HackTheBox – Lernaean Write Up

Tools:

- Burp Suite (Kali Linux)
- Hydra (Kali Linux)

Walkthrough:

Step	Description
1	Upon visiting the website http://docker.hackthebox.eu:(Port number)/#, the page displays a message “Please do not try to guess my password!” and a login form.
2	Start Burp Suite and analyze the response from the website after submitting a wrong password.
3	Next, use Hydra to perform a Brute Force attack with rockyou.txt Command "hydra -l admin -P /root/Downloads/rockyou.txt 139.59.202.58 http-post-form "/:password=^PASS^:Invalid password!" -s 32351 " hydra -l admin -P /root/Downloads/rockyou.txt (Observe ip address from Burp Suite)http-post-form "/:password=^PASS^:Invalid password!" -s (Port Number)
4	The login credentials are obtained from the Hydra tool results.
5	The login credentials are used and it was found based from the hints "Ooops Too slow!" that Burp Suite was required to intercept the connection to find the flag.
6	In Burp Suite, send to repeater to repeat the login action. The flag is obtained and found in the response.

Flag is HTB{Please find the flag yourself ☺}

**PS:

- Ensure that the proxy settings of the browser and Burp Suite are configured properly (For example port:8080).
- For first time users of Burp Suite, please configure the browser to have the certificate from Burp Suite before starting the challenge.