Week 1 – Security Assessment Report

Cybersecurity Internship – Strengthening Security Measures for a Web Application
Intern Name: Nabira Khan
Assessment Week: Week 1 – Security Assessment
Application Tested: https://github.com/Pranavk-official/user-management
Test Environment: Kali Linux
Application Running At: http://localhost:4000

1. Issues Found:

- Broken access control on `/admin` route (no authentication or role check)
- Application crashes on invalid input during login (missing validation)
- No anti-CSRF tokens used
- Missing Content Security Policy (CSP) header
- No anti-clickjacking headers (X-Frame-Options)
- Cookies lack SameSite attribute
- Server leaks information via "X-Powered-By" HTTP header
- Missing HTTP security headers (Strict-Transport-Security, X-Content-Type-Options)
- Suspicious comments in source code
- Weak or missing cache control headers

2. Suggested Fixes:

- Implement role-based access control for protected routes
- Add input validation and proper error handling on login
- Integrate CSRF protection middleware to secure forms
- Set a strict Content Security Policy header to control resource loading
- Add anti-clickjacking headers to prevent UI redress attacks
- Set `SameSite`, `Secure`, and `HttpOnly` attributes for cookies
- Remove or obfuscate server info from HTTP headers
- Configure HTTP headers to improve security posture
- Remove or sanitize development/debugging comments in production code
- Define proper cache control directives for sensitive data

3. Tools Used:

- OWASP ZAP
- Chrome Dev Tools
- Manual testing via browser

Nabira Khan