Weekly Zero-Day Vulnerability Coverage Bulletin

(10th December – 16th December)

Summary:

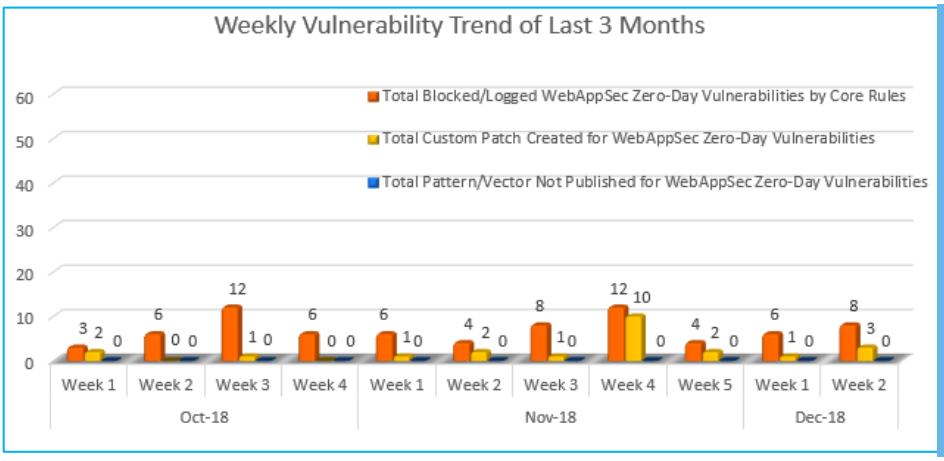
Total **11 Zero-Day Vulnerabilities** were discovered in **4 Categories** previous week

6	2	1	2
Cross Site Scripting	SQL Injection	Bruteforce Attack	Cross Site Request Forgery

Zero-Day Vulnerabilities Protected through Core Rules	8
Zero-Day Vulnerabilities Protected through Custom Rules	3*
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

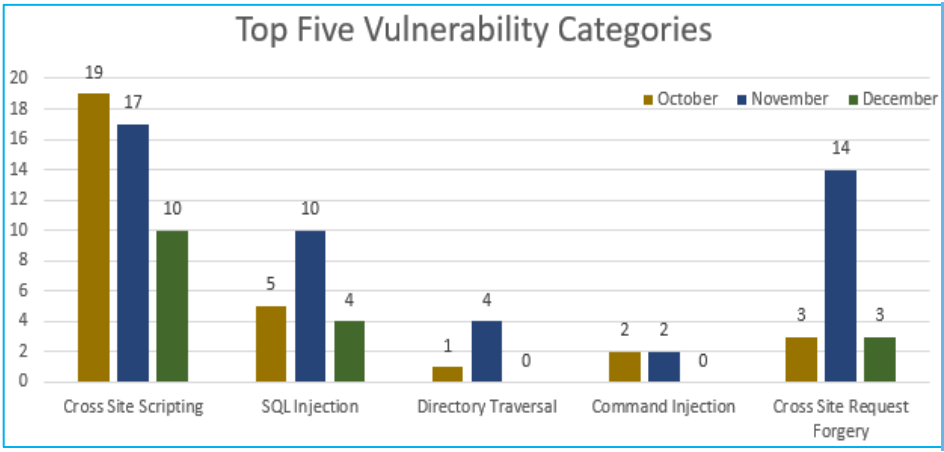
Vulnerability Trend:



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

77% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

23% 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 October compared to other months and categories so far.

Medium no. of SQL Injection 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-2018-20012	PHPCMF 4.1.3 index.php cross site scripting	A vulnerability was found in PHPCMF 4.1.3 and classified as problematic. This issue affects an unknown function of the file *index.php?s=member&c=register&m=index*. The manipulation with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance and would make it possible to initiate further attacks against site visitors.	Protected by Default Rules.
		CVE-2018-16636	Nucleus CMS 3.70 index.php body cross site scripting	A vulnerability which was classified as problematic, has been found in Nucleus CMS 3.70. An unknown function of the file *index.php* is affected. The manipulation of the argument body as part of a *Parameter* leads to a cross site scripting vulnerability (HTML Injection). Using CWE to declare the problem leads to CWE-79. Integrity is Impacted. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-1671	IBM Curam Social Program Management 7.0.3 HTML Injection cross site scripting	A vulnerability, which was classified as problematic, was found in IBM Curam Social Program Management 7.0.3. This affects an unknown function. The manipulation with an unknown input leads to a cross site scripting vulnerability (HTML Injection). CWE is classifying the issue as CWE-79. 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.

				This would alter the appearance and would make it possible to initiate.	
		CVE-2018-19970	phpMyAdmin up to 4.8.4 Navigation Tree Table Name cross site scripting	A vulnerability, which was classified as problematic, has been found in phpMyAdmin up to 4.8.4. This issue affects an unknown function of the component *Navigation Tree*. The manipulation as part of a *Table Name* leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-80. Impacted is integrity. An attacker might be able to inject arbitrary html and script code into the web site. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-1478	IBM BigFix Platform up to 9.5.9 Clickjacking cross site scripting	A vulnerability was found in IBM BigFix Platform. It has been declared as problematic. Affected by this vulnerability is an unknown function. The manipulation with an unknown input leads to a cross site scripting vulnerability (Clickjacking). The CWE definition for the vulnerability is CWE-451. As an impact it is known to affect integrity. An attacker might be able to inject arbitrary html and script code into the website. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-20136	Fuel CMS 1.4.3 Page Creation 1 Header/Body cross site scripting	A vulnerability classified as problematic has been found in Fuel CMS 1.4.3. This affects an unknown function of the file *pages/edit/1?lang=english* of the component *Page Creation*. The manipulation of the argument Header/Body as part of a *Variable* 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.
2.	SQL Injection	CVE-2018-20018	S-Cms 3.0 S_id sql injection	A vulnerability was found in S-Cms 3.0. It has been rated as critical. Affected by this issue is an	Protected by Default Rules.

				unknown function of the file */1/?type=productinfo&S_id=140*. The manipulation of the argument S_id as part of a *Parameter* leads to a sql injection vulnerability. Using CWE to declare the problem leads to CWE-89. Impacted is confidentiality, integrity, and availability. An attacker might be able inject and/or alter existing SQL statements which would influence the database exchange. The weakness was disclosed 12/10/2018.	
		CVE-2018-20061	ERPNext up to 10.x/11.0.3-beta.28 Item Argument sql injection	A vulnerability has been found in ERPNext up to 10.x/11.0.3-beta.28 and classified as critical. Affected by this vulnerability is an unknown function of the file */api/resource/Item?fields*. The manipulation as part of a *Argument* leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. As an impact, it is known to affect confidentiality, integrity, and availability. An attacker might be able to inject and/or alter existing SQL statements which would influence the database exchange. This weakness was disclosed.	Protected by Default Rules.
3.	Bruteforce Attack	NA	A botnet of over 20,000 WordPress sites is attacking other WordPress sites	This campaign has created a botnet of infected WordPress websites to perform its attacks, which attempt XML-RPC authentication to other WordPress sites in order to access privileged accounts.	Protected by Custom Rules.

4.	Cross Site Request Forgery	CVE-2018-20015	YzmCMS 5.2 admin/role/add.html cross site request forgery	A vulnerability was found in YzmCMS 5.2. It has been classified as problematic. Affected is an unknown function of the file *admin/role/add.html*. The manipulation with an unknown input leads to a cross site request forgery vulnerability. CWE is classifying the issue as CWE-352. This is going to have an impact on integrity. An attacker might be able to force legitimate users to initiate unwanted actions within the web application. The weakness was published 12/10/2018. This vulnerability is traded as CVE-2018-20015 ever since.	Protected by Custom Rules.
		CVE-2018-19969	phpMyAdmin up to 4.7.x/4.8.3 cross site request forgery [CVE-2018-19969]	A vulnerability classified as problematic was found in phpMyAdmin up to 4.7.x/4.8.3. This vulnerability affects an unknown function. 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 shared 12/11/2018. The advisory is shared for download at phpmyadmin.net.	Protected by Custom Rules.