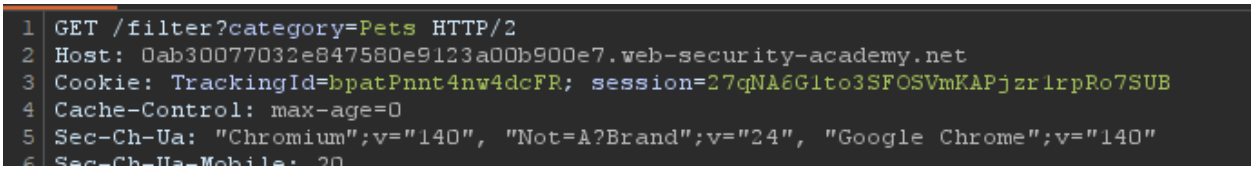
Blind SQL injection with conditional responses

1. This lab contains a blind SQL injection vulnerability. The application uses a tracking cookie for analytics and performs a SQL query containing the value of the submitted cookie.

2. The results of the SQL query are not returned, and no error messages are displayed. But the application includes a Welcome back message on the page if the query returns any rows.

3. I need to extract administrator password.

4. First, I intercepted the request by burpsuite to see tracking cookie, and I found it like this:



5. I try to inject it:

TrackingId=bpatPnnt4nw4dcFR' AND 1=1--

And

TrackingId=bpatPnnt4nw4dcFR' AND 1=1--

When I injected 1=1 I found "Welcome back!" message appeared on the page and when I injected 1=2 the message disappeared. I make sure that the tracking cookie is vulnerable to SQLi

6. I need to know the length of the administrator password to start bruteforcing, I send the request to intruder and try to inject it with this payload:
   `TrackingId=bpatPnnt4nw4dcFR' AND (SELECT username FROM users WHERE username='administrator' AND LENGTH(password) = X) = 'administrator'--`
   Then I prepare the payload of the intruder from 0 to 30, these numbers will be replaced wit X. When it finish, I checked the requests manually. In the request that the X is equal to 20 I found “Welcome back!” message so the length of the password is 20 characters.

7. At this point, We have two methods. The first one is burpsuite but we will need burpsuite pro to speed up the process. The second one is to write python script. I don’t have burpsuite pro so I will write python script. (The script attached)

8. The script is bruteforcing to extract the password using this payload:

   `TrackingId=bpatPnnt4nw4dcFR' AND SUBSTRING((SELECT password FROM users WHERE username = 'administrator'), 1, 1) = 'X'—`

Then, the script replace X with alphanumeric characters and when the response contains “Welcome back!” message that means that the current character is true so append it in the password variable, if the response does not contain the message that means that the current character is false, don’t append it. And so on.

The administrator password: **uur69kpikgjaa7desfgn**

9. Logged in successfully.