Error Based SQLi Report - 17.6.2 - 17

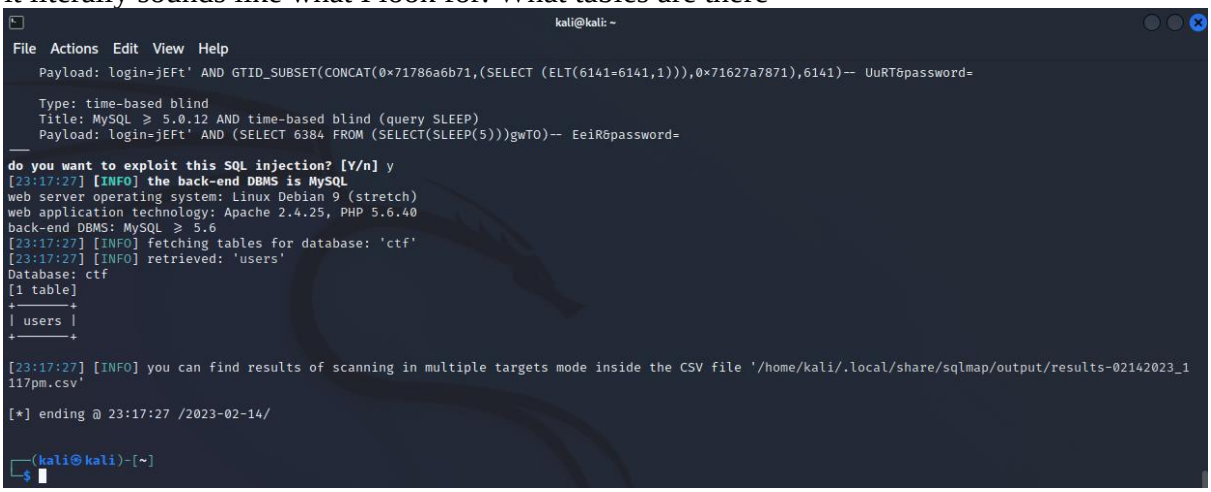
Tester's name: Stanley Ford

Lab 17.6.2 "Error Based SQLi":

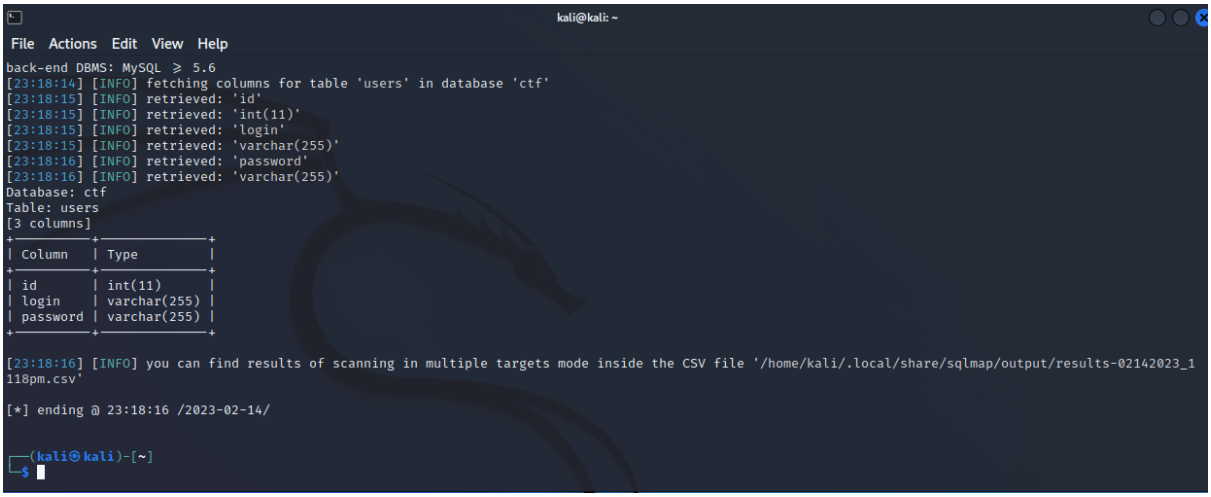
- General information:
  - Testing period: 15.02.2023
  - Test object: http://51.250.73.193:5009/
- Description of actions:Checking the page code did not bring anything. The task looks similar to the previous task, so I will do everything the same as there.

  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



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



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

: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.