Blind SQL injection with time delays and information retrieval

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 the application does not respond any differently based on whether the query returns any rows or causes an error. However, since the query is executed synchronously, it is possible to trigger conditional time delays to infer information.

3. This lab is the same as the previous lab, but there is one more step than the previous lab. The new step is to retrieve the password of administrator and login with his credentials.

4. First, I think to inject this payload:

   `TrackingId=' OR (SELECT pg_sleep(10) FROM users WHERE username='administrator' AND LENGTH(password)=X)--`

   I tried to bruteforce the X value to know the length of the password. But the database didn't sleep. So, I decided to think differently.

5. I will try to use CASE method that we use in lab 12. I change the payload to be like this:

   `TrackingId=VPfsmPRncGoUqqDP' || (SELECT CASE WHEN (username='administrator' AND LENGTH(password)=X) THEN pg_sleep(10) ELSE pg_sleep(-1) END FROM users)--`

   When username='administrator' AND LENGTH(password)=X, the case will be true and the database will sleep 10 seconds, and if the condition is false, the else will triggered and the database will not sleep.

6. The next step, I bruteforce the X value to know the length of password and already the database slept when X=20. So, I know that this injection is valid.
7. Then I try to extract the administrator's password, so I modify the payload to be:

TrackingId=VPfsmPRncGoUqqDP' || (SELECT CASE WHEN (username='administrator' AND SUBSTR((SELECT password FROM users WHERE username='administrator'), X, 1) = 'Y') THEN pg_sleep(10) ELSE pg_sleep(-1) END FROM users)--

And I use a python script to bruteforce X and Y values to extract the password.

8. Finally, I got the password and logged in successfully.