

■ SDV Toolbox - Rapport de Sécurité

Outil:	Nikto
Date:	06/06/2025 à 09:13:40
Cible:	http://testphp.vulnweb.com
Opérateur:	SDV Security Team

■ Résultats de Nikto

```
- Nikto v2.5.0
-----
+ Target IP: 44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2025-06-06 09:12:27 (GMT2)
-----
+ 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://www.netsparker.com/web-vulnerability-scanner/vulnerabiliti
es/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.m
icrosoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silve
rlight/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/vulnerabilit
ies/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossm
an.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time: 2025-06-06 09:13:33 (GMT2) (66 seconds)
-----
+ 1 host(s) tested

+ ERROR: Error limit (20) reached for host, giving up. Last error: error
reading HTTP response
```