VULNERABILITY ASSESSMENT REPORT

Target: Acunetix Test Website
URL: http://testphp.vulnweb.com

AUTHOR: OLADIMEJI PRECIOUS EMMANUEL

01/17/2026

EXECUTIVE SUMMARY

This assessment reviewed the Acunetix Test Website to identify security weaknesses. The review used browser inspection and network scanning. Three issues were found. Fixing them reduces exposure to common web attacks.

Scope

- Target website only

Tools

- Browser DevTools
- Nmap
- Canva

SCOPE AND TOOLS

FINDINGS TABLE

Finding 1

Name: Missing Security Headers
Risk: Medium
Description: The website lacks key browser security headers. This allows script abuse and clickjacking.
Evidence: Screenshot of response headers.
Fix: Add standard security headers at server level.

Finding 2

Name: Outdated PHP Version
Risk: High
Description: The server runs PHP 5.6, which no longer receives security updates.
Evidence: X-Powered-By header showing PHP version.
Fix: Upgrade PHP to a supported version.

Finding 3

Name: Open HTTP Port
Risk: Medium
Description: Port 80 allows unencrypted traffic.
Evidence: Nmap scan result.
Fix: Enforce HTTPS and redirect HTTP.

CONCLUSION

Applying these fixes improves security and lowers attack risk.