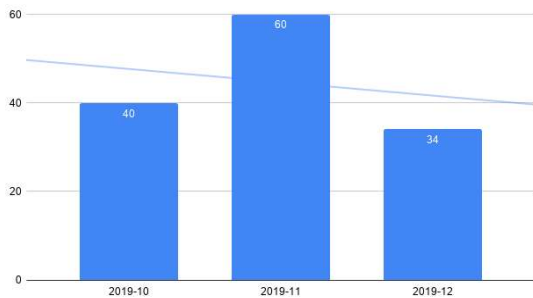## 분석 내용 정리 (작성: 펜타시큐리티시스템 보안성평가팀)

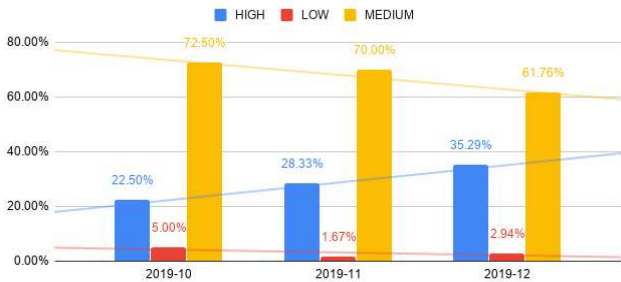2019년 10월부터 12월까지 EDB 분석 보고서에 공개된 취약점은 134건입니다. 공개된 취약점의 분석 내용은 다음과 같습니다.

1. 웹 취약점 발생 건수: 2019년 4분기 웹 취약점은 평균 44건으로, 11월에 보고된 취약점 수가 60건으로 가장 많았습니다.

2. CVSS(Common Vulnerability Scoring System)* Development: 매달 HIGH Level 취약점은 10월 22.50%를 시작으로 12월 35.29%까지 증가 추세를 보였으며, MEDIUM Level 취약점은 72.50%를 시작으로 61.76%까지 감소 추세를 보였습니다.
*취약점을 점수로 표기하기 위해 0부터 10까지 가중치를 줄 수 있도록 계산하는 방정식으로서, 점수가 높을수록 심각도가 높습니다.

3. 상위 5가지 웹 취약점 공격 동향: 2019년 4분기를 살펴보면 2019년 3분기와 다르게 Code Execution과 Cross Site Scripting이 주된 취약점으로 관찰되었습니다.
 1)10월: Code Execution 17.50%(7건) / Cross Site Scripting 25.00%(10건) / CSRF 7.50%(3건)
 2)11월: Code Execution 23.33%(14건) / Cross Site Scripting 21.67%(13건) / CSRF 10.00%(6건)
 3)12월: Code Execution 29.41%(10건) / Cross Site Scripting 20.59%(7건) / CSRF 14.71%(5건)

4. 웹 취약점 공격 유형: Code Execution이 23.13%(31건)으로 가장 많이 발생했고, Cross Site Scripting이 22.39%(30건)으로 두 번째로 많이 발생했습니다. 본 상위 2개 취약점이 4Q발생 웹 취약점의 약 절반(46%)을 차지하여 이에 대한 대비가 필요합니다.

해당 취약점을 예방하기 위해서 펜타시큐리티 EDB 분석 보고서 기반의 최신 패치와 시큐어 코딩을 권장합니다. 하지만 완벽한 시큐어 코딩은 불가능하며, 지속적으로 보안성을 유지하기 위해서 웹방화벽을 활용한 심층방어 (Defense indepth) 구현을 고려해야 합니다.
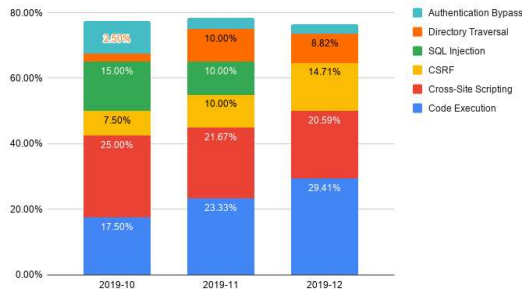
1. 웹 취약점 동향
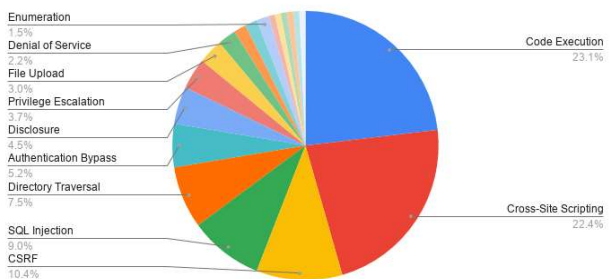
웹 취약점 발생 건수 (단위: 건)

CVSS 추이

상위 6가지 웹 취약점 공격 동향

웹 취약점 공격 유형

주요 웹 취약점 사례 (작성: 펜타시큐리티시스템 보안성평가팀)

2019년 10월부터 12월까지 EDB 분석 보고서에 공개된 취약점 중 가장 많은 취약점이 발견된 서비스는 WordPress입니다.

WordPress는 웹사이트, 블로그, 앱을 만들 수 있도록 도와주는 오픈소스 소프트웨어입니다. 해당 서비스는 많은 개인과 기업들이 이용하는 만큼 2019년 3분기에 이어 8건의 다양한 취약점이 발견되었습니다. 이렇게 보안 관리자가 미처 발견하지 못한 취약점을 노리는 웹 공격들이 많이 있습니다. 2019년 4분기에 WordPress에서 발견된 웹 취약점으로는 SQL Injection, Cross Site Scripting, Directory Traversal 등이 있습니다. 따라서 보안 정책 수립과 함께 웹 방화벽을 도입하여 발생할 수 있는 모든 웹 취약점에 대비해야 할 것입니다.

2019-10-11	47492	WordPress Arforms 3.7.1 - Directory Traversal	WordPress Arforms 3.7.1
2019-10-17	47516	Wordpress FooGallery 1.8.12 - Persistent Cross-Site Scripting	Wordpress FooGallery 1.8.12
2019-10-17	47517	WordPress 5.2.3 - Cross-Site Host Modification	WordPress 5.2.3
2019-10-17	47518	WordPress Plugin Sell Downloads 1.0.86 - Cross-Site Scripting	WordPress Plugin Sell Downloads 1.0.86
2019-10-24	47540	Wordpress Sliced Invoices 3.8.2 - 'post' SQL Injection	Wordpress Sliced Invoices 3.8.2
2019-10-29	47557	Wordpress 5.2.4 - Cross-Origin Resource Sharing	Wordpress 5.2.4
2019-11-28	47720	Wordpress 5.3 - User Disclosure	Wordpress 5.3
2019-12-17	47800	WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service	WordPress Core < 5.3.x

				2019.10.01~2019.12.31 Exploit-DB(http://exploit-db.com)에 공개된 취약점별로 분류한 정보입니다.		
날짜	EDB번호	취약점 분류	공격 위험도	취약점 이름	대상프로그램	대상환경
2019-09-02	47331	CrossSiteScripting	LOW	Opencart 3.x - Cross-Site Scripting	Opencart	Opencart 3.x
2019-10-01	47448	Cross-Site Scripting	MEDIUM	DotNetNuke < 9.4.0 - Cross-Site Scripting	DotNetNuke	DotNetNuke < 9.4.0
2019-10-02	47455	SQL Injection	MEDIUM	Detrix EDMS 1.2.3.1505 - SQL Injection	Detrix Edms	Detrix EDMS 1.2.3.1505
2019-10-03	47457	Code Execution	MEDIUM	mintinstall 7.9.9 - Code Execution	mintinstall	mintinstall 7.9.9
2019-10-03	47459	Disclosure	MEDIUM	AnchorCMS < 0.12.3a - Information Disclosure	AnchorCMS	AnchorCMS < 0.12.3a
2019-10-03	47462	Disable Functions Bypass	MEDIUM	PHP 7.0 < 7.3 (Unix) - 'gc' Disable Functions Bypass	PHP	PHP 7.0 < 7.3 (Unix)
2019-10-04	47460	SQL Injection	MEDIUM	LabCollector 5.423 - SQL Injection	LabCollector	LabCollector 5.423
2019-10-07	47465	Code Execution	MEDIUM	Joomla 3.4.6 - 'configuration.php' Remote Code Execution	Joomla	Joomla 3.4.6
2019-10-07	47467	Authentication Bypass	HIGH	Zabbix 4.2 - Authentication Bypass	Zabbix	Zabbix 4.2
2019-10-07	47469	Cross-Site Scripting	LOW	Subrion 4.2.1 - 'Email' Persistant Cross-Site Scripting	Subrion	Subrion 4.2.1
2019-10-07	47470	File Upload	HIGH	IBM Bigfix Platform 9.5.9.62 - Arbitrary File Upload	IBM Bigfix Platform	IBM Bigfix Platform 9.5.9.62
2019-10-07	47475	Code Execution	MEDIUM	vBulletin 5.0 < 5.5.4 - 'updateAvatar' Authenticated Remote Code Execution	vBulletin	vBulletin 5.0 < 5.5.4
2019-10-08	47474	Authentication Bypass	HIGH	Zabbix 4.4 - Authentication Bypass	Zabbix	Zabbix 4.4
2019-10-10	47480	CSRF	MEDIUM	SMA Solar Technology AG Sunny WebBox device - 1.6 - Cross-Site Request Forgery	SMA Solar Technology AG Sunny WebBox device	SMA Solar Technology AG Sunny WebBox device - 1.6
2019-10-10	47483	Authentication Bypass	HIGH	TP-Link TL-WR1043ND 2 - Authentication Bypass	TP-Link TL-WR1043ND	TP-Link TL-WR1043ND 2
2019-10-11	47491	Cross-Site Scripting	MEDIUM	Intelbras Router WRN150 1.0.18 - Persistent Cross-Site Scripting	Intelbras Router	Intelbras Router WRN150 1.0.18
2019-10-11	47492	Directory Traversal	MEDIUM	WordPress Arforms 3.7.1 - Directory Traversal	Wordpress	WordPress Arforms 3.7.1
2019-10-14	47496	Cross-Site Scripting	LOW	Express Invoice 7.12 - 'Customer' Persistent Cross-Site Scripting	Express Invoice	Express Invoice 7.12
2019-10-14	47497	Code Execution	MEDIUM	Ajenti 2.1.31 - Remote Code Execution	Ajenti	Ajenti 2.1.31
2019-10-14	47498	Disclosure	MEDIUM	Kirona-DRS 5.5.3.5 - Information Disclosure	Kirona-DRS	Kirona-DRS 5.5.3.5
2019-10-15	47501	CSRF	MEDIUM	Bolt CMS 3.6.10 - Cross-Site Request Forgery	Bolt CMS	Bolt CMS 3.6.10
2019-10-16	47505	Cross-Site Scripting	MEDIUM	Accounts Accounting 7.02 - Persistent Cross-Site Scripting	Accounts Accounting	Accounts Accounting 7.02
2019-10-17	47516	Cross-Site Scripting	MEDIUM	Wordpress FooGallery 1.8.12 - Persistent Cross-Site Scripting	Wordpress	Wordpress FooGallery 1.8.12
2019-10-17	47517	Cross-Site Scripting	MEDIUM	Wordpress Soliloquy Lite 2.5.6 - Persistent Cross-Site Scripting	Wordpress	Wordpress Soliloquy Lite 2.5.6
2019-10-17	47518	Cross-Site Scripting	MEDIUM	Wordpress Popup Builder 3.49 - Persistent Cross-Site Scripting	Wordpress	Wordpress Popup Builder 3.49
2019-10-17	47520	Code Execution	MEDIUM	Restaurant Management System 1.0 - Remote Code Execution	Restaurant Management System	Restaurant Management System 1.0
2019-10-18	47524	Code Execution	HIGH	Joomla! 3.4.6 - Remote Code Execution	Joomla	Joomla! 3.4.6
2019-10-23	47537	Cross-Site Scripting	MEDIUM	Rocket.Chat 2.1.0 - Cross-Site Scripting	Rocket.Chat	Rocket.Chat 2.1.0
2019-10-23	47539	Code Execution	MEDIUM	Joomla! 3.4.6 - Remote Code Execution (Metasploit)	Joomla	Joomla! 3.4.6
2019-10-24	47540	SQL Injection	MEDIUM	Wordpress Sliced Invoices 3.8.2 - 'post' SQL Injection	Wordpress	Wordpress Sliced Invoices 3.8.2
2019-10-24	47541	Incorrect Access Control	MEDIUM	AUO SunVeillance Monitoring System 1.1.9e - Incorrect Access Control	AUO SunVeillance Monitoring System	AUO SunVeillance Monitoring System 1.1.9e
2019-10-24	47542	SQL Injection	MEDIUM	AUO SunVeillance Monitoring System 1.1.9e - 'MailAdd' SQL Injection	AUO SunVeillance Monitoring System	AUO SunVeillance Monitoring System 1.1.9e
2019-10-25	47544	Improper Access Control	HIGH	ClonOs WEB UI 19.09 - Improper Access Control	ClonOs WEB UI	ClonOs WEB UI 19.09
2019-10-28	47545	CSRF	HIGH	Intelbras Router WRN150 1.0.18 - Cross-Site Request Forgery	Intelbras Router	Intelbras Router WRN150 1.0.18
2019-10-28	47546	SQL Injection	MEDIUM	waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.21 - 'start' SQL Injection	waldronmatt FullCalendar	waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.21
2019-10-28	47547	Authentication Bypass	MEDIUM	Part-DB 0.4 - Authentication Bypass	Part-DB	Part-DB 0.4
2019-10-28	47548	Cross-Site Scripting	MEDIUM	waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.21 - 'description' Cross-Site Scripting	waldronmatt FullCalendar	waldronmatt FullCalendar-BS4-PHP-MySQL-JSON 1.21

날짜	EDB번호	취약점 분류	공격 위험도	취약점 이름	대상프로그램	대상환경
2019-10-28	47550	SQL Injection	MEDIUM	delpino73 Blue-Smiley-Organizer 1.32 - 'datetime' SQL Injection	delpino73 Blue-Smiley-Organizer	delpino73 Blue-Smiley-Organizer 1.32
2019-10-28	47553	Remote Code Execution	HIGH	PHP-FPM + Nginx - Remote Code Execution	PHP-FPM + Nginx	PHP-FPM + Nginx
2019-10-29	47555	Remote Code Execution	HIGH	rConfig 3.9.2 - Remote Code Execution	rConfig	rConfig 3.9.2
2019-10-29	47557	Cross-Origin Resource Sharing	MEDIUM	Wordpress 5.2.4 - Cross-Origin Resource Sharing	Wordpress	Wordpress 5.2.4
2019-11-01	47569	SQL Injection	MEDIUM	TheJshen contentManagementSystem 1.04 - 'id' SQL Injection	TheJshen contentManagementSystem	TheJshen contentManagementSystem 1.04
2019-11-01	47571	CSRF	HIGH	ownCloud 10.3.0 stable - Cross-Site Request Forgery	ownCloud	ownCloud 10.3.0 stable
2019-11-01	47572	Code Execution	MEDIUM	Apache Solr 8.2.0 - Remote Code Execution	Apache Solr	Apache Solr 8.2.0
2019-11-05	47581	SQL Injection	MEDIUM	thejshen Globitek CMS 1.4 - 'id' SQL Injection	thejshen Globitek CMS	thejshen Globitek CMS 1.4
2019-11-05	47583	Cross-Site Scripting	MEDIUM	thrsrossi Millhouse-Project 1.414 - 'content' Persistent Cross-Site Scripting	thrsrossi Millhouse-Project	thrsrossi Millhouse-Project 1.414
2019-11-05	47585	SQL Injection	MEDIUM	rimbalinux AhadPOS 1.11 - 'alamatCustomer' SQL Injection	rimbalinux AhadPOS	rimbalinux AhadPOS 1.11
2019-11-05	47587	Cross-Site Scripting	MEDIUM	html5_snmp 1.11 - 'Remark' Persistent Cross-Site Scripting	html5_snmp	html5_snmp 1.11
2019-11-05	47588	SQL Injection	MEDIUM	html5_snmp 1.11 - 'Router_ID' SQL Injection	html5_snmp	html5_snmp 1.11
2019-11-05	47589	SQL Injection	MEDIUM	SD.NET RIM 4.7.3c - 'idtyp' SQL Injection	SD.NET RIM	SD.NET RIM 4.7.3c
2019-11-06	47595	Authentication Bypass	HIGH	Smartwares HOME easy 1.0.9 - Client-Side Authentication Bypass	Smartwares HOME easy	Smartwares HOME easy 1.0.9
2019-11-06	47596	Disclosure	HIGH	Smartwares HOME easy 1.0.9 - Database Backup Information Disclosure	Smartwares HOME easy	Smartwares HOME easy 1.0.9
2019-11-08	47598	Cross-Site Scripting	MEDIUM	Jenkins build-metrics plugin 1.3 - 'label' Cross-Site Scripting	Jenkins build-metrics plugin	Jenkins build-metrics plugin 1.3
2019-11-08	47600	Privilege Escalation	MEDIUM	Adive Framework 2.0.7 - Privilege Escalation	Adive Framework	Adive Framework 2.0.7
2019-11-08	47603	CSRF	MEDIUM	Nextcloud 17 - Cross-Site Request Forgery	Nextcloud	Nextcloud 17
2019-11-12	47612	Code Execution	HIGH	Prima FlexAir Access Control 2.3.38 - Remote Code Execution	Prima FlexAir Access Control	Prima FlexAir Access Control 2.3.38
2019-11-12	47613	Cross-Site Scripting	MEDIUM	Adrenalin Core HCM 5.4.0 - 'prntDDLCntrlName' Reflected Cross-Site Scripting	Adrenalin Core HCM	Adrenalin Core HCM 5.4.0
2019-11-12	47614	Cross-Site Scripting	MEDIUM	Computrols CBAS-Web 19.0.0 - 'username' Reflected Cross-Site Scripting	Computrols CBAS-Web	Computrols CBAS-Web 19.0.0
2019-11-12	47611	Cross-Site Scripting	MEDIUM	Adrenalin Core HCM 5.4.0 - 'strAction' Reflected Cross-Site Scripting	Adrenalin Core HCM	Adrenalin Core HCM 5.4.0
2019-11-12	47616	Directory Traversal	HIGH	eMerge E3 1.00-06 - Unauthenticated Directory Traversal	eMerge E3	eMerge E3 1.00-06
2019-11-12	47618	Privilege Escalation	HIGH	eMerge E3 1.00-06 - Privilege Escalation	eMerge E3	eMerge E3 1.00-06
2019-11-12	47619	Code Execution	HIGH	eMerge E3 1.00-06 - Remote Code Execution	eMerge E3	eMerge E3 1.00-06
2019-11-12	47620	CSRF	MEDIUM	eMerge E3 1.00-06 - Cross-Site Request Forgery	eMerge E3	eMerge E3 1.00-06
2019-11-12	47621	Directory Traversal	HIGH	Atlassian Confluence 6.15.1 - Directory Traversal	Atlassian Confluence	Atlassian Confluence 6.15.1
2019-11-12	47622	File Upload	HIGH	eMerge E3 1.00-06 - Arbitrary File Upload	eMerge E3	eMerge E3 1.00-06
2019-11-12	47623	Cross-Site Scripting	MEDIUM	eMerge E3 1.00-06 - 'layout' Reflected Cross-Site Scripting	eMerge E3	eMerge E3 1.00-06
2019-11-12	47624	Code Execution	HIGH	eMerge50P 5000P 4.6.07 - Remote Code Execution	eMerge50P	eMerge50P 5000P 4.6.07
2019-11-12	47627	Code Execution	HIGH	CBAS-Web 19.0.0 - Remote Code Execution	CBAS-Web	CBAS-Web 19.0.0
2019-11-12	47628	CSRF	MEDIUM	CBAS-Web 19.0.0 - Cross-Site Request Forgery (Add Super Admin)	CBAS-Web	CBAS-Web 19.0.0
2019-11-12	47630	Enumeration	MEDIUM	CBAS-Web 19.0.0 - Username Enumeration	CBAS-Web	CBAS-Web 19.0.0
2019-11-12	47631	SQL Injection	MEDIUM	CBAS-Web 19.0.0 - 'id' Boolean-based Blind SQL Injection	CBAS-Web	CBAS-Web 19.0.0

EDB 분석 보고서 (2019.4Q)

2019.10.01~2019.12.31 Exploit-DB(http://exploit-db.com)에 공개된 취약점별로 분류한 정보입니다.

날짜	EDB번호	취약점 분류	공격 위험도	취약점 이름	대상프로그램	대상환경
2019-11-12	47632	Header Injection	MEDIUM	Joomla 3.9.13 - 'Host' Header Injection	Joomla	Joomla 3.9.13
2019-11-12	47633	Cross-Site Scripting	LOW	Prima Access Control 2.3.35 - 'HwName' Persistent Cross-Site Scripting	Prima Access Control	Prima Access Control 2.3.35
2019-11-12	47634	File Upload	HIGH	Prima Access Control 2.3.35 - Arbitrary File Upload	Prima Access Control	Prima Access Control 2.3.35
2019-11-12	47635	Directory Traversal	MEDIUM	Atlassian Confluence 6.15.1 - Directory Traversal (Metasploit)	Atlassian Confluence	Atlassian Confluence 6.15.1
2019-11-12	47636	Code Execution	HIGH	Optergy 2.3.0a - Remote Code Execution	Optergy	Optergy 2.3.0a
2019-11-12	47638	Code Execution	MEDIUM	FlexAir Access Control 2.4.9api3 - Remote Code Execution	FlexAir Access Control	FlexAir Access Control 2.4.9api3
2019-11-12	47639	CSRF	MEDIUM	Optergy 2.3.0a - Cross-Site Request Forgery (Add Admin)	Optergy	Optergy 2.3.0a
2019-11-12	47640	Disclosure	MEDIUM	Optergy 2.3.0a - Username Disclosure	Optergy	Optergy 2.3.0a
2019-11-12	47641	Code Execution	HIGH	Optergy 2.3.0a - Remote Code Execution (Backdoor)	Optergy	Optergy 2.3.0a
2019-11-12	47643	Cross-Site Scripting	MEDIUM	Adrenalin Core HCM 5.4.0 - 'ReportID' Reflected Cross-Site Scripting	Adrenalin Core HCM	Adrenalin Core HCM 5.4.0
2019-11-12	47644	Authentication Bypass	MEDIUM	FlexAir Access Control 2.3.35 - Authentication Bypass	FlexAir Access Control	FlexAir Access Control 2.3.35
2019-11-12	47648	Denial of Service	MEDIUM	Bematech Printer MP-4200 - Denial of Service	Bematech Printer	Bematech Printer MP-4200
2019-11-13	47649	Code Execution	MEDIUM	Linear eMerge E3 1.00-06 - Remote Code Execution	Linear eMerge	Linear eMerge E3 1.00-06
2019-11-13	47650	Code Execution	HIGH	FUDForum 3.0.9 - Remote Code Execution	FUDForum	FUDForum 3.0.9
2019-11-13	47651	Code Execution	HIGH	Technicolor TD5130.2 - Remote Command Execution	Technicolor	Technicolor TD5130.2
2019-11-13	47652	Cross-Site Scripting	MEDIUM	Technicolor TC7300.B0 - 'hostname' Persistent Cross-Site Scripting	Technicolor	Technicolor TC7300.B0
2019-11-13	47653	Directory Traversal	MEDIUM	gSOAP 2.8 - Directory Traversal	gSOAP	gSOAP 2.8
2019-11-13	47654	Code Execution	MEDIUM	Fastweb Fastgate 0.00.81 - Remote Code Execution	Fastweb Fastgate	Fastweb Fastgate 0.00.81
2019-11-14	47659	File Upload	MEDIUM	Xfilesharing 2.5.1 - Arbitrary File Upload	Xfilesharing	Xfilesharing 2.5.1
2019-11-18	47663	Directory Traversal	MEDIUM	Lexmark Services Monitor 2.27.4.0.39 - Directory Traversal	Lexmark Services Monitor	Lexmark Services Monitor 2.27.4.0.39
2019-11-18	47666	Directory Traversal	MEDIUM	Crystal Live HTTP Server 6.01 - Directory Traversal	Crystal Live HTTP Server	Crystal Live HTTP Server 6.01
2019-11-18	47669	File Download	HIGH	Centova Cast 3.2.11 - Arbitrary File Download	Centova Cast	Centova Cast 3.2.11
2019-11-18	47670	CSRF	MEDIUM	TemaTres 3.0 - Cross-Site Request Forgery (Add Admin)	TemaTres	TemaTres 3.0
2019-11-18	47672	Cross-Site Scripting	MEDIUM	TemaTres 3.0 - 'value' Persistent Cross-site Scripting	TemaTres	TemaTres 3.0
2019-11-20	47691	Code Execution	MEDIUM	OpenNetAdmin 18.1.1 - Remote Code Execution	OpenNetAdmin	OpenNetAdmin 18.1.1
2019-11-21	47702	Cross-Site Scripting	MEDIUM	TestLink 1.9.19 - Persistent Cross-Site Scripting	TestLink	TestLink 1.9.19
2019-11-21	47704	Header Injection	MEDIUM	Network Management Card 6.2.0 - Host Header Injection	Network Management Card	Network Management Card 6.2.0
2019-11-28	47720	Disclosure	MEDIUM	Wordpress 5.3 - User Disclosure	Wordpress	Wordpress 5.3
2019-11-28	47722	Code Execution	MEDIUM	Mersive Solstice 2.8.0 - Remote Code Execution	Mersive Solstice	Mersive Solstice 2.8.0
2019-11-29	47725	Cross-Site Scripting	MEDIUM	Online Inventory Manager 3.2 - Persistent Cross-Site Scripting	Online Inventory Manager	Online Inventory Manager 3.2
2019-12-02	47730	CSRF	MEDIUM	SmartHouse Webapp 6.5.33 - Cross-Site Request Forgery	SmartHouse Webapp	SmartHouse Webapp 6.5.33
2019-12-02	47731	Enumeration	MEDIUM	Dokuwiki 2018-04-22b - Username Enumeration	Dokuwiki	Dokuwiki 2018-04-22b
2019-12-03	47737	Cross-Site Scripting	MEDIUM	Online Invoicing System 2.6 - 'description' Persistent Cross-Site Scripting	Online Invoicing System	Online Invoicing System 2.6
2019-12-03	47738	CSRF	MEDIUM	Intelbras Router RF1200 1.1.3 - Cross-Site Request Forgery	Intelbras Router	Intelbras Router RF1200 1.1.3
2019-12-03	47739	Code Execution	HIGH	Revive Adserver 4.2 - Remote Code Execution	Revive Adserver	Revive Adserver 4.2
2019-12-04	47741	HTML Injection	MEDIUM	Online Clinic Management System 2.2 - HTML Injection	Online Clinic Management System	Online Clinic Management System 2.2
2019-12-04	47744	Denial of Service	MEDIUM	Cisco WLC 2504 8.9 - Denial of Service (PoC)	Cisco WLC	Cisco WLC 2504 8.9
2019-12-04	47745	Disclosure	HIGH	OwnCloud 8.1.8 - Username Disclosure	OwnCloud	OwnCloud 8.1.8

EDB 분석 보고서 (2019.4Q)

2019.10.01~2019.12.31 Exploit-DB(http://exploit-db.com)에 공개된 취약점별로 분류한 정보입니다.

날짜	EDB번호	취약점 분류	공격 위험도	취약점 이름	대상프로그램	대상환경
2019-12-05	47748	Code Execution	HIGH	Broadcom CA Privilged Access Manager 2.8.2 - Remote Command Execution	Broadcom CA Privilged Access Manager	Broadcom CA Privilged Access Manager 2.8.2
2019-12-06	47749	Code Execution	HIGH	Verot 2.0.3 - Remote Code Execution	Verot	Verot 2.0.3
2019-12-09	47756	Cross-Site Scripting	MEDIUM	Snipe-IT Open Source Asset Management 4.7.5 - Persistent Cross-Site Scripting	Snipe-IT Open Source Asset Management	Snipe-IT Open Source Asset Management 4.7.5
2019-12-09	47758	Authentication Bypass	MEDIUM	PRO-7070 Hazzktr Profesyonel Web Sitesi 1.0 - Authentication Bypass	PRO-7070 Hazzktr Profesyonel	PRO-7070 Hazzktr Profesyonel Web Sitesi 1.0
2019-12-09	47760	Code Execution	HIGH	Yachtcontrol Webapplication 1.0 - Unauthenticated Remote Code Execution	Yachtcontrol Webapplication	Yachtcontrol Webapplication 1.0
2019-12-09	47761	Code Execution	MEDIUM	Alcatel-Lucent Omnivista 8770 - Remote Code Execution	Alcatel-Lucent Omnivista	Alcatel-Lucent Omnivista 8770
2019-12-09	47762	Cross-Site Scripting	MEDIUM	Oracle Siebel Sales 8.1 - Persistent Cross-Site Scripting	Oracle Siebel Sales	Oracle Siebel Sales 8.1
2019-12-10	47764	CSRF	HIGH	Inim Electronics Smartliving SmartLAN 6.x - Unauthenticated Server-Side Request Forgery	Inim Electronics Smartliving SmartLAN	Inim Electronics Smartliving SmartLAN 6.x
2019-12-10	47765	Code Execution	HIGH	Inim Electronics Smartliving SmartLAN 6.x - Remote Command Execution	Inim Electronics Smartliving SmartLAN	Inim Electronics Smartliving SmartLAN 6.x
2019-12-11	47770	Code Execution	MEDIUM	Apache Olingo OData 4.0 - XML External Entity Injection	Apache Olingo Odata	Apache Olingo OData 4.0
2019-12-12	47772	Code Execution	MEDIUM	OpenNetAdmin 18.1.1 - Command Injection Exploit (Metasploit)	OpenNetAdmin	OpenNetAdmin 18.1.1
2019-12-12	47773	Directory Traversal	MEDIUM	Bullwark Momentum Series JAWS 1.0 - Directory Traversal	Bullwark Momentum Series JAWS	Bullwark Momentum Series JAWS 1.0
2019-12-13	47774	Directory Traversal	MEDIUM	NVMS 1000 - Directory Traversal	NVMS	NVMS 1000
2019-12-16	47776	Cross-Site Scripting	LOW	D-Link DIR-615 Wireless Router - Cross-Site Scripting	D-Link	D-Link DIR-615 Wireless Router
2019-12-16	47777	Directory Traversal	MEDIUM	Roxy Fileman 1.4.5 - Directory Traversal	Roxy Fileman	Roxy Fileman 1.4.5
2019-12-16	47778	Privilege Escalation	MEDIUM	D-Link DIR-615 - Privilege Escalation	D-Link DIR	D-Link DIR-615
2019-12-17	47781	Cross-Site Scripting	HIGH	Zendesk App SweetHawk Survey 1.6 - Persistent Cross-Site Scripting	Zendesk App SweetHawk Survey	Zendesk App SweetHawk Survey 1.6
2019-12-17	47782	Code Execution	HIGH	Netgear R6400 - Remote Code Execution	Netgear	Netgear R6400
2019-12-17	47783	Privilege Escalation	MEDIUM	NopCommerce 4.2.0 - Privilege Escalation	NopCommerce	NopCommerce 4.2.0
2019-12-17	47800	Denial of Service	HIGH	WordPress Core < 5.3.x - 'xmlrpc.php' Denial of Service	Wordpress	WordPress Core < 5.3.x
2019-12-18	47785	CSRF	MEDIUM	Tautulli 2.1.9 - Cross-Site Request Forgery (ShutDown)	Tautulli	Tautulli 2.1.9
2019-12-18	47787	CSRF	MEDIUM	Xerox AltaLink C8035 Printer - Cross-Site Request Forgery (Add Admin)	Xerox AltaLink	Xerox AltaLink C8035 Printer
2019-12-18	47789	Cross-Site Scripting	MEDIUM	Rumpus FTP Web File Manager 8.2.9.1 - Reflected Cross-Site Scripting	Rumpus FTP Web File Manager	Rumpus FTP Web File Manager 8.2.9.1
2019-12-18	47793	Code Execution	HIGH	Telerik UI - Remote Code Execution via Insecure Deserialization	Telerik UI	Telerik UI
2019-12-19	47796	Privilege Escalation	HIGH	Deutsche Bahn Ticket Vending Machine Local Kiosk - Privilege Escalation	Deutsche Bahn Ticket Vending Machine Local Kiosk	Deutsche Bahn Ticket Vending Machine Local Kiosk
2019-12-20	47798	Cross-Site Scripting	MEDIUM	phpMyChat-Plus 1.98 - 'pmc_username' Reflected Cross-Site Scripting	phpMyChat-Plus	phpMyChat-Plus 1.98