Weekly Zero-Day Vulnerability Coverage Bulletin

(6th January – 12th January)

Summary:

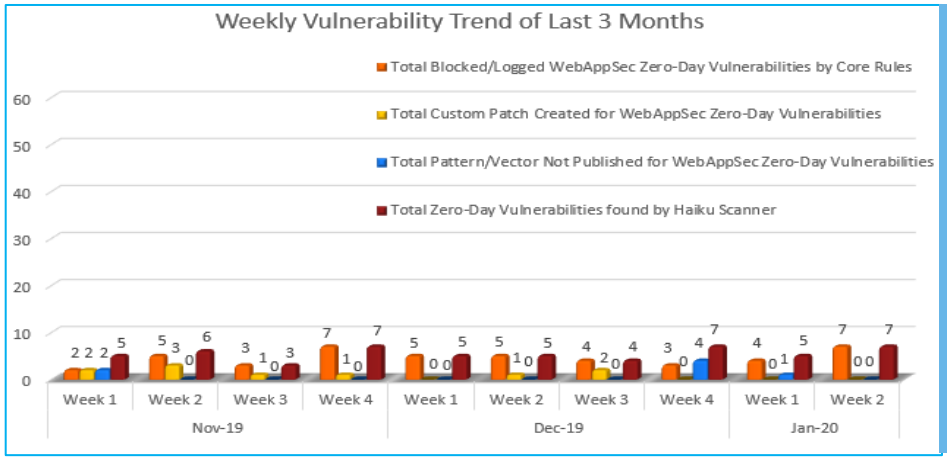
Total **7 Zero-Day Vulnerabilities** were discovered in **3 Categories** this week

4	2	1
Cross Site Scripting	Directory Traversal	SQL Injection

Zero-Day Vulnerabilities Protected through Core Rules	7
Zero-Day Vulnerabilities Protected through Custom Rules	0*
Zero-Day Vulnerabilities for which protection cannot be determined	0**
Zero-Day Vulnerabilities found by Haiku Scanner	7

* 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:

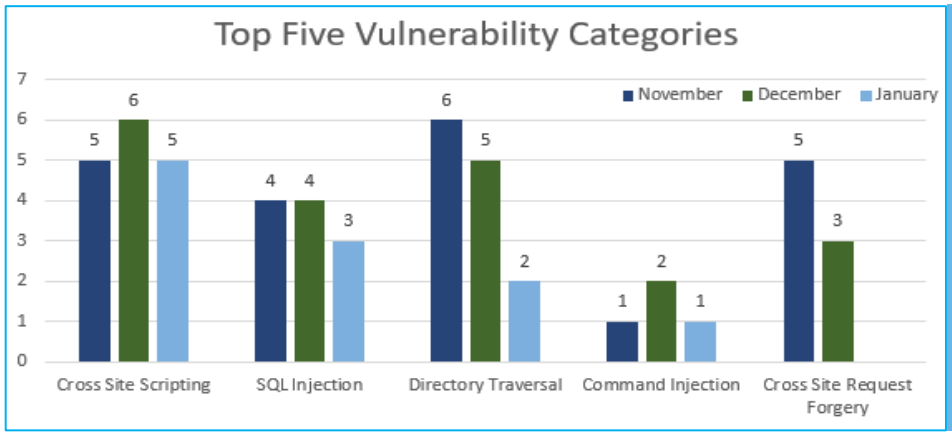


Weekly Vulnerability Trend displays the total no. of vulnerabilities discovered to the protection given for a quarter.

41% Of Zero-Day Vulnerabilities were protected by Core Rules in last quarter

9% Of Zero-Day Vulnerabilities were protected by Custom Rules in last quarter

50% Of Zero-Day Vulnerabilities were reported by Haiku Scanner in last quarter



From the graph, we infer that maximum Cross Site Scripting and Directory Traversal vulnerabilities are discovered in December and November respectively.

Zero Cross Site Request Forgery is found in January so far.

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	Haiku Scanner Coverage
1.	Cross Site Scripting	CVE-2020-5843	Codoforum 4.8.3 Admin Dashboard cross site scripting	A vulnerability was found in Codoforum 4.8.3 (Forum Software) and classified as problematic. Affected by this issue is an unknown code block of the component Admin Dashboard. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2020-6583	BigProf Online Invoicing System up to 2.6 on iOS cross site scripting	A vulnerability has been found BigProf Online Invoicing System up to 2.6 on iOS (iOS App Software) and classified as problematic. Affected by this vulnerability is an unknown part. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-20182	FooGallery Plugin 1.8.12 on WordPress post_title cross site scripting	A vulnerability was found in FooGallery Plugin 1.8.12 on WordPress (WordPress Plugin). It has been declared as problematic. This vulnerability affects an unknown code. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.
		CVE-2019-20378	Ganglia-web up to 3.7.5 Frontend header.php ce cross site scripting	A vulnerability classified as problematic was found in Ganglia-web up to 3.7.5. Affected by this vulnerability is an unknown functionality of the file header.php of the component Frontend. There is no information about	Protected by Default Rules.	Detected by scanner as Cross Site Scripting attack.

				possible countermeasures known. It may be suggested to replace the affected object with an alternative product.		
2.	Directory Traversal	CVE-2020-5512	Gila CMS 1.11.8 /admin/media path directory traversal	A vulnerability was found in Gila CMS 1.11.8 (Content Management System). It has been classified as critical. Affected is an unknown code of the file /admin/media?. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
		CVE-2020-5840	HashBrown CMS up to 1.3.1 Connection.js name/ID directory traversal	A vulnerability, which was classified as critical, has been found in HashBrown CMS up to 1.3.1 (Content Management System). This issue affects some unknown functionality of the file Server/Entity/Resource/Connection.js. Upgrading to version 1.3.2 eliminates this vulnerability.	Protected by Default Rules.	Detected by scanner as Directory Traversal attack.
3.	SQL Injection	CVE-2020-5515	Gila CMS 1.11.8 /admin/sql query sql injection	A vulnerability classified as critical has been found Gila CMS 1.11.8 (Content Management System). This affects an unknown function of the file /admin/sql. There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.	Protected by Core Rules.	Detected by scanner as SQL Injection attack.