Vulnerability Assessment Report

- Website URL: testphp.vulnweb.com
- Task: Cyber Security Task 1
- Name: Jerry Ofugbudie
- Date: February 6, 2026
- Future Interns

Executive Summary

This report presents the results of a read-only vulnerability assessment conducted on a publicly accessible website. The assessment focused on identifying common security misconfigurations and visible weaknesses without performing any exploitation. The goal is to provide clear, business-friendly insights and practical remediation recommendations.

Scope & Methodology

- Public-facing pages only
- Passive analysis and observation
- No authentication or exploitation
- Tools used:
    - Browser Developer Tools
    - OWASP ZAP (Passive Scan)
    - Nmap (Basic exposure analysis)

Findings

Finding 1: Missing Security Headers

Risk Level: Medium

Description:
The website does not implement several recommended HTTP security headers. These headers help protect users from common web-based attacks.

Why This Matters:
Without security headers, the website may be more vulnerable to threats such as clickjacking, cross-site scripting, and content injection.

Recommendation:
Configure standard HTTP security headers such as Content Security Policy (CSP), X-Frame-Options, and X-Content-Type-Options on the web server.

Findings

Finding 2: Information Disclosure via HTTP Headers

Risk Level: Low

Description:
Server response headers reveal information about the underlying technology and server configuration.

Why This Matters:
Exposing server details can provide useful information to attackers and make targeted attacks easier.

Recommendation:
Remove or mask unnecessary server information from HTTP response headers.

Findings

Finding 3: Insecure Cookie Attributes

Risk Level: Medium

Description:
Some cookies set by the website do not use secure attributes such as Secure and HttpOnly.

Why This Matters:
Cookies without proper security flags may be accessed through client-side scripts or transmitted over unencrypted connections.

Recommendation:
Configure cookies to include Secure and HttpOnly flags where applicable.

Findings

Finding 4: Unencrypted HTTP Traffic (Port 80 Open)

Risk Level: Low

Description:
The website allows access over unencrypted HTTP connections.

Why This Matters:
Unencrypted traffic can be intercepted, potentially exposing sensitive user data.

Recommendation:
Redirect all HTTP traffic to HTTPS and enforce secure communication.

Findings

Finding 5: General Security Misconfigurations

Risk Level: Low

Description:
The passive scan identified general security misconfigurations that do not pose an immediate threat but could weaken the site’s overall security posture.

Why This Matters:
Small misconfigurations can accumulate and increase long-term risk.

Recommendation:
Conduct periodic security reviews and apply recommended security best practices.

Conclusion

The assessment identified several low to medium risk security misconfigurations. While no critical vulnerabilities were observed, implementing the recommended security controls will significantly improve the website's overall security posture and reduce potential exposure to common web-based threats.