリケーションの文脈では的外れで無関係な問題には、「ノイズ」とマークを付けることができます。このメニュー項目では、そのような問題を取り消し線付きのテキストで表示するか、またはまったく表示しないかを切り替えます。これを選択すると「ノイズ」は取り消し線付きで表示され、選択解除すると「ノイズ」は表示されません。 221 ページの『問題の状態:「オープン」または「ノイズ」』 を参照してください。
脆弱でないバリアント	脆弱性がないと定義されたバリアントのリストを開きます。 239 ページの『脆弱でないバリアント』 を参照してください。
スキャン・ログ	現在のスキャン中に、AppScan によって実行されたすべてのアクションに関するログを開きます。 320 ページの『AppScan ログ』 を参照してください。
「ツールバーのカスタマイズ」 >	「大きいアイコン」を選択すると、より大きいツールバーのアイコンが表示されます。 ツールバー上に、選択したアイコンのすべてのアイコンの名前を表示する (デフォルト) か、またはいずれのアイコンの名前も表示しないかを選択します。 (いずれの場合も、アイコンの上にマウスをロールオーバーすると、ツールチップでその名前が表示されます。)

「スキャン」メニュー

スキャンを制御するために使用します。

コマンド	クリックで実行される機能
フル・スキャン	フル・スキャン (探査ステージとテスト・ステージ) を開始するか、または一時停止されていたスキャンを続行します。
一時停止	現在のスキャン (「フル・スキャン」、「探査のみ」、または「テストのみ」のいずれか) を一時停止します。後でスキャンを再開できます。また、一時停止したスキャンを保存しておき、後で続行することもできます。
「再スキャン」 >	現在のスキャンまたはスキャン・ステージを再実行します。以下のサブメニュー項目のいずれかを選択します。 再スキャン (フル):すべてのスキャン結果を削除して、フル・スキャンを現在の構成を使用して実行します。 再探査:すべてのスキャン結果を削除して、探査ステージのみを現在の構成を使用して実行します。 再テスト:テスト結果を削除して、新規テスト・ステージを現在の構成と探査結果を使用して実行します。
探査のみ	探査ステージのみを実行し、その後にテスト・ステージを実行しません。
マニュアル探査	サイトを手動で探査します。 149 ページの『AppScan の使用』 を参照してください。

コマンド	クリックで実行される機能
Web サービスの探査 (WSDL)	アプリケーションを手動で探査できるように Generic Service Client を開きます。これにより、要求と応答がテスト・ステージ中に使用されます。
テストのみ	最初に探査ステージを実行しないで、テスト・ステージのみを実行します (または、一時停止していたテストを続行します)。このオプションは、既に探査結果が存在する場合にのみアクティブになります。
マルチステップ操作のみをテスト	1 つ以上のマルチステップ操作 (98 ページの『「マルチステップ操作」ビュー』 を参照) が構成済みで、この操作がスキャン対象のサイトの重要なサブセットを構成している場合、この操作のシーケンスのみをテストすることができます。詳しくは、 205 ページの『マルチステップ操作のみをスキャン』 を参照してください。 スキャン・エキスパートをスキャンの前に実行するように構成している場合でも、この機能の前に自動的には実行されないことに注意してください。必要な場合は、スキャン・エキスパートを「マルチステップ操作のみをスキャン」(「ツール」 > 「スキャン・エキスパート評価の実行」) の前に個別に実行してください。
発見された問題の再テスト	このオプションでは、問題が明らかになったテストのみを送信します。これは、最後のスキャンで検出された問題が修正されたかどうかを素早く確認する方法です。
スキャン・データをすべて消去	スキャン構成だけを保持して、すべての探査結果とテスト結果を削除します。
ホスト/スキーム/ポートの変更	ログイン、マルチステップ操作、またはマニュアル探査 (あるいはそのすべて) の記録を既に完了し、その後に開始 URL のホスト、スキーム、またはポートを変更する場合、これらの記録内の要求と応答の更新および検証が必要になります。 「スキャン」 > 「ホスト/スキーム/ポートの変更」をクリックすると URL を変更できるダイアログ・ボックスが開き、AppScan によって必要な変更が自動的に更新、検証、および確認されます。 ダイアログ・ボックスには、実行されるステップが表示され、各ステップがいつ正常に完了したかを示します。 更新処理が正常に完了しなかった場合、ダイアログ・ボックスには失敗したステップが示され、変更を保存して手動で続行するか、あるいはすべての変更を元に戻すかの選択肢が示されます。 **重要:** 場合によって、AppScan は応答を不適切に更新することがあり、スキャンの一部またはすべてが失敗します。 その場合、問題がある手順を再記録する必要があります。 **注:** マニュアル 探査のデータは更新されても、開始 URL の変更時に自動 探査データとスキャン結果は削除されます。 **注:** このオプションを使用して変更できるのは、開始 URL のみ の、ホスト、スキーム、またはポートのみ です。開始 URL にその他の 変更を加えたり、またはスキャンのいずれかの追加 ドメインのホスト、スキーム、またはポートを変更したりする必要がある場合、このオプションは使用できません。代わりに、スキャンをテンプレートとして保存して、そのテンプレートを使用して新規スキャンを作成してください。
スキャン・エキスパート評価の実行	スキャン・エキスパートは、現在の構成がスキャンされているアプリケーションに最適であるかどうかを評価します。(172 ページの『スキャン・エキスパート (Scan Expert)』 を参照してください。) このオプションでは、完全な評価が実行されます。つまり、スキャン・エキスパートにより、アプリケーションが簡単に探査され、その応答が分析され、また最良の結果を得るための構成に対する変更点が提案されます。
スキャン・エキスパート分析のみ実行	このオプションは、分析ステージのみを実行し、分析の基となるスキャン結果が既に存在する場合にのみアクティブになります。スキャン・エキスパートでは、現在の結果が分析されて構成が最適であるかどうかが判断されます。

コマンド	クリックで実行される機能
スキャン構成	スキャンのプロパティーを定義します。 47 ページの『「スキャン構成」ダイアログ・ボックス』 を参照してください。

「ツール」メニュー

IBM Security パワー・ツールをはじめ、さまざまなレポート作成ツールやカスタマイズ・ツールが提供されます。

コマンド	クリックで実行される機能
レポート作成	現在のスキャンのレポートを作成します。 247 ページの『第 10 章 レポート』 を参照してください。
マニュアル・テスト	テスト・バリアントを手動で作成して、選択した URL に送信します。 236 ページの『マニュアル・テスト』 を参照してください。
すべての問題情報を生成	(このオプションは、スキャン結果が存在する場合のみアクティブになります) すべての問題について、「問題情報」タブに問題情報を生成/更新します。 225 ページの『「問題情報」タブ』 を参照してください。 **ヒント:** 特定の結果のみ についての問題情報を生成するには、「結果」ペインでその結果を右クリックして、「問題情報の生成」を選択します。
スキャン・スケジューラー	スキャンの自動実行の時刻と頻度を設定します。
ユーザー定義テスト	スキャンに新規テストを定義します。 289 ページの『ユーザー定義テスト』 を参照してください。
Glass Box エージェント	スキャンに Glass Box スキャンを含めることができるように、サーバー・サイド Glass Box エージェントを定義します。 174 ページの『Glass Box スキャン』 を参照してください。
拡張 >	
Web サービス・ウィザード (Open API)	ウィザードを開き、1 つ以上の Open API (v2 および v3) 記述ファイル (JSON または YAML) に基づく Web サービスのスキャンを構成します。Web サービス・ウィザードを参照してください。
Pyscan の開始	Pyscan を開き、Python インターフェースを使用して AppScan を制御します。 314 ページの『Pyscan』 を参照してください。
エクステンション・マネージャー	「エクステンション・マネージャー」を開いて、追加のアプリケーションを管理します。 312 ページの『エクステンション・マネージャー』 を参照してください。
パワー・ツール >	
Authentication Tester	Authentication Tester パワー・ツールを実行して、総当り攻撃の認証テストを実行します。
Connection Test	Connection Test パワー・ツールを実行して、ping プロトコルを使用せずに (このプロトコルは、多くのファイアウォールでブロックされます) Web サイトを ping します。
Encode/Decode	Encode/Decode パワー・ツールを実行して、ストリングの各種形式間でのエンコード/デコードを行います。
Expression Test	Expression Test パワー・ツールを実行して、正規表現を検査します。
HTTP Request Editor	HTTP Request Editor パワー・ツールを実行して、HTTP 要求を編集および送信し、またサイトの応答を表示します。

コマンド	クリックで実行される機能
外部ツール...	クリックして、以下のことを行えるダイアログ・ボックスを開きます。 • 「ツール」メニューのパワー・ツールの順序を調整する • 「ツール」メニューから開ける外部プログラムをさらに追加する
オプション	AppScan の各操作をカスタマイズします。 275 ページの『「オプション」ダイアログ・ボックス』 を参照してください。

「ヘルプ」メニュー

マニュアルへのアクセス、サポートの支援の要請、新規ライセンスの取得に使用します。

コマンド	クリックで実行される機能
AppScan ヘルプ	オンライン・ヘルプを開きます (F1 と同様)。
AppScan はじめに	PDF 形式のスタートアップ・ガイドを開きます (Adobe Acrobat Reader が必要)。
AppScanトレーニングおよびサポートのビデオ	トレーニングとサポートのビデオをリスト表示している Web ページを開きます。
アクセシビリティー制御	「アクセシビリティー」メニューをメニュー・バーの最初のメニュー (ファイル・メニューの前) として追加します。
アクセシビリティー資料	「アクセシビリティー制御」ページでオンライン・ヘルプを開きます。
AppScan 資料ライブラリー	IBM Web サイト上の「AppScan ユーザー・ガイド」へのリンクを含む IBM Security AppScan 資料ライブラリー・ページを開きます。これは、ヘルプ・ファイルの印刷可能な PDF バージョンです (Adobe Acrobat Reader が必要)。
AppScan Web サイト	IBM Security AppScan Standard Web サイトがブラウザーで開きます。
ライセンス	新しいライセンスをインストールするか、または要求します。AppScan Enterprise ライセンス許可をインポートします。
サポート >	「拡張サポート・モード」、「サポート・ファイルを暗号化」、または「サポート・リソース」Web ページに進みます。 「拡張サポート・モード」では、IBM サポート・チームがトラブルシューティングを行うことができるように、実行されたアクションに関する詳細ログが作成されます。これにより、AppScan のパフォーマンスが低下する可能性があるため、必要な場合にのみ有効にしてください。
AppScan ログ	システム・ログ・ファイルを開きます。
更新の確認	ご使用の AppScan のバージョンと統合される新しいセキュリティー評価ナレッジの要求を送信します。
更新ログ	ライブ更新インストールに関するログを開きます。
バージョン情報 IBM Security AppScan	全般的な製品情報を表示します。

メイン・ツールバー

ツールバーのアイコンを使用すると、頻繁に使用する機能に素早くアクセスできます (これらの機能へはメニューからもアクセスできます)。

アイコン	名前	クリックで実行される機能
	スキャン >	(スキャンがロードされて構成されている場合にのみ使用できます。) 以下のオプションがある長さの短い「スキャン」メニューを開きます。  フル・スキャンフル・スキャン (探査ステージとテスト・ステージ) を開始するか、または一時停止されていたスキャンを続行します。  探査のみ:探査ステージのみを実行 (または、一時停止している探査を続行) し、その後にテスト・ステージを実行しません。  テストのみ:最初に探査ステージを実行しないで、テスト・ステージのみを実行します (または、一時停止していたテストを続行します)。探査結果が既にある場合にのみ有効です。
	一時停止	(スキャンが実行中の場合にのみアクティブになります。) 現在のスキャン (「フル・スキャン」、「探査のみ」、または「テストのみ」のいずれか) を一時停止します。 後でスキャンを再開できます。また、一時停止したスキャンを保存しておき、後で続行することもできます。
	マニュアル探査	アプリケーションの URL に対してブラウザーを開き、このサイトを手動でブラウズし、進みながら必須パラメーターを入力します。次に、AppScan では、このサイト用のテストの作成時に、これらの探査データが自動的に収集された AppScan 自身の探査データに追加されます。詳しくは、 149 ページの『AppScan の使用』を参照してください。
	構成	「スキャン構成」ダイアログ・ボックスを開いてスキャンを構成します。詳しくは、 47 ページの『「スキャン構成」ダイアログ・ボックス』 を参照してください。
	レポート	現在のスキャン・データでレポートを作成します。詳しくは、 247 ページの『レポートの概要』 を参照してください。
	オンクラウドでスキャン	AppScan Standard 構成ファイル (SCAN または SCANT) を Application Security on Cloud にアップロードします。この構成を使用してフル・スキャンを実行することも、ファイルに保存された既存の探査ステージ結果を使用して「テストのみ」を実行することもできます。
	検索	結果を検索します。詳しくは、 322 ページの『検索結果』 を参照してください。
	スキャン・ログ	「スキャン・ログ」をスキャン中またはスキャン後に表示します。(スキャン中には、AppScan により実行されるすべてのアクションが、実行時にリストされます。)

アイコン	名前	クリックで実行される機能
	パワー・ツール	いずれかのパワー・ツール (AppScan が組み込まれたアプリケーション) を開き、さまざまなタスクの実行を支援します。詳しくは、 293 ページの『パワー・ツール』 を参照してください。

ビュー・セレクター

ツールバーの右側にある 3 つのアイコンは、「アプリケーション・データ」、「セキュリティーの問題」、および「修復タスク」の 3 つのビューを切り替えます。

アイコン	名前	クリックで表示されるビュー
	データ・ビュー	アプリケーション・データ・ビュー詳しくは、 211 ページの『第 7 章 結果:アプリケーション・データ』 を参照してください。
	問題ビュー	セキュリティー問題ビュー詳しくは、 219 ページの『第 8 章 結果:セキュリティー問題』 を参照してください。
	タスク・ビュー	修復タスク・ビュー詳しくは、 243 ページの『第 9 章 結果:修復タスク』 を参照してください。

ブラウザーのツールバー

アプリケーション応答に関するスクリーン・ショットの表示および保存に使用される、組み込みの AppScan ブラウザーのツールバー上のアイコン。

ボタン	説明
	戻る
	進む
	停止
	更新
	デフォルトの開始 URL に移動します。
	現在のページを開始 URL にします。
	このページをキャプチャーします (ブラウザーが 25 ページの『詳細ペイン』 内の「スクリーンショット」タブから開かれている場合にのみ有効)。

キーボード・ショートカット

AppScan は、次のキーボード・ショートカットを使用します。

ショートカット	機能
F1	AppScan オンライン・ヘルプを開きます
F2	「データ」ビューを開きます
F3	「問題」ビューを開きます
F4	「タスク」ビューを開きます
F5	フル・スキャンを開始します
[Shift] + F5	スキャンを一時停止します
F10	「構成」ダイアログ・ボックスを開きます
[Ctrl] + N	新規スキャンの作成
[Ctrl] + O	既存のスキャンを開きます
[Ctrl] + S	現在のスキャンを保存します
[Ctrl] + P	アプリケーション・ツリーの現在の内容および結果リストを印刷します。(アプリケーション・ツリーおよび結果リストをスクロールアップまたはスクロールダウンして表示できるすべてのノードが組み込まれますが、画面上で閉じているノードは印刷出力でも閉じた状態で表示されます。)
[Ctrl] + W	ようこそ画面を開きます

アクセシビリティー制御

すべてのキーボード・ショートカットおよび制御について説明します。

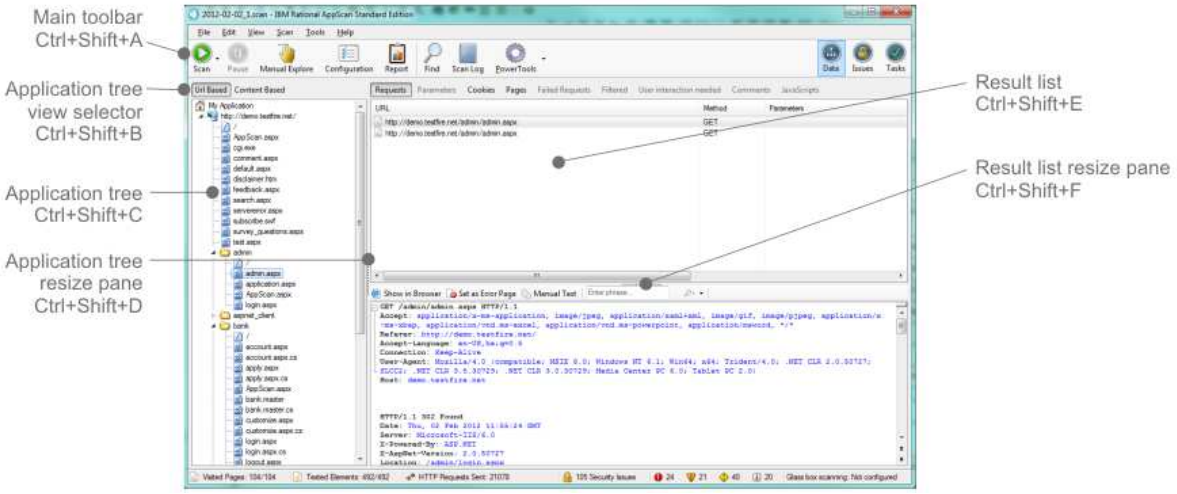
「ヘルプ」>「アクセシビリティー制御」をクリックしてチェック・マークを付けることで、すべてのキーボード・アクセシビリティー機能をアクティブにできます。「ファイル」メニューの左側に「アクセシビリティー」メニューが表示され、追加のキーボード制御 (以下を参照) が有効になります。

「アクセシビリティー」メニュー

「アクセシビリティー」メニューは、「ヘルプ」 > 「アクセシビリティー制御」にチェック・マークが付いている場合のみ表示されますが、ここにリストされているショートカットは、チェック・マークが付いていない場合でも機能します。最初の 3 つのセクションは、ユーザー・インターフェース・ビューを制御します。残りのセクションは、他のメニューからのキーボード・ショートカットです。

すべてのビュー

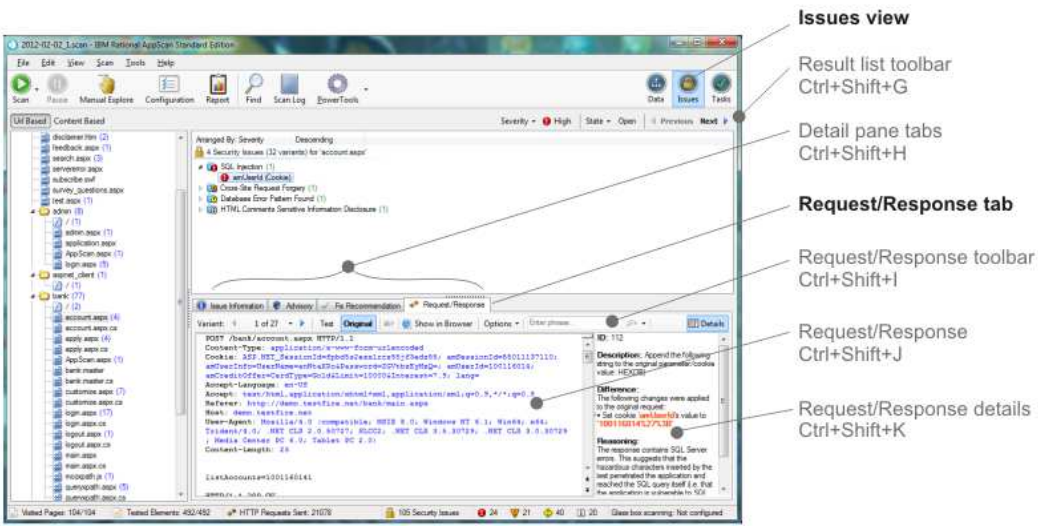
以下のショートカットは、すべてのビューに適用されます。



コマンド	ショートカット	説明
メイン・ツールバー	Ctrl+Shift+A	メイン・ツールバーにフォーカスを移動します。左矢印と右矢印を使用して、ツールバー・アイコンを選択します。 **注:** フォーカスには、ツールバーの右端に 3 つの「ビュー・セレクター」アイコンもあります。
アプリケーション・ツリー・ビュー・セレクター	Ctrl+Shift+B	アプリケーション・ツリー・ビュー・セレクターにフォーカスを移動します。 URL ベースのビューとコンテンツ・ベースのビューを切り替えるには、左矢印と右矢印を使用します。
アプリケーション・ツリー	Ctrl+Shift+C	アプリケーション・ツリーにフォーカスを移動します。上矢印と下矢印を使用してナビゲートします。ノードを開いたり閉じたりするには、左矢印と右矢印を使用します。
アプリケーション・ツリーのサイズ変更	Ctrl+Shift+D	アプリケーション・ツリー・ペインと結果リストの間の境界線にフォーカスを移動します。ペインを調整するには、矢印キーを使用します。
結果リスト	Ctrl+Shift+E	結果リストにフォーカスを移動します。上矢印と下矢印を使用してナビゲートします。ノードを開いたり閉じたりするには、左矢印と右矢印を使用します。
結果リストのペインのサイズ変更	Ctrl+Shift+F	結果リストと詳細ペインの間の境界線にフォーカスを移動します。ペインを調整するには、矢印キーを使用します。

問題ビュー

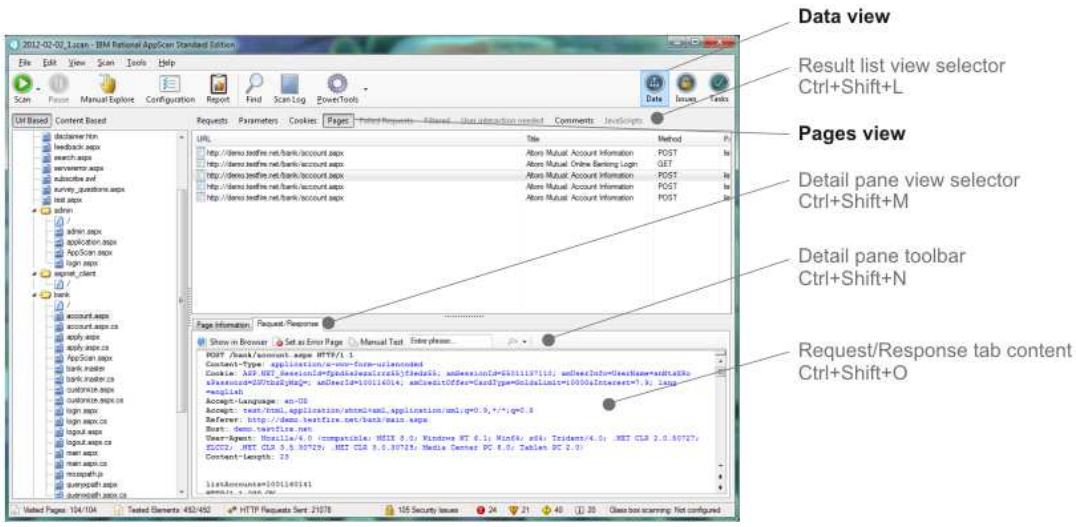
以下のショートカットは、問題ビューにのみ適用されます。



コマンド	ショートカット	説明
結果リスト・ツールバー	Ctrl+Shift+G	問題ビュー内: 結果リストにフォーカスを移動します。上矢印と下矢印を使用してナビゲートします。ノードを開いたり閉じたりするには、左矢印と右矢印を使用します。
詳細ペイン	Ctrl+Shift+H	「詳細ペイン」タブにフォーカスを移動します。
詳細ペイン > 「要求/応答」ツールバー	Ctrl+Shift+I	問題ビュー内: 詳細ペインの「要求/応答」タブ・ツールバーを開き、そのツールバーにフォーカスを移動します。
詳細ペイン > 要求/応答	Ctrl+Shift+J	問題ビュー内: 詳細ペインの「要求/応答」タブを開き、そこにフォーカスを移動します。
詳細ペイン > 要求/応答の詳細	Ctrl+Shift+K	問題ビュー内: 詳細ペインの「要求/応答」タブの「詳細」セクション (右側ペイン) を開き、そこにフォーカスを移動します。

データ・ビュー

以下のショートカットは、データ・ビューにのみ適用されます。



コマンド	ショートカット	説明
結果リスト・ビュー・セレクター	Ctrl+Shift+L	データ・ビュー内:「結果リスト」ツールバーにフォーカスを移動します。「要求」、「パラメーター」、「Cookie」などを選択するには、左矢印と右矢印を使用します。
詳細ペイン・ビュー・セレクター	Ctrl+Shift+M	データ・ビュー > ページ内「ページ情報」または「要求/応答」を選択できます。切り替えるには、左矢印と右矢印を使用します。
詳細ペイン >「要求/応答」ツールバー	Ctrl+Shift+N	データ・ビュー > ページ内「要求/応答」ツールバーにフォーカスを移動します。左矢印と右矢印を使用してナビゲートします。
詳細ペイン >「要求/応答」タブ	Ctrl+Shift+O	データ・ビュー > ページ内「要求/応答」タブの内容にフォーカスを移動します。

その他のキーボード・ショートカット

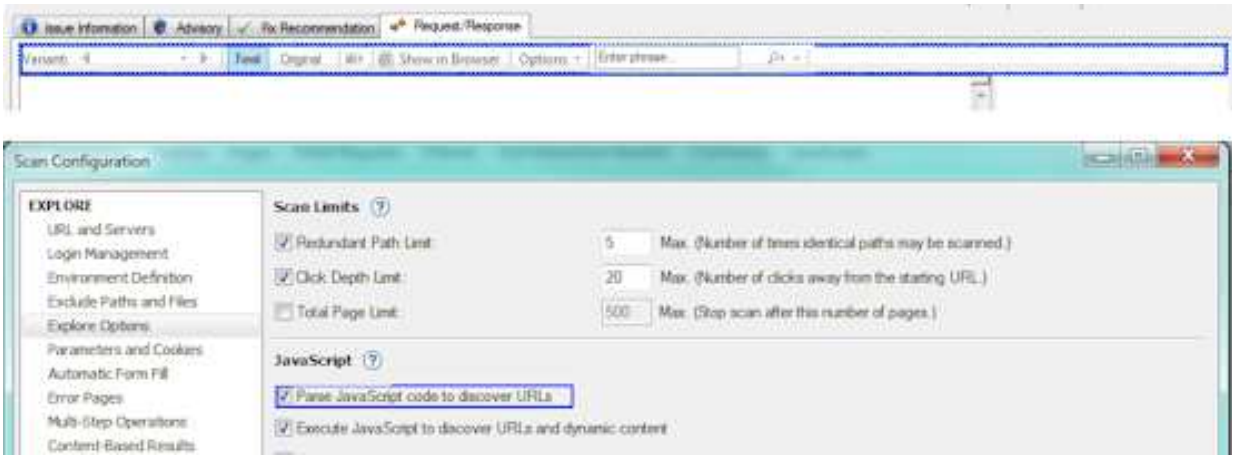
残りのショートカットは他のメニューにも存在しており、でリストされています。 403 ページの『キーボード・ショートカット』

追加のキーボード制御

「ヘルプ」>「アクセシビリティー制御」が有効な場合:

- アクセシビリティー・ショートカットを使用して、フォーカスをユーザー・インターフェースの別の場所に移動すると、新たなフォーカスが赤色で一時的にアウトライン表示されます。

- F7 を押すことで、メイン・ユーザー・インターフェースでも「構成」ダイアログ・ボックスでも、現在のフォーカスがある場所をいつでも確認できます。現在のフォーカスは、青色で簡潔にアウトライン表示されます。


Issue Information
Advisory
Fix Recommendation
Request/Response
Test
Original
Show in Browser
Options
Enter phrase
Scan Configuration
EXPLORE
URL and Servers
Login Management
Environment Definition
Exclude Paths and Files
Explore Options
Parameters and Cookies
Automatic Form Fill
Error Pages
Multi-Step Operations
Content-Based Results
Scan Limits
Redundant Path Limit
5
Max. (Number of times identical paths may be scanned.)
Click Depth Limit
20
Max. (Number of clicks away from the starting URL.)
Total Page Limit
500
Max. (Stop scan after this number of pages.)
JavaScript
Parse JavaScript code to discover URLs
Execute JavaScript to discover URLs and dynamic content

第 17 章 用語集

この用語集は、AppScan Standard のユーザー・インターフェースおよび資料で使用されている用語と頭字語について説明します。

その他の用語および定義については、IBM Terminology Web サイトを参照してください (新規にウィンドウが開きます)。

A

アクセス制御 **(access control)**
: コンピューター・セキュリティーで、ユーザーが権限を持つコンピューター・システムのリソースにしかアクセスできないようにするプロセス。

アクション・ベースのログイン **(action-based login)**
: このタイプのログイン再生は、ログイン手順を記録したときに実行されたアクションを再現します。通常、このログイン方法が優先されます。

アクション・ベースのログイン・プレイヤー **(action-based login player)**
: 2 つのペインから構成されるブラウザーで、検証およびトラブルシューティングのためにアクション・ベースのログインが再生されます。左側のペインには、アクションのリストが表示され、現在実行されているアクションが強調表示されます。右側のペインには、現行アクションの結果が表示されます。

アドバイザリー **(advisory)**
: 脅威や脆弱性に関する情報や分析が含まれている文書。

アプリケーション・ライフ・サイクル **(application lifecycle)**
: 開発から実動まで、製品が通る一連のステージ。

アプリケーション・サーバー **(application server)**
: アプリケーション・プログラムの実行環境を用意するために分散ネットワークに配置するサーバー・プログラム。

アプリケーション・テスト **(application test)**
: 不安定なソフトウェア開発によって生じるアプリケーション・ロジックやアプリケーション問題に重点を置くテストのタイプ。

アプリケーション・ツリー **(application tree)**
: ディレクトリーやファイルを含む、Web アプリケーションの構造のツリー表示。

攻撃 **(attack)**
: 権限を持たないユーザーがソフトウェア・プログラムやネットワーク化システムの操作を侵害しようとする行為。「攻撃者 (attacker)」も参照。

アタッカー **(attacker)**
: 情報システムに危害を加えたり、一般的なアクセスが意図されていない情報にアクセスしたりすることを試みる、ユーザー (人間またはコンピューター・プログラム)。「ハッカー (hacker)」、「攻撃 (attack)」も参照。

認証
: ユーザーの身元またはサーバーの身元を検証するプロセス。

Authentication Tester
総当り攻撃テスト用ユーティリティー。パワー・ツールのいずれかです。ユーザーの Web アプリケーションへのアクセス権限を取得する目的で使用される可能性がある、ユーザー名とパスワードの脆弱な組み合わせを検出する。

許可 **(authorization)**
ユーザーに付与する、コンピューター・システムと通信したり、コンピューター・システムを使用したりするための権限。

B

バックエンド **(back end)**
データベース管理システムなど、コンピューター・システムのサポート・コンポーネントの集合。

ブラック・ボックス **(black box)**
アプリケーションの内部コードを参照せずにアプリケーションの出力を調査する場合、そのアプリケーションを「ブラック・ボックス」、そのテストを「ブラック・ボックス・テスト」と表現することがあります。これは、内容の見えない「ブラック・ボックス」としてアプリケーションが処理されるためです。「white box」および「glass box」と比較してください。

リンク切れ **(broken link)**
選択されたときに無効な応答を返すリンク。

総当り攻撃 **(brute force)**
システムのセキュリティーを侵害するために、考えられるすべての資格情報を試みるプログラムによる攻撃。

バッファー **(buffer)**
処理中のデータを保持するために使用するメモリーの予約済みセグメント。

バッファー・オーバーフロー **(buffer overflow)**
メモリーの一部を上書きすることによってアプリケーションのフローを変更する攻撃技法。バッファー・オーバーフローは、ソフトウェアの誤動作の一般的な原因である。

C

大/小文字の区別 **(case-sensitive)**
大文字と小文字を区別できる機能を指す。

CGI 「コモン・ゲートウェイ・インターフェース (Common Gateway Interface)」を参照。

文字エンコード **(character encoding)**
所定のセットに含まれる一連の文字を、自然数、オクテット、電気パルスなど、何か他のものと対応付けるコードで構成される文字セット。エンコードにより、通信ネットワークを介したテキストの保管や伝送が容易になる。

下位ノード **(child node)**
別のノードの範囲内にあるノード。

クライアント **(client)**
ネットワークに接続されているユーザーのワークステーション。ホスト (host) も参照。

クライアント・サイド **(client-side)**
サーバー上ではなく、クライアント・アプリケーション上で実行される操作を指す。

コード・インジェクション **(code injection)**
アプリケーションに新しいコードを挿入する手法。コード・インジェクションが攻撃者によって使用されて、コンピューター・プログラムにコードが挿入され、実行の流れが変更される可能性がある。

コモン・ゲートウェイ・インターフェース **(CGI) (Common Gateway Interface (CGI))**
HTTP 要求を介して、Web サーバーとアプリケーション・プログラムとの間で情報を受け渡すスクリプトを定義するためのインターネット標準。

通信タイムアウト **(communication timeout)**
指定された時間が過ぎた後で、未完了のタスクを意図的に終了すること。

同時ログイン **(concurrent login)**
他のログインと同時に発生するログイン。

条件パターン **(condition pattern)**
正規表現で、正規表現が定義するパターン。正規表現を使用して、パターンと一致する項目を検出することができる。

Cookie
サーバーがクライアント・マシンに保管して、後続のセッションでアクセスする情報。サーバーは、Cookie を使用してクライアントに関する特定の情報を取得できる。

クロール **(crawl)**
インターネットまたはイントラネット上のさまざまな Web ページで情報を検索すること。

クロスサイト・スクリプティング **(XSS) (cross-site scripting (XSS))**
クライアントから入力されたデータを Web サイトでそのまま書き出すように強制設定することによって、そのデータをユーザーの Web ブラウザーで実行する攻撃技法。

カスタム・エラー・ページ **(custom error page)**
ユーザーがデフォルトのエラー・メッセージをアプリケーション用にカスタム・デザインされたメッセージに置き換えることができる、ほとんどの Web サーバー・ソフトウェアにある機能。

CVE 共通脆弱性と暴露 (Common Vulnerabilities and Exposures)。公的に認識されている情報セキュリティーの脆弱性と暴露に関する一般名を提供する業界標準のリストです。

CVSS 共通脆弱性評価システム (Common Vulnerability Scoring System)。脆弱性に関連付けられているリスクを評価するためのオープン・フレームワーク。

CWE 共通脆弱性タイプ一覧 (Common Weakness Enumeration)。公的に認識されているソフトウェアの脆弱性に関する一般名を提供する業界標準のリスト。

D

データベース管理システム **(DBMS) (database management system (DBMS))**
データベースの作成、編成、変更、およびデータベースに格納されているデータへのアクセスを制御する、ソフトウェア・システム。

データベース・サービス **(database service)**
データベースへのデータの保管およびデータベースからのデータの取得を提供するサービス。

DBMS
「データベース管理システム (database management system)」を参照。

デバッグ・コマンド **(debug command)**
ソフトウェア開発プロセス中のプログラミング・エラーの識別に役立つ機能またはコマンド。

デルタ **(delta)**
2 つのインスタンス間の差異、または増分値。

サービス拒否攻撃 **(DoS) (denial-of-service attack (DoS))**
ネットワークに存在する 1 つ以上のホストをダウンさせることによって、そのホストが自身の機能を正しく実行できないようにする攻撃を指すコンピューター・セキュリティー用語。一定の期間、ネットワーク・サービスが中断される。

深さ **(depth)**
ソース・ページからターゲット・ページに移動するために、ユーザー、または自動クローラーが実行する必要があるクリックの回数。

ディレクトリー索引付け **(directory indexing)**
インデックス・ページが表示されない場合にディレクトリーの内容を公開する Web サーバーの機能。

ディレクトリー・トラバーサル **(directory traversal)**
文書ルート・ディレクトリーの先にあるファイルおよびコマンドにアクセスすることによって Web サイトを悪用する場合に使用される手法。

ドメイン **(domain)**
1 つのセキュリティー・データベースの制御下にあるクライアントおよびサーバーのサブネットワーク。

DoS サービス拒否攻撃 (denial-of-service attack) を参照。

ダンプ・ファイル **(dump file)**
レポート・フォーマット設定のないメモリーのコンテンツ。

E

組み込みブラウザー **(embedded browser)**
AppScan に組み込まれている Web ブラウザー。スキャンを処理するための専用のツールバーから開く。

エンコード攻撃 **(encoding attack)**
ユーザー提供のデータのフォーマットを変更してサニティー・チェック・フィルターを迂回することで攻撃を助長する悪用手法。

暗号化 **(encryption)**
オリジナルのデータを取得できないように、または復号化プロセスを使用した場合のみ取得できるように、データを理解不能な形式に変換するプロセス。

除外 **(exclusion)**
テストの際に値が除外されるパラメーターまたはプロセス。

実行可能ファイル **(executable)**
特定の環境で実行する準備が整っているプログラム・ファイル。

探査の設定 **(Explore setting)**
アプリケーションを AppScan でどう探査するかを制御するパラメーターを構成する設定。

探査ステージ
テストの前の、アプリケーションのロジックとオブジェクトの識別が実施される AppScan スキャンのステージ。

エクスポート **(export)**
現行の文書、データベース、またはイメージのコピーを、別のアプリケーションが必要とするファイル・フォーマットに保存すること。

拡張サポート・モード **(extended support mode)**
ユーザーが、使用オプションと動作を記録し、ファイルにそのデータを保存してテクニカル・サポートに送ることができるモード。

F

誤検出 **(false positive)**
検出 (サイトが攻撃に対して脆弱であることを示す) として分類されるが、ユーザーの判断は実際には検出なし (脆弱ではない) であるテスト結果。

推奨される修正 **(fix recommendation)**
検出された問題から Web アプリケーションを保護するための Web アプリケーションの修正に関する具体的な技術上の詳細情報。

Flash Web ブラウザーにムービーやアニメーションをスムーズに表示することを可能にするプログラミング手法。

フォーム・プロパティー **(form property)**
フォームに自動的に入力するときに使用される値。

絶対パス名 **(full path name)**
ルート・ディレクトリーから始まるディレクトリーおよびファイルのストリングとして表現されるディレクトリーまたはファイルの名前。

G

glass box
内容の見えない「ブラック・ボックス」としてアプリケーションが処理される「ブラック・ボックス・テスト」とは異なり、「glass box」テストではアプリケーションのコードを調査することで「ボックスの中身」を調べます。そのため、glass box テストでは、ブラック・ボックス・テストでは特定できないセキュリティー上の脆弱性を正確に特定できる場合があります。

グラフィカル・ユーザー・インターフェース **(GUI) (graphical user interface (GUI))**
高解像度グラフィックス、ポインティング・デバイス、メニュー・バーやその他のメニュー、オーバーラップ・ウィンドウ、アイコン、およびオブジェクト - アクション関係を組み合わせることで、実在のシーン (多くの場合はデスクトップ) を視覚的に表現するコンピューター・インターフェースのタイプ。

GUI 「グラフィカル・ユーザー・インターフェース (graphical user interface)」を参照。

H

ハードコーディング **(hard-coding)**
出力や構成データをプログラムやその他の実行可能オブジェクトのソース・コードに直接埋め込むソフトウェア開発方法。

危険な文字 **(hazardous character)**
XSS や SQL インジェクションなど、Web アプリケーション攻撃を行うために使用される文字。

非表示のパラメーター **(hidden parameter)**
Web ページに表示されない HTML フォームのパラメーター。

ホスト **(host)**
ネットワークに接続し、そのネットワークへのアクセス・ポイントを提供するコンピューター。ホストは、クライアントの場合もサーバーの場合もある。クライアントとサーバーが同時にホストになることもある。「クライアント (client)」も参照。

HTML フォーム要素 **(HTML form element)**
テキスト・フィールド、テキスト域フィールド、ドロップダウン・メニュー、ラジオ・ボタン、チェック・ボックスなど、ユーザーがフォームに情報を入力する場合に使用できる要素。

HTTP 要求 **(HTTP request)**
スキャンの探査ステージまたはテスト・ステージのいずれかでサイトに送信される要求。

HTTP 応答 **(HTTP response)**
サーバーから送信される応答。

I

ID 「識別子 (identifier)」を参照。

識別子 **(ID) (identifier (ID))**
データ要素を識別したり指定したりする場合に使用されるだけでなく、そのデータ要素の特定のプロパティーを示す場合にも使用されることがある、1 つ以上の文字。

インポート **(import)**
使用中のアプリケーションに固有ではないフォーマットでファイルを読み取ること。

業界標準のレポート **(Industry Standards report)**
選択された業界標準に従った、ユーザーの Web アプリケーションで検出された問題と関連情報のレポート。 AppScan の業界標準のレポートには、「SANS トップ 20 (SANS Top 20)」、「OWASP トップ 10 (OWASP Top 10)」、および「WASC 脅威の分類」がある。

セッション内検出
まだログインしていることを確認するための、AppScan が受信する応答でのセッション内パターンの検出。

セッション内パターン **(in-session pattern)**
まだログインしていることを確認するために AppScan が使用できる、ログアウト・リンクなど、ログイン・ページで識別されるパターン。

自動化の停止が不適切 **(insufficient anti-automation)**
手動でのみ実行するべきプロセスをアタッカーが自動化してしまうことが可能な Web サイトの状態。

対話型 **URL (interactive URL)**
ユーザーが手動で入力するフォームを含む URL。

安全でないテスト **(invasive test)**
アプリケーションで実行した場合に、サービス妨害状態を招く可能性があるオプション・テスト。

問題 **(issue)**
Web アプリケーションが脆弱であるセキュリティー上のリスク、または場合によっては、権限を持たないユーザーが確認できる機密情報。

J

Java アプレット **(applet)**
Java で作成され、Java 仮想マシン (JVM) を使用して Web ブラウザーで実行できるアプレット。

Java 仮想マシン (JVM) (Java virtual machine (JVM))
コンパイル済みの Java コード (アプレットやアプリケーション) を実行するプロセッサーのソフトウェア実装。

L

リンク抽出 (link extraction)
Web アプリケーションからリンクを検出および収集するためのコードの構文解析または実行。

ログイン手順 (login sequence)
AppScan がスキャンを行うために Web アプリケーションにログインできるようにするユーザー入力のシーケンス。ログインを手動で記録することが推奨されます。その後、AppScan はスキャン中にログインが必要になるたびにこのシーケンスを再生します。ログイン手順を記録すると、AppScan はアクションと要求の両方を分析します。ログインの再生時には、AppScan は (デフォルトでは) アクション・ベースのログインを再現しよう試みます。これが正常に行われない場合は、要求ベースのログインに戻ります。

M

マルウェア
悪意のあるソフトウェアまたは実行可能コードのことであり、多くの場合、無害に見えるファイルの形式でダウンロードまたは受信される。

操作 (manipulation)
1 つまたは複数のプロパティーに基づくデータ要素、要素のグループ、アクション、またはアクションのグループのアタッカーによる変更。例えば、必須引数を削除したり、ステップを不適切な順序で実行したりすることによる入力の変更。

マニュアル探査
Web アプリケーションを手動でクローリングし、サイトの一部 (実際のユーザーからの入力によって異なる) にアクセスしてテストするプロセス。

メタキャラクター (metacharacter)
パターン処理の際に特別な意味を持つ ASCII 文字。このような文字を使用して、処理時に突き合わせることができる 1 バイトまたはマルチバイト文字パターンを表す。

マルチパート要求 (multipart request)
複数のコンテンツ・タイプが含まれている要求。 不必要なメモリー消費を減らすため、スキャン中にマルチパート要求から一部のコンテンツ・タイプが自動的にフィルターで除外されます。フィルターに掛けられないタイプは、「構成」>「詳細構成」>「マルチパート・コンテンツ・タイプ・フィルター」で設定できます。

マルチフェーズ・スキャン (multiphase scan)
2 つ以上のフェーズで構成されるスキャン。

マルチステップ操作 (multi-step operation)
アプリケーションの特定の部分にアクセスするために特定の順序で送信する必要がある複数の要求のシーケンス。 (例: アイテムを買い物かごに追加する > 支払詳細を入力する > 注文確認を受け取る。) スキャン構成の一部としてそのようなマルチステップ操作を記録することで、サイトのその部分が確実にスキャンされるようになります。

N

ネットワーク・サービス (network service)
ネットワークでデータを送信したり、データの変換を提供したりするサービス。

NTLM
Windows NT LAN マネージャーを参照。

数値オーバーフロー **(numeric overflow)**
指定された保持スペースを超える算術計算の結果。

P

親ノード **(parent node)**
現行ノードを含むノード。

構文解析 **(parse)**
コマンドやファイルなどの情報のストリングを、その構成パーツに分割すること。

パス　インターネット・リソースの場所を指す URL の一部。

パス・フィルタリング **(path filtering)**
設定された基準に従ってページを除外または包含するプロセス。

パス・トラバーサル **(path traversal)**
URL で要求されている文書やリソースの場所を変更し、Web 文書のルート・ディレクトリーの外部にあるファイル、ディレクトリー、およびコマンドへのアクセスを強制設定する攻撃技法。

パターン **(pattern)**
1 つ以上の正規表現を使用して、識別するテキストを表す方法。

PCI　「Peripheral Component Interconnect」を参照。

侵入テスト **(penetration test)**
ハッカーによる攻撃をシミュレートすることで Web アプリケーションのセキュリティーを評価する方法。

Peripheral Component Interconnect (PCI)
プロセッサーと接続デバイスの間に高速データ・パスを提供するローカル・バス。

許可 **(permission)**
ローカル・ファイルの読み取りや書き込み、ネットワーク接続の確立、ネイティブ・コードのロードなどのアクティビティーを実行するための権限。

個人識別番号 **(PIN) (personal identification number (PIN))**
暗号サポートで、組織が個人に割り当て、身元の証明として使用する一意の番号。通常、PIN は、金融機関から顧客に割り当てられる。

フェーズ **(phase)**
探査ステージの後にテスト・ステージが続くスキャンのプロセス。

フェーズ限度 **(phase limit)**
スキャンで認められるフェーズの最大数。この限度は構成可能である。

PIN　個人識別番号 (Personal Identification Number)。

プラットフォーム **(platform)**
プログラムが実行される稼働環境を構成するオペレーティング・システムとハードウェアの組み合わせ。

ポート
アプリケーションどうしの通信の終点。通常は論理接続を指す。ポートには、データの送受信のためのキューが用意されている。各ポートには識別のためのポート番号がある。

ポート・リスナー **(port listener)**
帯域外の接続を listen することによって製品が特定のテストを検証することを可能にするメカニズム。

予測可能なリソースの位置
Web サイトの隠しコンテンツや隠し機能を見つけ出すための攻撃技法。公開表示を意図していないコンテンツ (一時ファイル、バックアップ・ファイル、構成ファイル、サンプル・ファイルなど) を標準的な場所から探し出す攻撃。

権限拡張 **(privilege escalation)**
特権リソースにアクセス許可が不十分なユーザーがアクセス可能であるかどうかをテストするために、さまざまなユーザー特権を使用して実行されたスキャンを参照するプロセス。

プロンプト **(prompt)**
情報またはユーザー処置を求めるメッセージまたは表示シンボル。ユーザーは、プログラムが継続できるように応答する必要がある。

プロキシー **(proxy)**
あるネットワークと別のネットワークの間にある、Telnet、FTP など、特定のネットワーク・アプリケーション用のアプリケーション・ゲートウェイ。例えば、ファイアウォールのプロキシー Telnet サーバーは、ユーザーの認証を実行した後、まるでそこに存在していないかのようにトラフィック・フローにプロキシーを通過させる。機能は、クライアント・ワークステーションではなく、ファイアウォールで実行されるので、ファイアウォールの負荷の増加を招く。

R

冗長なパスの制限 **(redundant path limit)**
スキャン時間を削減し、重複する結果を除くために、1 回のスキャンで同一パスをスキャンすることができる最大回数。

正規表現 **(regular expression)**
検索パターンでストリングまたはストリングのグループを定義する、文字、メタ文字、および演算子の集合。

コンプライアンス・レポート **(regulatory compliance report)**
選択された規制または法定標準に準拠していない、Web アプリケーションで検出された問題のレポート。規制には、カナダ、欧州連合、日本、英国、およびアメリカ合衆国の法令、法案、法規、および MasterCard と Visa の規則が含まれる。カスタムのコンプライアンス・レポート・テンプレートを作成することもできる。

相対パス **(relative path)**
現行作業ディレクトリーから始まるパス。

修復　問題の解決方法に対する提案。

要求ベースのログイン **(request-based login)**
このタイプのログイン再生は、ログイン手順を記録したときに送信された要求を再現します。

制限 **(restriction)**
スキャンをリスト内の URL のみに制限するフィルターのタイプ。

結果エキスパート **(Result Expert)**
CVSS 設定、画面キャプチャー、およびその他の情報を、スキャン結果の「問題情報」タブに追加するために、スキャンの実行後に実行できるオプション機能。

リバース・エンジニアリング **(reverse engineer)**
デバイスまたはシステムの設計、構成、および操作の詳細を把握するためにそのデバイスまたはシステムを分析すること。

リスク分析 **(risk analysis)**
Web アプリケーションで検出されたセキュリティー問題の分析。

リスク評価 **(risk assessment)**
アクションまたはシナリオのメリットおよび結果の評価。

リスク管理 **(risk management)**
組織内で防止策への費用効果の高い投資を実現するためのリソースの最適な割り振り。

ロール **(role)**
許可の集合。

S

サニタイズ **(sanitize)**
Web アプリケーション・セキュリティーで、使用する前に、悪影響のある文字や危険な文字をユーザー入力から取り除くこと。

スキャン **(scan)**
AppScan がアプリケーションを探査およびテストして結果を提供するプロセス。

スキャン構成 **(scan configuration)**
ユーザーのアプリケーション/サービス、環境、および選択されたスキャン・メソッドを定義する、AppScan 設定の集合。

スキャン・エキスパート **(Scan Expert)**
アプリケーションおよびネットワークの動作を探査し、スキャンを最適化するための構成変更を推奨する、オプション機能。

スキャン・エキスパート分析モジュール **(Scan Expert analysis module)**
スキャン・エキスパートが分析中に実施する 1 回のチェック。

スキャン・エキスパート評価 **(Scan Expert evaluation)**
ユーザーの構成についてのスキャン・エキスパートの評価。

スキャン・テンプレート **(scan template)**
スキャンに使用するためにロードすることができるスキャン構成。

スケジューラー **(scheduler)**
単純な時間計画に基づいて、ジョブのスケジューリングと起動を処理するように設計された、マルチスレッド、マルチプロセスのバックグラウンド・サーバー。

セキュリティー監査 **(security audit)**
システムやアプリケーションの手動によるまたは体系的な測定可能の技術審査。

セキュリティー上のリスク **(security risk)**
結果的に発生するおそれのある脅威や損傷の潜在的な影響。

シーケンス **(sequence)**
記録された URL のリスト。

セッション
ネットワーク上の 2 つの端末、ソフトウェア・プログラム、またはデバイス間の論理接続または仮想接続。この接続により、2 つの要素は通信したり、データを交換したりすることができる。「トランザクション (transaction)」も参照。

セッション証明書 **(session credential)**
Web サーバーが提供し、Cookie や URL 内に保管され、ユーザーを識別して、そのユーザーにさまざまなアクションを実行する権限を与える、データのストリング。

セッションの固定 **(session fixation)**
アタッカーがユーザーのセッション ID を固定化して、そのオンライン ID を乗っ取る攻撃技法。

セッション・ハイジャック **(session hi-jacking)**
攻撃者によるユーザーのセッションのセキュリティー侵害。攻撃者は、この盗んだセッションを再利用してユーザーのふりをすることができる。

セッション **ID (session ID)**
「セッション識別子 (session identifier)」を参照。

セッション **ID (session identifier)**
攻撃者によるユーザーのセッションのセキュリティー侵害。攻撃者は、この盗んだセッションを再利用してユーザーのふりをすることができる。

セッション・トークン **(session token)**
ブラウザーからパラメーターまたは Cookie として送信される ID であり、Web アプリケーションではその ID によってユーザーと現行セッションの関連付けが行われる。 「セッション ID」、「トランジエント・トークン」も参照。

重大度の格付け **(severity rating)**
スキャンによって問題に割り当てられたレベル。その問題が表すセキュリティー上のリスクを示す。

シェル **(shell)**
ユーザーとオペレーティング・システムの間のソフトウェア・インターフェース。通常、シェルは、コマンド行シェル (オペレーティング・システムへのコマンド行インターフェースを提供する) と、グラフィカル・シェル (グラフィカル・ユーザー・インターフェース (GUI) を提供する) の 2 つのカテゴリーのいずれかに分類される。

ソース・コード **(source code)**
人間が読み取ることのできるフォーマットのコンピューター・プログラム。ソース・コードは、コンピューターで使用できるバイナリー・コードに変換される。

スプーフィング **(spoofing)**
セキュアなシステムに不正侵入するために、伝送用の送信アドレスを偽装する手法。

SQL 構造化照会言語 (Structured Query Language) を参照。

SQL 注入 **(SQL injection)**
「構造化照会言語インジェクション (Structured Query Language injection)」を参照。

ステージ **(stage)**
AppScan がサイトの探査またはテストのいずれかを行うスキャン・フェーズの一部。

ステートレス・プロトコル **(stateless protocol)**
コマンド間の関係を維持しないプロトコル。HTTP はステートレス・プロトコルの一例。

構造化照会言語 **(SQL) (Structured Query Language (SQL))**
リレーショナル・データベースのデータを定義および操作するための標準化言語。

構造化照会言語注入 **(SQL 注入) (Structured Query Language injection (SQL injection))**
アプリケーション入力を操作してバックエンドの SQL ステートメントを変更することによって、Web サイトを不正に利用するための攻撃技法。

構文 **(syntax)**
コマンドまたはステートメントの構造についての規則。

T

テスト・フィックス **(test fix)**
報告された問題に対応して特定のユーザーに提供される、テストのための一時的なフィックス。

テスト・ポリシー **(test policy)**
特定のカテゴリーやタイプのテストにスキャンを限定するポリシー。

テスト要求 **(Test request)**
スキャンのテスト・ステージでアプリケーションに送信される要求。テスト要求の目的は、セキュリティーの脆弱性を明らかにすることである。

テスト・ステージ **(Test stage)**
スキャンするアプリケーションのオブジェクトおよびロジックに対して、広範囲に及ぶ大量の、典型的で、エラーがあり、悪意をシミュレートした使用法を適用し、それにより、セキュリティー上の脆弱性をくまなく調査する、スキャンのステージ。

スレッド **(thread)**
プロセスを制御するコンピューター命令のストリーム。一部のオペレーティング・システムでは、スレッドはプロセスにおける操作の最小単位である。複数のスレッドを並行して実行し、異なるジョブを実行することもできる。

脅威 **(threat)**
ウィルスの展開や不正なネットワーク侵入などの、セキュリティー問題、または有害な行為。

脅威クラス **(threat class)**
WASC-TC のカテゴリーを基準に分類された、セキュリティー問題のグループ。脅威クラスごとに、数多くの特定のテストがあり、テストごとに、数多くのバリアントがある。

トランザクション **(transaction)**
(アプリケーションに対する) 要求、およびその要求によって生成された (アプリケーションからの) 応答。

トランジエント・トークン **(transient toke)**
値が変わるトークン (通常はセッション・トークン)。有効期限が切れたトランジエント・トークンを送信すると、AppScan がテスト中のアプリケーションからログアウトされるため、トランジエント・トークンを最新の状態に保っておく必要がある。「セッション・トークン (session token)」も参照。

U

Uniform Resource Locator (URL)
インターネットなどのネットワークでアクセスできる情報リソースの固有のアドレス。URL には、情報リソースにアクセスするために使用するプロトコルの省略名と、そのプロトコルに基づいて情報リソースの場所を特定するための情報を組み込む。

UNIX マルチユーザー環境におけるマルチプログラミングを特徴とする移植性の高いオペレーティング・システム。 UNIX オペレーティング・システムは、本来はミニコンピューターでの使用を目的として開発されたものだったが、メインフレームやマイクロコンピューター向けに改変された。 AIX オペレーティング・システムは、UNIX オペレーティング・システムの IBM の実装である。

URL Uniform Resource Locator を参照。

ユーザー定義テスト **(user-defined test)**
自動的に作成されて実施されるテスト以外の、ユーザーによって作成されるテスト。

V

検証 **(validation)**
特定のテストがその目標の達成に成功したか、失敗したかを確認するプロセス。

脆弱性 **(vulnerability)**
オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

Web アプリケーション **(Web application)**
Web ブラウザーからアクセス可能であり、例えば、ユーザーがデータベースを照会できるようにすることによって、情報の静的な表示以外の機能を提供するアプリケーション。 Web アプリケーションの一般的なコンポーネントとしては、HTML ページ、JSP ページ、サーブレットなどがある。

Web ブラウザー **(Web browser)**
Web サーバーに要求を送り、そのサーバーが返す情報を表示する、クライアント・プログラム。

Web コンテンツ **(Web content)**
Web サイトを構成するファイルおよびその他のリソース。Web コンテンツは、イメージ・ファイル、音声ファイル、HTML ファイル、JSP ファイル、スタイル・シート、データベース項目など、Web サイト上に表示できるあらゆるもので構成することができる。

Web セキュリティー **(Web security)**
WWW、HTTP、および Web アプリケーション・ソフトウェアに関連する機密保護の理論および実践。

Web サーバー **(Web server)**
Hypertext Transfer Protocol (HTTP) 要求に対応するサービスを提供できるソフトウェア・プログラム。

Web サービス **(Web service)**
特定のタスクを実行し、HTTP や SOAP などのオープン・プロトコルを介してアクセス可能なアプリケーション。

Web サービス記述言語 **(WSDL) (Web Services Description Language (WSDL))**
ドキュメント指向またはプロシージャー指向のいずれかの情報を含むメッセージに基づいて動作する一連のエンドポイントとしてネットワーク・サービスを記述するための XML ベースの仕様。

white box
white box スキャンは、静的分析の場合の JavaScript コードなど、実際のコードを分析する。「black box」および「glass box」と比較してください。

Windows NT LAN マネージャー **(NTLM) (LAN Manager (NTLM))**
認証用のさまざまな Microsoft ネットワーク・プロトコルで使用されるプロトコル。

WSDL
「Web サービス記述言語 (Web Services Description Language)」を参照。

X

XSS クロスサイト・スクリプティング (cross-site scripting) を参照。

第 18 章 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

IBM本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能なオファリングについては、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。IBM 製品、プログラムまたはサービスに代えて、IBM の知的所有権を侵害することのない機能的に同等のプログラムまたは製品を使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒*242-8502*
神奈川県大和市下鶴間*1623*番*14*号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing Legal and Intellectual Property Law IBM Japan Ltd.19-21, Nihonbashi-Hakozakicho, Chuo-ku

IBM およびその直接または間接の子会社は、 本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様自身の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

〒*242-8502*
神奈川県大和市下鶴間*1623*番*14*号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、 IBM所定のプログラム契約の契約条項、 IBMプログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

本書に含まれるパフォーマンス・データは、特定の動作および環境条件下で得られたものです。実際の結果は、異なる可能性があります。

IBM 以外の製品に関する情報は、その製品の供給者もしくは公開されているその他のソースから入手したものです。 IBMは、それらの製品のテストは行っておりません。したがって、非 IBM 製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者が対応します。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、類似する個人や企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、保守容易性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態で提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入

このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。
© Copyright IBM Corp. 2000, 2017. に由来します。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標または登録商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml の「著作権と商標情報」をご覧ください。

製品資料に関するご使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商用使用

これらの資料は、すべての著作権表示その他の所有権表示をこれらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「"ソフトウェア・オファリング"」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、これらの「ソフトウェア・オファリング」により個人情報が収集されることはありませ

ん。一部の「ソフトウェア・オファリング」では、個人情報を収集することができます。この「ソフトウェア・オファリング」が Cookie を使用して個人情報を収集する場合、このオファリング'での Cookie の使用に関する具体的事項を以下に明記します。

この「ソフトウェア・オファリング」では、個人情報を収集するために Cookie またはその他のテクノロジーを使用することはありません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人情報を収集する機能を提供する場合、 お客様は、個人情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意取得の要求も含まれます。

このような目的での Cookie を含むさまざまなテクノロジーの使用について詳しくは、『'IBM プライバシー・ステートメント』(http://www.ibm.com/privacy/jp/ja) および『IBM 'オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details) の『"クッキー、Web ビーコン、その他のテクノロジー』"と『"IBM ソフトウェア製品と Software-as-a Service のプライバシー・ステートメント"』(http://www.ibm.com/software/info/product-privacy/jp/ja) のセクションを参照してください。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21