VULNERABILITY ASSESSMENT REPORT

- **TARGET : TESTPHP.VULNWEB.COM**
- **PREPARED BY : MOHAMMAD AMAAN TANVEER SHAIKH**
- **DATE : JANUARY 2026**
- **CLASSIFICATION : CONFIDENTIAL**

Executive Summary

A security assessment was performed on testphp.vulnweb.com using a read-only, passive methodology. The audit identified several security gaps ranging from High to Low risk. While the website is functional, it lacks modern security "armor" (headers) and is running on an outdated server version. These issues could allow attackers to steal user data or hijack user sessions. Immediate remediation is recommended to align with industry security standards.

Scope & Methodology

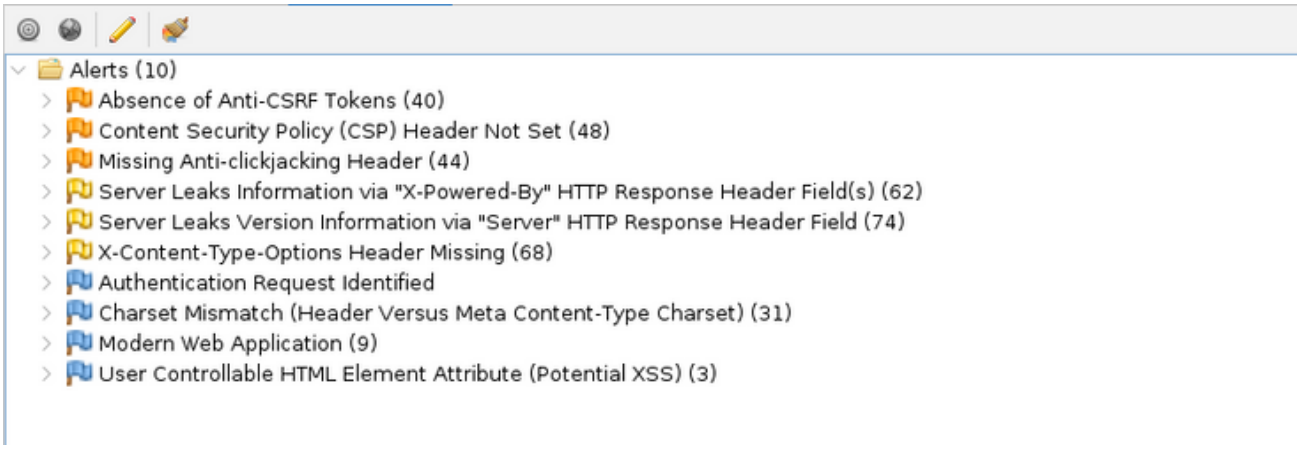
- **Scope:** Public-facing pages of http://testphp.vulnweb.com/.
- **Methodology:** Read-only passive analysis (no exploitation).

Tools Used:

- **Nmap:** Network service and version detection.
- **Browser DevTools:** Manual header and configuration audit.
- **OWASP ZAP:** Passive vulnerability scanning.

Summary of Findings

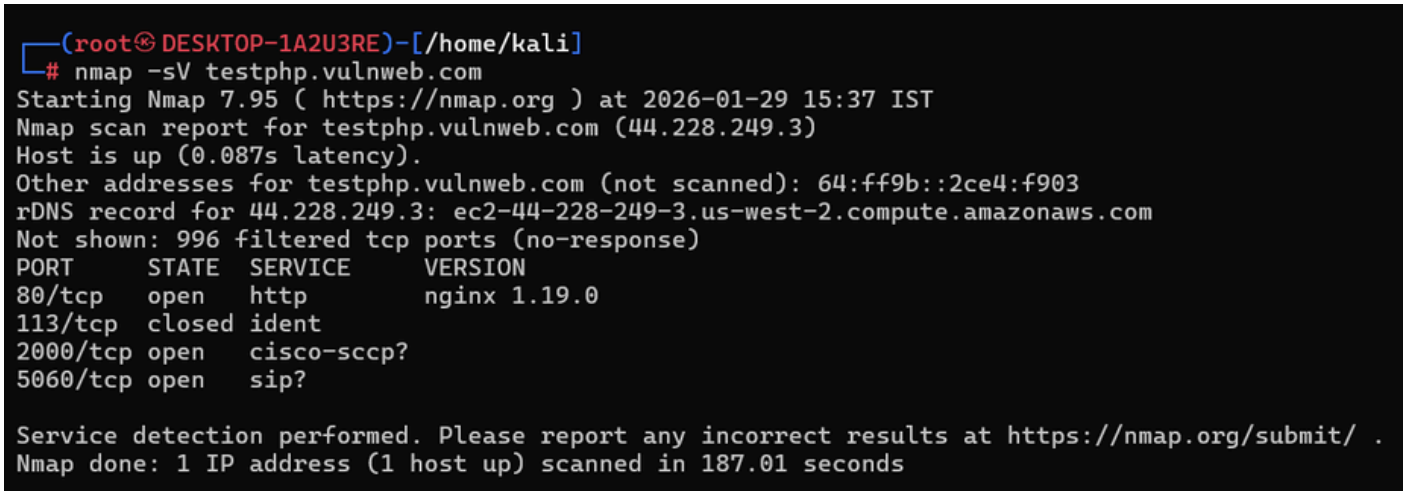
Vulnerability	Risk Level	Tool Used
Outdated Web Server (Nginx 1.19.0)	**High**	Nmap
Missing Content Security Policy (CSP)	**High**	OWASP ZAP / DevTools
Absence of Anti-CSRF Tokens	**Medium**	OWASP ZAP
Missing Anti-Clickjacking Headers	**Medium**	OWASP ZAP / DevTools
Unnecessary Open Ports (2000, 5060)	**Low**	Nmap



Detailed Findings & Remediation

Outdated Web Server (Nginx 1.19.0)

- Issue: The server is running Nginx version 1.19.0, which has multiple known security vulnerabilities (CVEs).
- Impact: Attackers can exploit documented bugs to cause system crashes (DoS) or gain unauthorized access.
- Remediation: Update Nginx to the latest stable version (e.g., 1.25+).
- Code Fix (Linux): ```bash sudo apt update && sudo apt upgrade nginx



Missing Content Security Policy (CSP)

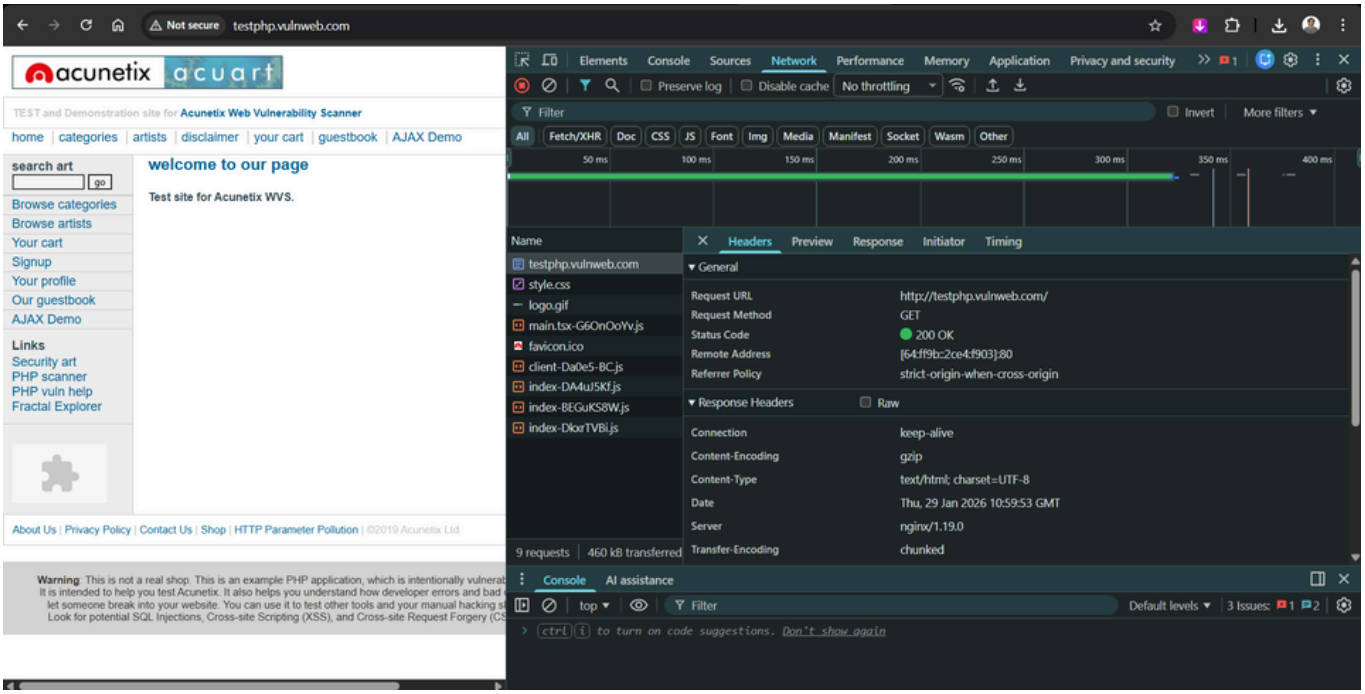
- Issue: The Content-Security-Policy header is not defined.
- Impact: This allows "Cross-Site Scripting" (XSS), where a hacker can inject a malicious script into the page to steal user passwords.
- Remediation: Add a CSP header to the Nginx configuration.
- Code Fix (Nginx Config): ```nginx add_header Content-Security-Policy "default-src 'self'; script-src 'self'; style-src 'self';";

Absence of Anti-CSRF Tokens

- Issue: Forms on the website do not use unique security tokens.
- Impact: An attacker could trick a logged-in user into submitting a form (like a password change) without their knowledge.
- Remediation: Implement a "Synchronizer Token Pattern" where every form includes a hidden, unique token.

Missing Anti-Clickjacking Header

- Issue: The X-Frame-Options header is missing.
- Impact: Attackers can "overlay" this website onto a malicious one, tricking users into clicking buttons they can't see.
- Remediation: Configure the server to block the site from being put in a frame.
- Code Fix (Nginx Config): ```nginx add_header X-Frame-Options "SAMEORIGIN";



Conclusion & Roadmap

The security posture of the audited site requires improvement.

To protect user data and maintain service availability, the following steps should be taken in order:

1. **Immediate:** Update Nginx software and add security headers.
2. **Short-term:** Update application code to include Anti-CSRF tokens.
3. **Ongoing:** Conduct monthly passive scans to detect new configuration drifts.