1.1 Technology Stack :

Technology Stack & Tools Explored for the Project :

1. Web Technologies :

- HTML, CSS, JavaScript – Used to analyse web application vulnerabilities like Cross-Site Scripting (XSS) and security misconfigurations.

- PHP & MySQL – Common backend stack in vulnerable applications like bWAPP, where SQL Injection (SQLi) vulnerabilities can be tested.

- Node.js & Express – Many modern web applications use Node.js, making it essential for testing API security and authentication flaws.

2. Penetration Testing Tools :

- Burp Suite – Used for intercepting HTTP requests, testing authentication flaws, SQL Injection, and Cross-Site Scripting (XSS).

- OWASP ZAP – Open-source web security scanner to detect vulnerabilities like broken authentication and security misconfiguration.

- SQLMap – Automated SQL injection tool to identify database vulnerabilities and test for data exfiltration risks.

- Nikto – Web server scanner to check for misconfigurations, outdated components, and common exploits.

- Hydra – A powerful tool for brute-force testing against login forms and network services.

3. Vulnerable Testing Environments :

- bWAPP (Buggy Web Application) – Intentionally vulnerable web app used to simulate real-world attacks like SQLi, XSS, IDOR, and authentication flaws.

- OWASP Juice Shop – A modern web app designed to practice testing OWASP Top 10 vulnerabilities in a legal environment.

- DVWA (Damn Vulnerable Web App) – Another platform used to test web security weaknesses in a controlled setting.

4. Network Security Tools :

- Nmap – A powerful network scanner used for port scanning, service detection, and finding open vulnerabilities.

- Metasploit Framework – Used for exploiting vulnerabilities, testing payload execution, and conducting penetration testing.

- Wireshark – A network traffic analyser used to monitor packet-level data, detecting MITM attacks and unsecured communications.

5. Secure Development & Defence Mechanisms :

- Content Security Policy (CSP) – Implemented to prevent Cross-Site Scripting (XSS) attacks.

- Web Application Firewalls (WAF) – Explored in security defence mechanisms to block SQLi, XSS, and DDoS attacks.

- Multi-Factor Authentication (MFA) – Implemented as a countermeasure to brute-force attacks and credential stuffing.

- Input Validation & Sanitization – Used to prevent injection attacks and IDOR vulnerabilities.