

|  |
| --- |
| OWASP JUICE\_SHOP |
|  |
| mUHAMMAD aDnan Ali  DHC-261  Cybersecurity Internship |

Week 1: Security Assessment – Document Findings

1. Vulnerabilities Found

1. Cross-Site Scripting (XSS) Vulnerability
   * The application did not sanitize user inputs on the signup and profile update pages.
   * Test <script>alert('XSS');</script> executed successfully, triggering a JavaScript alert.
   * This indicates that malicious scripts could be injected and executed in users’ browsers.
2. SQL Injection Vulnerability
   * Login form is vulnerable to SQL injection using payload:

' OR 1=1--

* + Successful login was achieved without valid credentials, indicating poor query handling and lack of parameterized queries.

1. Weak Password Storage
   * Upon inspecting the backend (via code review), passwords were stored in plain text in the database.
   * This is a major security risk if the database is compromised.
2. Security Misconfigurations
   * Debug mode was enabled in the application’s configuration, exposing detailed error messages.
   * No HTTPS configuration detected; data is transmitted in plain text.
   * Lack of HTTP security headers such as Content-Security-Policy and X-Frame-Options.

2. Areas of Improvement

1. Input Validation & Output Encoding
   * Implement server-side input validation for all user input fields.
   * Apply proper output encoding to prevent XSS attacks.
2. Use Parameterized Queries
   * Modify database queries to use prepared statements or ORM query builders to prevent SQL injection.
3. Secure Password Storage
   * Hash passwords using strong hashing algorithms like bcrypt or Argon2.
   * Store only the hashed version of the password, never in plain text.
4. Disable Debug Mode in Production
   * Turn off verbose error logging and stack trace display in production environments.
5. Enforce HTTPS
   * Configure SSL/TLS certificates to ensure secure communication.
6. Add Security Headers
   * Implement HTTP headers such as:
     + Content-Security-Policy
     + Strict-Transport-Security
     + X-Frame-Options
     + X-Content-Type-Options