# Weekly Zero-Day Vulnerability Coverage Bulletin

*(11th February – 17th February)*

Summary:

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

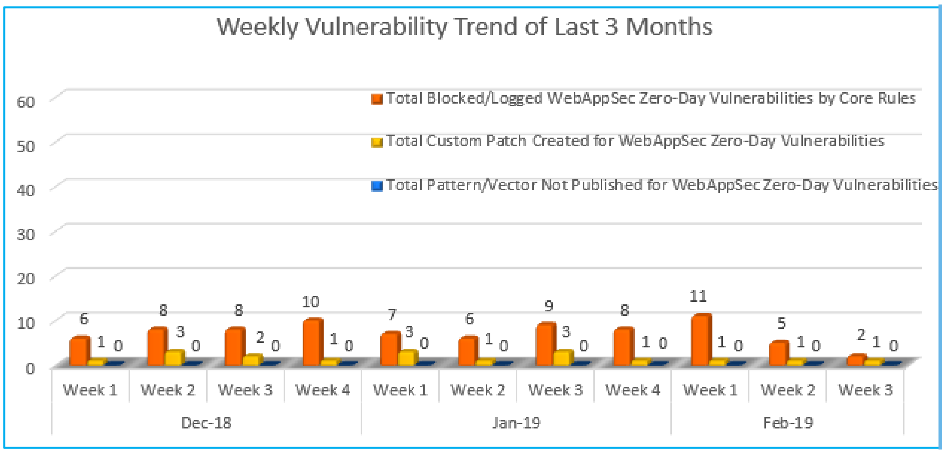
| | | |
|---|---|---|
| **1**<br>Cross Site Scripting | **1**<br>Directory Traversal | **1**<br>Cross Site Request Forgery |

| | |
|---|---|
| Zero-Day Vulnerabilities Protected through Core Rules | 2 |
| 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

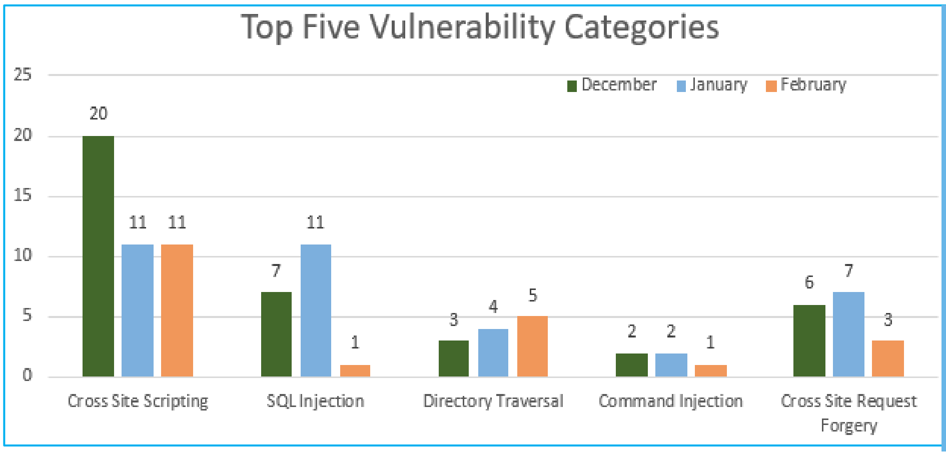
## Vulnerability Trend:



Weekly Trend displays the total no. of discovered vulnerabilities to the type of protection provided for the last quarter.

**82%** Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

**18%** 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-2018-13403 | Atlassian JIRA up to 7.6.9/7.12.3/7.13.0 Two-Dimensional Filter Statistics Gadget cross site scripting | A vulnerability has been found in Atlassian JIRA up to 7.6.9/7.12.3/7.13.0 (Bug Tracking Software) and classified as problematic. This vulnerability affects a functionality of the component *Two-Dimensional Filter Statistics Gadget*. The manipulation with an unknown input 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. | Directory Traversal | CVE-2015-4617 | Easy2map-photos Plugin 1.09 on WordPress MapPinImageUpload.php directory traversal | A vulnerability classified as critical was found in Easy2map-photos Plugin 1.09 on WordPress. Affected by this vulnerability is the functionality of the file *MapPinImageUpload.php*. 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 summary by CVE is:Vulnerability in Easy2map-photos WordPress Plugin v1.09 MapPinImageUpload.php and MapPinIconSave.php allows path traversal. | Protected by Default Rules. |

| | | | | | |
|---|---|---|---|---|---|
| 3. | Cross Site Request Forgery | CVE-2019-7730 | MyWebSQL 3.7 ?q=wrkfrm&type=databases cross site request forgery | A vulnerability was found in MyWebSQL 3.7. It has been classified as problematic. This affects code of the file */?q=wrkfrm&type=databases*. 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 force legitimate users to initiate unwanted actions within the web application. The weakness was shared 02/11/2019. This vulnerability is uniquely identified as CVE-2019-7730 since 02/11/2019. | Protected by Custom Rules. |