Weekly Zero-Day Vulnerability Coverage Bulletin

(7th January – 13th January)

Summary:

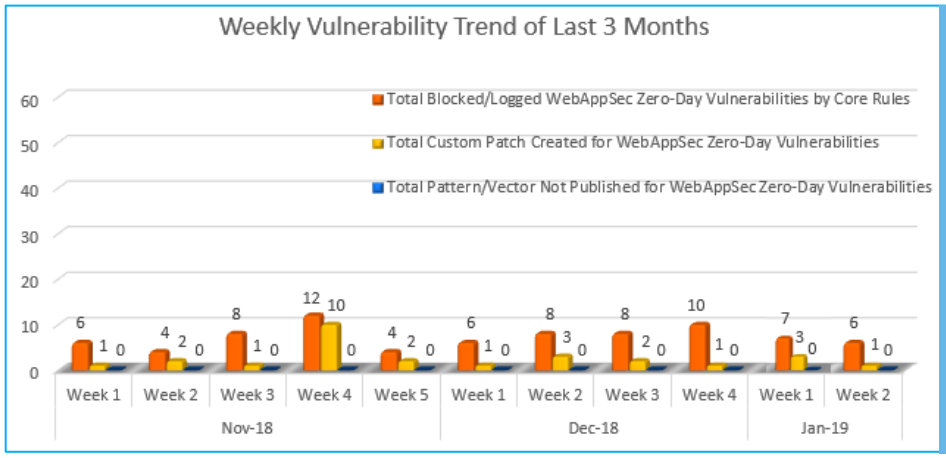
Total **7 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

3	1	2	1
Cross Site Scripting	SQL Injection	Directory Traversal	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	6
Zero-Day Vulnerabilities Protected through Custom Rules	1*
Zero-Day Vulnerabilities for which protection cannot be determined	0**

* To enable custom rules please contact support@indusface.com
** Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

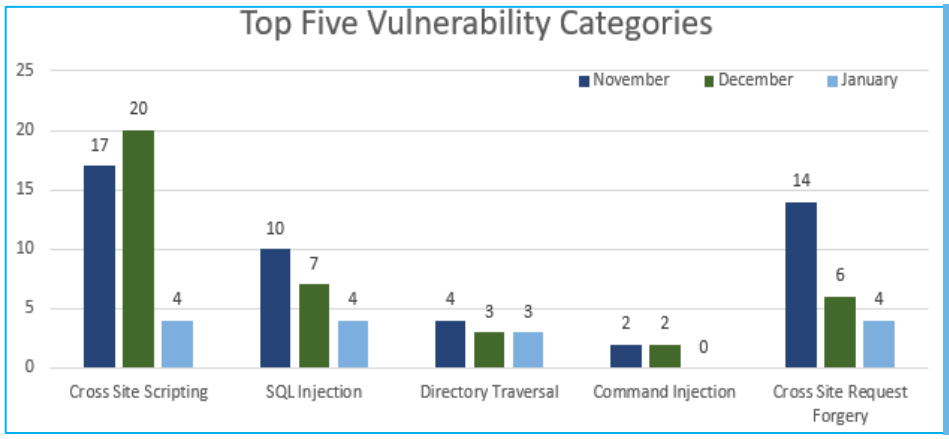
Vulnerability Trend:



Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

75% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

25% Of Zero-Day Vulnerabilities were protected by Custom Rules in last 3 months



From the graph, we infer that maximum Cross Site Scripting vulnerabilities were discovered in December compared to other months and categories so far.

Medium no. of SQL Injection and CSRF attacks was found in all the months.

Note: Our Sig-Dev team constantly monitors the security landscape and leading security websites to identify any new vulnerabilities identified/published and monitors/updates rules to ensure around the clock protection for customer sites.

Details:

S. No.	Vulnerability Type	Public ID	Vulnerability Name	Vulnerability Description	AppTrana Coverage
1.	Cross Site Scripting	CVE-2019-5311	YUNUCMS 1.1.8 Show.php cw cross site scripting	A vulnerability was found in YUNUCMS 1.1.8. It has been declared as problematic. Affected by this vulnerability is a code block of the file *app/index/controller/Show.php*. The manipulation of the argument cw as part of a *Parameter* leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
		CVE-2019-5310	YUNUCMS 1.1.8 System.php site_title cross site scripting	A vulnerability classified as problematic has been found in YUNUCMS 1.1.8. Affected is an unknown function of the file *app/admin/controller/System.php*. The manipulation of the argument site_title as part of a *POST Request* leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-80. This is going to have an impact on integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
		CVE-2018-19414	Plikli CMS 4.0.0 groups.php keyword cross site scripting	A vulnerability classified as problematic was found in Plikli CMS 4.0.0. This vulnerability affects the functionality of the file *groups.php*. The manipulation of the argument keyword as part of a *Parameter* leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is CWE-80. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website.	Protected by Default Rules.
2.	SQL Injection	CVE-2019-5488	EARCLINK ESPCMS-P8	A vulnerability was found in EARCLINK ESPCMS-P8	Protected by Default Rules.

			index.php verify_key sql injection	(the affected version unknown). It has been classified as critical. This affects code of the file *install_pack/index.php?ac=Member&at=verifyAccount*. The manipulation of the argument verify_key as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is going to have an impact on confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange.	
3.	Directory Traversal	CVE-2018-11798	Apache Thrift Node.js Static Web Server up to 0.11.0 directory traversal	A vulnerability has been found in Apache Thrift Node.js Static Web Server up to 0.11.0 and classified as critical. The manipulation with an unknown input leads to a directory traversal vulnerability. The CWE definition for the vulnerability is CWE-22. As an impact it is known to affect confidentiality, integrity, and availability. The weakness was presented in 01/07/2019. This vulnerability is known as CVE-2018-11798 since 06/05/2018. The attack can be launched remotely.	Protected by Default Rules.
		CVE-2019-5725	qibosoft up to V7 member/index.php main directory traversal	A vulnerability classified as critical has been found in qibosoft up to V7. Affected is an unknown function of the file *member/index.php*. The manipulation of the argument main as part of a *Parameter* leads to a directory traversal vulnerability. CWE is classifying the issue as CWE-22. This is going to have an impact on	Protected by Default Rules.

				confidentiality, integrity, and availability. The weakness was published in 01/08/2019. This vulnerability is traded as CVE-2019-5725 since 01/08/2019. It is possible to launch the attack remotely.	
4.	Cross Site Request Forgery	CVE-2019-6244	UsualToolCMS 8.0 a_sqlbackx.php cross site request forgery	A vulnerability classified as problematic was found in UsualToolCMS 8.0. This vulnerability affects the functionality of the file *cmsadmin/a_sqlbackx.php?t=sql*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. The CWE definition for the vulnerability is CWE-352. As an impact it is known to affect integrity. An attacker might be able force legitimate users to initiate unwanted actions within the web application. The weakness was presented in 01/12/2019. This vulnerability was named CVE-2019-6244 since 01/11/2019.	Protected by Custom Rules.