

Vulnerability Assessment Report:

testphp.vulnweb.com

SECURITY SCORE: 91/100

OVERALL RISK LEVEL: LOW

**Score capped at 97 due to professional residual uncertainty (Black-box surface scan limitation).*

1. Network Scan Results (Nmap)

Port	Service	Version	Evidence
80	http	1.19.0	http-title: Home of Acunetix Art...

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: 2026-02-24 14:58:27 (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: 2026-02-24 14:59:04 (GMT0) (37 seconds)
-----
+ 1 host(s) tested

[stderr]
+ ERROR: Host maximum execution time of 600 seconds reached
```

3. Crawled & Fuzzed Endpoints

- http://testphp.vulnweb.com/privacy.php
- http://testphp.vulnweb.com/AJAX/index.php
- http://testphp.vulnweb.com/cart.php
- http://testphp.vulnweb.com
- http://testphp.vulnweb.com/userinfo.php
- http://testphp.vulnweb.com/index.php
- mailto:wvs@acunetix.com

- <http://testphp.vulnweb.com/hpp/>
- <http://testphp.vulnweb.com/categories.php>
- <http://testphp.vulnweb.com/guestbook.php>
- <http://testphp.vulnweb.com/artists.php>
- <http://testphp.vulnweb.com/style.css>
- <http://testphp.vulnweb.com/login.php>
- <http://testphp.vulnweb.com/disclaimer.php>
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/

4. Vulnerability Intelligence (CVE Mapping)

No relevant CVEs identified.

5. Attack Possibilities & Mitigation

[LOW] Attack: Missing Anti-Clickjacking Protection

Mitigation: Implement DENY or SAMEORIGIN X-Frame-Options.

[NOTE] Attack: Missing Content-Security-Policy (CSP)

Mitigation: Implement a strict CSP header.