Web Application Testing Lab

Author: Harshal Harekar
Date: 14/10/2025

Objective

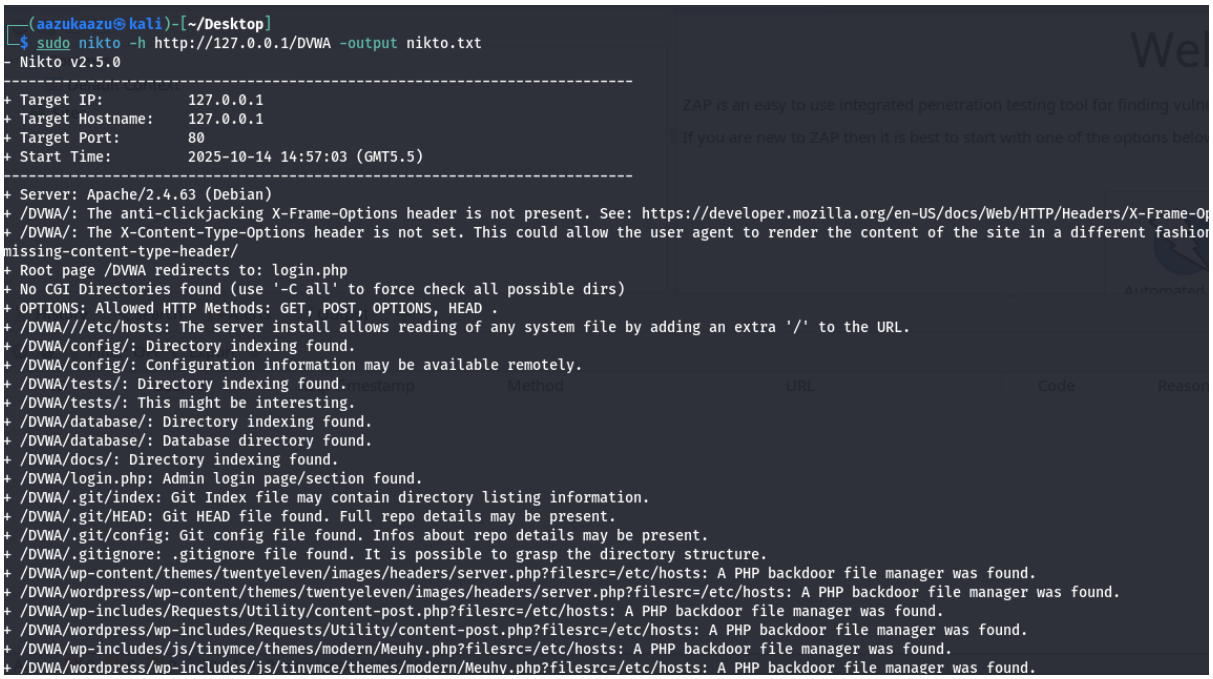
Conduct systematic OWASP Top 10 testing on DVWA to identify, exploit, and document SQL Injection and Cross-Site Scripting vulnerabilities.

Environment

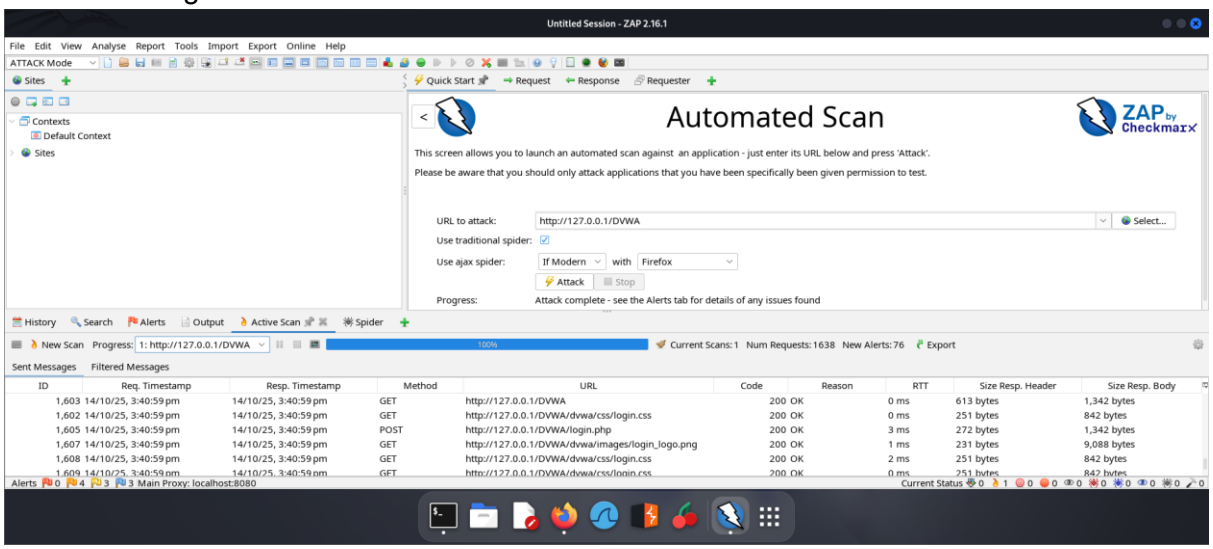
- Attacker: Kali Linux
- Target: DVWA
- Tools: Burp Suite, sqlmap, OWASP ZAP, Nikto

Steps

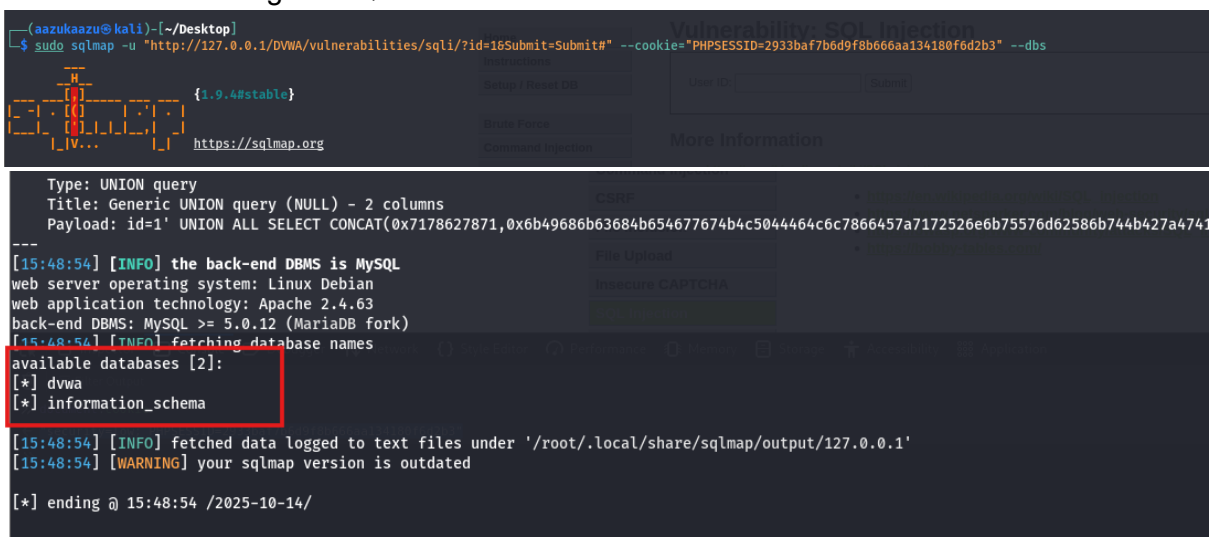
1. Recon using Nikto
nikto -h http://127.0.0.1/DVWA -output nikto.txt



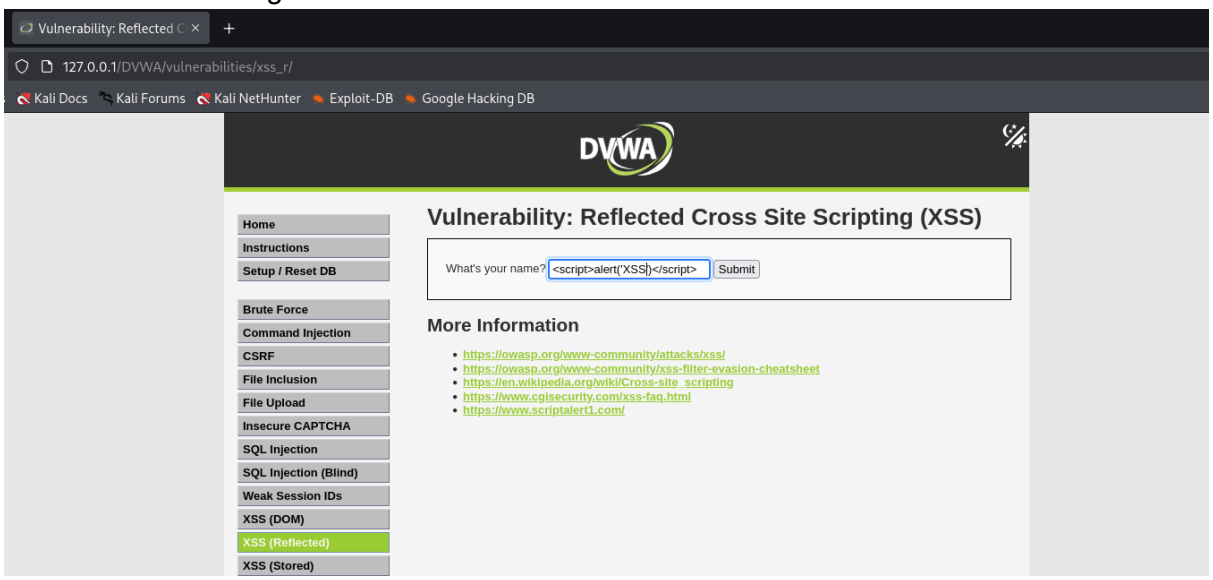
2. Recon using OWASP-ZAP

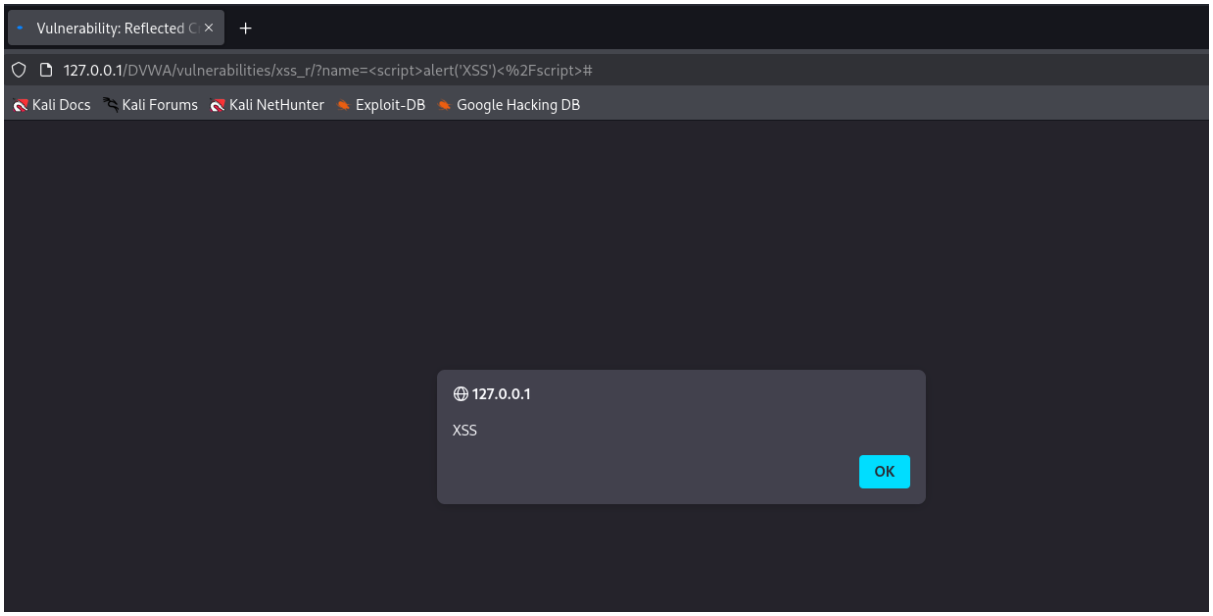


3. Automated Testing for SQLi

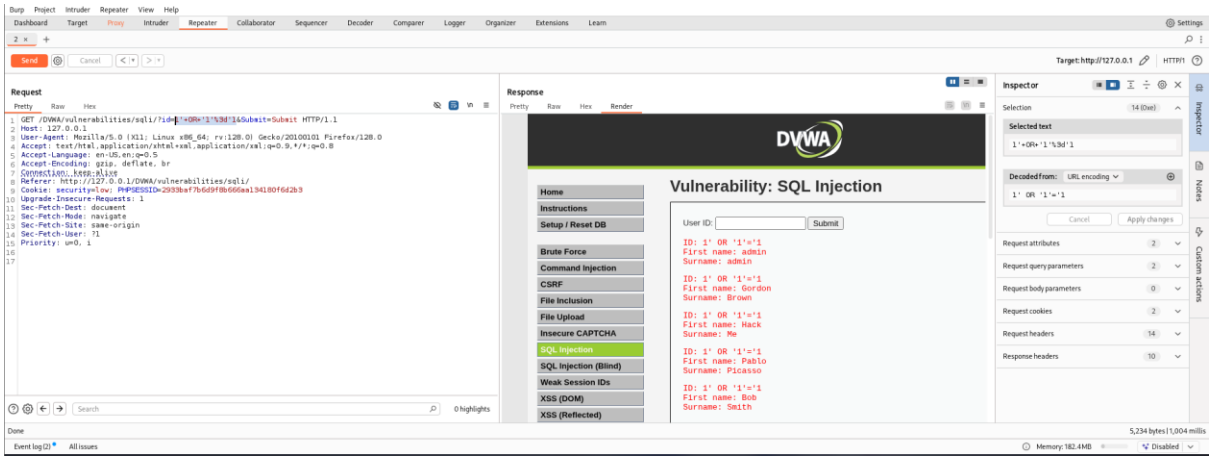


4. Automated Testing for XSS

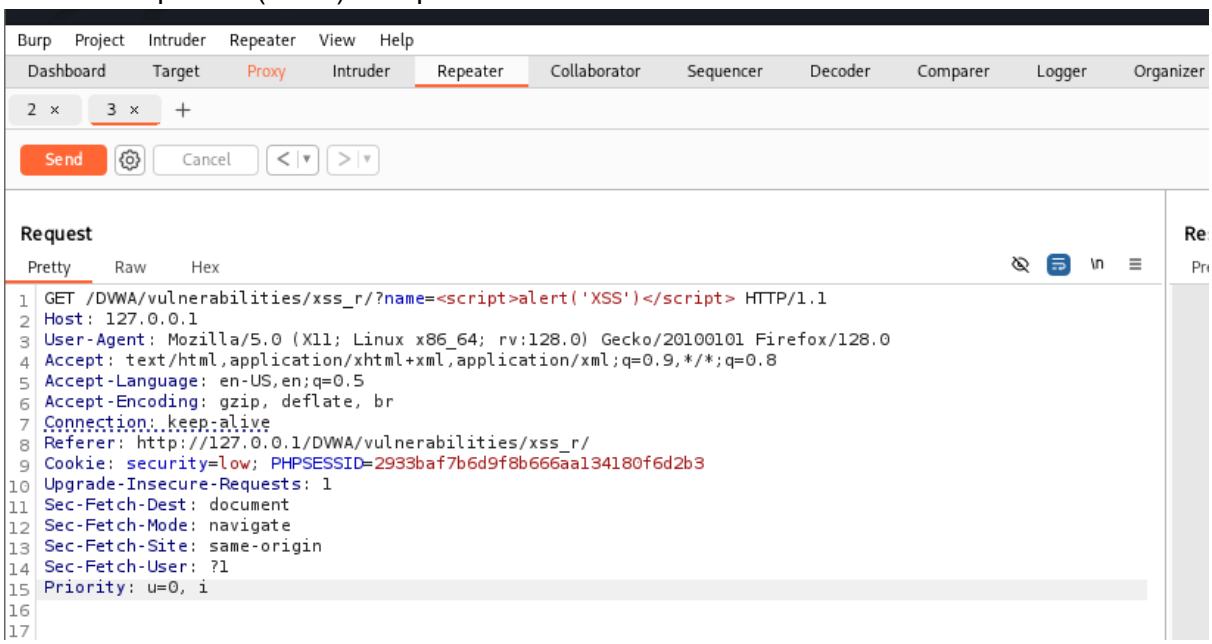


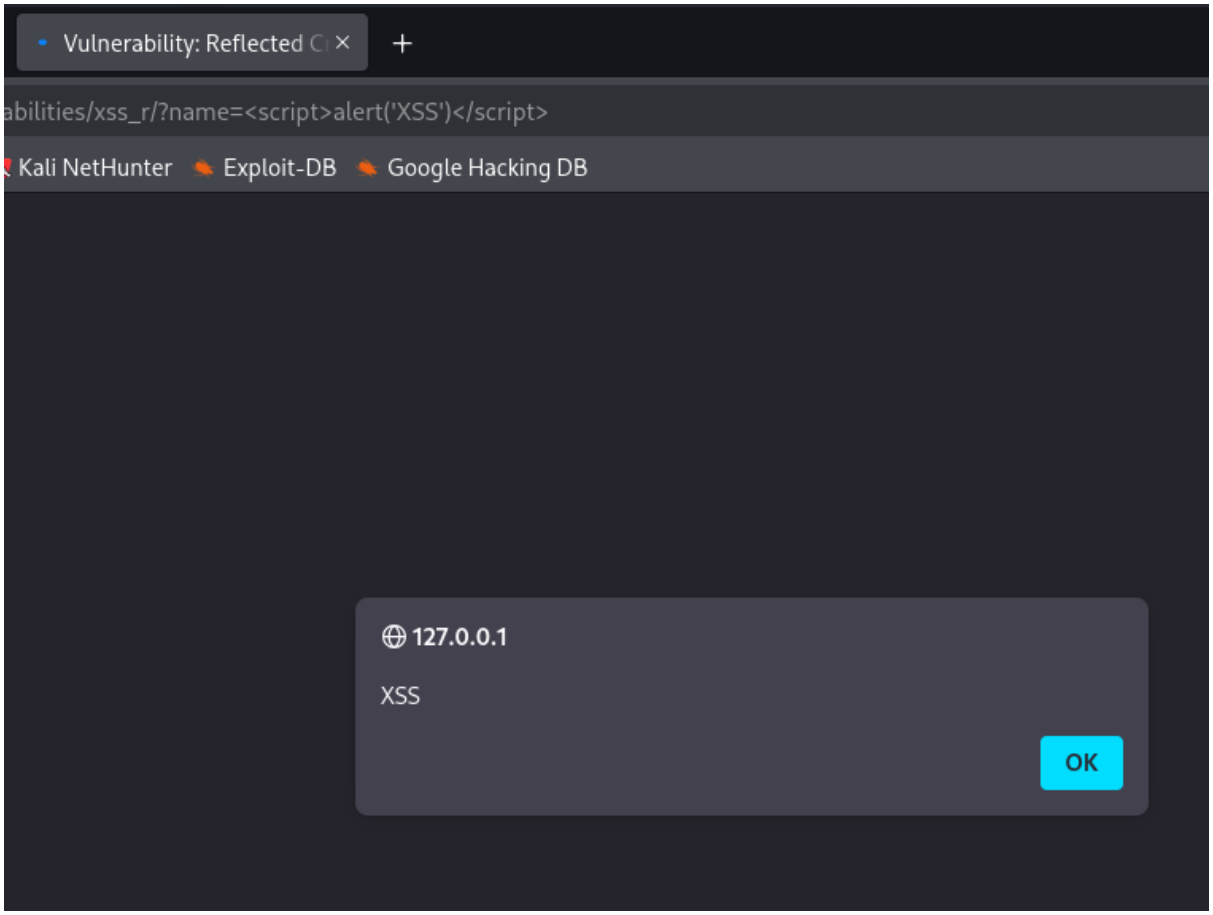


5. Manual Testing for SQLi
Configure the browser to use burp suite as proxy.
Login to ‘DVWA’ and navigate to ‘SQL injection’ page.
Enter a value like 1 and click Submit
In burp, capture this request and send it to the repeater
In Repeater, modify the id parameter: (remember to URL-encode parameter)
id=1' OR '1'='1



6. Manual Testing for XSS
Configure the browser to use burp suite as proxy.
Login to ‘DVWA’ and navigate to ‘XSS (reflected)’ page.
Enter a value and click Submit
In burp, capture this request and send it to the repeater
In Repeater, modify the name parameter: (remember to URL-encode parameter)
name=<script>alert('XSS')</script>





Log

Test ID	Vulnerability	Severity	Target URL
1	SQL Injection	Critical	http://127.0.0.1/DVWA/vulnerabilities/sqli/
2	XSS Reflected	Medium	http://127.0.0.1/DVWA/vulnerabilities/xss_r/