

# Vulnerability Assessment Report: testphp.vulnweb.com

## SECURITY SCORE: 40/100

OVERALL RISK LEVEL: CRITICAL

### 1. Network Scan Results (Nmap)

Port	Service	Version	State
80	http	1.19.0	open

### 2. Web Vulnerability Results (Nikto)

```
- Nikto v2.1.5
-----
+ Target IP: 44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2026-02-22 13:33:11 (GMT0)
-----
+ Server: nginx/1.19.0
+ Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
+ The anti-clickjacking X-Frame-Options header is not present.
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml, fields:
0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See
http://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
+ /crossdomain.xml contains a full wildcard entry. See
http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ /crossdomain.xml contains 0 line which should be manually viewed for improper domains
or wildcards.
+ 26 items checked: 4 error(s) and 7 item(s) reported on remote host
+ End Time: 2026-02-22 13:33:48 (GMT0) (37 seconds)
-----
+ 1 host(s) tested

[nikto stderr]
+ ERROR: Host maximum execution time of 180 seconds reached
```

### 3. Crawled Website Endpoints

- http://testphp.vulnweb.com/categories.php
- http://testphp.vulnweb.com/Mod\_Rewrite\_Shop/
- http://testphp.vulnweb.com/guestbook.php
- http://testphp.vulnweb.com/index.php
- http://testphp.vulnweb.com/AJAX/index.php
- http://testphp.vulnweb.com/userinfo.php
- http://testphp.vulnweb.com/privacy.php
- http://testphp.vulnweb.com/hpp/

- <http://testphp.vulnweb.com/cart.php>
- <http://testphp.vulnweb.com/disclaimer.php>
- <http://testphp.vulnweb.com/artists.php>
- [FORM] <http://testphp.vulnweb.com/search.php?test=query>
- <http://testphp.vulnweb.com/login.php>

## 4. Vulnerability Intelligence (CVE Mapping)

### Legacy Vulnerability Intelligence

- ■■ NOTICE: Engine identified 5 additional legacy vulnerabilities (pre-2016).

## 5. Attack Possibilities & Mitigation

**Attack:** Clickjacking Vulnerability

**Mitigation:** Implement X-Frame-Options: SAMEORIGIN or DENY in your web server configuration.

**Attack:** Cross-Site Scripting (XSS) / Data Injection

**Mitigation:** Implement a strict Content-Security-Policy (CSP) to restrict untrusted script execution.

**Attack:** Cross-Site Request Forgery (CSRF) / Data Theft

**Mitigation:** Replace full wildcard '\*' entries in crossdomain.xml or clientaccesspolicy.xml with specific, trusted domain origins.

**Attack:** Remote Code Execution (RCE) / Known Exploit Utilization

**Mitigation:** Upgrade to a supported version of PHP (8.2+). Legacy versions do not receive security patches.