VULNERABILITY ASSESSMENT REPORT

WEBSITE SECURITY REVIEW

http://testphp.vulnweb.com

Future Interns – Cyber Security Internship

Prepared By:
Mohammed Naseeh Syed

February 2026

EXECUTIVE SUMMARY

This report presents the results of a passive vulnerability assessment conducted on the publicly accessible website:
http://testphp.vulnweb.com
The objective of this assessment was to evaluate the website's security posture through non-intrusive configuration analysis, header inspection, and service enumeration.
The assessment identified multiple security weaknesses, primarily related to:

- Lack of HTTPS encryption
- Missing security headers
- Exposure of server and application version information

These issues increase the website's exposure to common web-based threats such as data interception, clickjacking, and information disclosure.
This engagement was conducted strictly within ethical boundaries. No exploitation, brute-force attacks, or active attack techniques were performed.

SCOPE OF ASSESSMENT

Scope Limitations

The assessment was limited to:

- Public-facing pages only
- Read-only inspection
- No authentication testing
- No account creation testing
- No exploitation of vulnerabilities
- No denial-of-service testing

Out of Scope

- Database exploitation
- Source code access
- Administrative access
- Active attack simulations

This ensures compliance with ethical testing standards.

METHODOLOGY

The assessment followed a structured passive security review approach.

1. Service Enumeration
Tool Used: Nmap 7.98
Purpose: Identify exposed services and open ports.

2. Security Header Analysis
Tool Used: SecurityHeaders.com
Purpose: Identify missing or misconfigured HTTP security headers.

3. Passive Configuration Review
Tool Used: OWASP ZAP (Passive Mode)
Purpose: Inspect response headers and identify configuration weaknesses.

4. Browser Inspection
Tool Used: Chrome DevTools
Purpose: Verify encryption status and certificate configuration.
All tools were used in non-intrusive, passive mode.

RISK SUMMARY

ID	Finding	Risk Level
1	Website served over HTTP (No HTTPS)	High
2	Missing Content-Security-Policy	Medium
3	Missing X-Frame-Options	Medium
4	Server Version Disclosure (nginx 1.19.0)	Medium
5	X-Powered-By Header Disclosure (PHP version)	Medium
6	Missing X-Content-Type-Options	Low
7	Missing Referrer-Policy	Low

Risk levels were determined based on:

- Potential impact
- Likelihood of exploitation
- Industry best practices (OWASP guidelines)

FINDING 1: NO HTTPS ENCRYPTION (HIGH RISK)

Description
The website is served over HTTP and does not enforce HTTPS encryption.
Port 80 was identified as open, and no automatic redirection to HTTPS was observed
.

Evidence

- Nmap scan identified port 80 open.
- Browser displayed "Not Secure" in the address bar.
- SecurityHeaders scan confirmed HTTP usage.

Impact
Without HTTPS:

- Data transmitted between users and the server is unencrypted.
- Sensitive information may be intercepted by attackers.
- The website is vulnerable to Man-in-the-Middle (MITM) attacks.

Recommendation

- Implement SSL/TLS certificate.
- Redirect all HTTP traffic to HTTPS.
- Enable HTTP Strict Transport Security (HSTS).
- Disable insecure protocols.

MEDIUM RISK FINDINGS

Finding 2: Missing Content-Security-Policy

Description

The Content-Security-Policy (CSP) header is not implemented.

Impact

Without CSP, the website is more vulnerable to:

- Cross-Site Scripting (XSS)
- Malicious script injection

Recommendation

Implement a restrictive CSP header that allows only trusted domains.

Finding 3: Missing X-Frame-Options

Description

The X-Frame-Options header is not set.

Impact

The website may be vulnerable to clickjacking attacks.

Recommendation

Set:

X-Frame-Options: SAMEORIGIN

Finding 4: Server Version Disclosure

Description

Nmap and response headers revealed:

Server: nginx/1.19.0

Impact

Attackers can identify known vulnerabilities associated with this version.

Recommendation

- Disable server version exposure
- Configure server_tokens off in nginx

Finding 5: X-Powered-By Header Disclosure

Description

The server exposes:

X-Powered-By: PHP/5.6.40

Impact

This reveals backend technology and version information.

Recommendation

Remove or suppress the X-Powered-By header.

LOW RISK FINDINGS

Missing X-Content-Type-Options

Impact

Allows browsers to perform MIME sniffing, which can increase attack surface.

Recommendation

Set:

X-Content-Type-Options: nosniff

Missing Referrer-Policy

Impact

Sensitive URL information may be leaked to third-party websites.

Recommendation

Set:

Referrer-Policy: strict-origin-when-cross-origin

REMEDIATION ROADMAP

Priority 1 (Immediate)

- Implement HTTPS
- Configure HSTS

Priority 2 (Short-Term)

- Add missing security headers
- Remove version disclosure

Priority 3 (Ongoing)

- Regular patch management
- Periodic vulnerability assessments
- Security header monitoring

CONCLUSION

The assessment identified several configuration weaknesses that increase the website's exposure to common web threats.

The most critical issue is the absence of HTTPS encryption, which significantly impacts confidentiality and data integrity.

By implementing the recommended remediation steps, the website's overall security posture can be substantially improved.

This assessment was conducted strictly within passive and ethical boundaries in alignment with industry best practices.