Detect SQL Injection Vulnerabilities using OWASP ZAP

ILABS
CEH PRACTICAL

@mmar

Aim

OWASP Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners and a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.

In this task, we will use OWASP ZAP to test a web application for SQL injection vulnerabilities. We will scan the www.moviescope.com website that is hosted on the Windows Server 2019 machine.

Other SQL Injection detection tools

✓ Acunetix Web Vulnerability Scanner (https://www.acunetix.com)
✓ Snort (https://snort.org)
✓ Burp Suite (https://www.portswigger.net)
✓ w3af (https://w3af.org)

DEMO

THANKS