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 v2.5.0
---------------------------------------------------------------------------
+ Target IP: 44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2026-01-16 10:34:06 (GMT-5)
---------------------------------------------------------------------------
+ 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. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type. See: https://ww
w.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.c
om/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs
.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper
domains or wildcards. See:
https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See:
http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time: 2026-01-16 10:35:36 (GMT-5) (90 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```