Weekly Zero-Day Vulnerability Coverage Bulletin

(3rd December – 9th December)

Summary:

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

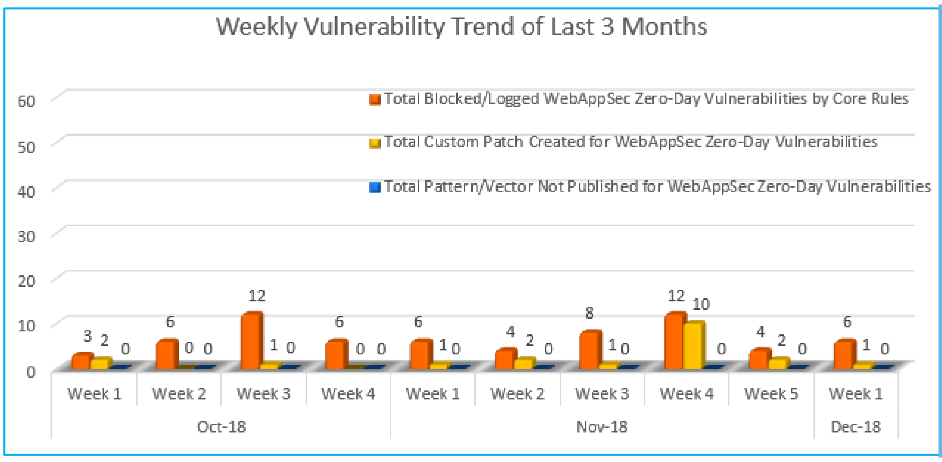
4 Cross Site Scripting	**2** SQL Injection	**1** Cross Site Request Forgery

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

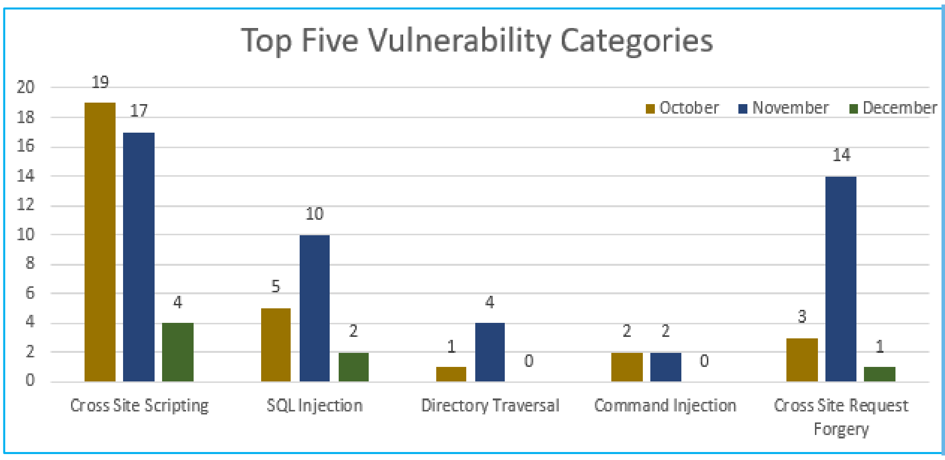
Vulnerability Trend:



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

78% Of Zero-Day Vulnerabilities were protected by Core Rules in last 3 months

22% 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 and CSRF are found in all 3 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-2018-19787	lxml up to 4.2.4 javascript URL lxml/html/clean.py cross site scripting	A vulnerability, which was classified as problematic, was found in lxml up to 4.2.4. Affected is an unknown function of the file *lxml/html/clean.py* of the component *javascript URL Handler*. The manipulation with the input value javascript: 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.	Protected by Default Rules.
		CVE-2018-19835	MetInfo 6.1.3 admin/column/move.php lang_columnerr4 cross site scripting	A vulnerability, which was classified as problematic, was found in MetInfo 6.1.3. This affects an unknown function of the file *admin/column/move.php*. The manipulation of the argument lang_columnerr4 as part of a *Parameter* leads to a cross site scripting vulnerability (Reflected). 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 web site. This would alter the appearance.	Protected by Default Rules.
		CVE-2018-18991	SCADA Webserver up to 2.03 Reflected cross site scripting	A vulnerability has been found in SCADA Webserver up to 2.03 and classified as problematic. This vulnerability affects an unknown function. The manipulation with an unknown input leads to a cross site scripting vulnerability (Reflected). 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 web site. This would alter the appearance and would make it possible to initiate.	Protected by Default Rules.

		CVE-2018-19924	Sales & Company Management System up to 2018-06-06 Request cross site scripting	A vulnerability, which was classified as problematic, has been found in Sales & Company Management System up to 2018-06-06. This issue affects an unknown function. The manipulation as part of a *Request* 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 and would make it possible to initiate further.	Protected by Default Rules.
2.	SQL Injection	CVE-2018-1002000	Arigato Autoresponder and Newsletter 2.5.1.8 on WordPress del_ids Blind sql injection	A vulnerability was found in Arigato Autoresponder and Newsletter 2.5.1.8 on WordPress. It has been rated as critical. This issue affects an unknown function. The manipulation of the argument del_ids as part of a *POST Request* leads to a sql injection vulnerability (Blind). 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 published in 12/03/2018.	Protected by Default Rules.
		CVE-2018-19925	Sales & Company Management System 2018-06-06 member/member_order.php type/O_state sql injection	A vulnerability which was classified as critical, was found in Sales & Company Management System in 2018-06-06. Affected is an unknown function of the file *member/member_order.php*. The manipulation of the argument type/O_state as part of a *Parameter* leads to a sql injection vulnerability. CWE is classifying the issue as CWE-89. This is	Protected by Default Rules.

				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.	Cross Site Request Forgery	CVE-2018-19923	Sales & Company Management System up to 2018-06-06 member_email.php Cross Site Request Forgery	A vulnerability classified as problematic was found in Sales & Company Management System up to 2018-06-06. This vulnerability affects an unknown function of the file *member/member_email.php?action=edit*. 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.	Protected by Custom Rules.