OWASP-ZAP- Web Application Scanner

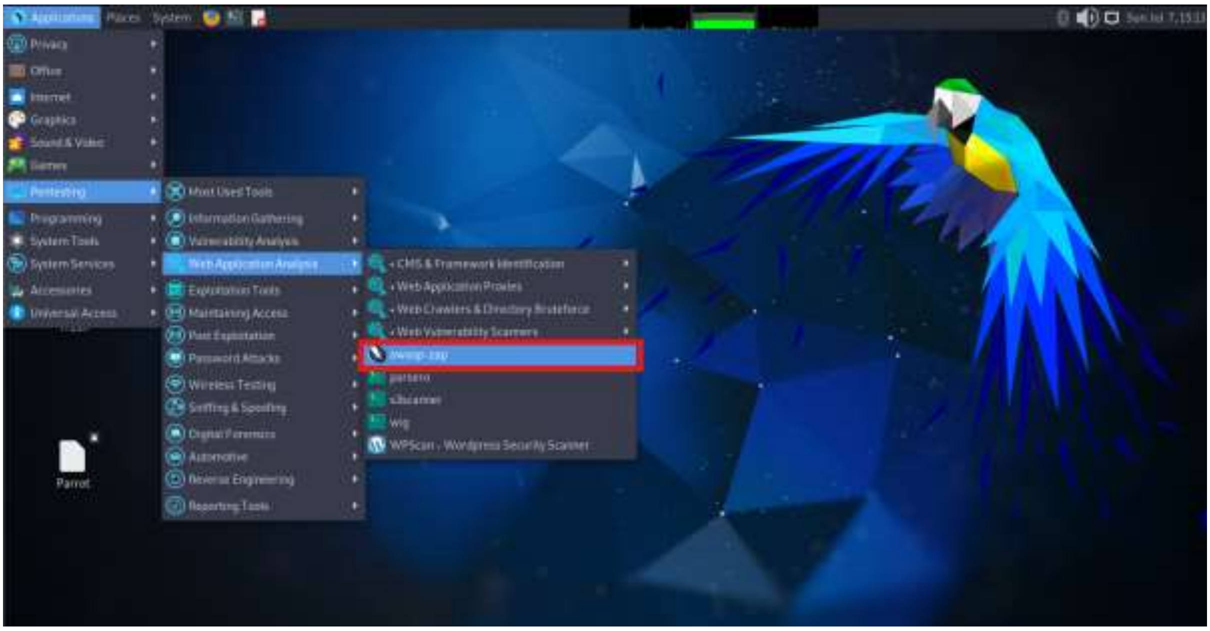
OWASP Zed Attack Proxy (ZAP) is a widely used open-source web application security scanner for Linux, developed under the OWASP (Open Web Application Security Project) umbrella. It is designed to find security vulnerabilities in web applications, making it a valuable tool for security professionals, developers, and QA testers. ZAP provides a range of features including automated scanners to identify common vulnerabilities, a powerful spider to crawl web applications, and a manual testing interface for more advanced analysis. It supports both passive and active scanning, where passive scanning analyzes traffic without interfering with it, while active scanning actively probes the application for vulnerabilities. ZAP also offers a variety of plugins to extend its functionality, integration with other tools through APIs, and a scripting interface for custom tests. Additionally, its user-friendly GUI makes it accessible for users with varying levels of security expertise. Using ZAP, users can conduct comprehensive security assessments of their web applications, helping to identify and remediate potential threats before they can be exploited.

Using OWASP Zed Attack Proxy (ZAP), you can perform a comprehensive range of scans to assess and enhance the security of web applications. The tool supports automated scans, including passive scans that analyze traffic without interfering and active scans that probe for vulnerabilities like

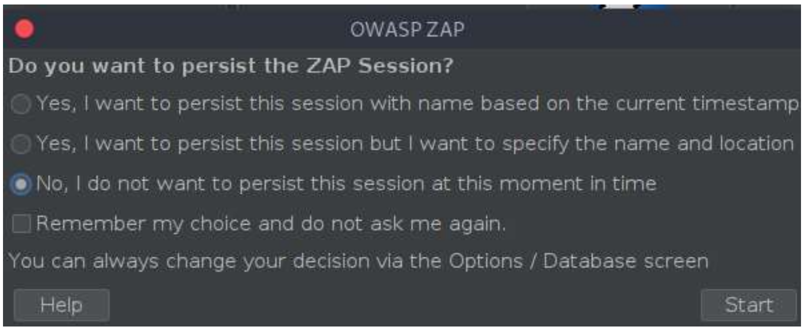
SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF). ZAP's spidering and crawling capabilities allow it to map web applications thoroughly, discovering all pages and resources, including those loaded dynamically via JavaScript. Forced browsing attempts to access hidden or unprotected resources by brute-forcing URLs. Additionally, ZAP's fuzzing feature tests the robustness of web applications by sending varied inputs to detect buffer overflows and input validation issues. Port scanning identifies open ports on the target server, uncovering potentially vulnerable services. Authentication and session management testing ensure the strength and security of login mechanisms and session handling. For real-time applications, ZAP includes WebSocket testing to find protocol-specific issues. By leveraging these diverse scanning capabilities, ZAP helps developers and security professionals identify and mitigate security vulnerabilities, ensuring more secure web applications.

Examples: -

1. OWASP-ZAP is pre-installed tool in Linux Distribution. You can open it from the Application Menu.



2. Now it will ask about the saving the session. If you want to save the session then choice the option one else option three.


OWASP ZAP

Do you want to persist the ZAP Session?

○ Yes, I want to persist this session with name based on the current timestamp

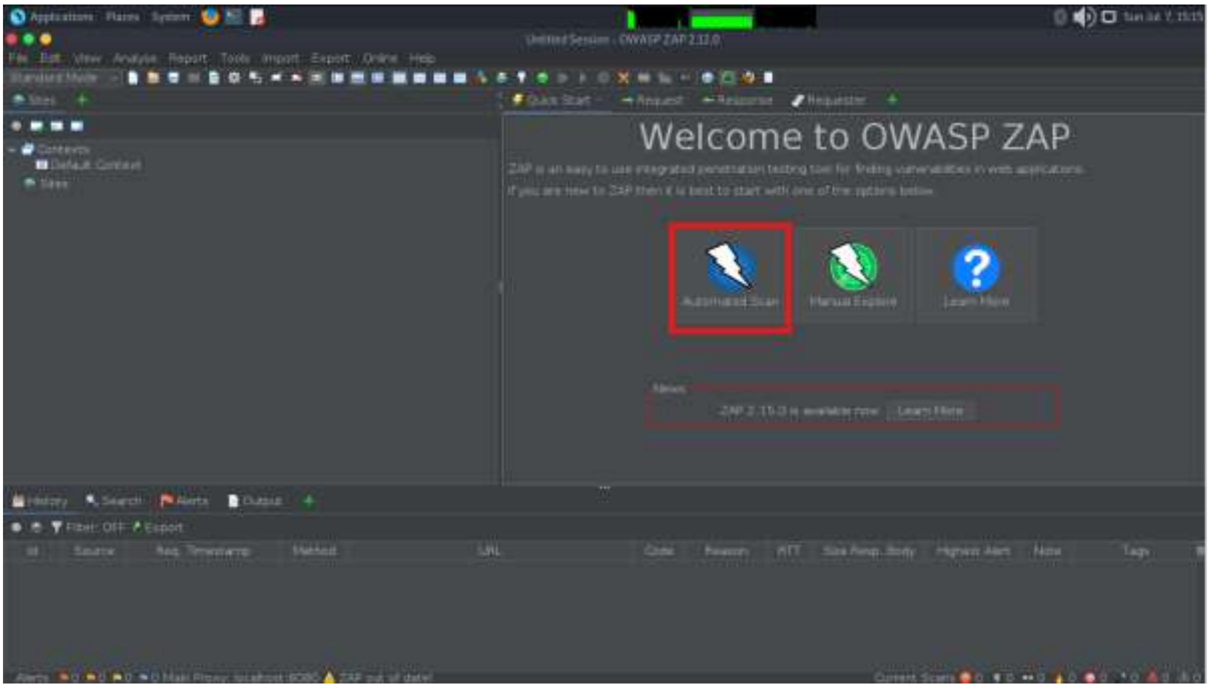
○ Yes, I want to persist this session but I want to specify the name and location

● No, I do not want to persist this session at this moment in time

□ Remember my choice and do not ask me again.

You can always change your decision via the Options / Database screen

3. In order to perform an Active scan. click the large Automated Scan button.



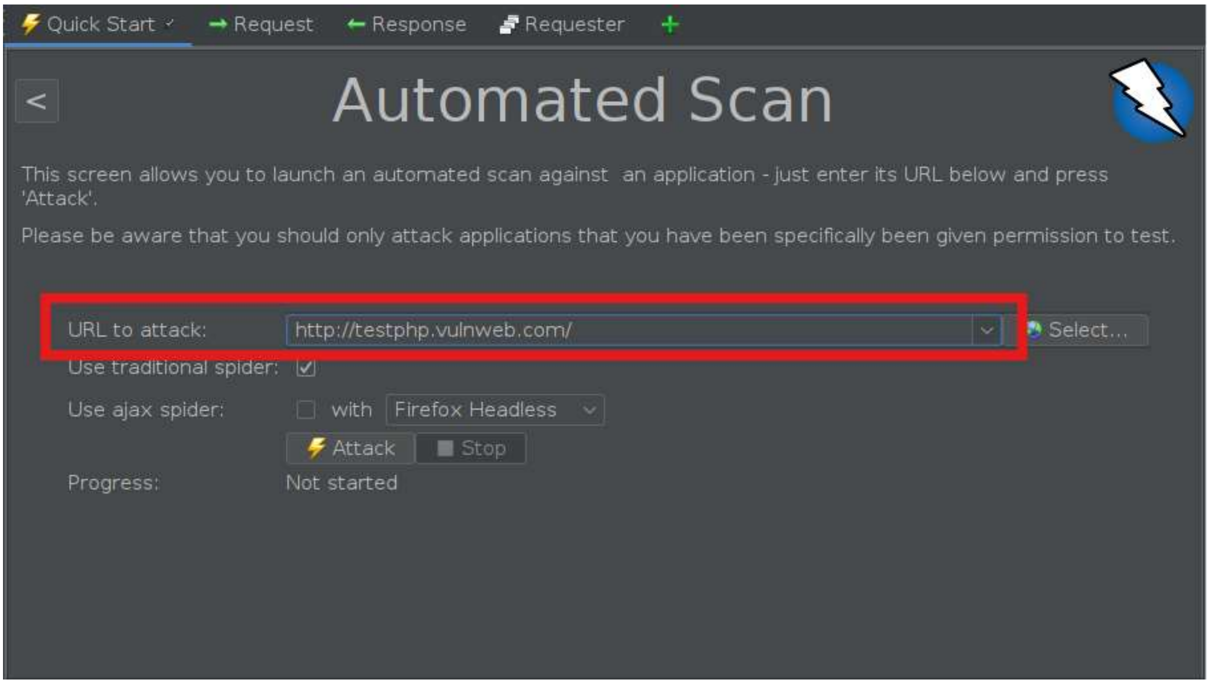
Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

ZAP 2.13.0 is available now

4. Now give the URL of target web application to perform the scan.



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

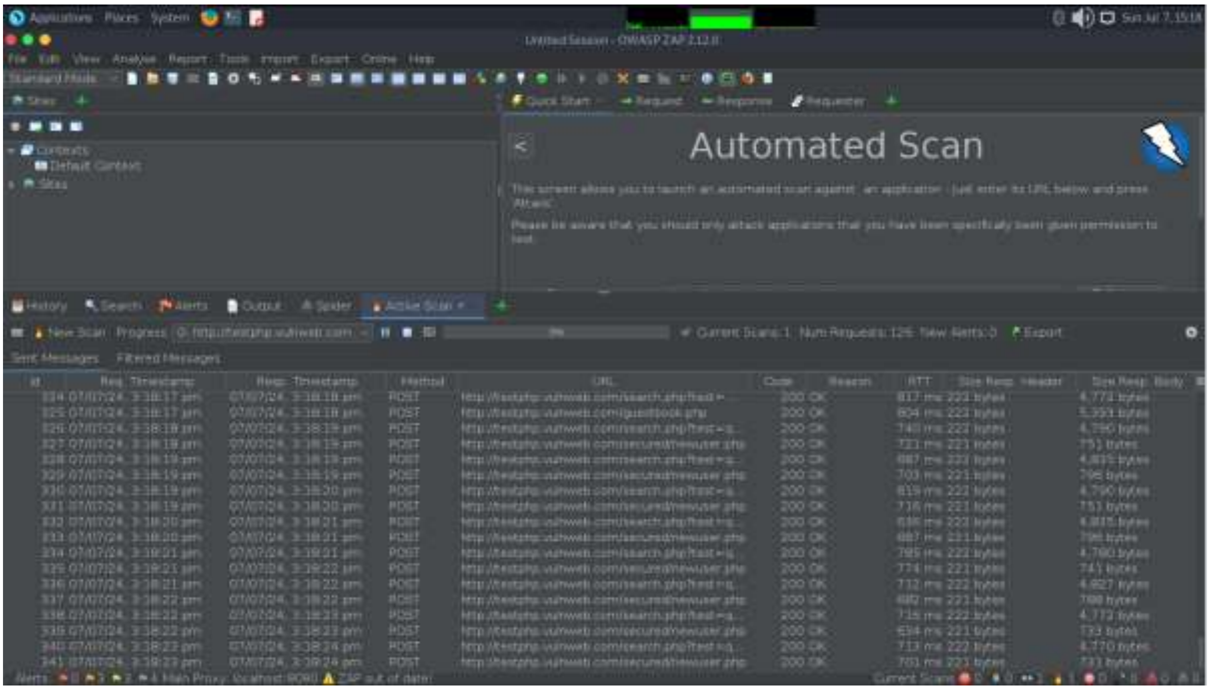
URL to attack: http://testphp.vulnweb.com/

Use traditional spider: ☑

Use ajax spider: ☐ with Firefox Headless

Progress: Not started

5. It will start an active scan and the result will be display in the output window.


Applications Places System
[redacted]
Sun Jul 7, 15:18
Untitled Session - OWASP ZAP 2.12.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Contexts
Default Context
Sites
Quick Start
Request
Response
Requester
History Search Alerts Output Spider Active Scan
New Scan Progress: 0: http://testphp.vulnweb.com
Export
Sent Messages Filtered Messages

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Current Scans: 1 Num Requests: 126 New Alerts: 0

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
324	07/07/24, 3:38:17 pm	07/07/24, 3:38:18 pm	POST	http://testphp.vulnweb.com/search.php?test=	200	OK	817 ms	222 bytes	4,773 bytes
325	07/07/24, 3:38:17 pm	07/07/24, 3:38:18 pm	POST	http://testphp.vulnweb.com/guestbook.php	200	OK	604 ms	222 bytes	5,393 bytes
326	07/07/24, 3:38:18 pm	07/07/24, 3:38:19 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	740 ms	222 bytes	4,790 bytes
327	07/07/24, 3:38:18 pm	07/07/24, 3:38:19 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	721 ms	221 bytes	751 bytes
328	07/07/24, 3:38:19 pm	07/07/24, 3:38:19 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	687 ms	222 bytes	4,835 bytes
329	07/07/24, 3:38:19 pm	07/07/24, 3:38:19 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	703 ms	221 bytes	795 bytes
330	07/07/24, 3:38:19 pm	07/07/24, 3:38:20 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	819 ms	222 bytes	4,790 bytes
331	07/07/24, 3:38:19 pm	07/07/24, 3:38:20 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	716 ms	221 bytes	751 bytes
332	07/07/24, 3:38:20 pm	07/07/24, 3:38:21 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	636 ms	222 bytes	4,835 bytes
333	07/07/24, 3:38:20 pm	07/07/24, 3:38:21 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	687 ms	221 bytes	795 bytes
334	07/07/24, 3:38:21 pm	07/07/24, 3:38:21 pm	POST	http://testphp.vulnweb.com/search.php?test=q	200	OK	785 ms	222 bytes	4,780 bytes
335	07/07/24, 3:38:21 pm	07/07/24, 3:38:22 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	774 ms	221 bytes	741 bytes
336	07/07/24, 3:38:21 pm	07/07/24, 3:38:22 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	732 ms	222 bytes	4,827 bytes
337	07/07/24, 3:38:22 pm	07/07/24, 3:38:22 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	682 ms	221 bytes	788 bytes
338	07/07/24, 3:38:22 pm	07/07/24, 3:38:23 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	715 ms	222 bytes	4,773 bytes
339	07/07/24, 3:38:22 pm	07/07/24, 3:38:23 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	634 ms	221 bytes	733 bytes
340	07/07/24, 3:38:23 pm	07/07/24, 3:38:24 pm	POST	http://testphp.vulnweb.com/search.php?test=q...	200	OK	713 ms	222 bytes	4,770 bytes
341	07/07/24, 3:38:23 pm	07/07/24, 3:38:24 pm	POST	http://testphp.vulnweb.com/secured/newuser.php	200	OK	701 ms	221 bytes	731 bytes

Alerts 0 1 2 4 Main Proxy: localhost:8080 ZAP out of date! Current Scans 0 0 1 1 0 0 0 0

ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.

The traditional ZAP spider which discovers links by examining the HTML in responses from the web application. This spider is fast, but it is not always effective when exploring an AJAX web application that generates links using JavaScript.