OVERVIEW OF ZAP:

In this stage, we aimed to conduct an automated vulnerability scan to identify security weaknesses in DVWA (Damn Vulnerable Web Application). Initially, we planned to use Nessus, but due to setup issues, we switched to OWASP ZAP (Zed Attack Proxy), a widely used security tool for scanning web applications.

From our research on Nessus, we understood that it is primarily used for network vulnerability scanning, identifying misconfigurations, weak passwords, and outdated software versions. Unlike manual penetration testing, Nessus provides automated risk assessment, prioritizing vulnerabilities based on severity. However, OWASP ZAP is better suited for web application security testing, focusing on issues like injection attacks, session security, and authentication flaws.

Through OWASP ZAP scanning, we discovered multiple vulnerabilities in DVWA, categorized as High, Medium, and Low risk. The scanning process involved crawling the web application, intercepting HTTP requests, and analyzing responses for security weaknesses. The results from ZAP provided valuable insights into potential attack vectors and recommended mitigation strategies.