Vulnerability Assessment Report: testphp.vulnweb.com

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: 2026-01-31 06:09:12 (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: 2026-01-31 06:09:48 (GMT0) (36 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

3. Crawled Website Endpoints

- http://testphp.vulnweb.com/hpp/
- http://testphp.vulnweb.com/login.php
- http://testphp.vulnweb.com/privacy.php
- http://testphp.vulnweb.com/categories.php
- http://testphp.vulnweb.com/guestbook.php
- http://testphp.vulnweb.com/disclaimer.php
- [FORM] http://testphp.vulnweb.com/search.php?test=query
- http://testphp.vulnweb.com/Mod_Rewrite_Shop/
- http://testphp.vulnweb.com/cart.php
- http://testphp.vulnweb.com/index.php
- http://testphp.vulnweb.com/userinfo.php
- http://testphp.vulnweb.com/AJAX/index.php
- http://testphp.vulnweb.com/artists.php

4. Vulnerabilities Detected

- Missing Security Headers

5. Vulnerability Intelligence (CVE Mapping)

Vulnerabilities in nginx 1.19.0
- [HIGH 7.5] CVE-2009-2629: Buffer underflow in src/http/ngx_http_parse.c in nginx 0.1.0 through 0.5.37, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.15 allows ...
- [MEDIUM 5.0] CVE-2009-3896: src/http/ngx_http_parse.c in nginx (aka Engine X) 0.1.0 through 0.4.14, 0.5.x before 0.5.38, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x befor...
- [MEDIUM 4.9] CVE-2009-3898: Directory traversal vulnerability in src/http/modules/ngx_http_dav_module.c in nginx (aka Engine X) before 0.7.63, and 0.8.x before 0.8.17, allows rem...
- [MEDIUM 6.8] CVE-2009-4487: nginx 0.7.64 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window's title, or ...
- [MEDIUM 5.0] CVE-2010-2263: nginx 0.8 before 0.8.40 and 0.7 before 0.7.66, when running on Windows, allows remote attackers to obtain source code or unparsed content of arbitrary...

6. Attack Possibilities & Mitigation

Attack: Clickjacking / Cross-Site Scripting (XSS)
Mitigation: Implement X-Frame-Options and Content-Security-Policy headers.