Vulnerability Assessment Report

1. Executive Summary

This vulnerability assessment was conducted on a publicly accessible web application used for learning and testing purposes. The objective of the assessment was to identify common security misconfigurations and potential risks using ethical, non-intrusive techniques.

The assessment focused on basic network exposure, secure communication practices, HTTP security headers, and cookie security configurations. No active exploitation or intrusive testing was performed during this assessment.

The findings indicate that while secure communication using HTTPS is enabled and cookie security controls are properly implemented, certain areas such as unencrypted HTTP access and missing security headers could be improved to strengthen the overall security posture.

2. Scope of Assessment

In Scope:

- Basic network port exposure analysis
- HTTP and HTTPS accessibility
- Security header inspection
- Cookie security flag review

Out of Scope:

- Exploitation or penetration testing
- Authentication bypass attempts
- Brute force or denial-of-service testing
- Any activity that could disrupt the target system

3. Methodology

The assessment was carried out using passive and ethical security analysis techniques. Reference-based Nmap scan outputs were used to understand exposed network ports due to local system constraints. Browser Developer Tools were used to inspect HTTP headers and cookie configurations.

No automated attacks or aggressive scanning techniques were used during this assessment.

4. Tools Used

- **Nmap (Reference-based scan)** – Network port analysis
- **Browser Developer Tools (Chrome)** – Header and cookie inspection

- **Manual Browser Testing** – HTTP to HTTPS behavior observation

5. Findings & Risk Analysis

🔹 Finding 1: Open HTTP Port (Port 80)

Risk Level: Low

Description:
The application is accessible over HTTP (port 80), which allows unencrypted communication between the client and the server.

Impact:
If sensitive data is transmitted over HTTP, it may be exposed to interception through man-in-the-middle attacks, particularly on unsecured networks.

Recommendation:
Redirect all HTTP traffic to HTTPS and disable unencrypted access where possible.

🔹 Finding 2: Secure HTTPS Port Enabled (Port 443)

Risk Level: Informational

Description:
The application supports HTTPS (port 443), enabling encrypted communication between users and the server.

Impact:
Encrypted communication helps protect sensitive information and enhances user trust.

Recommendation:
Continue enforcing HTTPS across the application.

🔹 Finding 3: Missing HTTP Security Headers

Risk Level: Medium

Description:
Several common HTTP security headers were not observed during inspection, including headers that help protect against clickjacking and content injection attacks.

Impact:
Missing security headers may increase the risk of client-side attacks such as cross-site scripting (XSS) and clickjacking.

Recommendation:
Implement standard HTTP security headers such as:

- Content-Security-Policy
- X-Frame-Options
- X-Content-Type-Options
- Strict-Transport-Security

🔹 Finding 4: Cookie Security Flags Properly Configured

Risk Level: Informational

Description:
Cookies observed during authenticated browsing were configured with Secure and HttpOnly flags.

Impact:
These flags help protect session data from interception and client-side script access.

Recommendation:
Maintain Secure and HttpOnly flags on all session-related cookies.

6. Overall Risk Summary

Category	Observation
Network Ports	HTTP and HTTPS open
Encrypted Communication	Enabled
HTTP Security Headers	Partially missing
Cookie Security	Properly configured

7. Conclusion

The vulnerability assessment identified minor configuration-related risks rather than critical security flaws. The presence of HTTPS and secure cookie attributes indicates a good baseline security posture. However, improvements such as enforcing HTTPS redirection and implementing missing security headers would further enhance security.

This assessment demonstrates the importance of proactive configuration reviews as part of a comprehensive cybersecurity strategy.