

Access Control Vulnerabilities

Refer for theory: <https://portswigger.net/web-security/access-control>

Vulnerability labs (Apprentice):

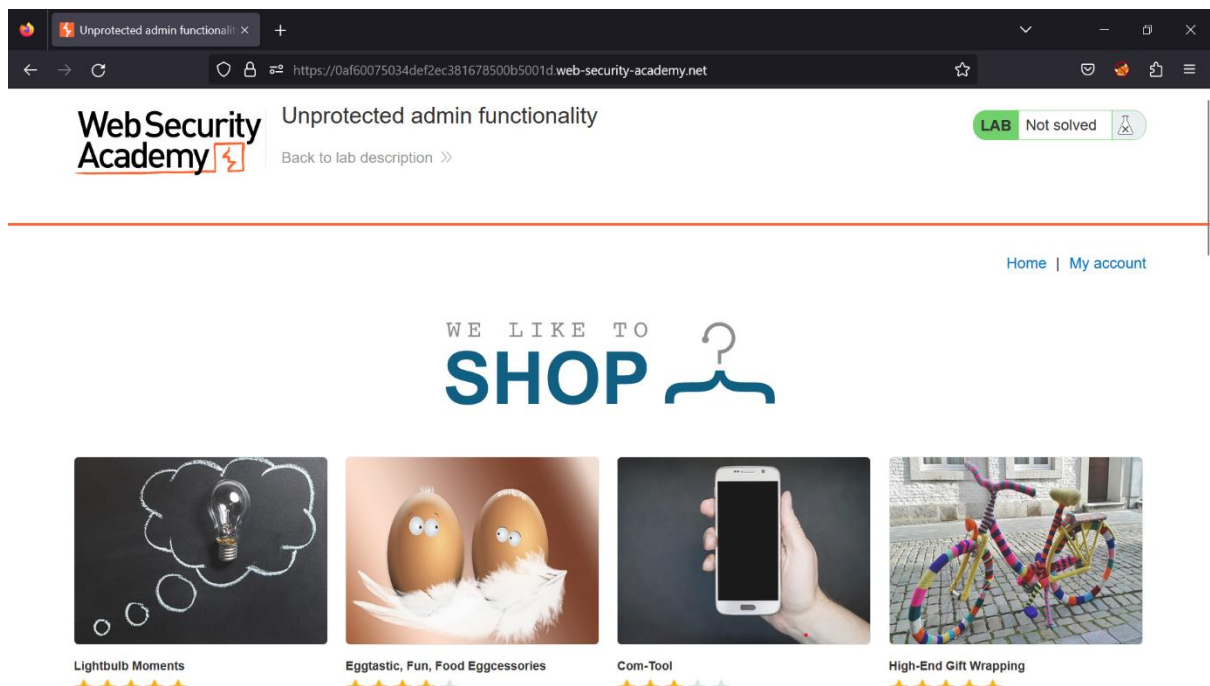
1. Unprotected admin functionality.

This lab has an unprotected admin panel.

Solve the lab by deleting the user, Carlos.

Solution:

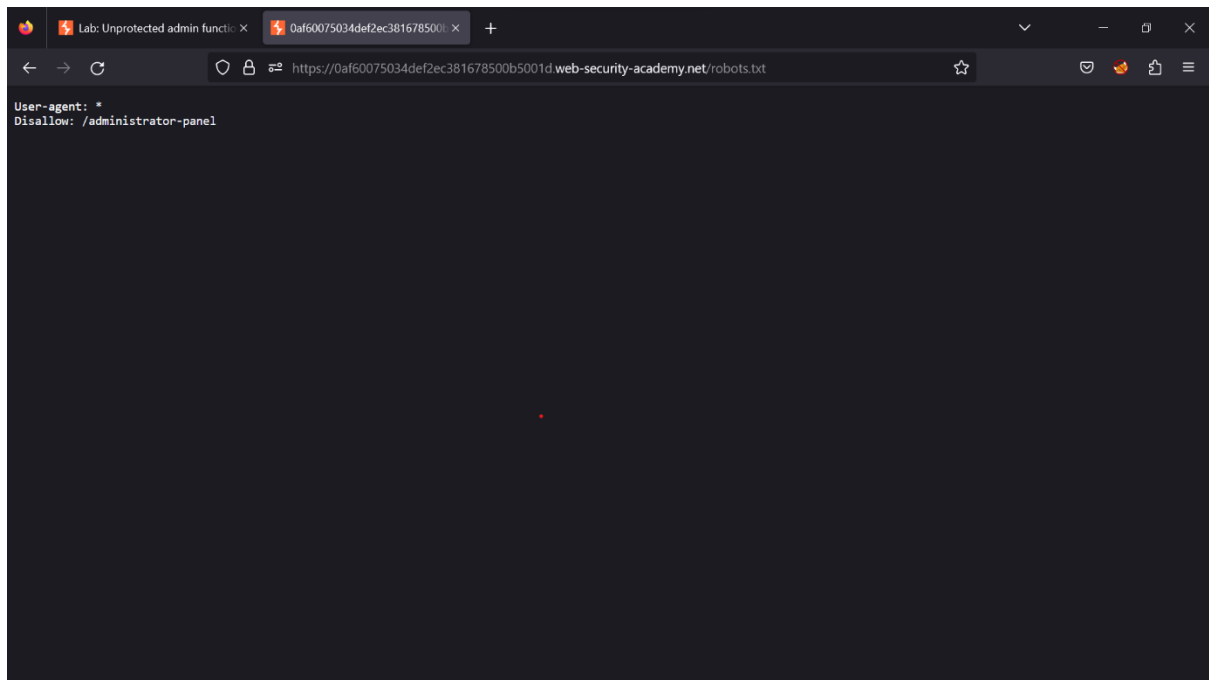
- The goal of this lab is to find the admin panel.



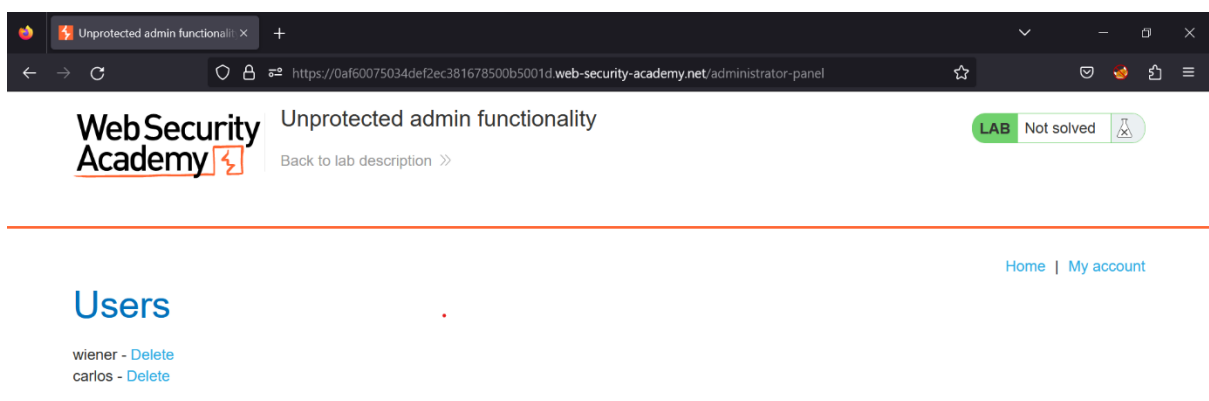
- In the URL, append the following code:

/robots.txt

- This will redirect to a different site where some information about the admin panel will be given.



- By analyzing the above information, we can try to append **/administrator-panel** to the URL to check out the possibility of admin panel being accessed.
- Enter the URL and you will see that the admin panel has appeared.



- Delete the account Carlos and your lab will be completed.

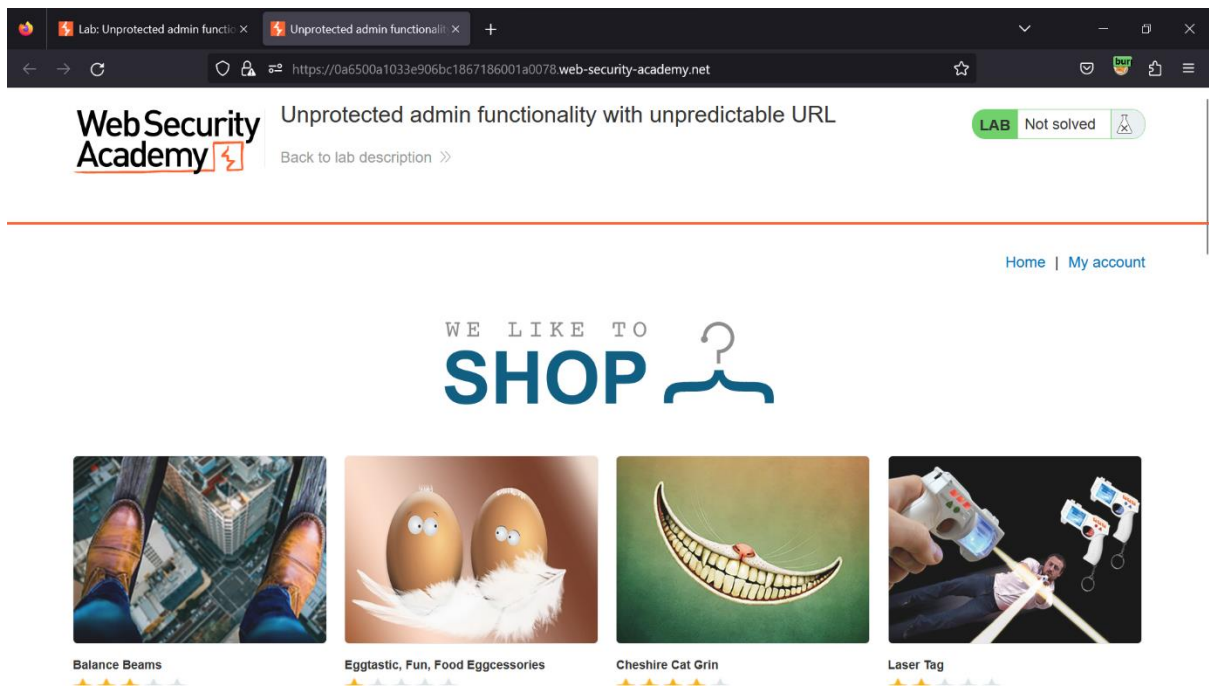
2. Unprotected admin functionality with unpredictable URL.

This lab has an unprotected admin panel. It's located at an unpredictable location, but the location is disclosed somewhere in the application.

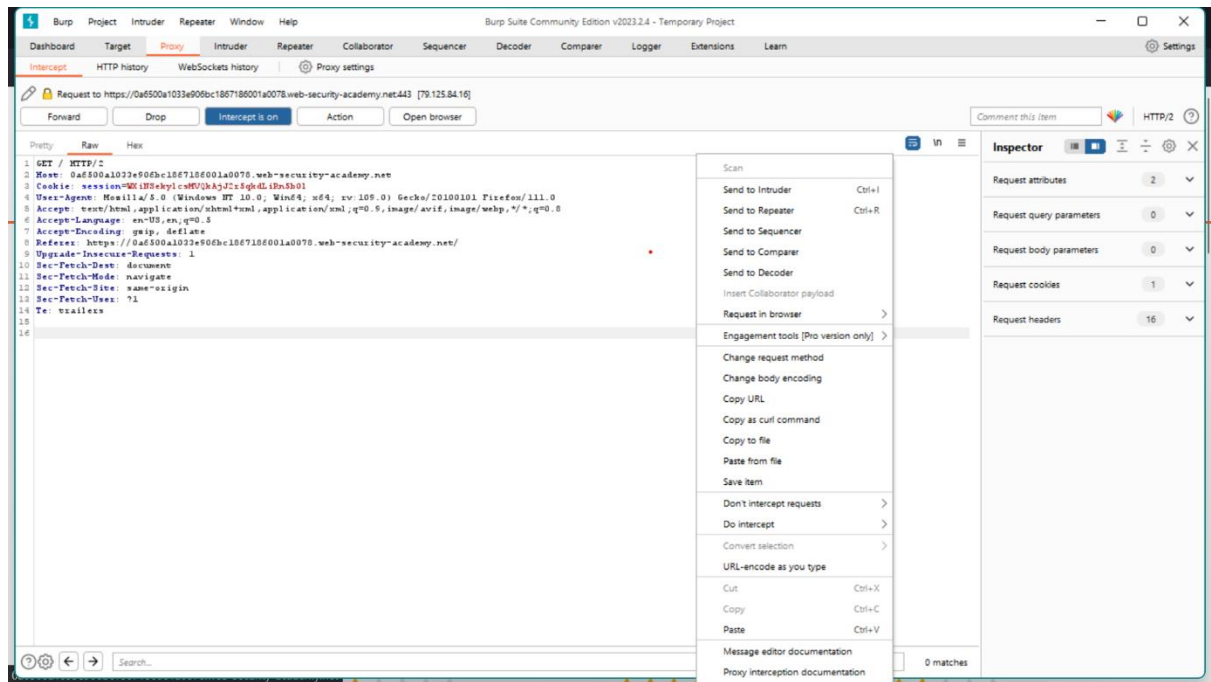
Solve the lab by accessing the admin panel, and using it to delete the user, Carlos.

Solution:

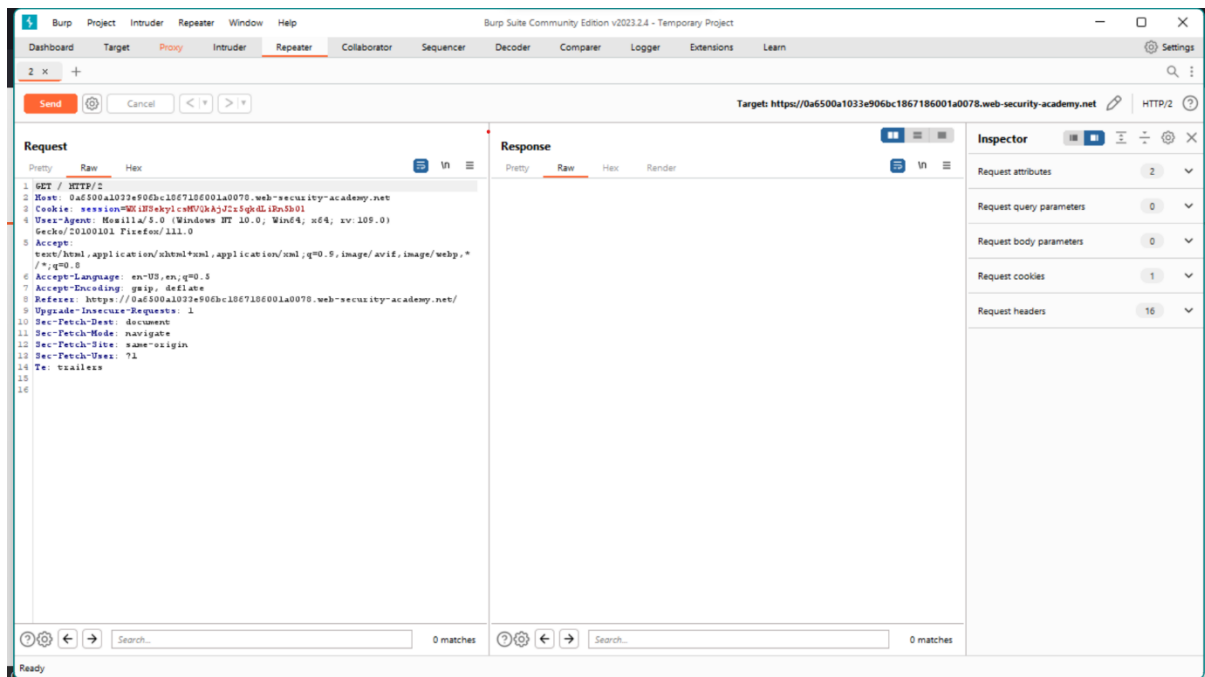
- Once the lab is accessed, turn on the proxy and keep intercept on in the burp suite.
- Refresh the page and when the warning is received, click on accept the risk and continue to give the burp suite the necessary privileges.



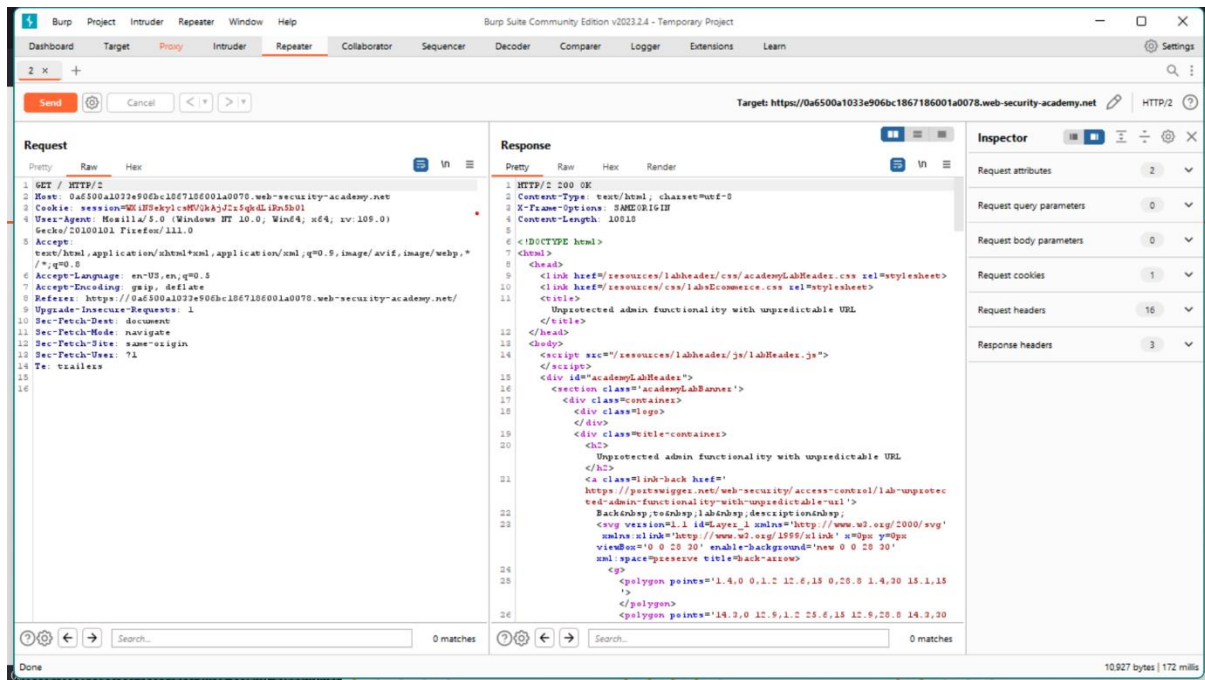
- Click on the home button and you will see that the packets will start getting captured on the burp suite.



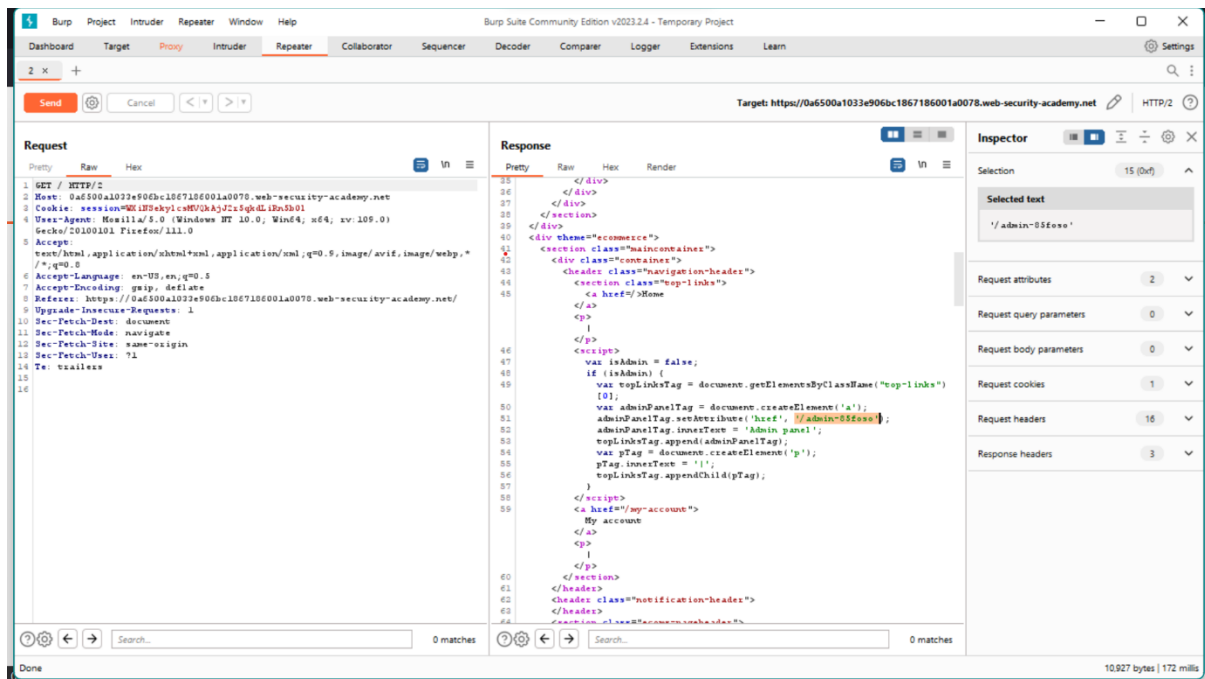
- In your burp suite send the packets to the burp repeater by right clicking on the packet and selecting the option send to repeater.
- The burp repeater can be thought of like a playground. You can test out different requests and analyze the predicted responses that may be received from the server.



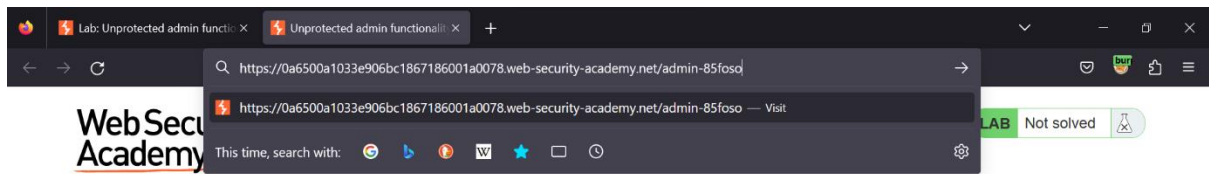
- Open the repeater and you'll see that the packet is present there. Click on send to view the predicted response from the server.



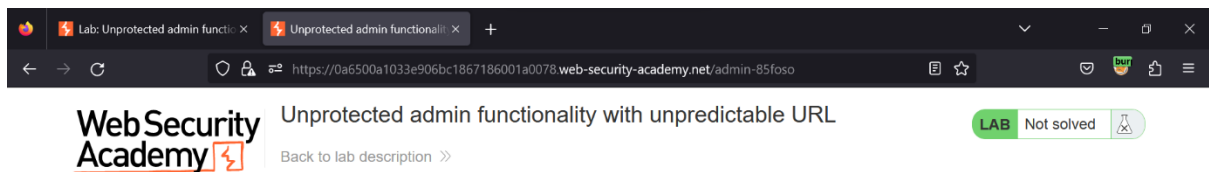
- You will notice a HTML code will be shown. You need to analyze this code to find a script in which there will be a URL tag of the admin panel.



- Once you find the specifics, copy it. You can close the intercept and proxy on the browser now.
- Append the copied code to the URL.



- Submit the URL and you will notice that the admin panel will be opened.



- Refresh the browser and your lab should be solved.

3. User role controlled by request parameter.

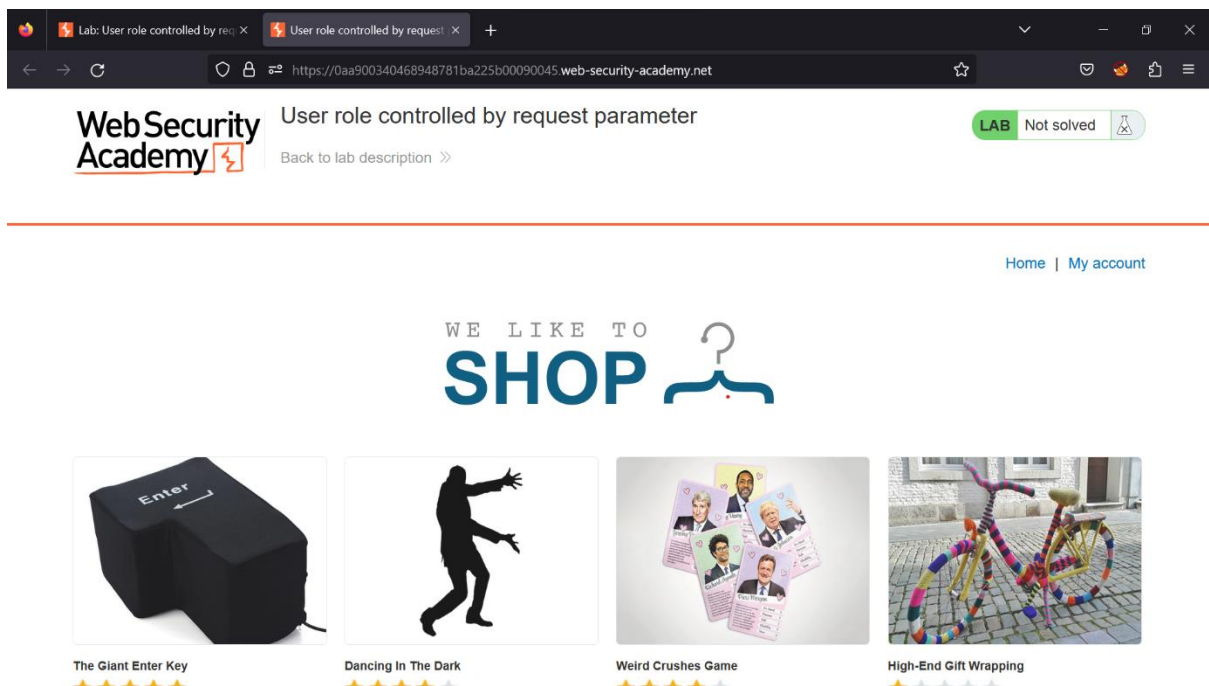
This lab has an admin panel at /admin, which identifies administrators using a forgeable cookie.

Solve the lab by accessing the admin panel and using it to delete the user, Carlos.

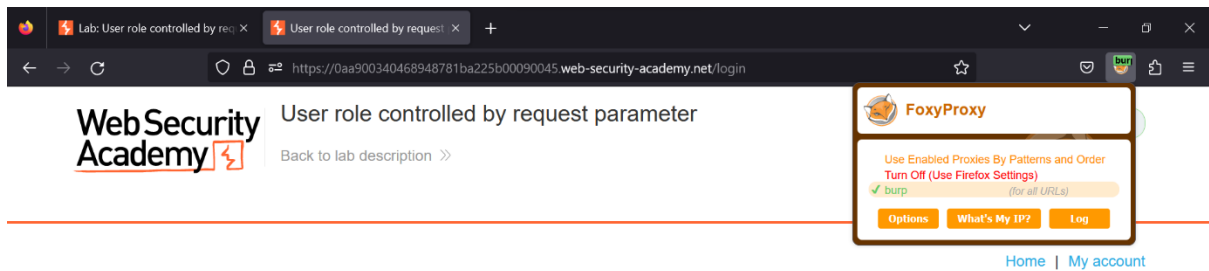
You can log in to your own account using the following credentials: wiener: peter

Solution:

- Once you access the lab, you will see my account option on the right side of the screen. Click on it.



- You will see that a login form will appear. At this step turn on your foxy proxy and turn on the intercept on the burp suite.



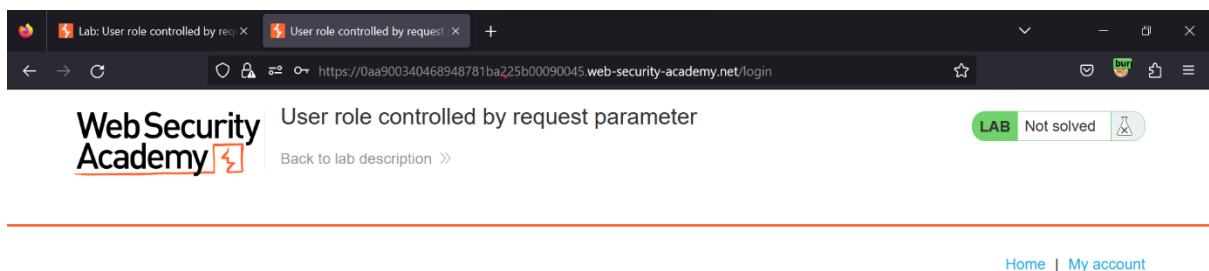
Login

Username

Password

Log in

- Enter your credentials that are given in the problem statement and click on log in.



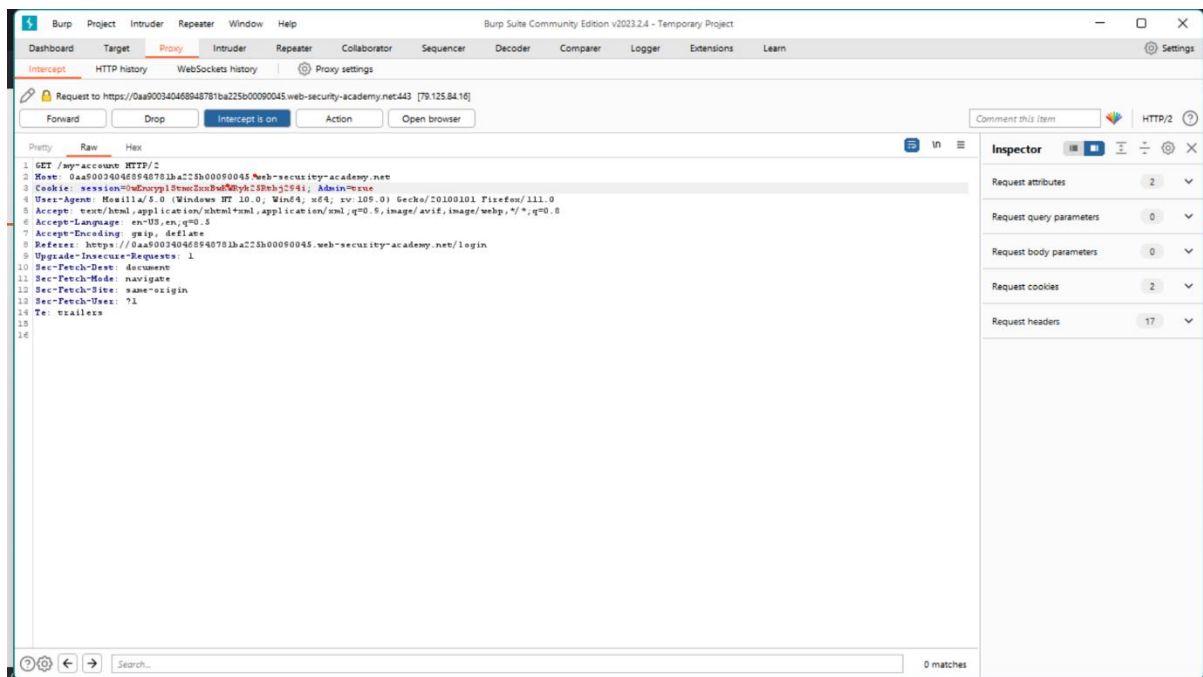
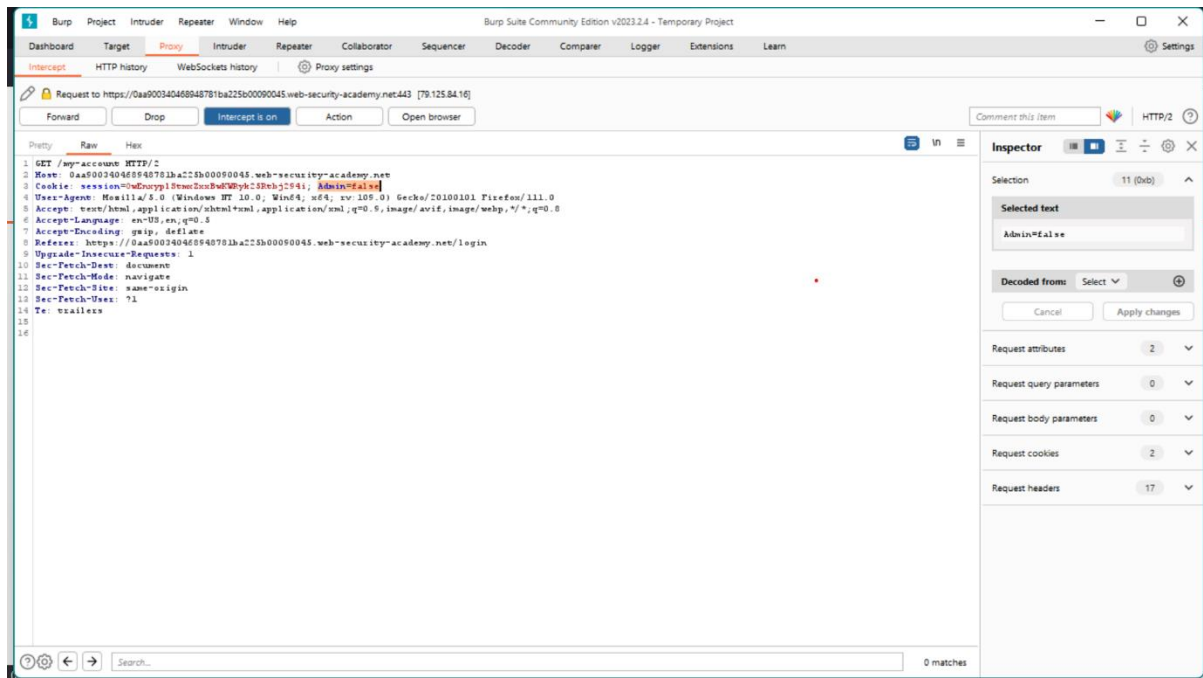
Login

Username

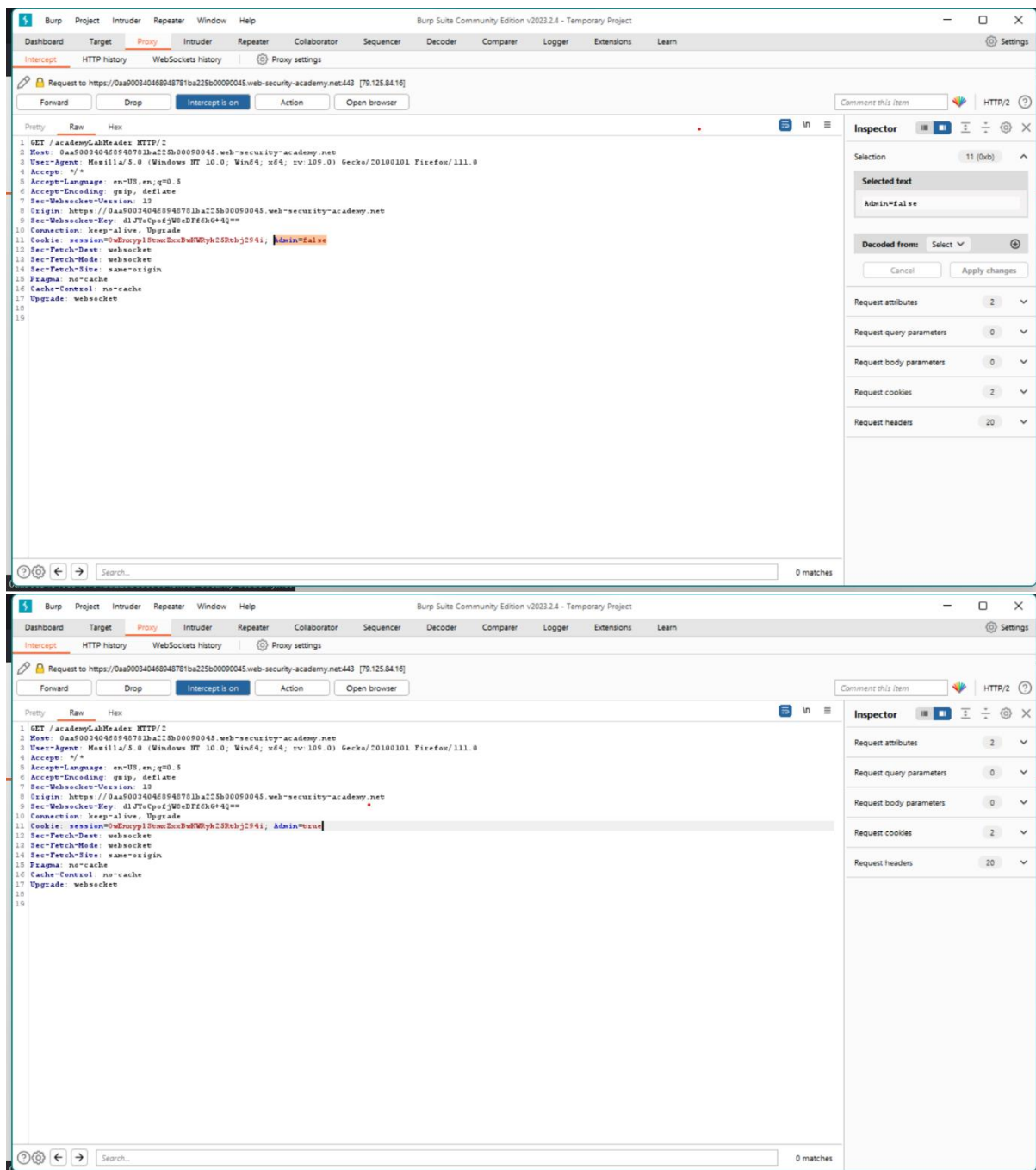
Password

Log in



- As burp suite is on, all the request packets will be captured on the tool. Notice that almost every packet hence forth will have an admin parameter in it. You need to analyze each and every packet so that you do not miss this parameter.
- This parameter is what defines whether to give the user admin privileges or not.
- You will need to change the value of admin in every packet from false to true.



- You may analyze and see that the admin parameter may be located at different locations in the packet hence make sure the analysis is done properly.



- You will notice that once the changes have been made and the packets have been forwarded, you will find an admin panel on my account page of wiener.
- Once you click on it you will again have to forward all the packets after making the change of admin parameter from false to true.
- After forwarding all the packets you will see that you are given the privileges to delete the users accounts.

WebSecurity Academy  User role controlled by request parameter LAB Not solved 

[Back to lab description >>](#)

Users

wiener - [Delete](#)
carlos - [Delete](#)

[Home](#) | [Admin panel](#) | [My account](#)

0aa900340468948781ba225b00090045.web-security-academy.net

- Go ahead and delete the Carlos account.
- You will again have to change the value of admin in each packet until all packets have been forwarded.
- Close foxy proxy and refresh the page and you'll see that the lab has been solved.

4. User role can be modified in user profile.

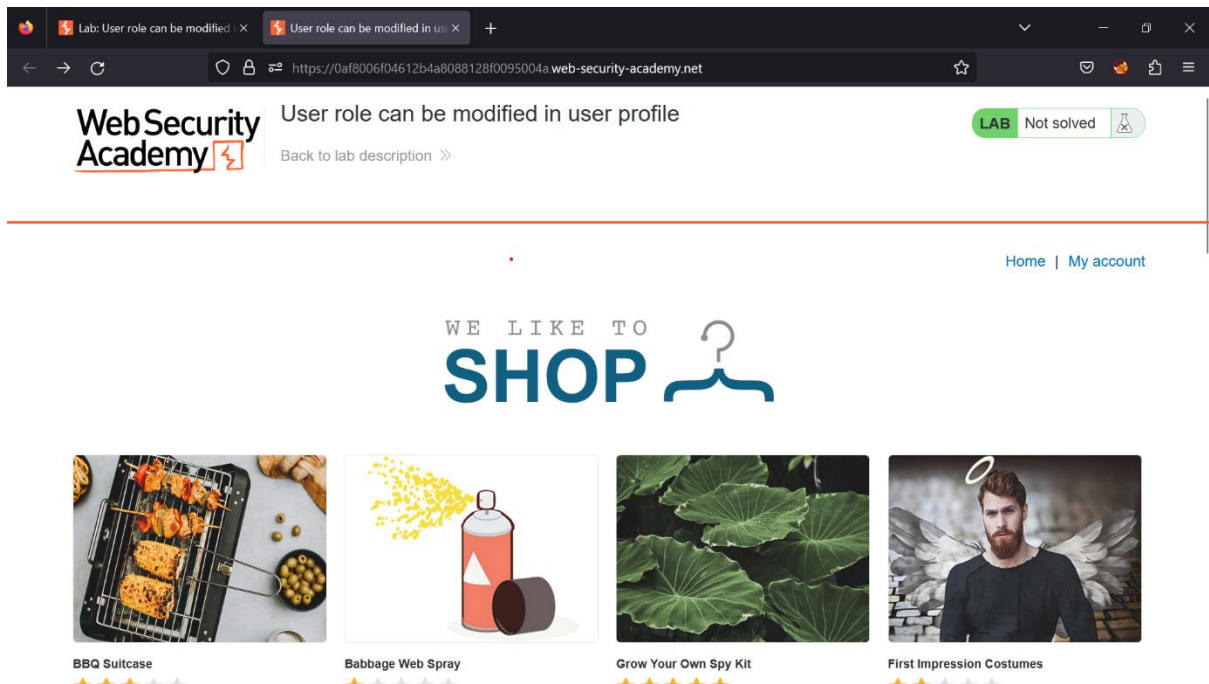
This lab has an admin panel at /admin. It's only accessible to logged-in users with a roleid of 2.

Solve the lab by accessing the admin panel and using it to delete the user carlos.

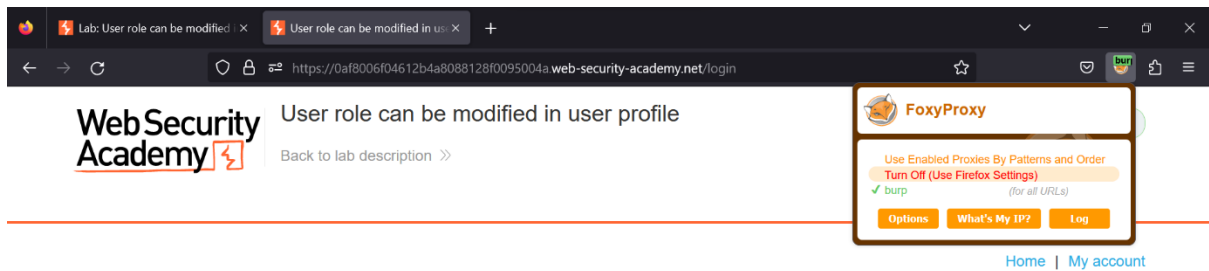
You can log in to your own account using the following credentials: wiener:peter.

Solution:

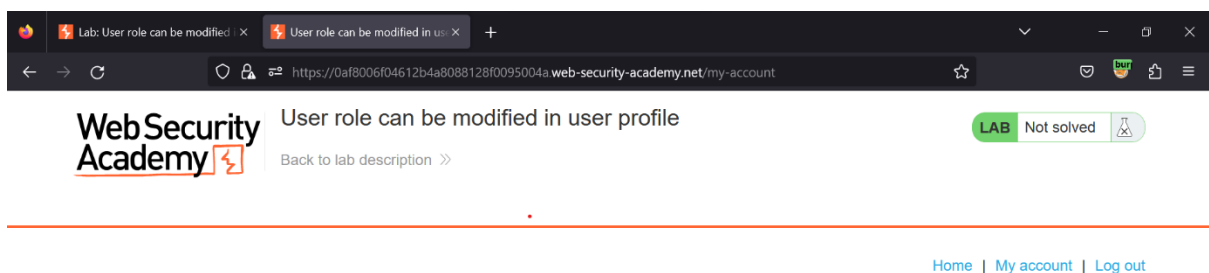
- Once you access the lab click on the my account option on the right side.



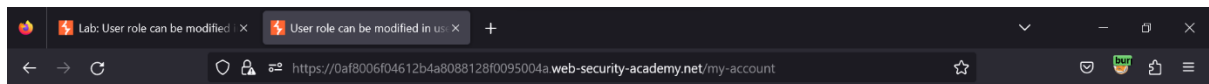
- You will be redirected to a login form. Turn on your foxy proxy and intercept on in the burpsuite.



- Enter the credentials given in the problem statement and click on login. You will be at the account page.



- Type a random email address in the text field and click on update email.



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: wiener

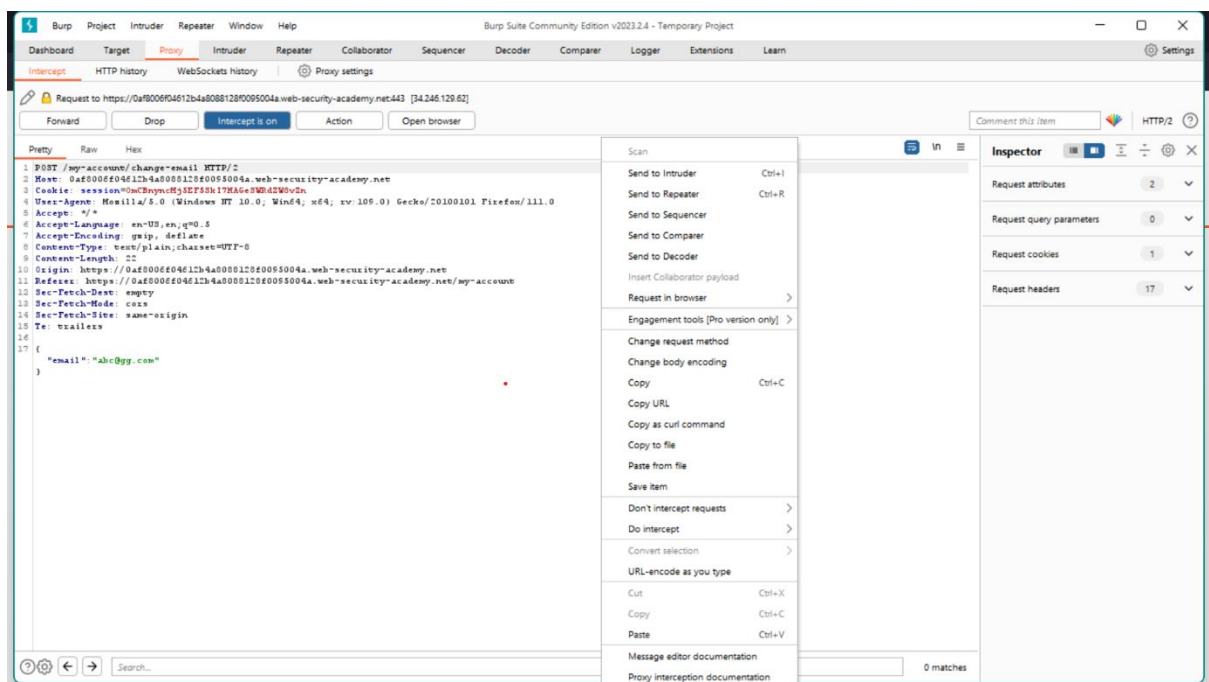
Your email is: wiener@normal-user.net

Email

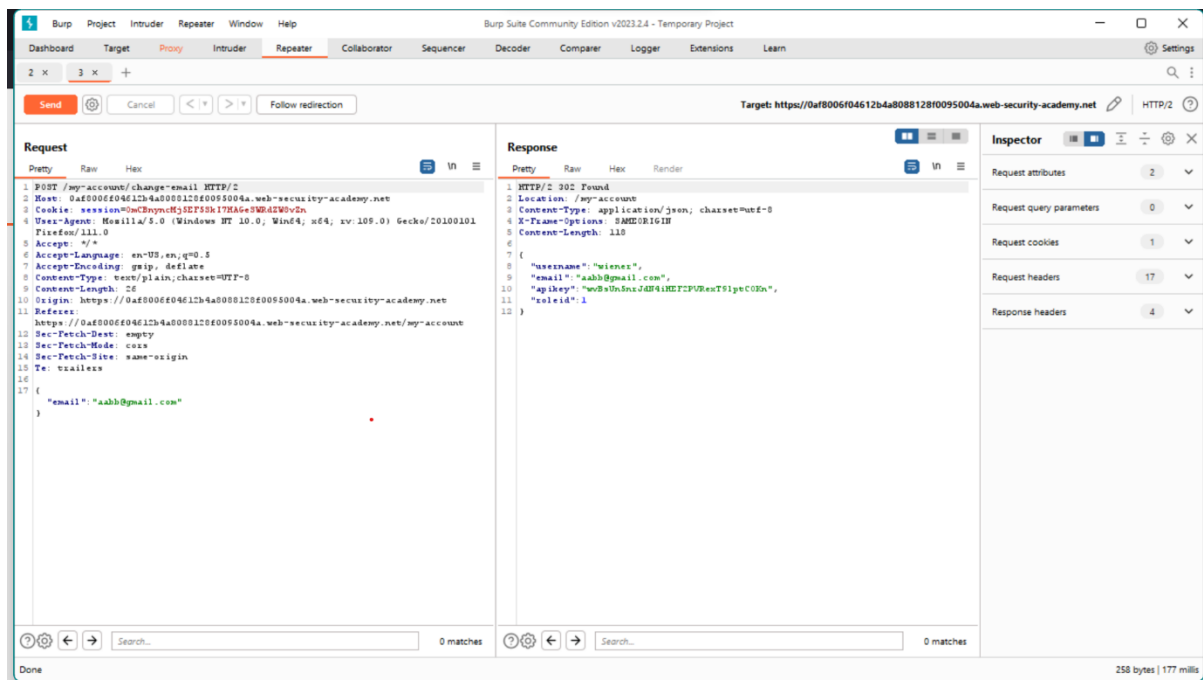
abc@gg.com

Update email

- Open your burpsuite and analyze the packets. You will see that there is a JSON part in the request on one of the packets. Send that packet to the repeater.

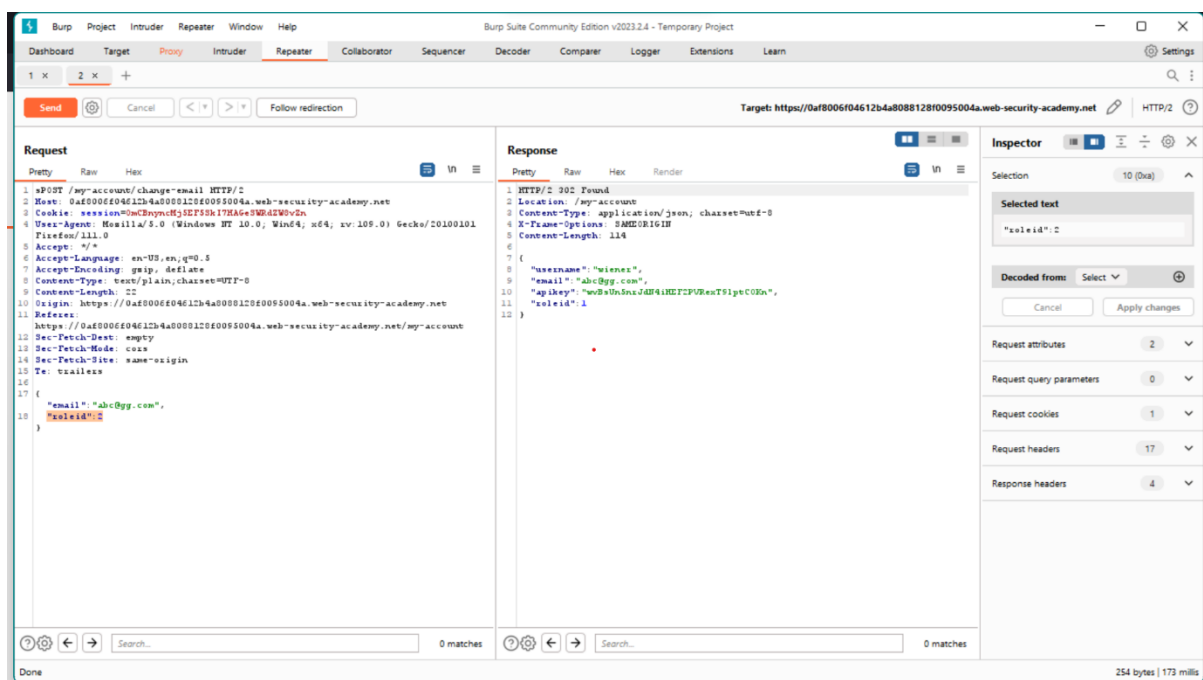


- Once you send the packet to the repeater, click on send and analyze the response.

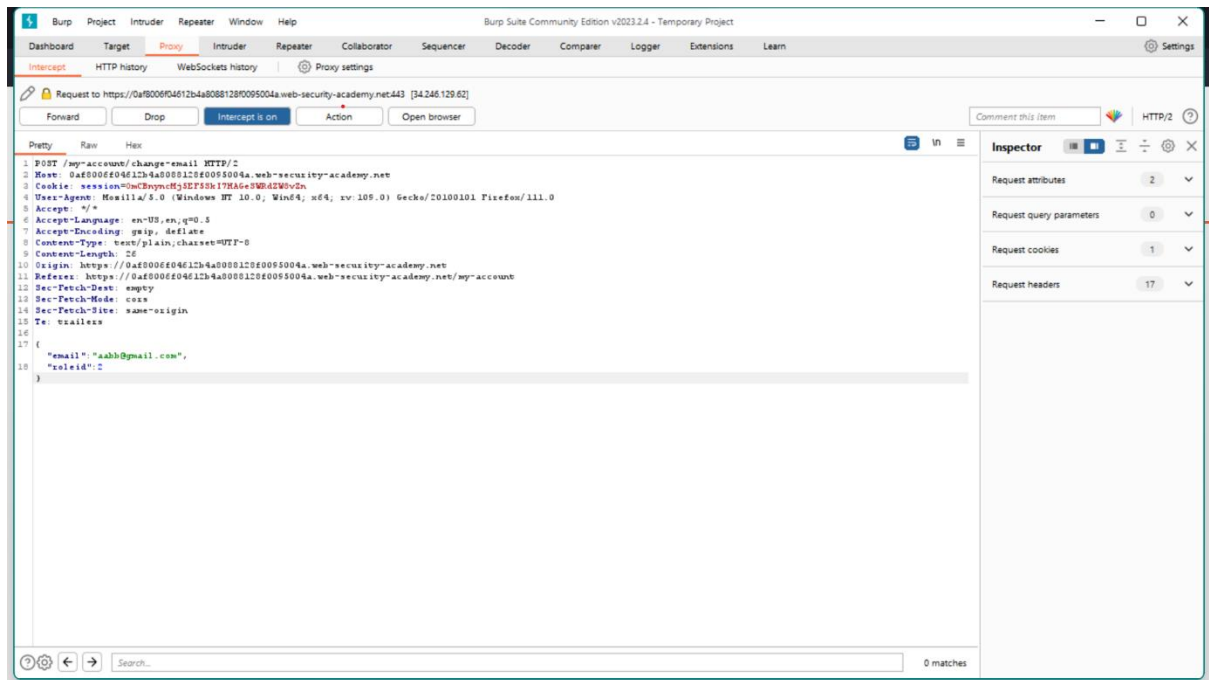


- The response will contain several parameters, one of them being a roleid.
- You need to change the value of roleid from 1 to 2.
- On the request side type the following in the JSON part:

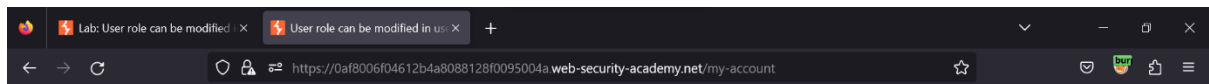
“roleid”:2



- Analyze the response and see that the parameter value has changed.
- Go to the proxy tab and make the similar changes in the packet and forward the packets.



- Open the browser and you'll notice that there is an admin panel present now. Click on the admin panel and delete carlos.



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [Admin panel](#) | [My account](#) | [Log out](#)

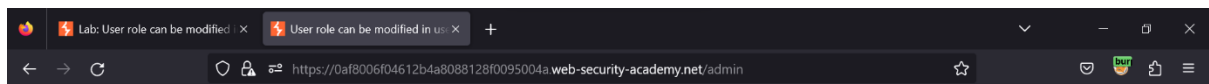
My Account

Your username is: wiener

Your email is: aabb@gmail.com

Email

Update email



User role can be modified in user profile

[Back to lab description >>](#)

LAB Not solved

[Home](#) | [Admin panel](#) | [My account](#)

Users

wiener - [Delete](#)

carlos - [Delete](#)

- Once the account is deleted, your lab will be solved.

5. User ID controlled by request parameter, with unpredictable user IDs.

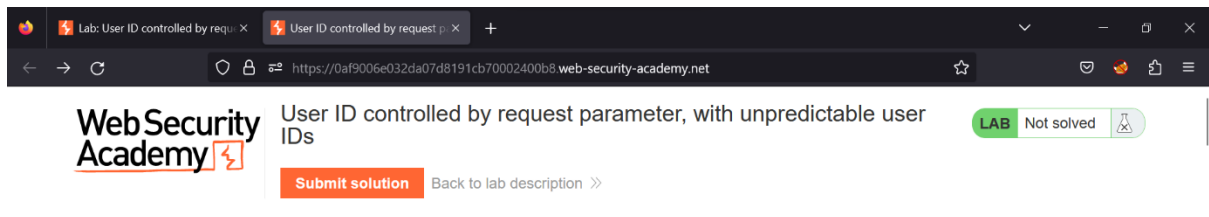
This lab has a horizontal privilege escalation vulnerability on the user account page, but identifies users with GUIDs.

To solve the lab, find the GUID for Carlos, then submit his API key as the solution.

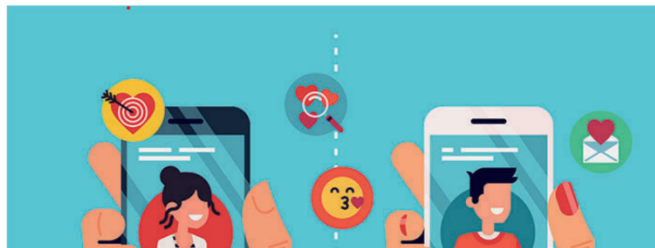
You can log in to your own account using the following credentials: wiener: peter.

Solution:

- This lab contains that is related to blogs. You need to go through every blog to see which blog has Carlos as the author.



WE LIKE TO
BLOG 



- Once you find a blog who's author is Carlos, click on the author's name.



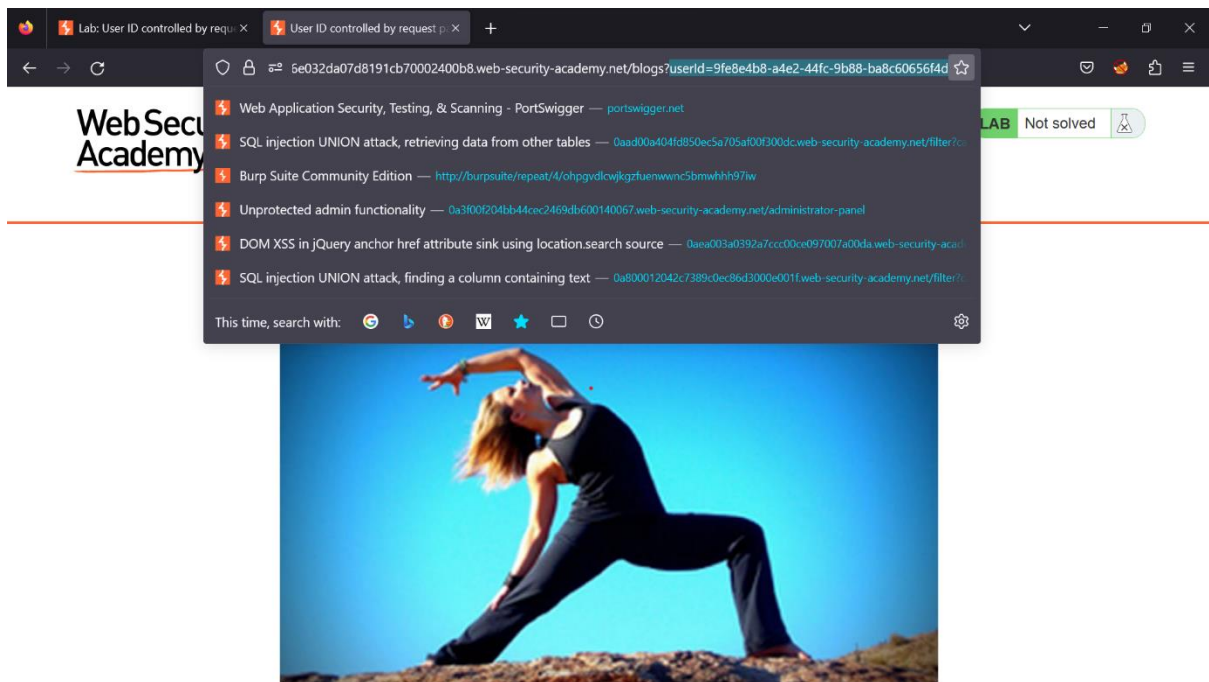
Awkward Breakups

carlos | 10 March 2023

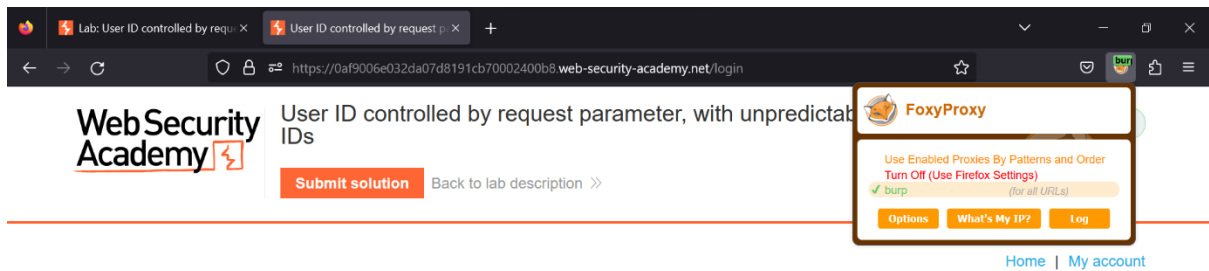
'Tis better to have loved and lost than to never to have loved at all? A beautiful thought, but maybe Tennyson never had to go around his ex's house to collect his parchment and quills after an awkward break up. I concede there are amicable breakups where both parties mutually agree that they're better off apart. But the real headline makers are the ones that are like pulling teeth. Returning possessions, angry messages and probably worst of all - finances.

When it comes to money, settling mortgages and other similar affairs can get very tense. But, after a break up, the real vindictiveness in people can come out. It isn't always the huge financial ties that become a messy business, it's the petty ones. Perhaps you're after some debt that's owed, you send a polite message requesting that said ex returns the funds at their earliest convenience, but you get a itemised bill in response. 'Well, don't forget I drove you about or that sandwich I bought you last year.' Suddenly every tiny transaction can come back to haunt you. Pettiness can

- Analyze the URL next. You will see that it contains the user id of Carlos.
- Copy the userid and save it for future use.



- Click on my account and enable foxy proxy and intercept on the burp suite.



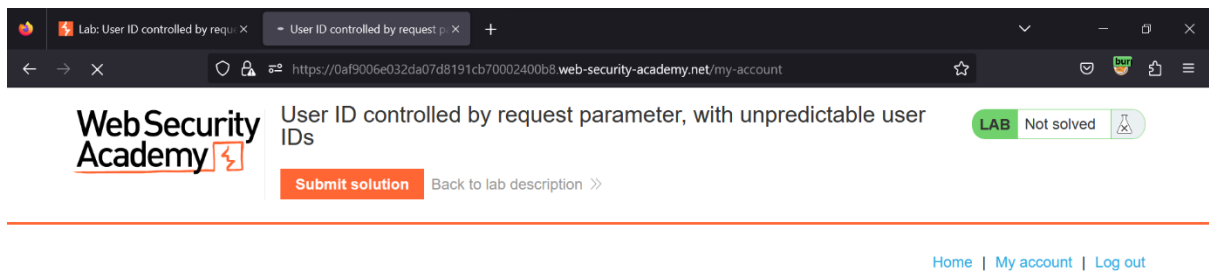
Login

Username

Password

[Log in](#)

- Enter your credentials and login. You'll then be on your account page.



My Account

Your username is: wiener

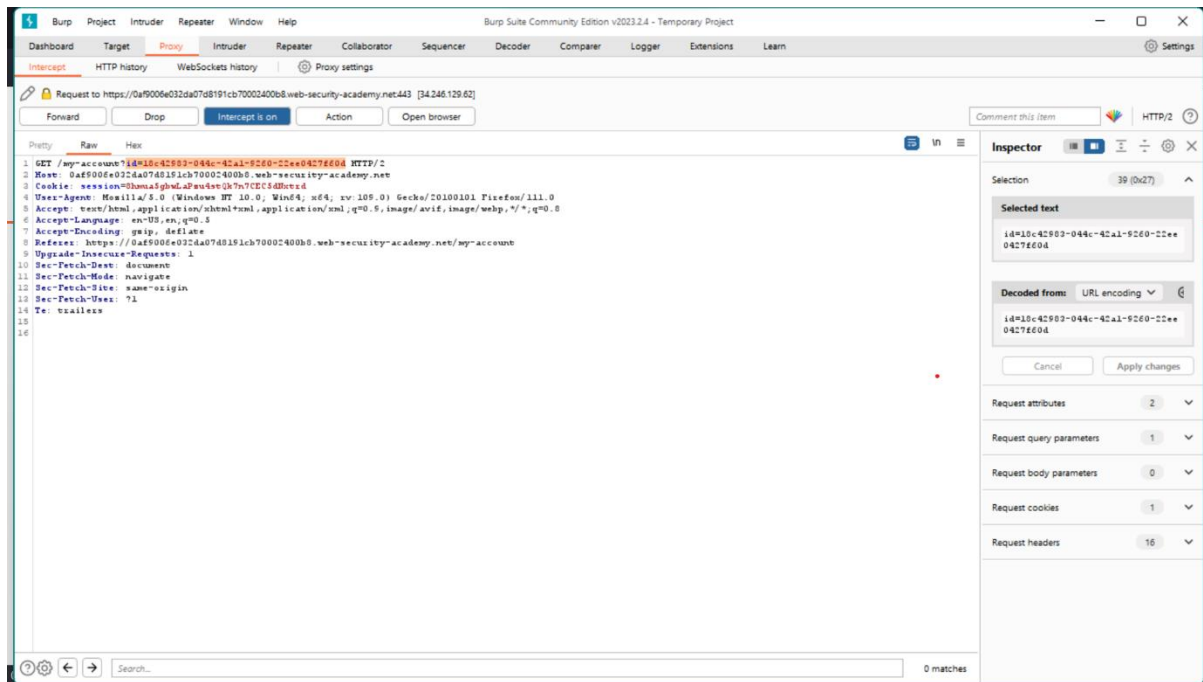
Your API Key is: 8MM0mhQKC92tJ7J3IWKMkfVKIsoWR3Hg

Email

[Update email](#)

0af9006e032da07d8191cb70002400b8.web-security-academy.net

- Click on my account option and open burp suite to analyze the packet.
- You will notice that the packet will contain a parameter named id which will contain the value referring to wiener's account.
- You'll need to change the value of id to Carlos's id that we copied from the URL.



- Once you forward all the packets, you'll notice that you'll be logged in as Carlos.
- Copy the API key then and paste it in the solution. Your lab will be solved.

The rest of the labs of this topic have similar method to complete the lab. Practice the burp repeater to understand further concepts.