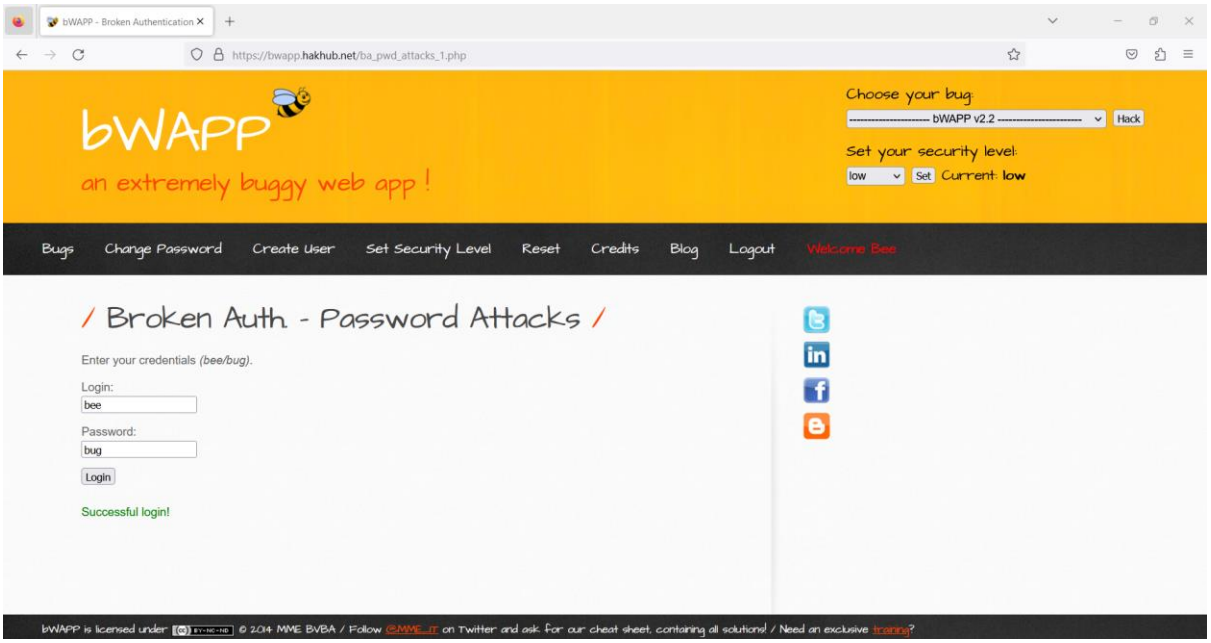
BROKEN AUTHENTICATION – PASSWORD ATTACKS

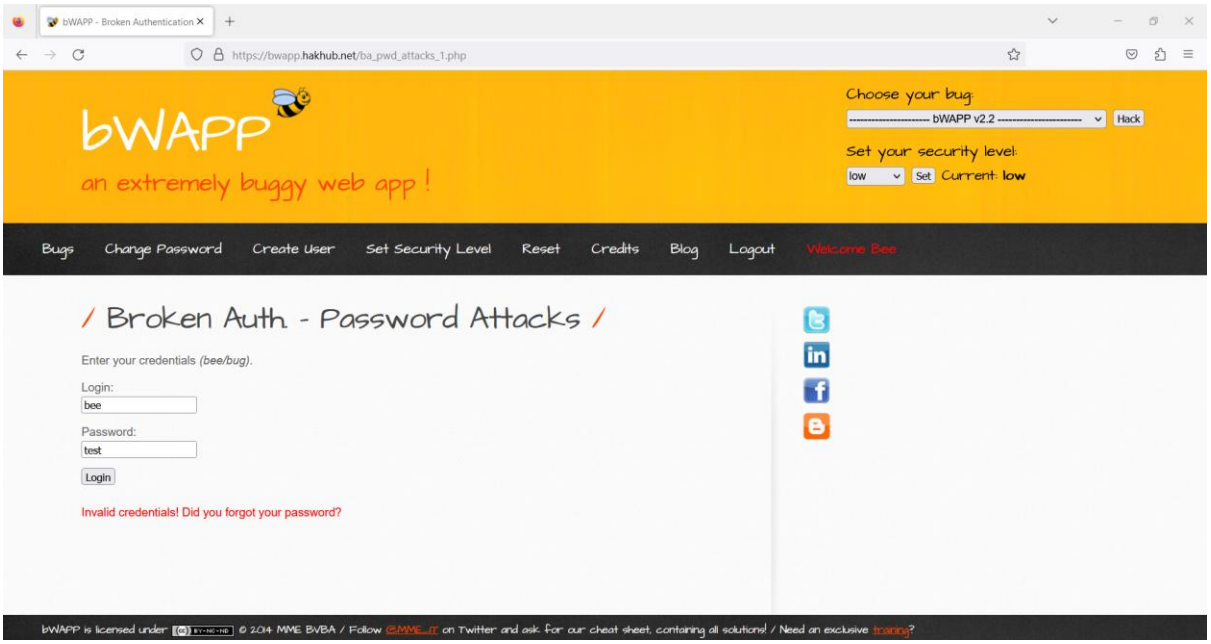
SECURITY LEVEL -low

Go to Challenge

Login using given credentials,

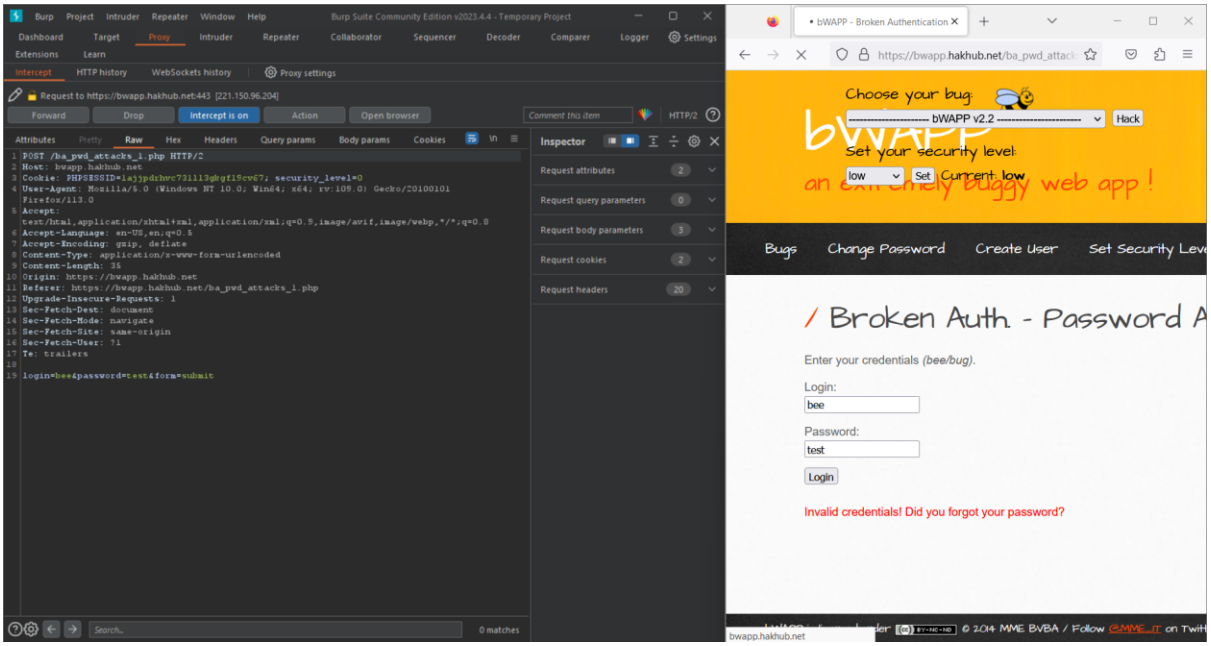


Try login through wrong password



Now we will use Burp Suite to intercept the request.

Intercept the request of the login page, send it to “Intruder” to carry out the attack.

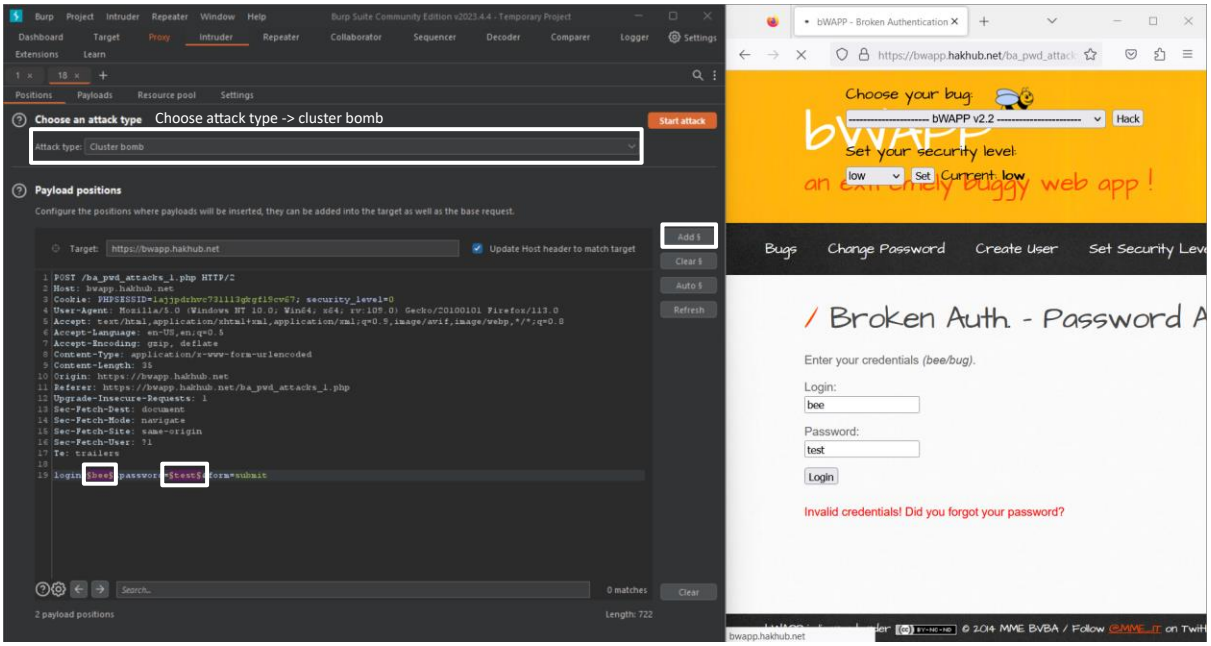


In “Intruder -> Positions”,

Choose Attack type → Cluster Bomb

For payload position, select <login_value> and <password_value> (in this case bee and test)

‘Add §’

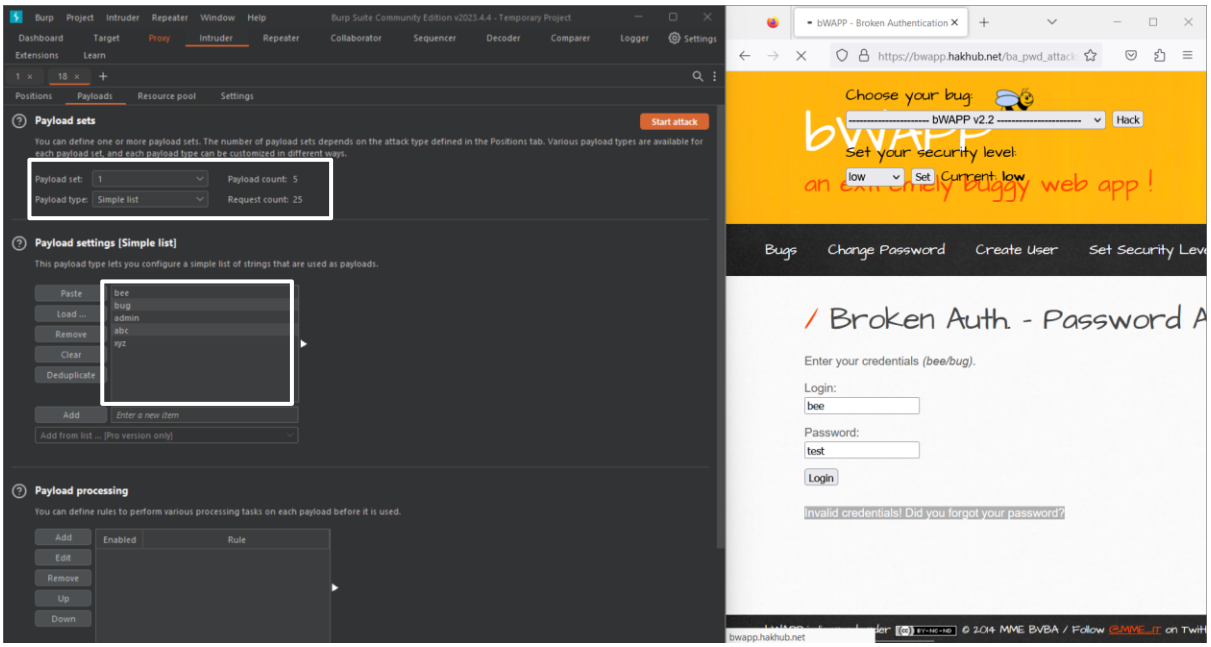


Go to “Intruder -> payloads”

Payload set 1 -

{for payload position “login”}

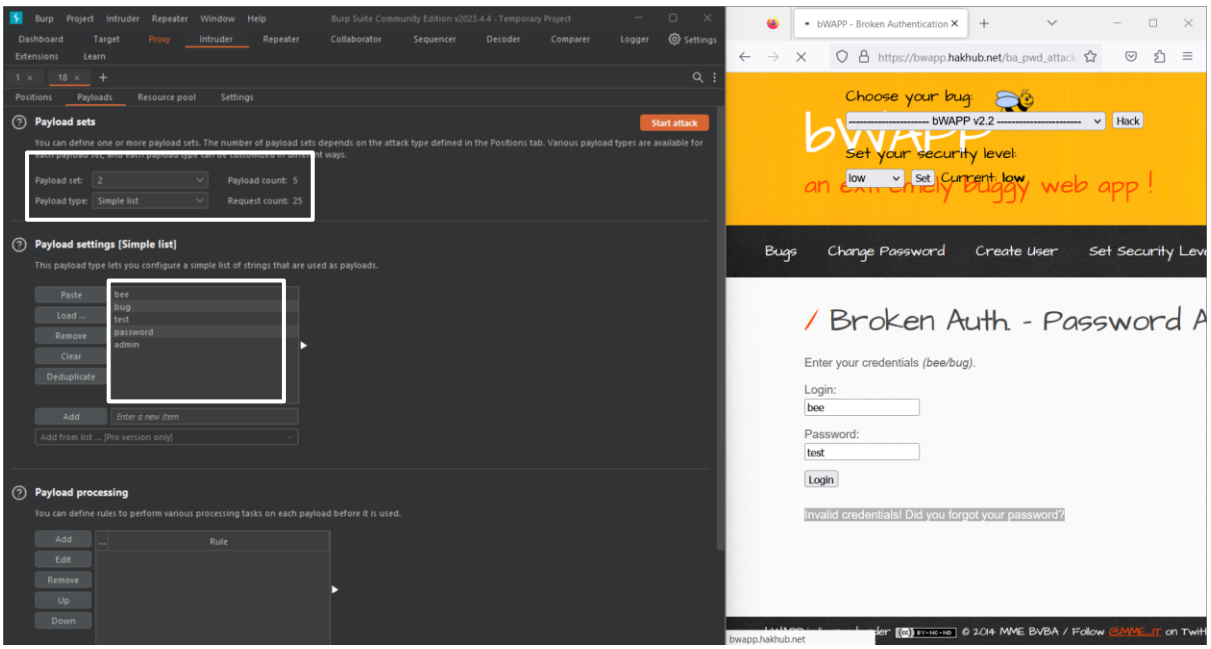
Clear the default list and add few random login usernames



Payload set 2 -

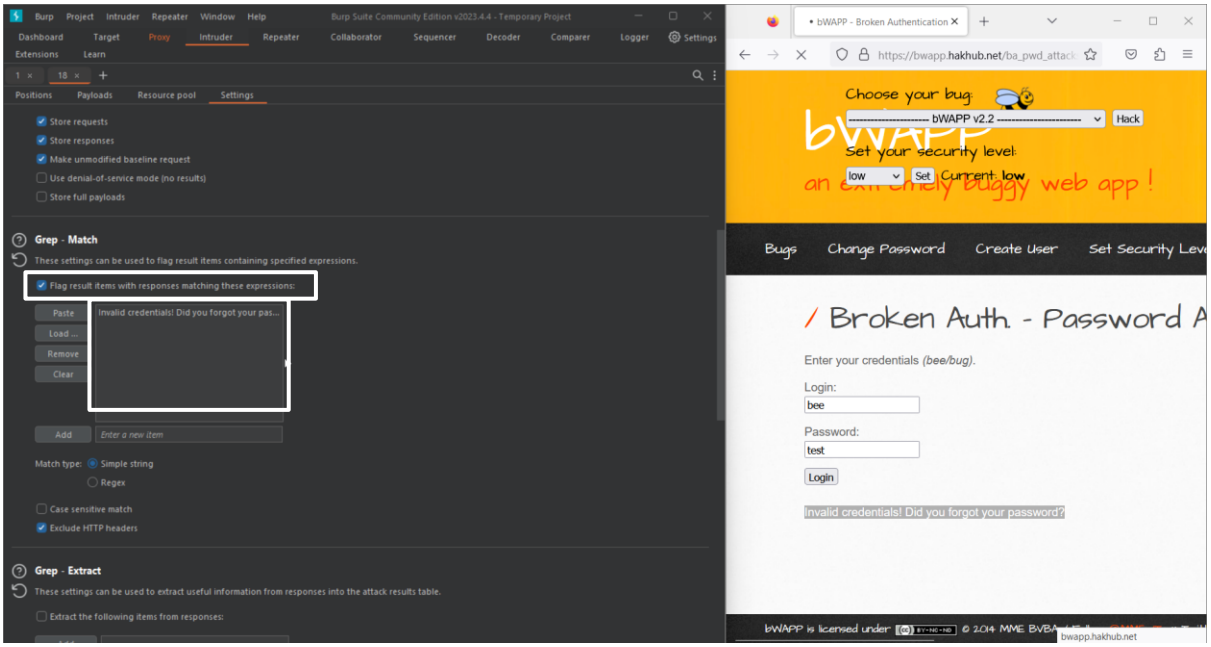
{for payload position “password”}

Clear the default list and add few random and common passwords



Go to “Intruder -> Settings”

Look for following settings

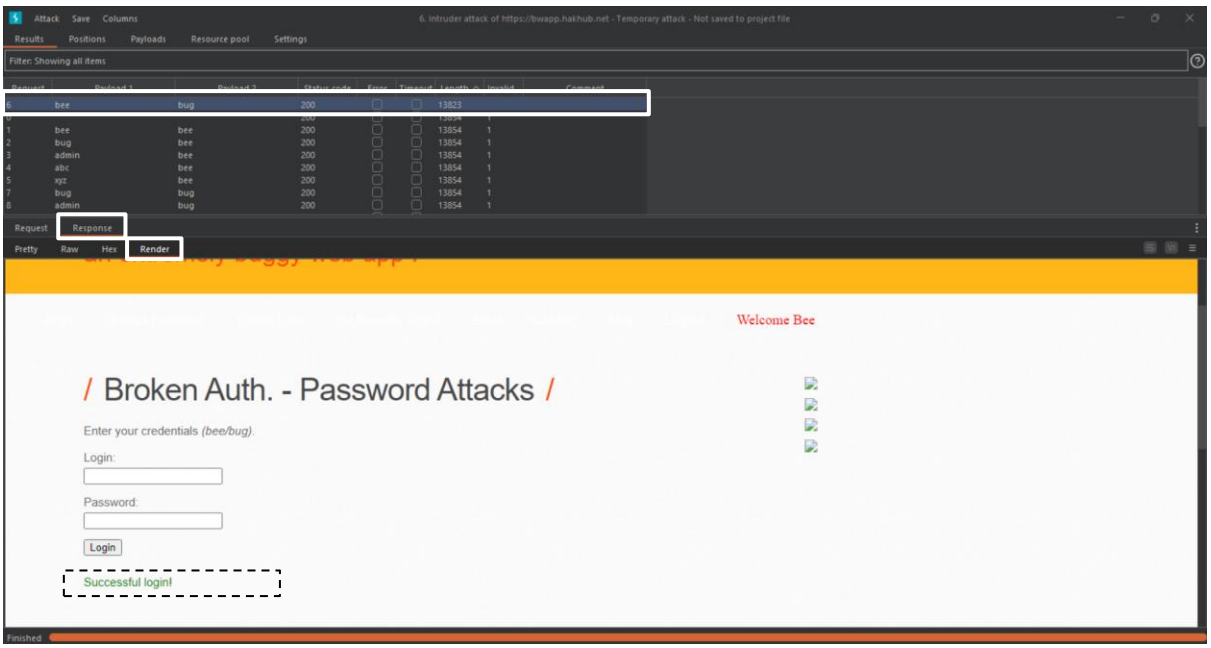


Now go back to “Intruder -> Payloads”

And start attack

After attack is finished, sort the length column

Click on “bee” and “bug” credentials → Response -> Render



CHALLENGE SOLVED…!!