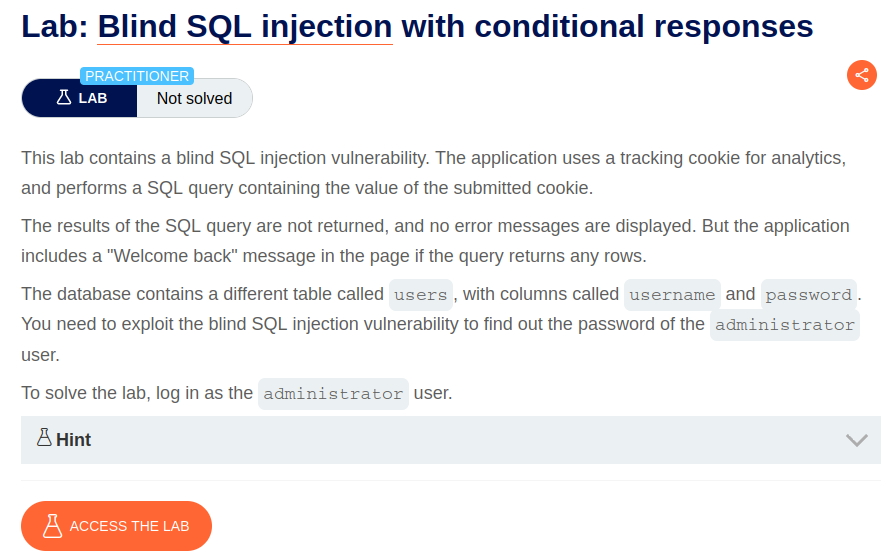
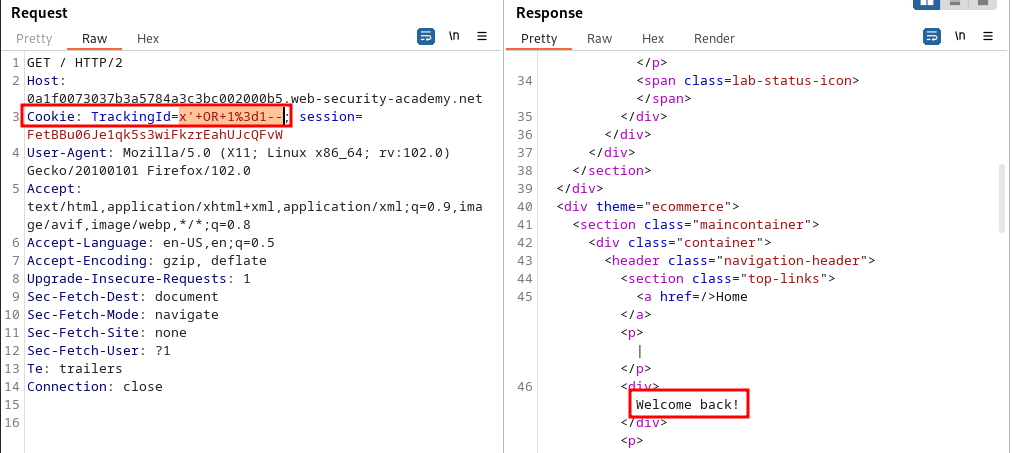
To Access the Lab –



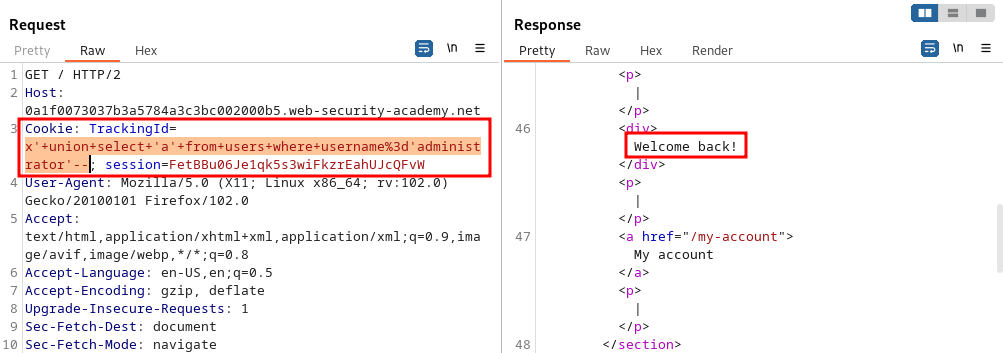
Intercept the request on Burp and send to repeater,

In the Tracking ID – edit the ID to x’ OR 1=1--



We can see a 200 response.

Next, we can find users with the name administrator and print it out.

x'+union+select+'a'+from+users+where+username%3d'administrator'--

Similarly, we get a 200 response.

Next, we set a password length parameter

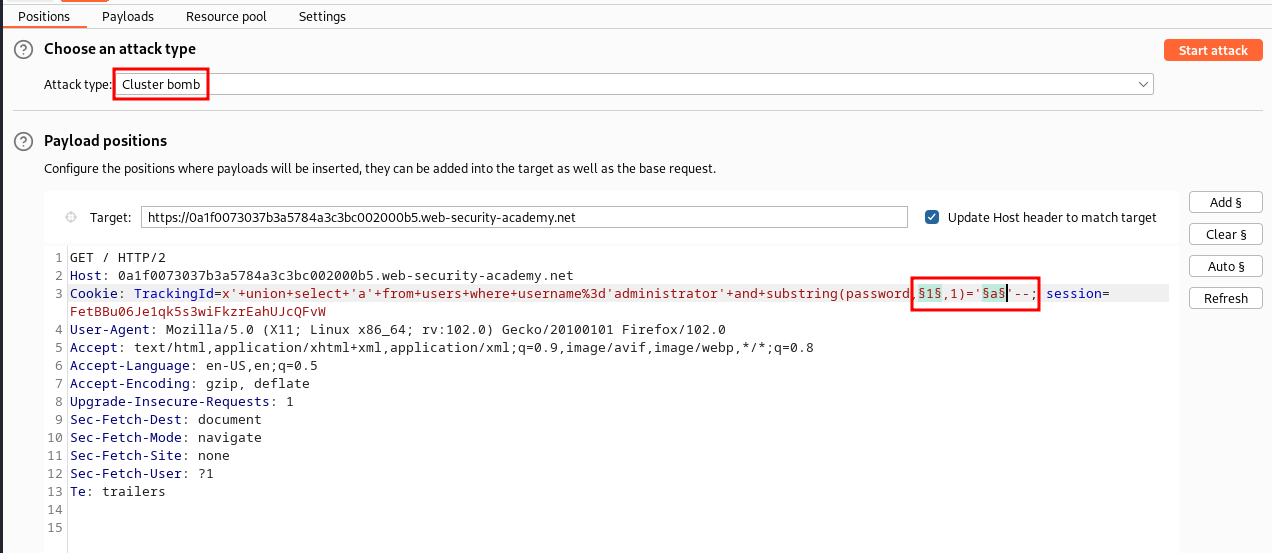
x'+union+select+'a'+from+users+where+username%3d'administrator'+and+length(password)>1—



Now we keep incrementing the value of password length till the time we don’t get the “Welcome Back” message.

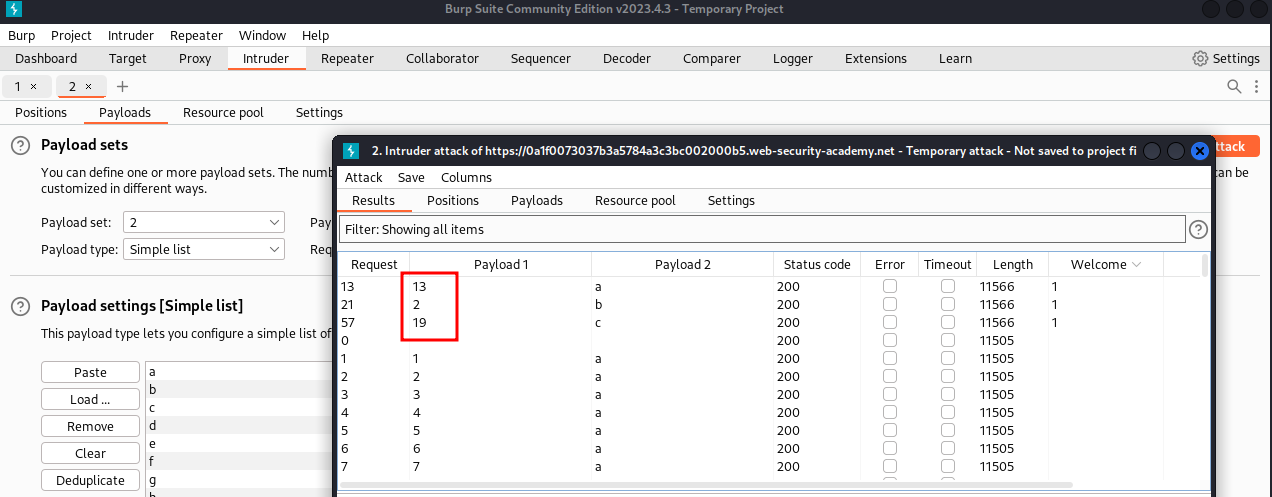
We get it at 20, therefore the password length is 19.

Send this request to intruder.

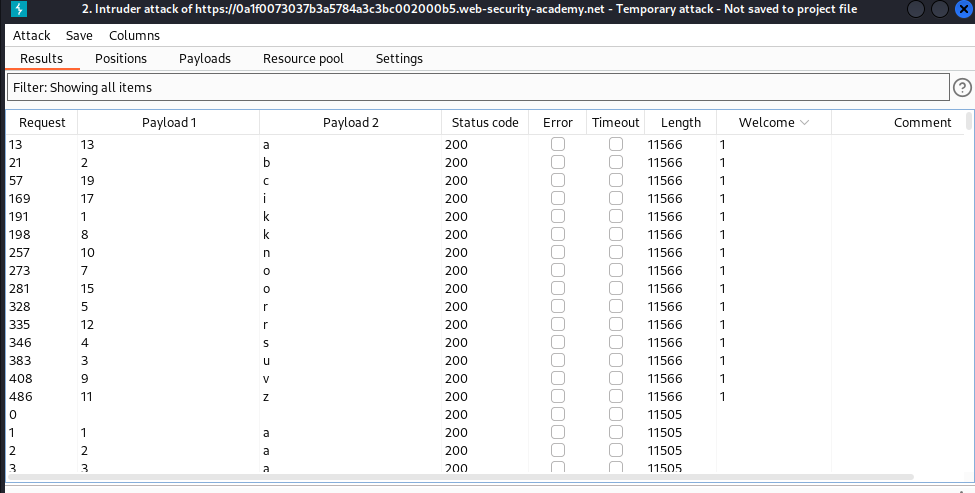


Payload 1 add 1-19 and payload 2 add a-z

And then grep select is “Welcome” and start the attack



Here we get the location of the word in payload1



Once we get the password,

Login to the administrator account.

