

Pen test (Penetration testing)

Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit. Penetration testing can be automated with software applications or performed manually. Either way, the process involves gathering information about the target before the test, identifying possible entry points, attempting to break in – either virtually or for real – and reporting back the findings.

The main objective of penetration testing is to identify security weaknesses. The information about security weaknesses that are identified or exploited through pen testing is aggregated and provided to the organization's IT and networking system managers, enabling them to make strategic decisions and prioritize remediation efforts.

Pen testers often use automated tools to uncover standard application vulnerabilities. Penetration tools scan code in order to identify malicious code in applications that could result in a security breach.

Here, we used Zap Proxy as tools for Pen testing in Kali Linux. It is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Zap Proxy

The OWASP Zed Attack Proxy (ZAP) is one of the most popular free security tools and is actively maintained by hundreds of international volunteers. It can help us automatically find security vulnerabilities in our web applications while we are developing and testing our applications. It is also a great tool for experienced Pen testers to use for manual security testing. It is Java interface.

In order to use this tool for Pen testing in our Kali Linux we must go through following steps.

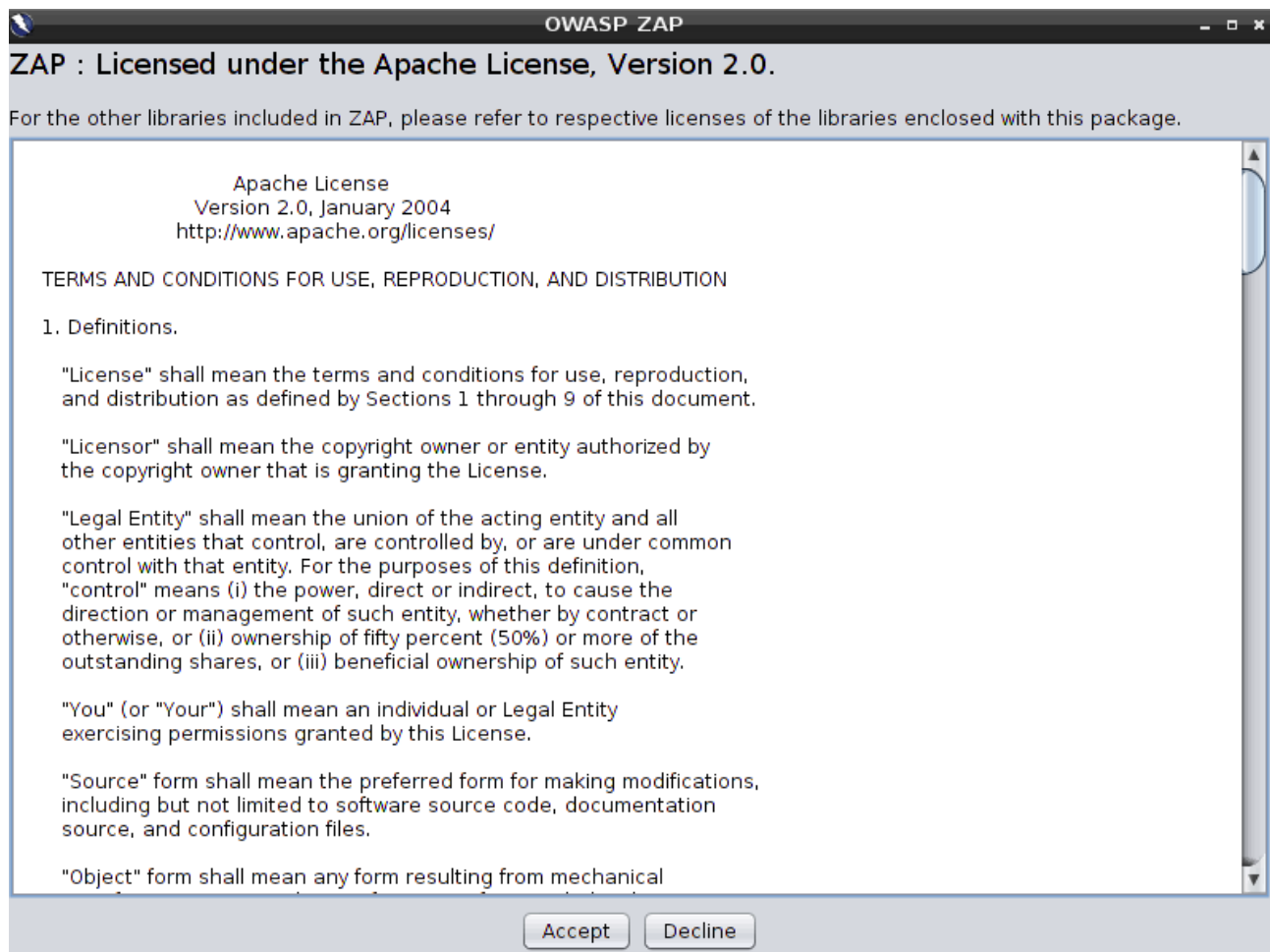
Step 1: Open OWASP Zap

In this step first we'll open Zap Proxy, to open that first we'll go to Applications then from there we'll choose 03-Web Application Analysis and then open OWASPZap.



Step 2: Accept licensing

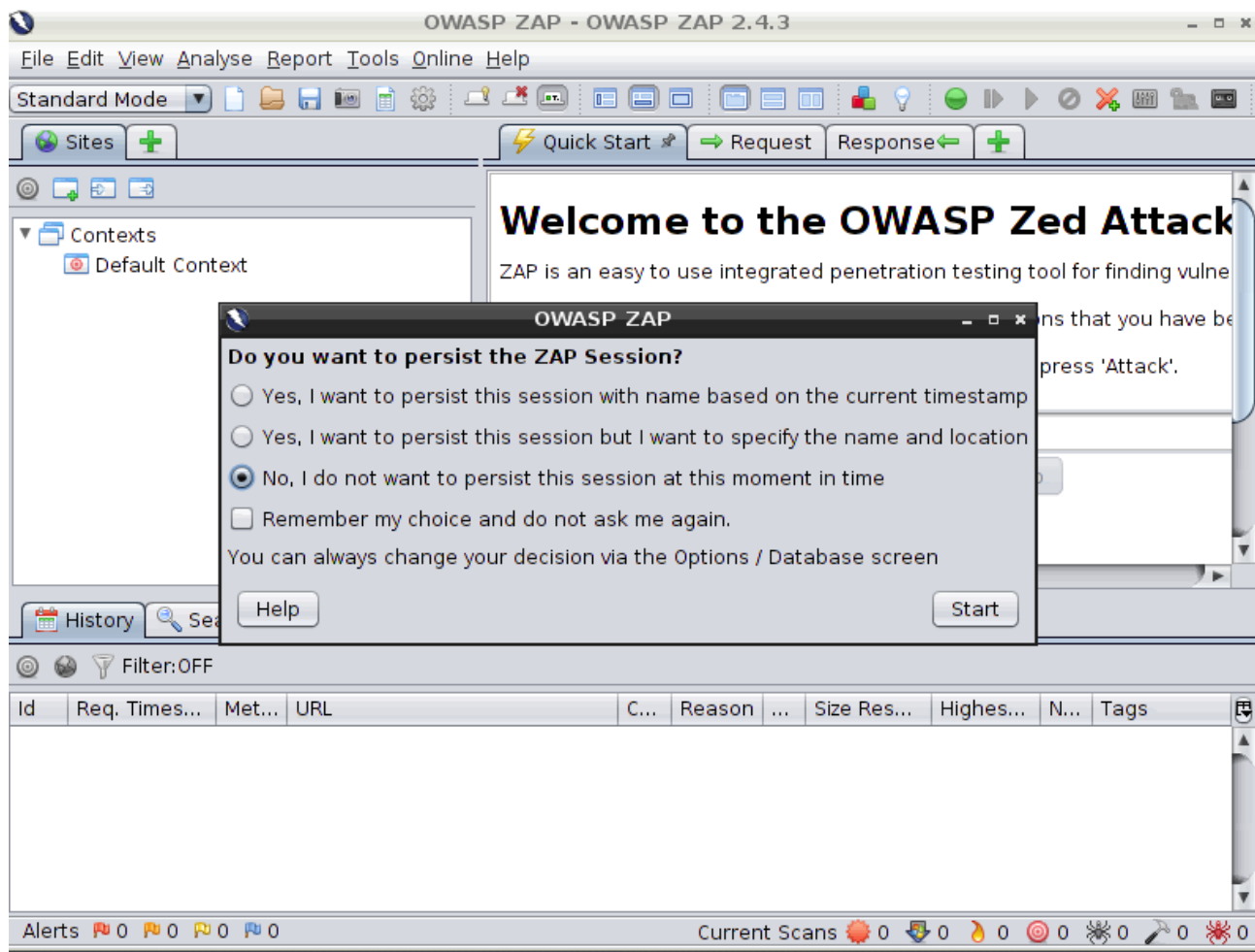
In this step we'll accept licensing agreement of OWASP ZAP before using it.



Once we'll accept licensing ZAP will start to load.

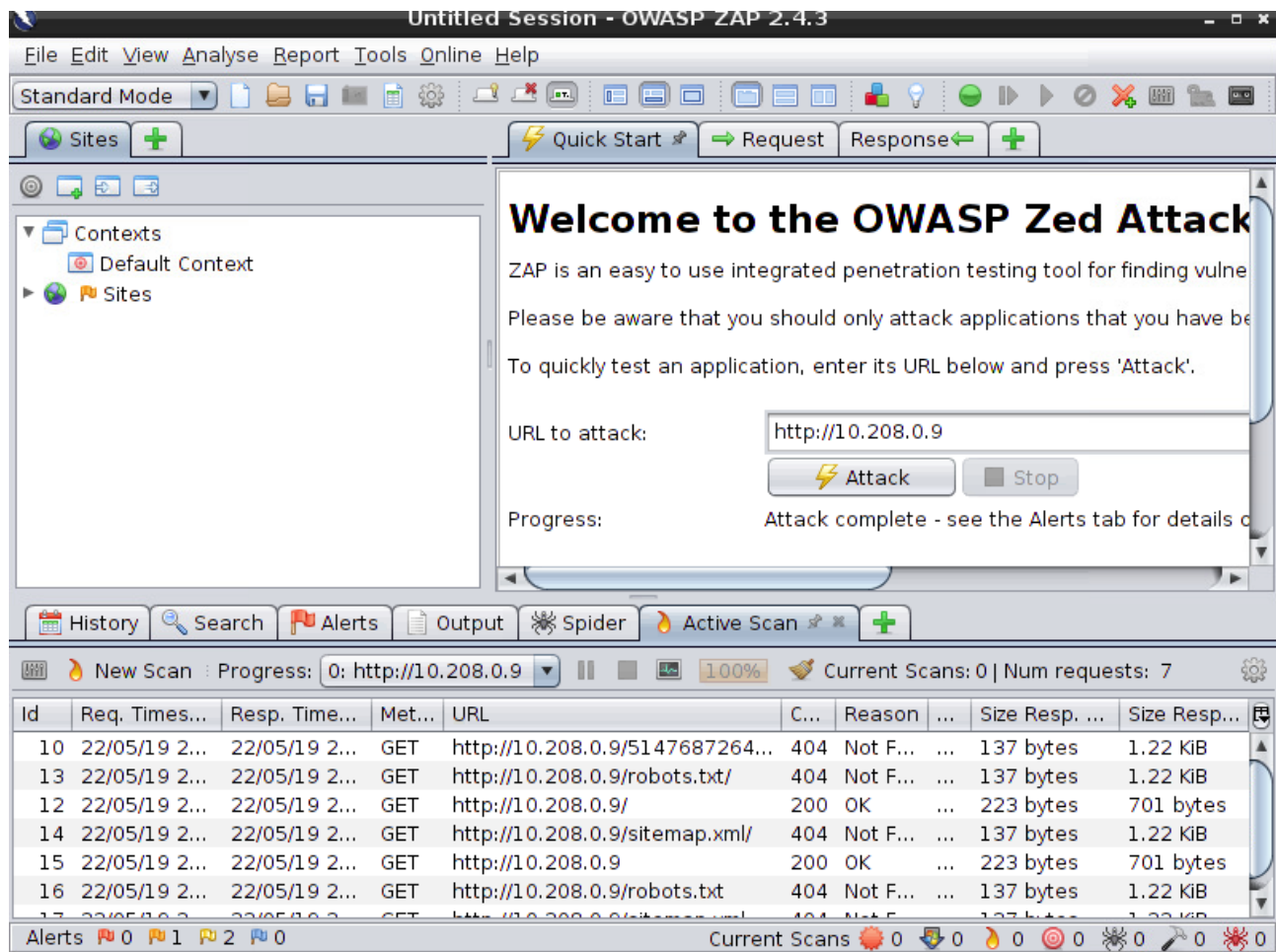
Step 3: Starting OWASP ZAP

Here we can choose one of the options from as shown in the following options and then click "Start".



Step 4: Enter URL of the testing web at “URL to attack” > click “Attack”.

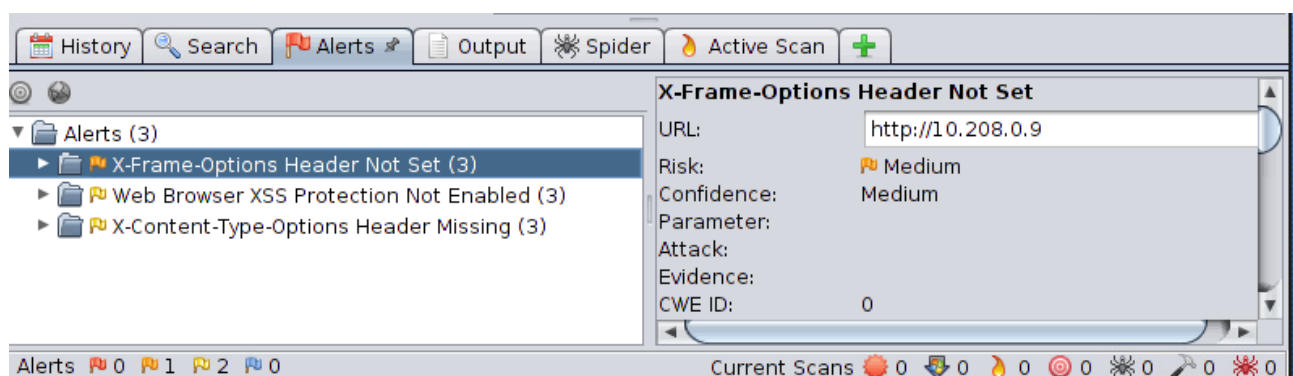
Here, I put IP on my WIN S1 – 10.208.0.9 then I clicked attack and the result is as shown.



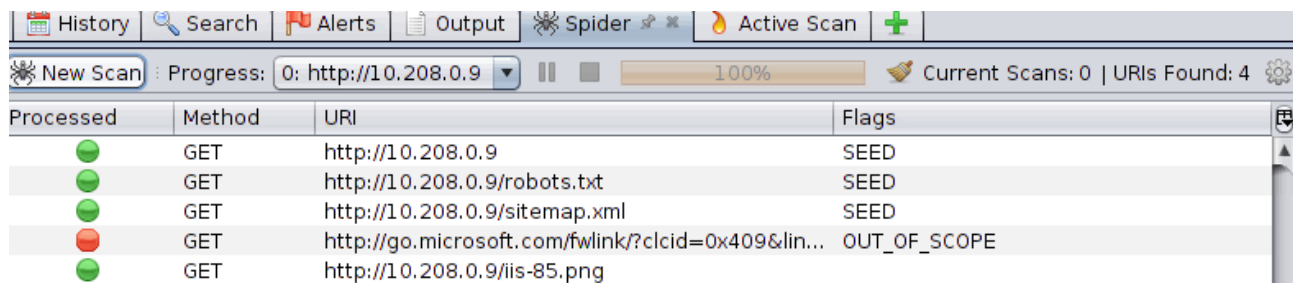
After the scan is completed, on the top left panel we will see all the crawled sites.

Step 5:

Similarly, in the left panel Alerts, we can see all the finding along with the description.



Step 6: On clicking “Spider” we can see all the links scanned.



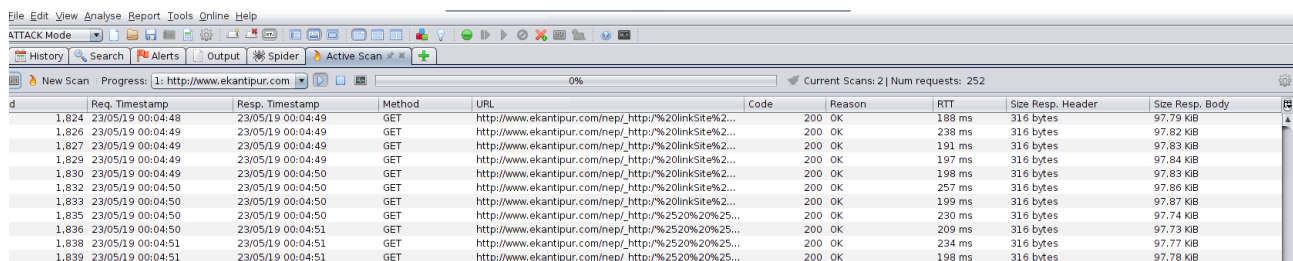
The screenshot shows the Burp Suite Spider tool interface. The top bar includes tabs for History, Search, Alerts, Output, Spider, and Active Scan. Below the tabs, a progress bar shows 'Progress: 0: http://10.208.0.9' and 'Current Scans: 0 | URLs Found: 4'. The main table displays the following data:

Processed	Method	URI	Flags
●	GET	http://10.208.0.9	SEED
●	GET	http://10.208.0.9/robots.txt	SEED
●	GET	http://10.208.0.9/sitemap.xml	SEED
●	GET	http://go.microsoft.com/fwlink?clcid=0x409&lin...	OUT_OF_SCOPE
●	GET	http://10.208.0.9/iis-85.png	

Again, I took one more example to test using this tool.

A newspaper website “www.ekantipur.com” and my finding are here as follows with snippets and descriptions.

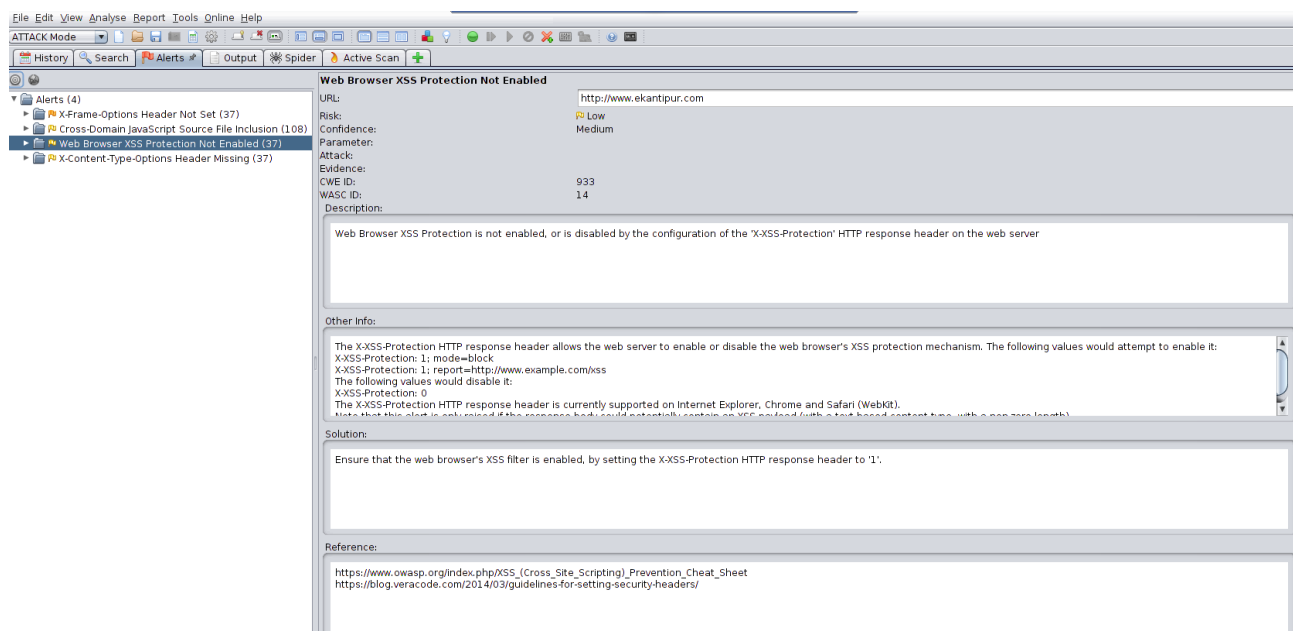
Here, we can see all the “Active scan” going on:



The screenshot shows the Burp Suite Active Scan tool interface. The top bar includes tabs for History, Search, Alerts, Output, Spider, and Active Scan. Below the tabs, a progress bar shows 'Progress: 1: http://www.ekantipur.com' and 'Current Scans: 2 | Num requests: 252'. The main table displays the following data:

d	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
1,824	23/05/19 00:04:48	23/05/19 00:04:49	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	188 ms	316 bytes	97.79 KB
1,826	23/05/19 00:04:49	23/05/19 00:04:49	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	238 ms	316 bytes	97.82 KB
1,827	23/05/19 00:04:49	23/05/19 00:04:49	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	191 ms	316 bytes	97.83 KB
1,829	23/05/19 00:04:49	23/05/19 00:04:49	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	197 ms	316 bytes	97.84 KB
1,830	23/05/19 00:04:49	23/05/19 00:04:50	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	198 ms	316 bytes	97.83 KB
1,832	23/05/19 00:04:50	23/05/19 00:04:50	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	257 ms	316 bytes	97.86 KB
1,833	23/05/19 00:04:50	23/05/19 00:04:50	GET	http://www.ekantipur.com/nep/_http/%20linkSite%2...	200	OK	199 ms	316 bytes	97.87 KB
1,835	23/05/19 00:04:50	23/05/19 00:04:50	GET	http://www.ekantipur.com/nep/_http/%2520%20%25...	200	OK	230 ms	316 bytes	97.74 KB
1,836	23/05/19 00:04:50	23/05/19 00:04:51	GET	http://www.ekantipur.com/nep/_http/%2520%20%25...	200	OK	209 ms	316 bytes	97.73 KB
1,838	23/05/19 00:04:51	23/05/19 00:04:51	GET	http://www.ekantipur.com/nep/_http/%2520%20%25...	200	OK	234 ms	316 bytes	97.77 KB
1,839	23/05/19 00:04:51	23/05/19 00:04:51	GET	http://www.ekantipur.com/nep/_http/%2520%20%25...	200	OK	198 ms	316 bytes	97.78 KB

In “Alert” section we can see all the findings along with the description.



The screenshot shows the Burp Suite Alerts section. The left sidebar lists alerts, including 'Web Browser XSS Protection Not Enabled (37)'. The main panel displays the details for this alert:

Alerts (4)	Web Browser XSS Protection Not Enabled
▶ X-Frame-Options Header Not Set (37)	URL: http://www.ekantipur.com
▶ Cross-Domain JavaScript Source File Inclusion (108)	Risk: Low
▶ Web Browser XSS Protection Not Enabled (37)	Confidence: Medium
▶ X-Content-Type-Options Header Missing (37)	Parameter:
	Attack:
	Evidence:
	CWE ID: 933
	WASC ID: 14
	Description:
	Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server
	Other Info:
	The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length).
	Solution:
	Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.
	Reference:
	https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/

If we click “Spider” we can see all the links scanned.

History		Search	Alerts	Output	Spider	Active Scan	
New Scan		Progress: 0: http://www.ekantipur.com		100%		Current Scans: 0 URIs Found: 1493	
Processed		Method	URI	Flags			
	●	GET	http://www.ekantipur.com	SEED			
	●	GET	http://www.ekantipur.com/robots.txt	SEED			
	●	GET	http://www.ekantipur.com/sitemap.xml	SEED			
	●	GET	http://www.ekantipur.com/				
	●	GET	https://www.kantipurdaily.com/	OUT_OF_SCOPE			
	●	GET	http://kathmandupost.ekantipur.com/	OUT_OF_SCOPE			
	●	GET	http://saptahik.ekantipur.com/	OUT_OF_SCOPE			
	●	GET	http://nepal.ekantipur.com/	OUT_OF_SCOPE			
	●	GET	http://nari.ekantipur.com/	OUT_OF_SCOPE			
	●	GET	http://radiokantipur.ekantipur.com/	OUT_OF_SCOPE			
	●	GET	http://kantipur.tv.com/	OUT_OF_SCOPE			
	●	GET	http://www.ekantipur.com/sitemap.xml/world				
	●	GET	http://www.ekantipur.com/sitemap.xml/nepal				
	●	GET	http://www.ekantipur.com/sitemap.xml/politics				
	●	GET	http://www.ekantipur.com/sitemap.xml/sports				
	●	GET	http://www.ekantipur.com/sitemap.xml/economy				
	●	GET	http://www.ekantipur.com/sitemap.xml/entertainment				
	●	GET	http://www.ekantipur.com/sitemap.xml/others				
	●	GET	http://www.ekantipur.com/%22+c.url+%22				
	●	GET	http://jcss-cdn.ekantipur.com/ekantipur/images/ekantipur-icon1.png	OUT_OF_SCOPE			
	●	GET	http://jcss-cdn.ekantipur.com/ekantipur/stylesheets/common.v2.23.css	OUT_OF_SCOPE			
	●	GET	http://jcss-cdn.ekantipur.com/common/javascript/jquery/jquery.min.js	OUT_OF_SCOPE			
	●	GET	http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	OUT_OF_SCOPE			
	●	GET	http://jcss-cdn.ekantipur.com/ekantipur/javascripts/common.v2.23.js	OUT_OF_SCOPE			
	●	GET	http://jcss-cdn.ekantipur.com/ekantipur/images/ekantipur-newlogo2.png	OUT_OF_SCOPE			
	●	GET	http://jcss-cdn.ekantipur.com/ekantipur/images/sidebar-icon.png	OUT_OF_SCOPE			
	●	GET	https://d5rxst8fruw4z.cloudfront.net/atrk.gif?account=pzk+1laU8KL3em	OUT_OF_SCOPE			
	●	GET	http://www.ekantipur.com/%22+c.thumbnail+%22				