Challenge: KORP Terminal

# Challenge Description :

## Your faction must infiltrate the KORP™ terminal and gain access to the Legionaries' privileged information and find out more about the organizers of the Fray. The terminal login screen is protected by state-of-the-art encryption and security protocols.

# Context :

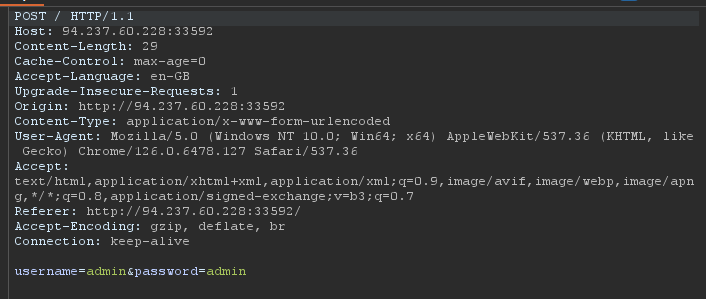
## I intercept a POST http request to the login end-point, with this request capture I use it with Sqlmap to find a SQL injection to gain credentials to login to the web-application, to hopefully get the flag.

# Notes :

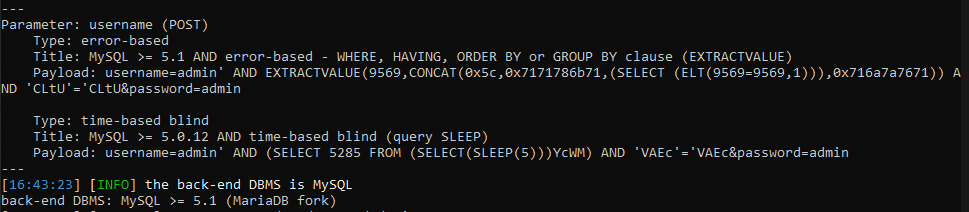
* Tools:
  + - BurpSuite - To intercept the http request and send forged ones.
    - SQLMAP - To get a sql injection and gain the username / password hashes to crack using hashcat / JohnTRipper

# Flag :

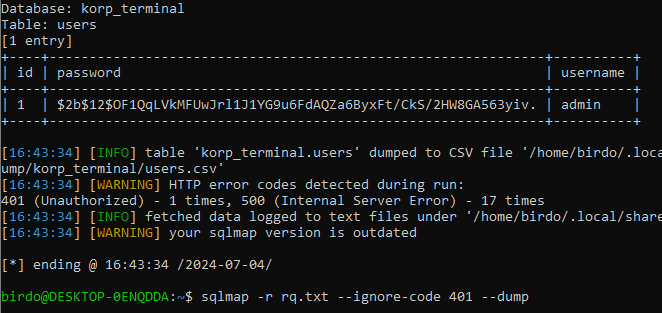
* First Start the instance, go to the website with the burp suite proxy to intercept the http POST request to login. Enter false credentials and keep the interception on.



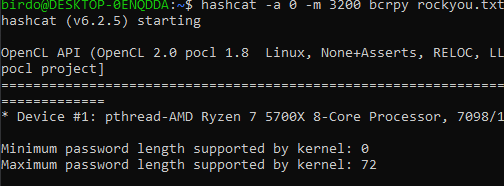
* You should successfully get a request like this, when you get it make sure to copy and paste it into a text file [.txt] and run it with Sqlmap.
* When running with Sqlmap, it automatically attempts to find an injection vulnerability using the provided request. Sqlmap replaces the input for username and password to check if either argument (or both) is vulnerable to injection.



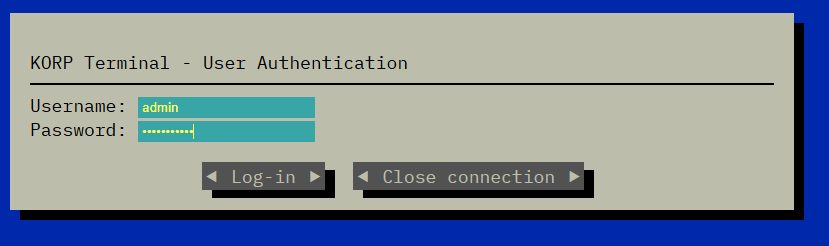
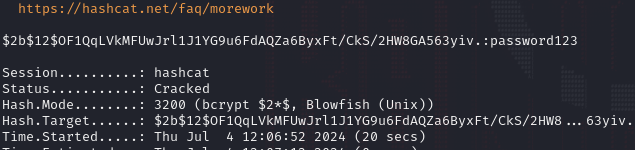
* We have seem to have found two SQL injections, we can now dump all the DB table entries by running it with the options ‘--dump’



* We now need to crack this hash to gain the password to login successfully.
* After gaining the hash we will copy and paste it in a text file [.txt] to run with hashcat, we also need to run it with ‘HashID’ to get the hash type to successfully decrypt it, Look at the Hash we can tell its Bcrypt as $2a$ is the hash identifier.
* We find the hashcat Mode for Bcrypt which should be “-m 3200”, as well as the attacking mode set to ‘-a 0’.



* We then get the cracked hash : ” Password123 ” , making the Credentials for the login page: “ **Admin:Password123** ”
* I switched to a Kali Linux machine due to limitations on WSL for running hashcat. E.g Reading hardware temperatures.



* Now logging into the login page with the cracked password and the username will display a flag straight away.
* The Flag will be : **HTB{t3rm1n4l\_cr4ck1ng\_4nd\_0th3r\_sh3n4nig4n5}**

