Week 1: Security Assessment Report

1. Application Setup

In the first week, I successfully set up a mock web-based application sourced from GitHub for cybersecurity testing purposes. The steps included:

- Installing all required dependencies
- Launching the server locally
- Accessing the application at http://localhost:5000
- Exploring critical components such as the Signup, Login, and Profile pages

This setup provided a controlled environment to evaluate and identify security weaknesses.

---

2. Vulnerability Assessment

Tools Utilized:

- **OWASP ZAP** – For automated scanning of web vulnerabilities
- **Browser Developer Tools** – For manual testing and code inspection
- **Input-Based Tests**, including:
    - Cross-Site Scripting (XSS) payloads
    - SQL Injection attempts

Vulnerabilities Discovered:

1. **Missing SameSite Attribute in Cookies**
    - Could enable Cross-Site Request Forgery (CSRF) attacks.
2. **Absence of Content Security Policy (CSP) Header**
    - Increases susceptibility to Cross-Site Scripting (XSS) and code injection.
3. **Missing X-Content-Type-Options Header**
    - Allows browsers to misinterpret MIME types, potentially opening paths for XSS.
4. **X-Frame-Options Header Not Configured**
    - Leaves the application open to clickjacking threats.

5. **Exposed Developer Comments in Code**
    - May unintentionally disclose sensitive logic or internal workings.
6. **Server Version Disclosure**
    - Revealing the server version makes the system easier to target using known exploits.

---

3. Key Areas for Improvement

- Implement the **SameSite** attribute in cookies to mitigate CSRF risks.
- Define a **Content Security Policy (CSP)** to prevent XSS and other code injection attacks.
- Add essential HTTP headers such as **X-Content-Type-Options** and **X-Frame-Options** to enhance browser security.
- Remove or obfuscate **developer comments** in the source code to avoid leaking sensitive details.
- Suppress **server version information** from HTTP response headers to reduce attack surface.