TECHNOLOGY STACK

Tools Explored

During the vulnerability assessment, the following tools were utilized:

Burp Suite:

- Used for intercepting and analyzing HTTP requests to detect vulnerabilities such as Insecure Direct Object Reference (IDOR) and Cross-Site Scripting (XSS).
- Helps in manual and automated penetration testing of web applications.

OWASP ZAP (Zed Attack Proxy):

- Assisted in automated vulnerability scanning for web application security testing.
- Identified issues like injection flaws, broken authentication, and security misconfigurations.

SQL map:

- Used to identify SQL Injection (SQLi) vulnerabilities by testing database query manipulation.
- Helps in detecting unauthorized access risks in database systems.

Nmap (Network Mapper):

- Conducted network scanning to identify open ports, services, and potential attack surfaces.
- Used for gathering information about live hosts and their security posture.

Postman:

- Used for API testing and security analysis.
- Helped validate API endpoints for misconfigurations and vulnerabilities.

Nikto:

- Performed web server vulnerability scanning to detect outdated software, misconfigurations, and insecure settings.
  - Helped assess server security against known exploits.