**Lab: Blind SQL injection with out-of-band data exfiltration**

Problem: This lab contains a [blind SQL injection](https://portswigger.net/web-security/sql-injection/blind) vulnerability. The application uses a tracking cookie for analytics, and performs a SQL query containing the value of the submitted cookie.

The SQL query is executed asynchronously and has no effect on the application's response. However, you can trigger out-of-band interactions with an external domain.

Goal: 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.

Solve:

1-

A screenshot of a computer

Description automatically generated

2- A screenshot of a computer

Description automatically generated

3- A screenshot of a computer

Description automatically generated

4-

A screenshot of a computer

Description automatically generated

You will go to burp collaborate client and get the password