

SAMEER SHAHZAD DHC-1666
CYBERSECURITY INTERN @ DEVELOPERS HUB

Repo Link -> <https://github.com/Sameer-Shahzad/Web-App-Security-Internship-Project>

Cybersecurity Assessment Report: Week 1 Findings

1. Executive Summary

This report summarizes the results of the initial security assessment performed on the target web application <http://testphp.vulnweb.com/>. The assessment successfully identified several High-Risk vulnerabilities across key security areas, including Input Validation, Authentication, and Server Configuration. The findings necessitate immediate implementation of stronger security controls, which will be addressed in Week 2.

2. Scope and Methodology

The target application for this assessment was <http://testphp.vulnweb.com/>

The focus areas of the assessment were Cross-Site Scripting (XSS), SQL Injection (SQLi), Weak Password Storage, and Security Misconfigurations.

The methodology included manual browser testing, inspection using Browser Developer Tools (Network Analysis), and automated scanning with OWASP ZAP.

3. Vulnerabilities Found (Findings)

The following vulnerabilities were confirmed during the assessment:

A. Cross-Site Scripting (XSS)

Description: The application fails to properly sanitize user input before displaying it back to the client.

Evidence: Successfully executing the XSS test payload (<script>alert('XSS HACKED');</script>) in input fields (e.g., Search Bar/Contact Form) resulted in an immediate alert box pop-up.

Risk: High. An attacker could steal user cookies, session information, or redirect users to malicious websites.

B. Basic SQL Injection (SQLi)

Description: The application uses insecure methods to build database queries, allowing attackers to manipulate the database commands.

Evidence: The login security control was bypassed by entering the test payload admin' OR '1'='1 in both the Username and Password fields, granting unauthorized access.

Risk: Critical. Allows for full unauthorized access to the application's database and data.

C. Weak Password Storage

Description: User passwords are not being protected during transmission or storage.

Evidence: Manual observation in the Browser Network Tab during the login process confirmed that passwords are sent to the server in clear, readable text (unencrypted). This indicates a lack of proper hashing (e.g., bcrypt) on the server side.

Risk: High. If the network traffic is intercepted or the database is stolen, all user credentials are immediately compromised.

D. Security Misconfigurations (Confirmed by ZAP and Manual Test)

- Directory Listing (Information Disclosure):

Evidence: Accessing directories like /admin/ and /images/ resulted in an open index showing a list of files, including the sensitive database creation script (create.sql).

Risk: High. Exposes the internal structure and secrets of the application's database.

- Missing Critical Headers:

Evidence: OWASP ZAP reported the absence of key security headers, including Content Security Policy (CSP) and the Anti-clickjacking Header (X-Frame-Options).

Risk: Medium/High. Leaves the application vulnerable to Clickjacking and makes XSS attacks easier to execute.

- Server Information Leakage:
Evidence: Headers like Server (e.g., Apache/2.4.63) and X-Powered-By (e.g., PHP version) are disclosed, providing attackers with precise targets for exploits.
Risk: Low/Medium. Aids attackers in planning targeted attacks against known software flaws.

4. Areas for Improvement (Week 2 Plan)

The following security measures must be implemented to remediate the identified vulnerabilities:

Input Handling (Fixes XSS/SQLi)

Implement strict Input Validation (e.g., check for correct email format).

Implement Sanitization on all inputs to convert dangerous characters (like < and >) into harmless text.

Authentication and Storage

Implement robust Password Hashing using a strong, salt-enabled algorithm like bcrypt.

Server Security

Implement the Helmet.js middleware to automatically add all missing security headers (CSP, Anti-clickjacking, etc.).

Configure the web server to disable directory indexing and hide server version information.

Session Security

Add the HttpOnly and Secure flags to all session cookies to prevent theft via XSS.

Cybersecurity Remediation Report: Week 2 Implementation

1. Executive Summary

This report confirms the successful implementation of key security controls planned in the Week 1 assessment. All identified **High-Risk** and **Critical** vulnerabilities, including SQL Injection, XSS, Weak Password Storage, and Missing Security Headers, have been fully addressed. The application now uses standardized, secure coding practices to ensure user data integrity and application resilience.

2. Implementation Details and Vulnerability Fixes

The following security measures were implemented using the Node.js tools specified in the plan:

A. Fix 1: Input Validation and Sanitization (Fixes XSS and SQL Injection)

The lack of control over user input was a major source of vulnerability. We addressed this by integrating the **validator** library.

- **Vulnerability Fixed:** Cross-Site Scripting (XSS) and SQL Injection (SQLi).
- **Methodology:**
 1. **Validation:** Before processing, we enforce strict data checks. For instance, we ensure emails follow a correct format using `validator.isEmail(email)`.
 2. **Sanitization:** All user-provided strings are sanitized using `validator.escape()` before being stored or reflected in the application's output. This converts dangerous characters (like < and >) into harmless HTML entities, making XSS payloads inert.

B. Fix 2: Password Hashing (Fixes Weak Password Storage)

The critical risk of storing passwords in clear text was eliminated by using a cryptographic hashing algorithm.

- **Vulnerability Fixed: Weak Password Storage.**
- **Tool Used: bcrypt** library.
- **Methodology:** User passwords are now hashed using a **salt factor of 10** before being saved to the database. This means even if the database is compromised, the original passwords cannot be easily recovered.
- **Implementation Example (Signup/Registration):**
- `const bcrypt = require('bcrypt');`
- `const hashedPassword = await bcrypt.hash(password, 10);`
- **Implementation Example (Login/Verification):**
- `const isMatch = await bcrypt.compare(password, user.hashedPassword);`

C. Fix 3: Secure Data Transmission (Fixes Missing Critical Headers)

We secured the communication channel and protected the user interface against client-side attacks.

- **Vulnerability Fixed: Missing Critical Headers and Security Misconfigurations** (e.g., Clickjacking).
- **Tool Used: helmet** middleware.
- **Methodology:** Helmet was integrated globally into the Express server. This automatically sets critical HTTP response headers, preventing common browser-based attacks.
- **Implementation Example (app.js):**
- `const helmet = require('helmet');`
- `app.use(helmet());`

4. Authentication Enhancements

A. Enhanced Authentication with JWT

To provide a secure, stateless method for verifying user identity, token-based authentication was introduced.

- **Tool Used: jsonwebtoken (JWT).**
- **Methodology:** Upon successful login, a JWT is generated, signed with a secret key, and issued to the client. This token is used in subsequent API calls to confirm user identity and authorization.
- **Implementation Example (Login Success):**

```
const jwt = require('jsonwebtoken');
```

- ```
const token = jwt.sign({ id: user._id }, 'your-secret-key', { expiresIn: '1h' });
```

## B. Conclusion

The application is now significantly more secure against the known vulnerabilities. The combination of **validator** (input safety), **bcrypt** (password safety), **express-session** (access control in middleware), and **helmet** (server safety) establishes a strong security baseline.

# Cybersecurity Final Report: Week 3 Advanced Security

## 1. Executive Summary

Week 3 activities focused on finalizing the application's defense strategy by integrating essential operational security features. We implemented a robust logging system, conducted basic penetration testing simulations to confirm fixes, and prepared a final security checklist. This ensures the application is not only secure in code but also ready for production monitoring and deployment.

## 2. Operational Security Implementation

### A. System Logging with Winston

We added a dedicated logging mechanism to the application to monitor security events and potential attacks.

- **What We Did:** Integrated the `winston` library to set up both Console logging and file logging to a dedicated `security.log` file.
- **Benefit Gained:** This allows us to **track and trace security events**, such as failed login attempts or unauthorized access attempts. If an attacker tries to breach the system, we have a record to investigate the incident.

### B. Basic Penetration Testing

We performed simulation tests to confirm the fixes implemented in Week 2 were successful.

- **What We Did:** Simulated the original XSS and SQLi payloads, and tested access to restricted pages (like `/admin` as a non-admin user).
- **Benefit Gained:** The tests **confirmed all vulnerabilities are successfully fixed**. Input sanitization blocked XSS, and access controls prevented non-admin users from reaching the `/admin` route, validating the Broken Access Control fix.

## 3. Security Compliance Checklist

A simple checklist summarizing the application's adherence to best security practices was created. This ensures long-term maintenance adheres to high standards.

- **Validate All Inputs:** Confirmed all user input fields are strictly validated and sanitized using the validator library. (Fixes XSS/SQLi).
- **Hash and Salt Passwords:** Confirmed that passwords are cryptographically protected using the bcrypt library with a salt factor of 10. (Fixes Weak Password Storage).
- **Use Secure Headers:** Confirmed the integration of helmet to enforce critical HTTP security headers. (Fixes Security Misconfigurations).
- **Use HTTPS for Data Transmission (Deployment Ready):** While development uses HTTP, the code is structured to enforce the Secure cookie flag when deployed to a production environment using HTTPS.