

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 While the website is functional, it lacks modern security "armor" (headers) and is running on an outdated server version.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Outdated Web Server (Nginx 1.19.0)	High	Nmap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

The screenshot shows the OWASP ZAP interface with a sidebar containing icons for Home, Scan, Tools, and Help. A dropdown menu is open under 'Tools' with options: Alerts (10), Network, Session, and Script. The main pane displays a hierarchical list of alerts:

- Alerts (10)
 - > Absence of Anti-CSRF Tokens (40)
 - > Content Security Policy (CSP) Header Not Set (48)
 - > Missing Anti-clickjacking Header (44)
 - > Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (62)
 - > Server Leaks Version Information via "Server" HTTP Response Header Field (74)
 - > X-Content-Type-Options Header Missing (68)
 - > Authentication Request Identified
 - > Charset Mismatch (Header Versus Meta Content-Type Charset) (31)
 - > Modern Web Application (9)
 - > User Controllable HTML Element Attribute (Potential XSS) (3)

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Outdated Web Server (Nginx 1.19.0)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

```
(root㉿DESKTOP-1A2U3RE)-[/home/kali]
└─# nmap -sV testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-29 15:37 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.087s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE     SERVICE      VERSION
80/tcp    open      http        nginx 1.19.0
113/tcp   closed    ident
2000/tcp  open      cisco-sccp?
5060/tcp  open      sip?

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 187.01 seconds
```

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";

The screenshot shows a browser window with the URL `testphp.vulnweb.com`. The page content is a simple test site for Acunetix Web Vulnerability Scanner, featuring a sidebar with links like 'search art', 'Browse categories', and 'Links'. The main content area says 'welcome to our page' and 'Test site for Acunetix WVS.'.

In the browser's developer tools, the Network tab is open. A request to `testphp.vulnweb.com` is selected. The Headers section of the Network tab shows the following response headers:

Name	Value
Request URL	<code>http://testphp.vulnweb.com/</code>
Request Method	GET
Status Code	200 OK
Remote Address	[64:ff9bc2c4:f903]:80
Referrer Policy	strict-origin-when-cross-origin
Connection	keep-alive
Content-Encoding	gzip
Content-Type	text/html; charset=UTF-8
Date	Thu, 29 Jan 2026 10:59:53 GMT
Server	nginx/1.19.0
Transfer-Encoding	chunked

A warning message at the bottom of the browser window states: "Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad practices let someone break into your website. You can use it to test other tools and your manual hacking skills. Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF) vulnerabilities."

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.