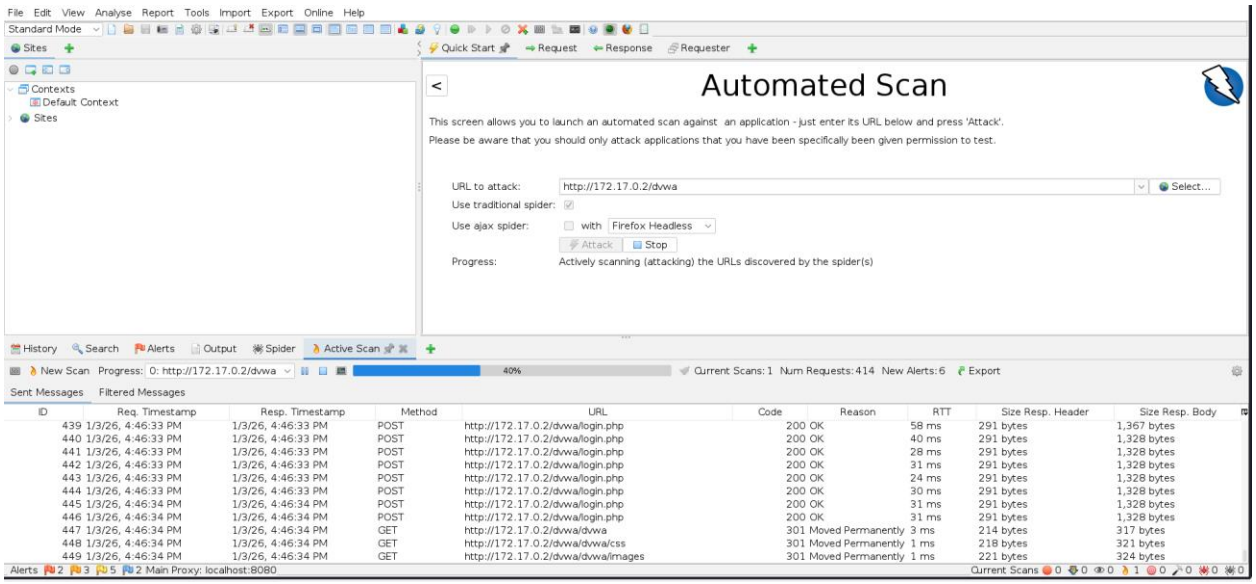
OWASP ZAP TOOL

OWASP ZAP is a free, open-source web application security testing tool maintained by the Open Web Application Security Project (OWASP). It is designed to help security professionals and beginners identify vulnerabilities in web applications. ZAP works as an intercepting proxy, allowing testers to observe, modify, and analyze HTTP/HTTPS traffic between a browser and a web application.

At its core, ZAP acts as a man-in-the-middle proxy. It sits between your web browser and the target application, allowing it to intercept, inspect, and even modify the data being sent back and forth.

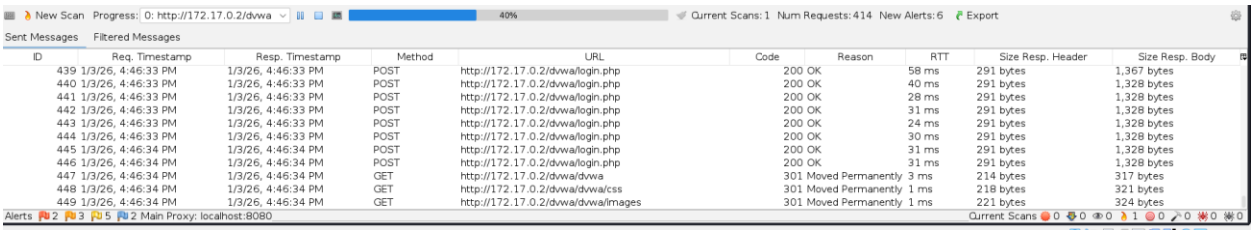
Key Features Include:

- ✓ **Automated Scanning:** Quickly identifies common flaws like SQL Injection and Cross-Site Scripting (XSS).
- ✓ **Passive Scanning:** Analyzes traffic in the background without modifying it (non-intrusive).
- ✓ **Active Scanning:** Actively attacks the application with known payloads to find deeper vulnerabilities.
- ✓ **Spidering:** Automatically "crawls" a website to map out its entire structure and hidden pages.
- ✓ **API & Automation:** Can be integrated into CI/CD pipelines to ensure security is checked with every code update.



The screenshot shows OWASP ZAP (Zed Attack Proxy) running an Automated Scan against a deliberately vulnerable web application, DVWA (Damn Vulnerable Web Application) hosted at

http://172.17.0.2/dvwa. The Automated Scan interface allows a tester to enter a target URL and launch a combined crawling and attack process. In this case, ZAP is actively scanning the application, as indicated by the progress bar (around 40%) and the status message showing that URLs discovered by the spider are being tested.



At the bottom panel, the Active Scan tab displays real-time HTTP traffic generated during the scan. It shows multiple GET and POST requests sent to endpoints such as login.php, along with HTTP response codes like 200 OK and 301 Moved Permanently. This confirms that ZAP is interacting with the application by submitting forms and navigating pages to identify vulnerabilities. The counters indicate the number of requests sent and alerts found so far, demonstrating that ZAP is already detecting potential security issues.

CONCLUSION

ZAP provides both passive scanning, which detects issues without sending malicious requests, and active scanning, which safely attempts attacks to uncover vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), authentication weaknesses, and security misconfigurations. Its Automated Scan feature combines crawling (spidering) and active testing, making it suitable for quick security assessments and learning environments. Overall, OWASP ZAP is a powerful tool for improving web application security and understanding common web vulnerabilities.