VULNERABILITY ASSESSMENT REPORT

Cyber Security Internship – Future Interns (2026)

Target Application: http://testphp.vulnweb.com/
Prepared By: Rohith Rachapudi
Assessment Type: Passive, Read-Only Security Assessment

1. Executive Summary

A structured vulnerability assessment was conducted to evaluate publicly exposed services, HTTP security configuration, and session management controls of the target web application. Testing was limited strictly to passive, non-intrusive techniques.

The assessment identified configuration-level weaknesses that significantly increase exposure to browser-based attacks and session compromise risks.

Category	Assessment Result
Open Services	1 (HTTP – nginx 1.19.0)
Critical Security Headers	Not Implemented
Session Cookie Protection	Weak Configuration
HTTPS Enforcement	Not Enabled
Overall Risk Rating	HIGH

2. Technical Findings

2.1 Public Service Exposure (Low Risk)

Port 80 (HTTP) was identified as open and running nginx version 1.19.0. Public service exposure is expected for web applications; however, service version disclosure may assist adversaries during reconnaissance and vulnerability mapping activities.

Recommendation: Maintain updated server versions, restrict unnecessary banner disclosure, and consider deployment of a Web Application Firewall (WAF).

2.2 Missing Security Headers (High Risk)

The application does not implement several critical HTTP security headers, including Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, and Permissions-Policy. Additionally, HTTPS is not enforced.

Impact: Increased exposure to Cross-Site Scripting (XSS), Clickjacking, MIME-type sniffing, browser feature abuse, and Man-in-the-Middle attacks.

Recommendation: Enforce HTTPS across the application and implement all critical security headers with secure configuration policies.

2.3 Insecure Session Cookie Configuration (High Risk)

The 'login' cookie was identified without Secure, HttpOnly, and SameSite attributes. Improper session cookie configuration increases the likelihood of session hijacking, XSS-based cookie theft, and interception over unencrypted channels.

Recommendation: Enforce HTTPS, enable Secure and HttpOnly flags, configure SameSite attribute appropriately, and implement secure session management policies.

3. Final Security Assessment

Overall Security Posture: HIGH RISK.

Although only a single public HTTP service is exposed, the absence of essential browser security controls and improper session configuration significantly increase the application's attack surface.

Immediate remediation is strongly recommended to enhance defensive posture, protect user sessions, and align with modern web security best practices.