

Vulnerability Assessment Report: testphp.vulnweb.com

SECURITY SCORE: 94/100

OVERALL RISK LEVEL: LOW

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 16:03:53 (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.
+ /: Potential PHP MySQL database connection string found.
+ 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.
+ /index.php: Potential PHP MySQL database connection string found.
+ 26 items checked: 4 error(s) and 9 item(s) reported on remote host
+ End Time: 2026-02-22 16:04:32 (GMT0) (39 seconds)
-----
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 84600 seconds reached
```

3. Crawled Website Endpoints

- http://testphp.vulnweb.com/cart.php
- [FORM] http://testphp.vulnweb.com/search.php?test=query
- http://testphp.vulnweb.com/guestbook.php
- http://testphp.vulnweb.com/hpp/
- http://testphp.vulnweb.com/privacy.php
- http://testphp.vulnweb.com/index.php

- http://testphp.vulnweb.com/Mod_Rewrite_Shop/
- <http://testphp.vulnweb.com/login.php>
- <http://testphp.vulnweb.com/AJAX/index.php>
- <http://testphp.vulnweb.com/categories.php>
- <http://testphp.vulnweb.com/disclaimer.php>
- <http://testphp.vulnweb.com/userinfo.php>
- <http://testphp.vulnweb.com/artists.php>

4. Vulnerability Intelligence (CVE Mapping)

Note: Duplicate findings are consolidated for scoring.

Legacy Vulnerability Intelligence

- ■■ NOTICE: Our engine identified 5 additional legacy vulnerabilities (pre-2016) associated with these services. These have been filtered to prioritize current threats.

5. Attack Possibilities & Mitigation

[LOW] Attack: Clickjacking / Cross-Site Scripting (XSS)

Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.

[LOW] Attack: Cross-Site Request Forgery (CSRF) / Data Theft

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

[LOW] Attack: Full Database Compromise / SQL Injection

Mitigation: Immediately remove hardcoded connection strings from public-facing directories and use environment variables.