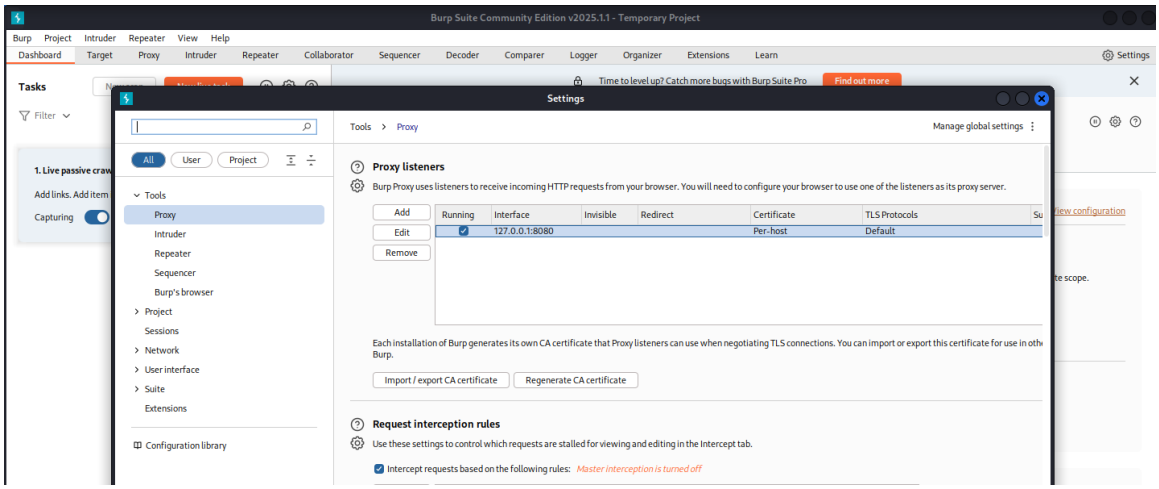
DVWA-Low-Level Brute Force Attack

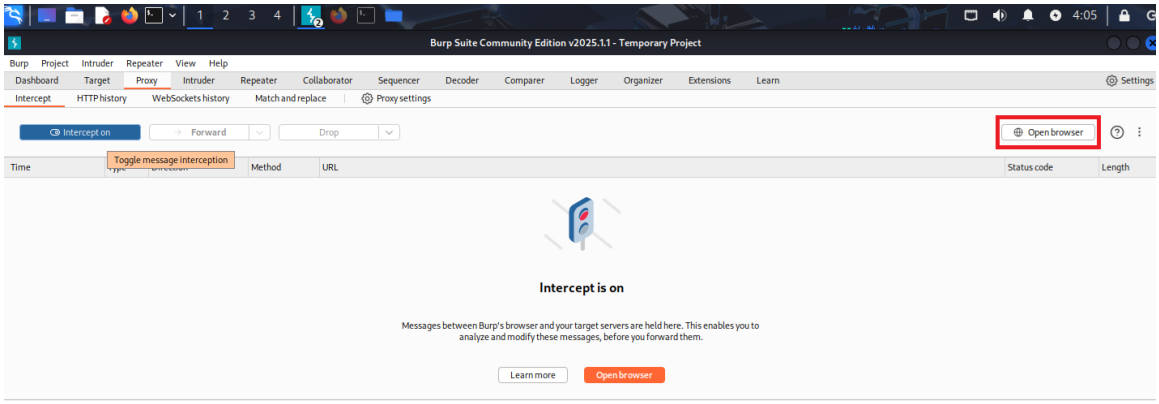
--MagicDragonB

Using the tool called Burp Suite, which has already been installed in Kali Linux 2025.

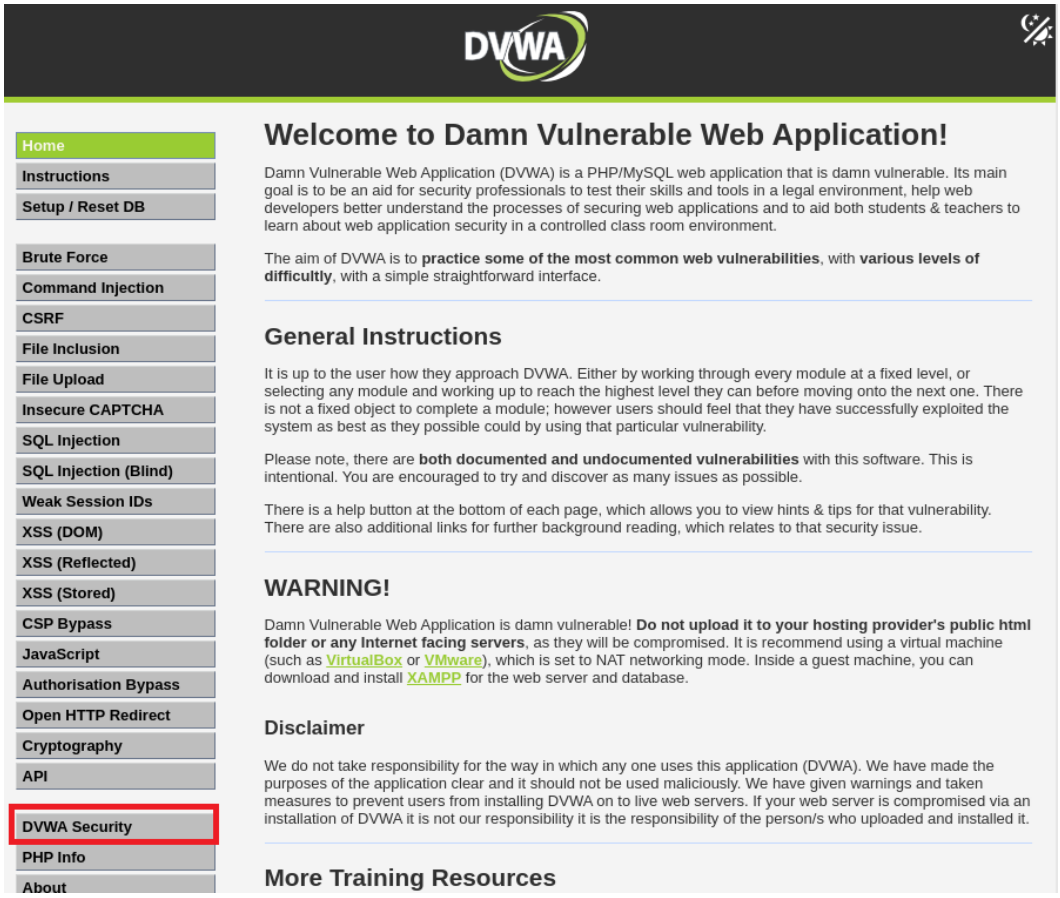
Once you open this tool, make sure that the proxy listener protocol is running.

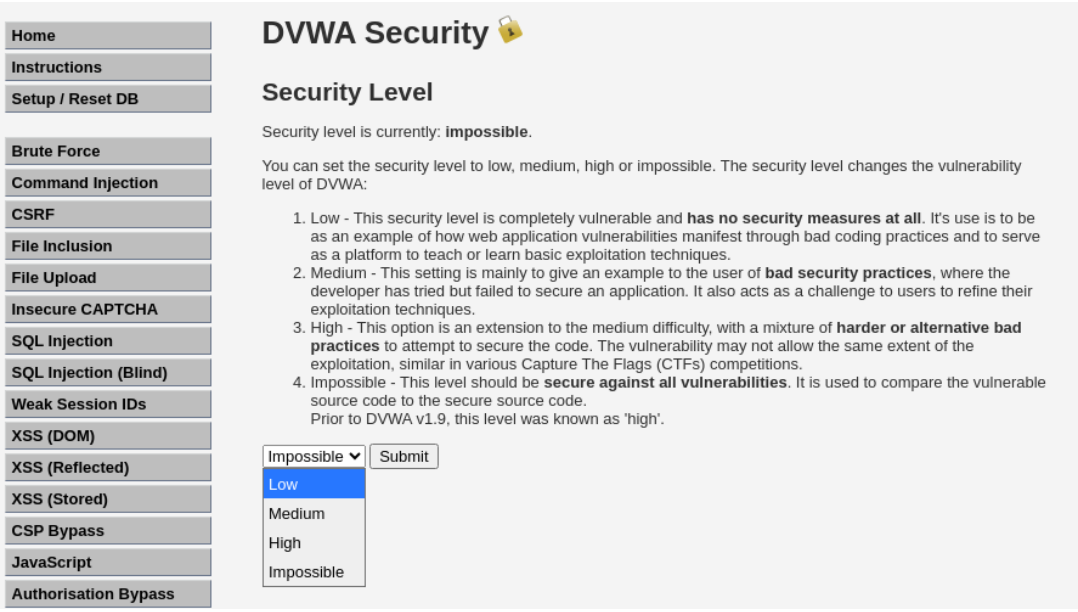


Then click Proxy Option → open browser and log in to the DVWA.

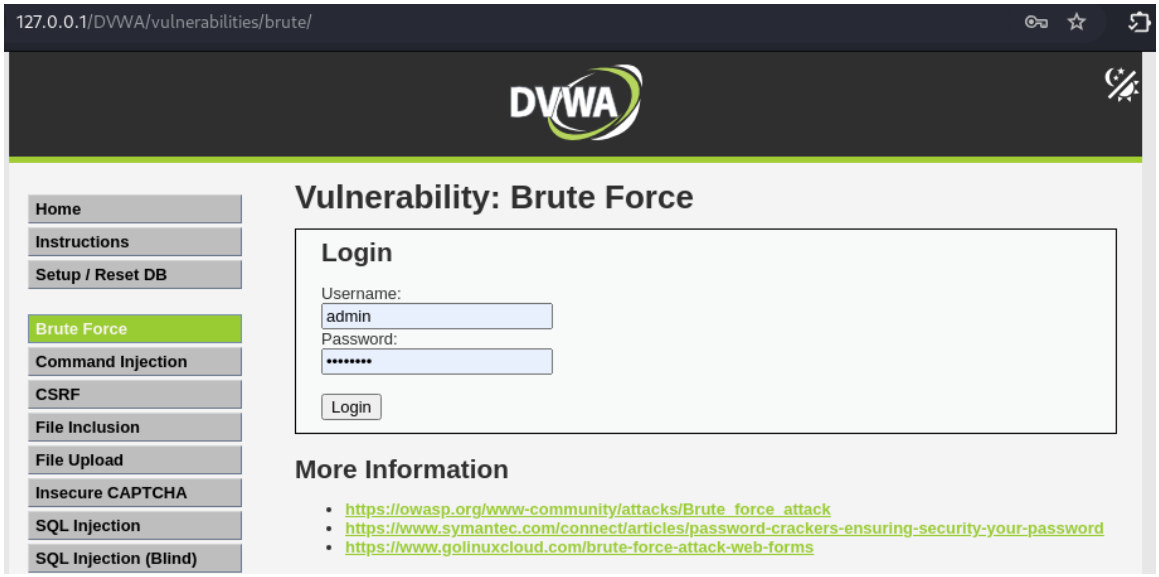


Once logged into the DVWA, select the ‘DVWA Security’ option and choose ‘low,’ then submit.

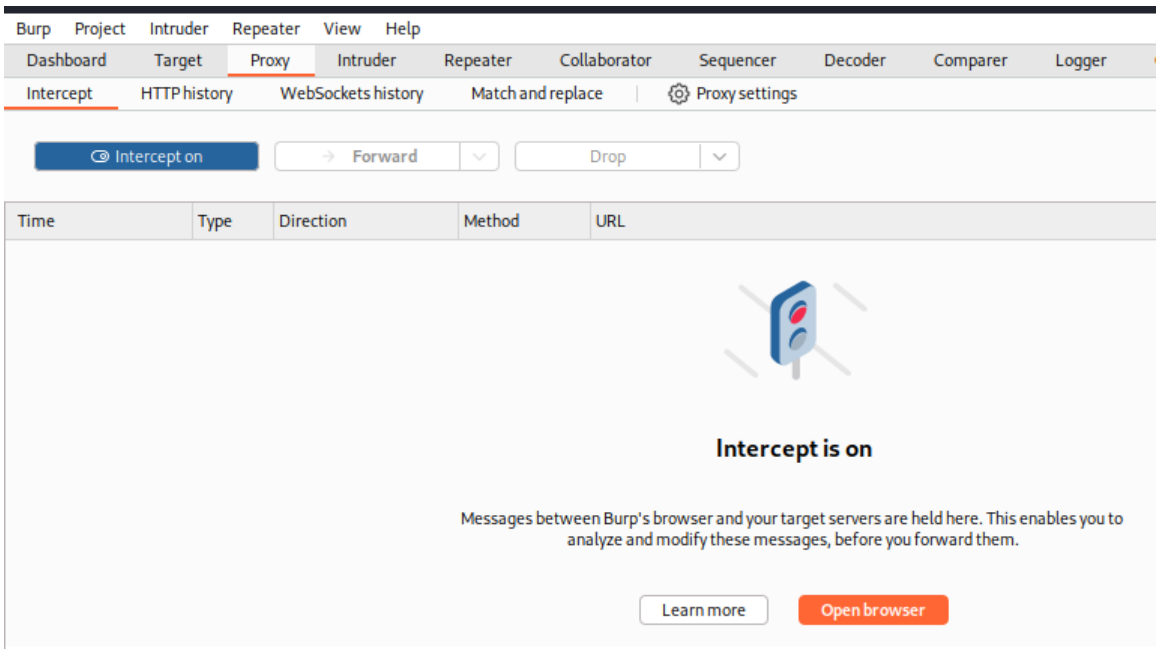




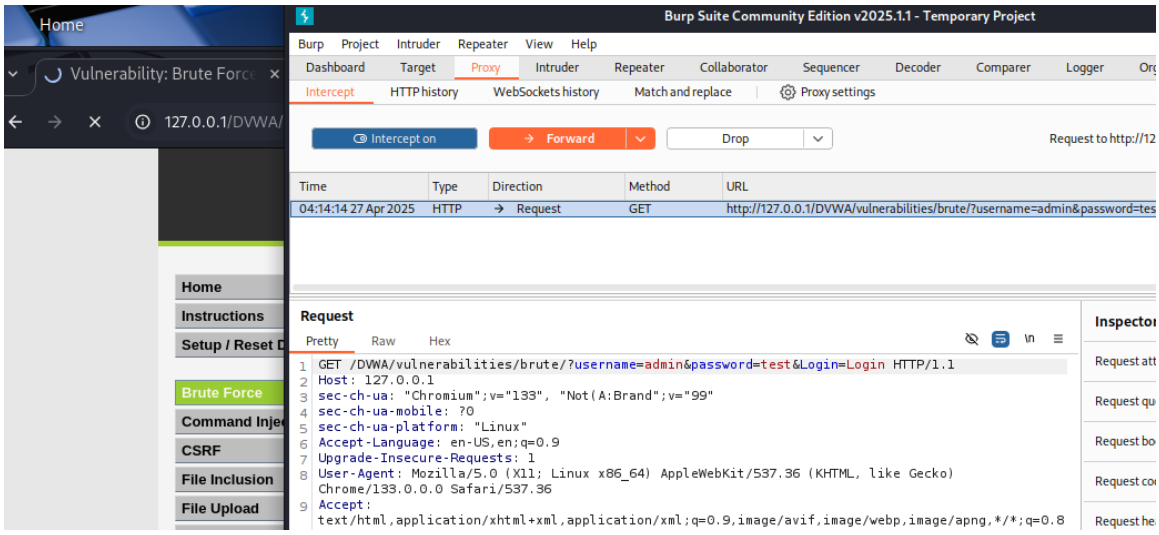
Then click Brute Force session, then can start the low-level brute force challenge.



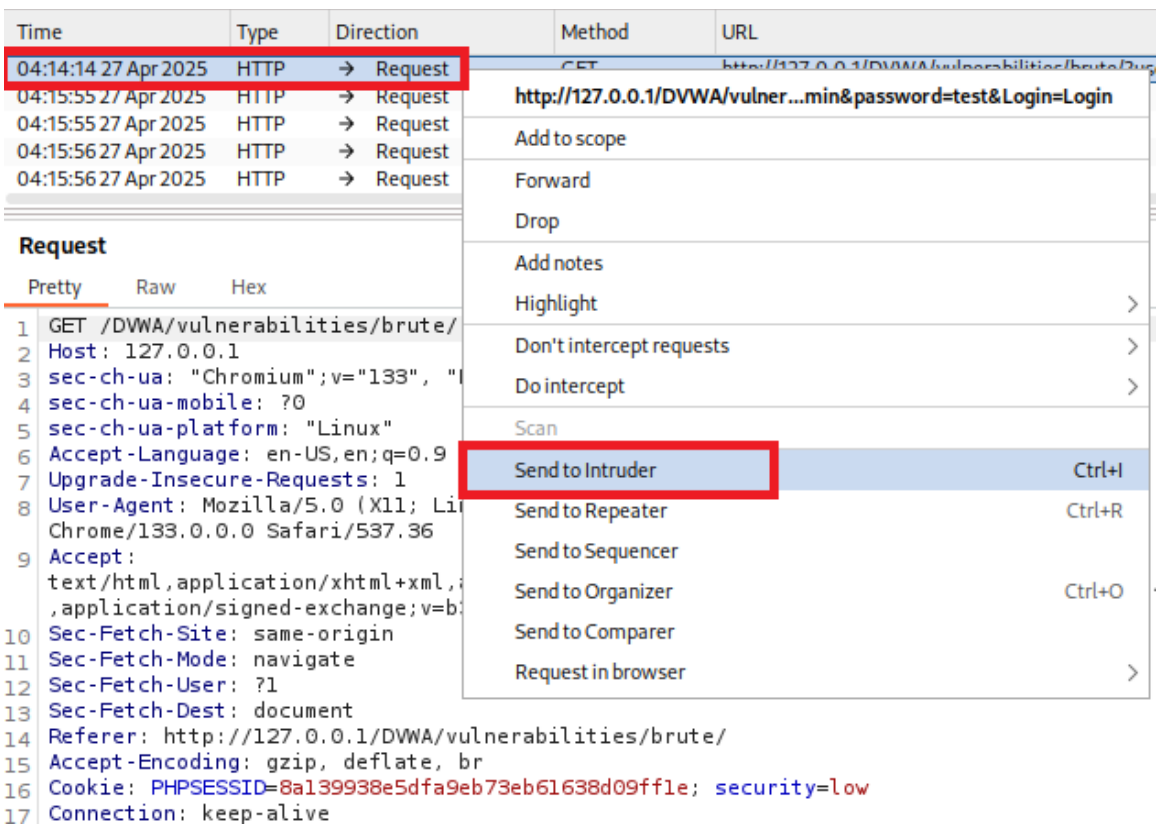
Turn on the 'intercept' button.



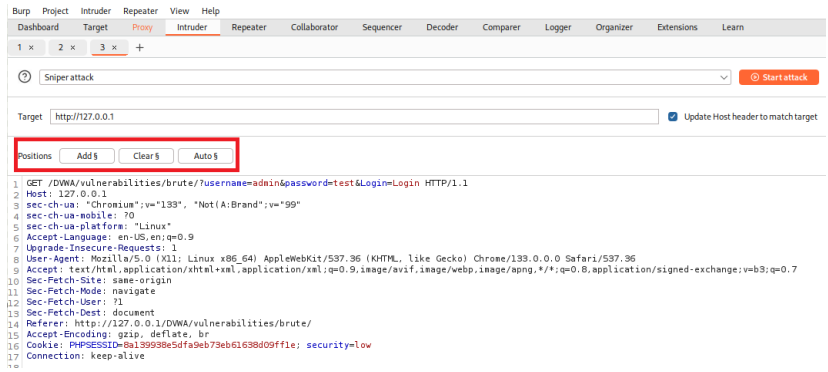
At the password section, enter an incorrect password, such as ‘test.’ (We know the correct password is ‘password.’) Then we can capture the message, including the website method (GET method), HTTP type, user’s operating system, and more.



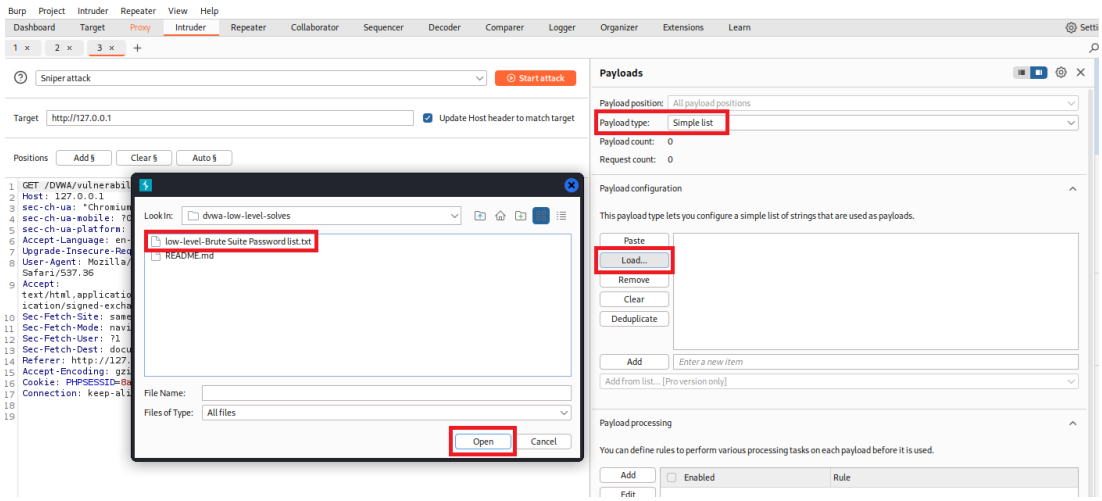
Right click on it and click send to intruder

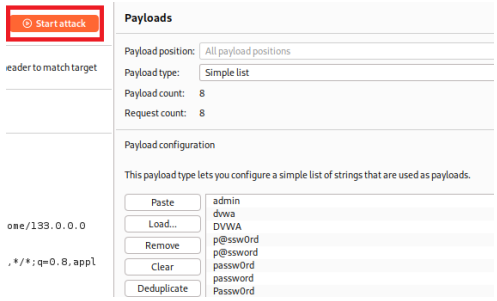


In this page have three options, this option means you can add, clear the attack part. In this session we are focused on the part of password, so we should choose the ‘password’ and click ‘add’

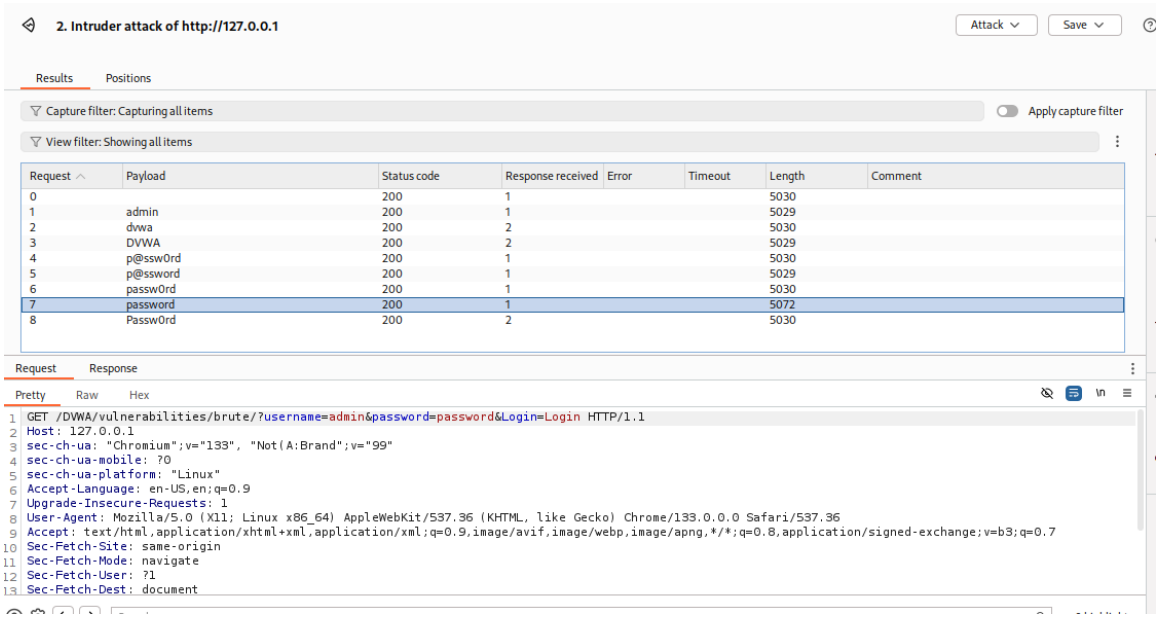


The payload page will update after you click "Add." Load the "Low-level-Brute Force Password list" after selecting the "Simple list" Payload Type. Click "start attack" after that.



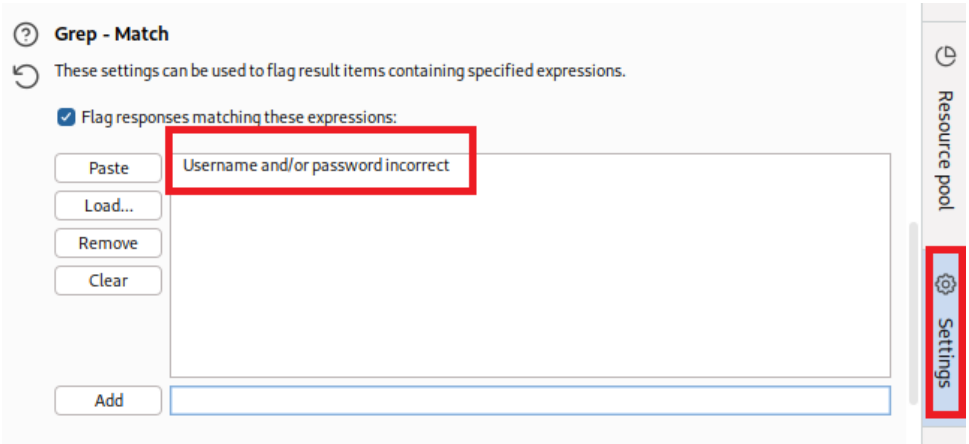


However, the outcome is difficult to tell which password is wrong and which is right. After that, we may select the Grep-Match option by clicking the settings button.



You will see that the screen will notify you that your 'username and/or password are incorrect' if you have attempted to log in previously with an invalid password.

So, we add Username and/or password incorrect into the Grep-Match, after that, we click the attack button again.



Then we can clearly see that the 'password' row does not match, indicating that this is the correct password. We can view the details in the 'Response' option, select 'Render,' and then we can see the successful page.