■ SDV Toolbox - Rapport de Sécurité

Outil:	Nikto
Date:	06/06/2025 à 21:54:43
Cible:	192.168.236.142
Opérateur:	SDV Security Team

■ Résultats du Scan Nikto

Métrique	Valeur
■ Vulnérabilités trouvées	7
■ Fichiers exposés	2
■ Niveau de risque	ÉLEVÉ

■ Vulnérabilités détectées :

#1: + /: HTTP TRACE method is active which suggests the host is vulnerable to XST. S...

Référence: Nikto DB

#2: + /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve...

Référence: CVE-1999-0678

#3: + /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive ...

Référence: OSVDB-12184

#4: + /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive ...

Référence: OSVDB-12184

#5: + /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive ...

Référence: OSVDB-12184

■ Log détaillé du scan :

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP: 192.168.236.142
+ Target Hostname: 192.168.236.142
+ Target Port: 80
+ Start Time: 2025-06-06 21:54:33 (GMT2)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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.netsparke
r.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to
easily brute force file names. The following alternatives for 'index' were found: index.php.
See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/v
```

```
ulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is
the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false
positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See:
https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information
via certain HTTP requests that contain specifi

[... Log tronqué pour le PDF ...]
```

■ Recommandations de sécurité :

- ■ URGENT : Corrigez les vulnérabilités critiques détectées
- Effectuez un audit de sécurité complet de l'application web
- Configurez les en-têtes de sécurité manquants (X-Frame-Options, CSP)
- Supprimez ou protégez les fichiers/dossiers sensibles exposés
- Maintenez votre serveur web et vos applications à jour
- Effectuez des scans Nikto réguliers
- Implémentez un WAF (Web Application Firewall)