■ SDV Toolbox - Rapport de Sécurité

Outil:	Wapiti
Date:	07/06/2025 à 17:11:53
Cible:	http://isrp.fr
Opérateur:	SDV Security Team

■ Rapport de Sécurité Web Wapiti

■ VULNÉRABILITÉS WEB DÉTECTÉES

Métrique	Valeur
■ URL scannée	http://isrp.fr
■ Vulnérabilités trouvées	11
■■ Avertissements	0
■ Pages analysées	0
■ Type de scan	Scan web complet
■ Date du scan	07/06/2025 à 17:11:53

■ Types de vulnérabilités détectées :

Type de vulnérabilité	Occurrences	Criticité
Cross-Site Scripting (XSS)	5	CRITIQUE
SQL Injection	4	CRITIQUE
Cross-Site Request Forgery	1	MOYENNE

■ URLs affectées :

• https://wapiti3.ovh/get_ssrf.php?id=wzeg7t,

■ Extrait du rapport technique :

```
__ __ .__ __ ._________
/ \ / \_____ ______ |__|/ |_|__\_____ \
\ \/\/ /\__ \ \____ \| \ __\ | _(__ <
\ / / __ \| |_> > || | | |/ \
\__/\ / (____ / __/|__||__| |__/______ /
\/ \/|__| \/
Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Reprise du scan depuis la session enregistre, veuillez patienter
[*] Enregistrement de l'tat du scan, veuillez patienter...

Note
========
Ce scan a t sauv dans le fichier /root/.wapiti/scans/isrp.fr_url_42027fdd.db
[*] Wapiti a trouv 63 URLs et formulaires lors du scan
[*] Chargement des modules :
```

```
backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess,
http_headers, methods, nikto, permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe

[*] Lancement du module csp
CSP n'est pas dfini

[*] Lancement du module http_headers
Vrification de X-Frame-Options :
OK
Vrification de X-XSS-Protection :
```

■■ Recommandations de sécurité web :

• ■ URGENT : Corrigez les vulnérabilités web détectées

• Validez et échappez toutes les entrées utilisateur

• Implémentez une protection CSRF appropriée

• ■ Implémentez une politique CSP (Content Security Policy) stricte

• ■ Utilisez des requêtes préparées pour toutes les interactions avec la base de données

• ■■ Configurez des en-têtes de sécurité appropriés

• ■ Utilisez HTTPS pour toutes les communications

• ■ Effectuez des scans Wapiti réguliers

• ■ Intégrez Wapiti dans votre pipeline CI/CD

• ■ Formez l'équipe aux vulnérabilités web OWASP Top 10

• ■ Implémentez un processus de développement sécurisé

• ■ Effectuez des tests de pénétration périodiques