Access control vulnerabilities.

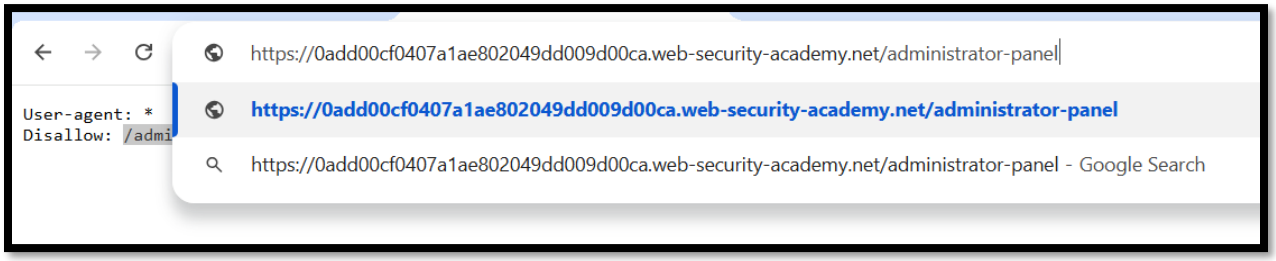
Lab 1

Unprotected admin functionality.

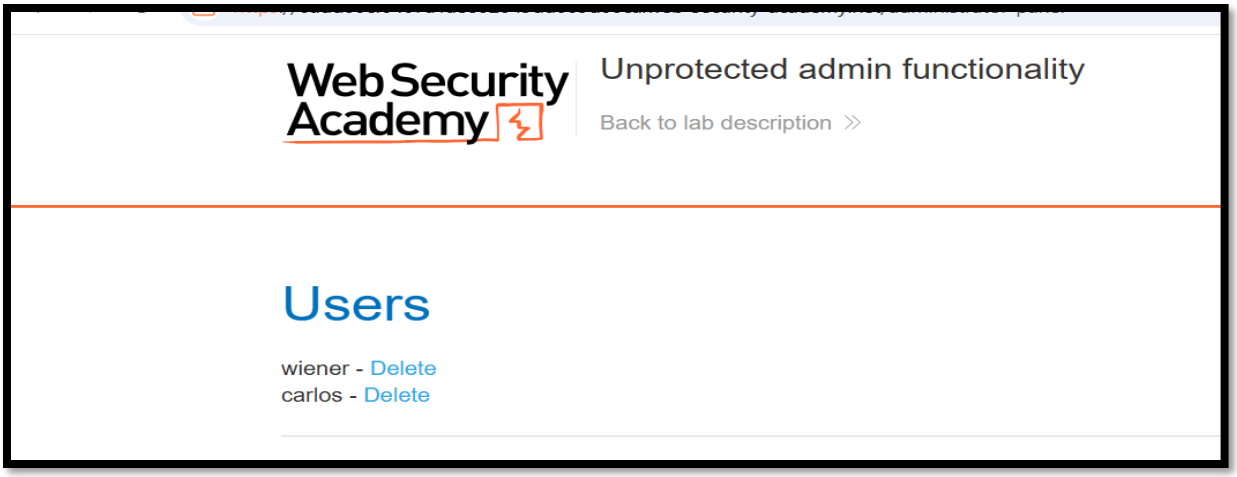
To solve this lab, all we need to do is simply delete the user named Carlos.

We can inject robots.txt to the URL to view the users.

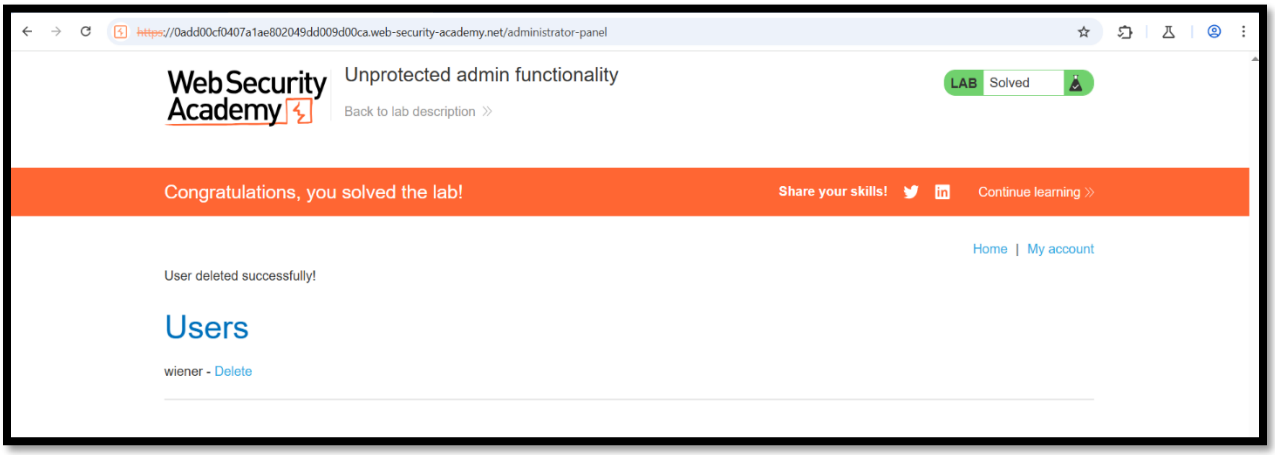
It shows us the path to the administrator panel.



Replace robots.txt with the disallowed parameter.



And finally delete the user carlos.



The lab is solved.

Lab 2

Unprotected admin functionality with unpredictable URL.

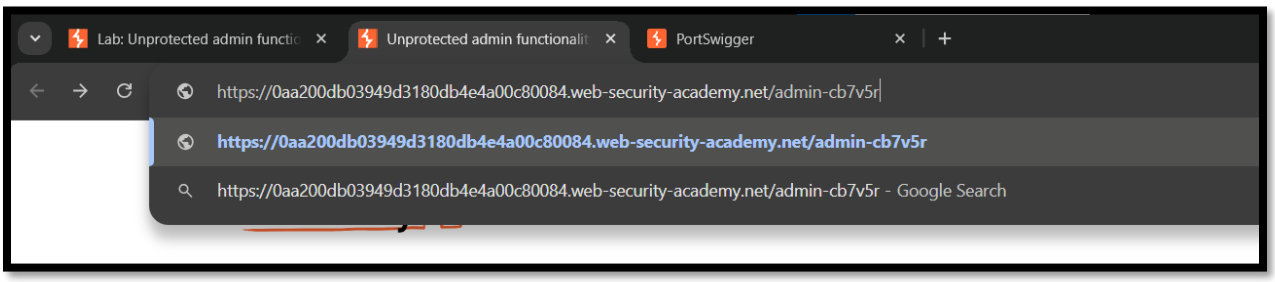
To solve this lab, we must delete the user carlos, again.

However, we don’t know where the admin panel is.

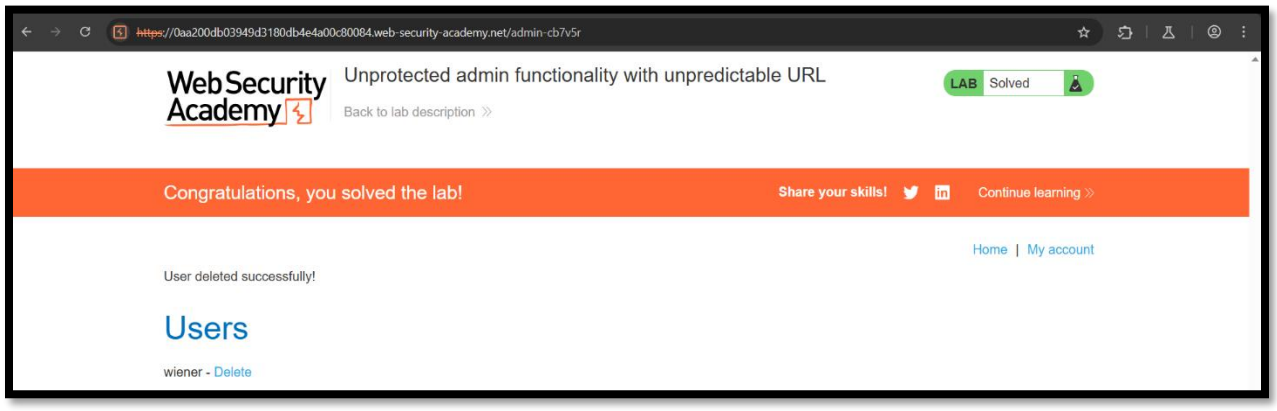
To find it, we can view the page source of the homepage of the lab.

```
                        <script>
var isAdmin = false;
if (isAdmin) {
   var topLinksTag = document.getElementsByClassName("top-links")[0];
   var adminPanelTag = document.createElement('a');
   adminPanelTag.setAttribute('href', '/admin-cb7v5r');
   adminPanelTag.innerText = 'Admin panel';
   topLinksTag.append(adminPanelTag);
   var pTag = document.createElement('p');
   pTag.innerText = '|';
   topLinksTag.appendChild(pTag);
}
</script>
```

As we can see, the homepage source has some JavaScript code that discloses the URL of the admin panel.
inject that into the lab URL.

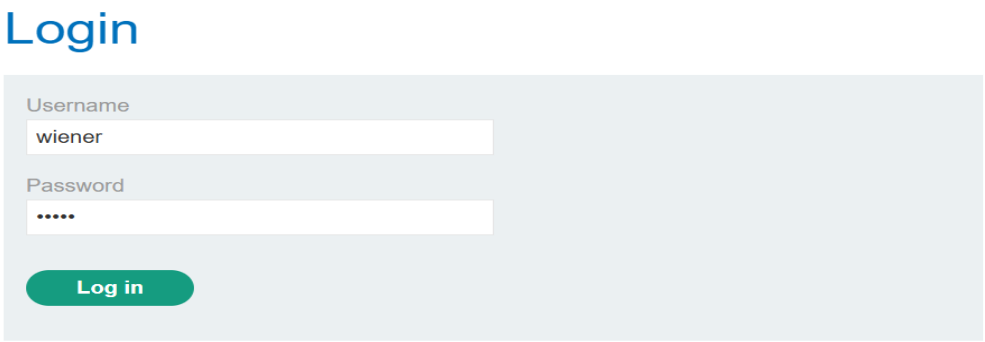


After that we can access the admin panel and delete the user carlos.



Lab 3

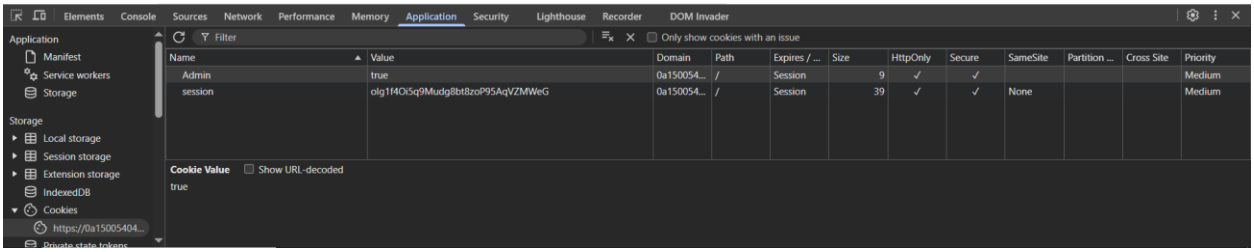
User role controlled by request parameter.

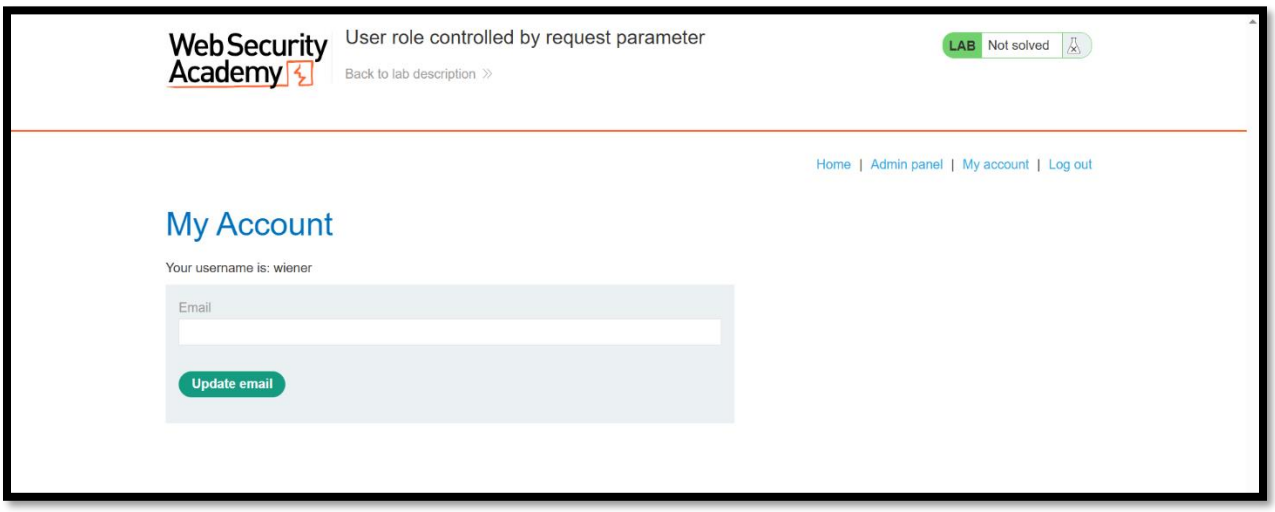


Login to the account using given credentials.

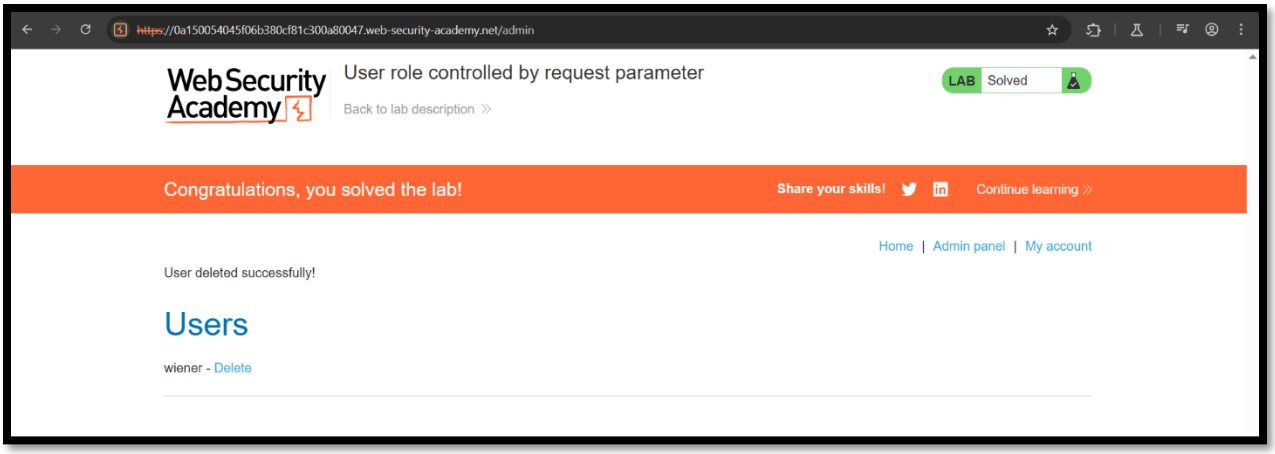
After that inspect the cookies. It is set to Admin=false.

Change it to Admin=true.





now we can see there is an admin panel. Click it and delete user carlos.



The lab is solved.

Lab 4

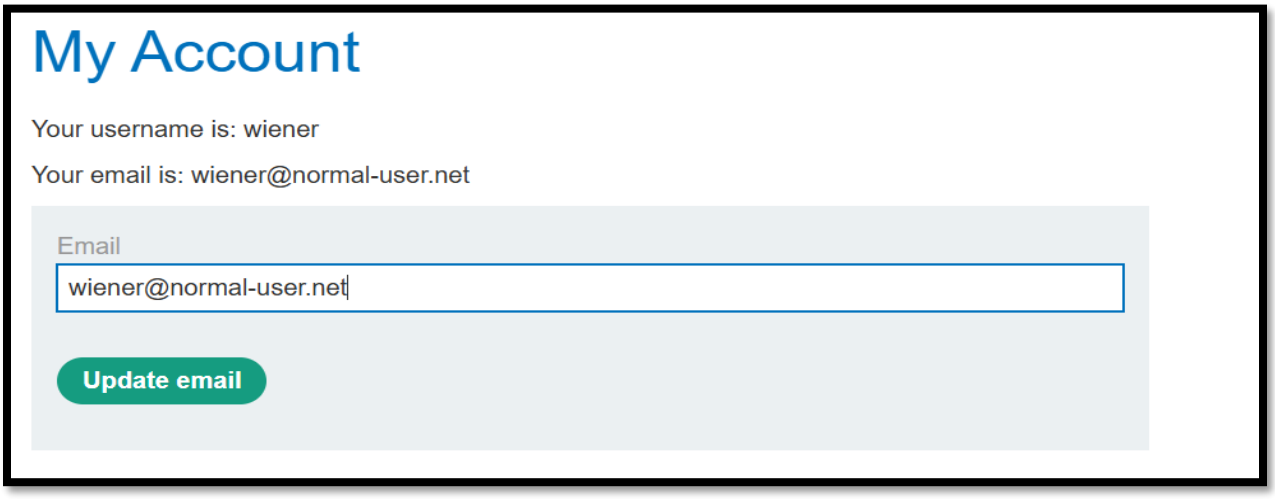
User role can be modified in user profile.

The admin panel is disabled.

It is only accessible to users with the roleid,2.

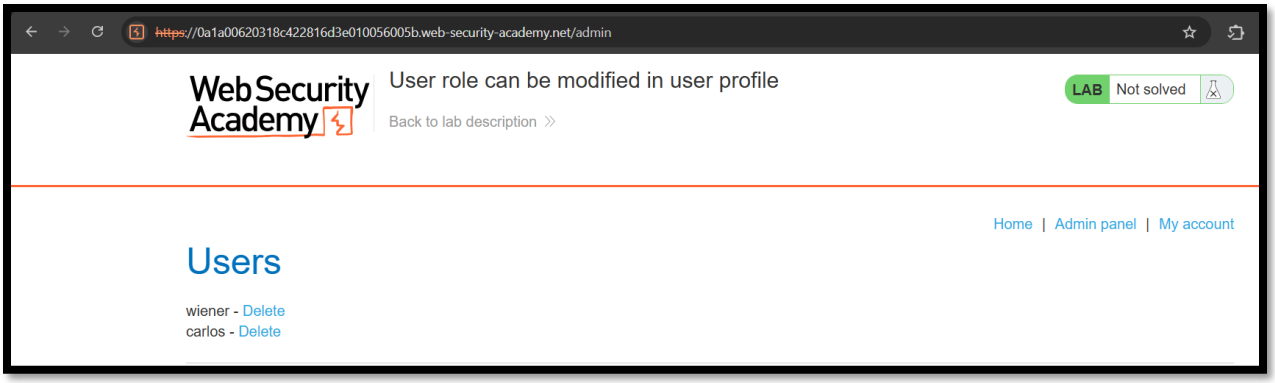
Login to the my account tab using the provided credentials.

Once logged in, use the provided email address to update the email address and capture the request.

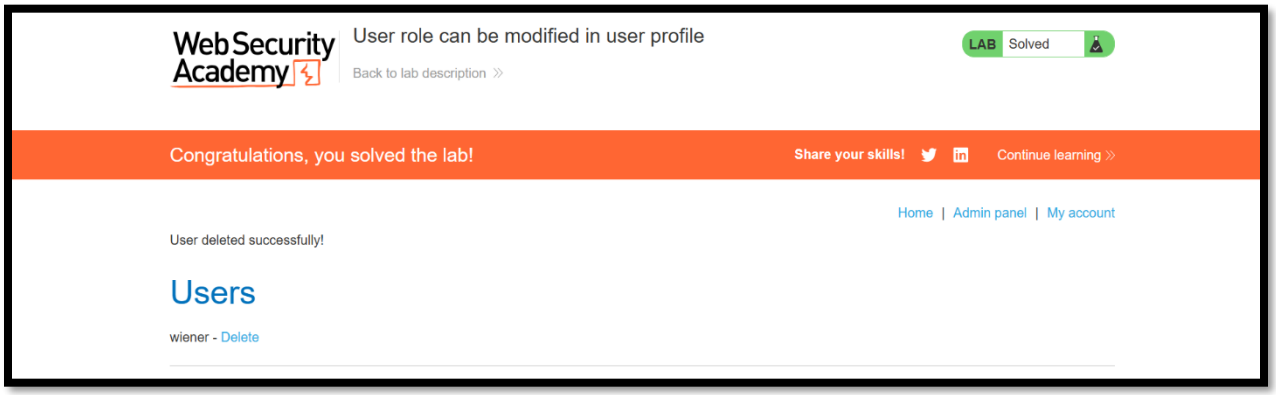


In the captured request, add “roleid”:2 into the JSON part and send it.

Now we should be able to access the admin panel.



Delete user carlos.



Lab 5

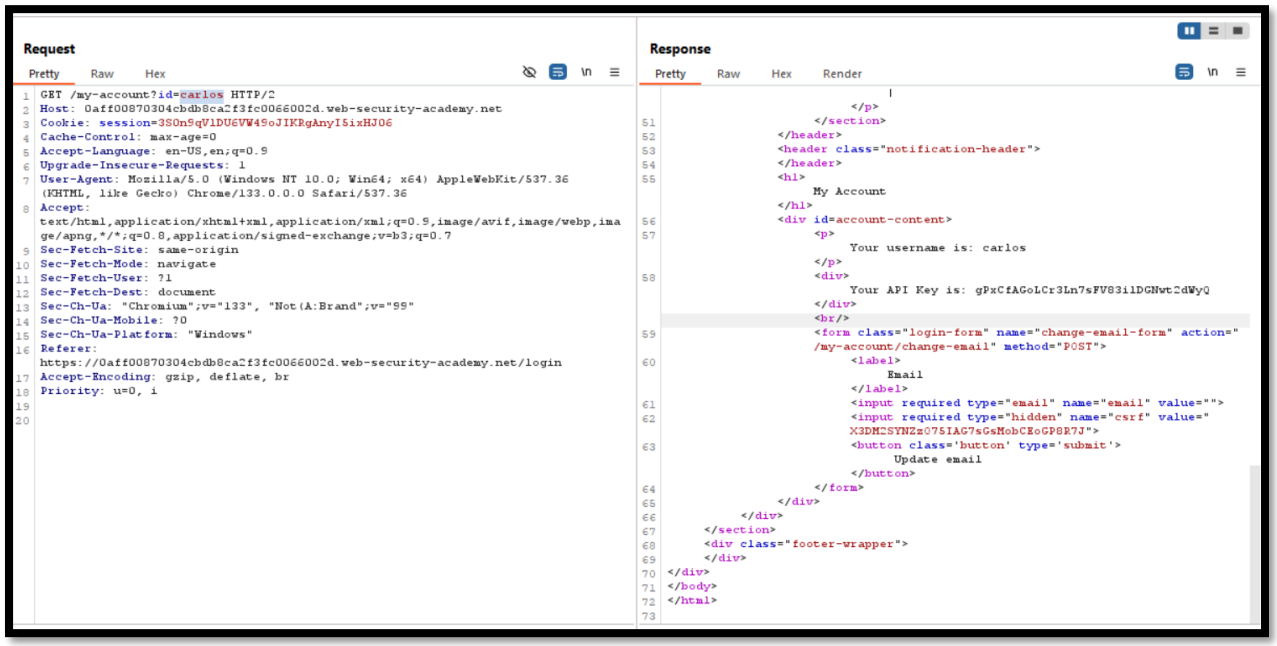
User ID controlled by request parameter.

To solve the lab, we must find API key to the user carlos.

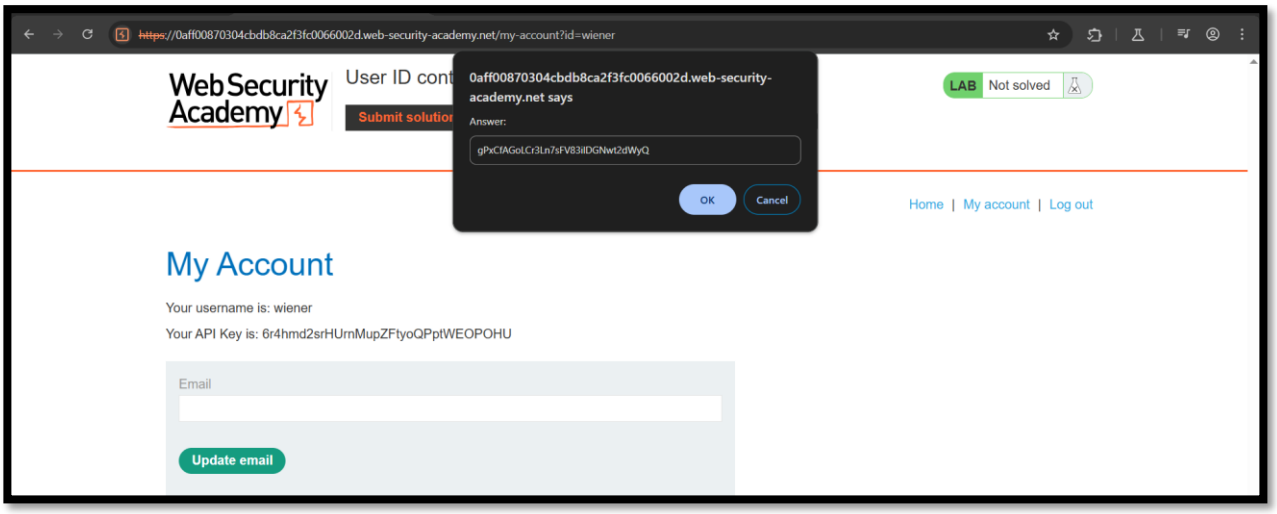
First login using the provided credentials.

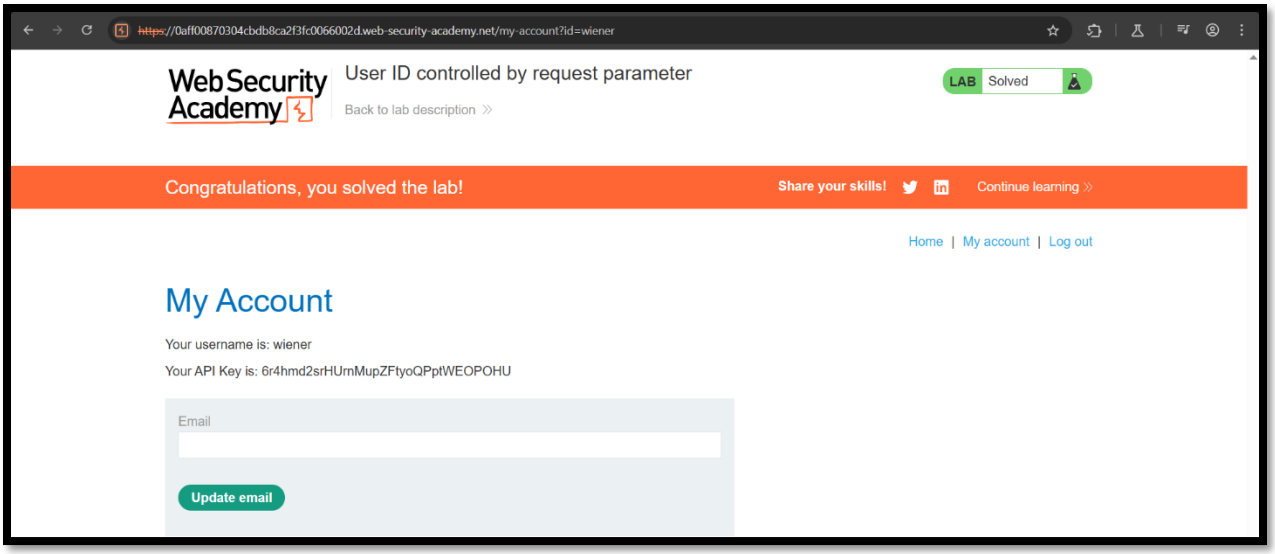
We have the API key for weiner.

After that Change the id parameter to carlos to obtain his API key.



copy and submit the api key.





The lab is solved.

Lab 6

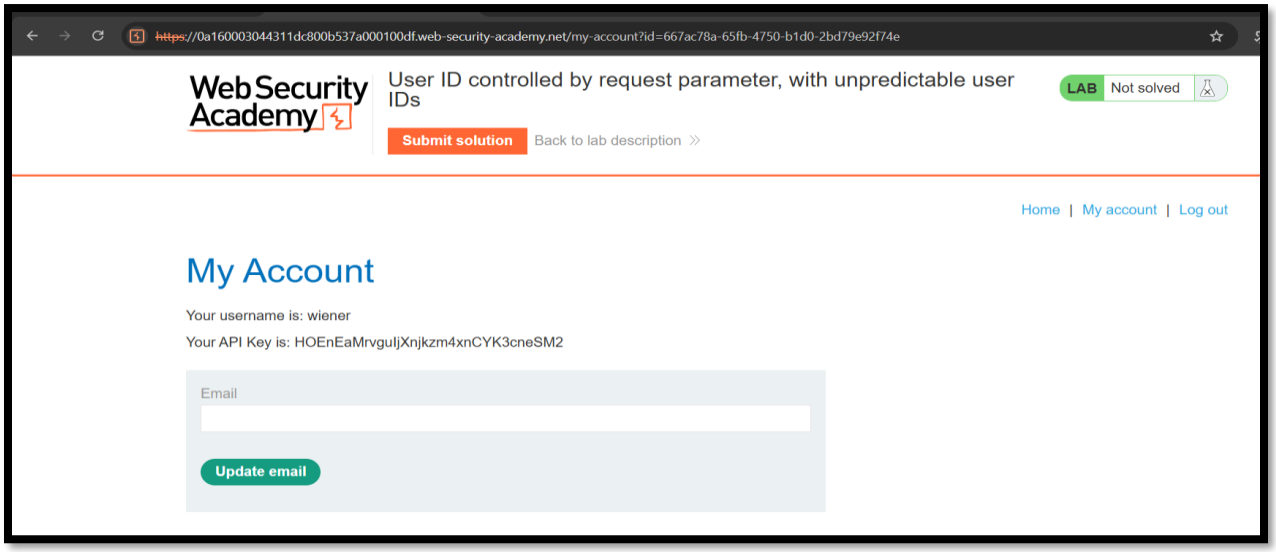
User ID controlled by request parameter, with unpredictable user IDs.

To solve this lab, we must find and submit the API key for the user, Carlos.

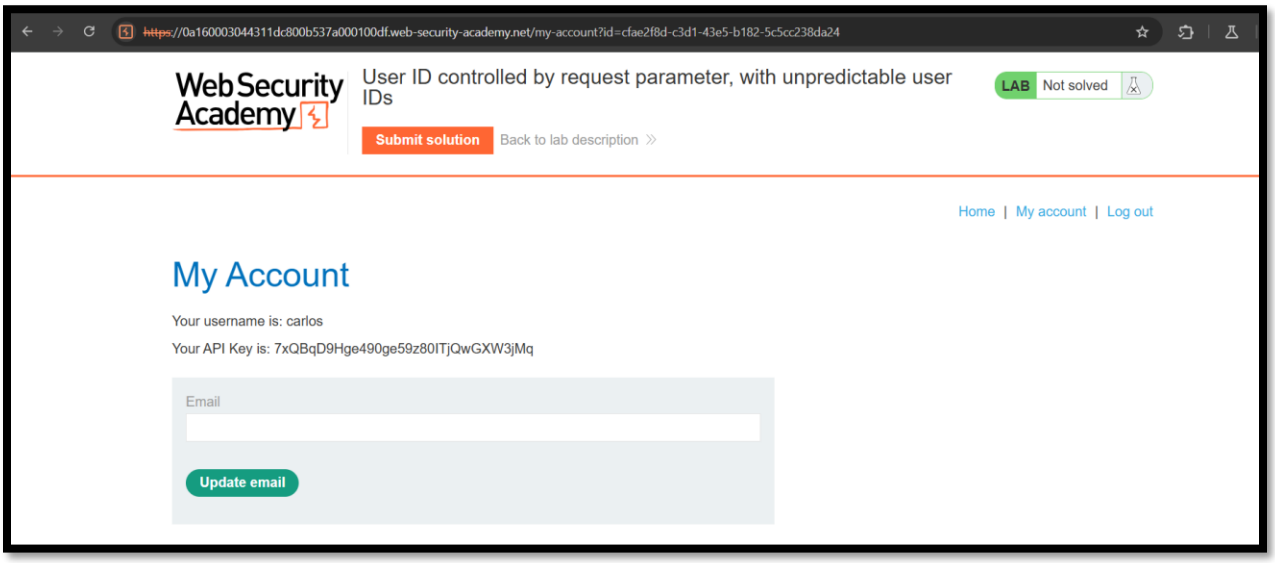
This lab identifies users via GUID's, so first find a blog post by carlos.

We can see that the user id in the URL is list of characters.

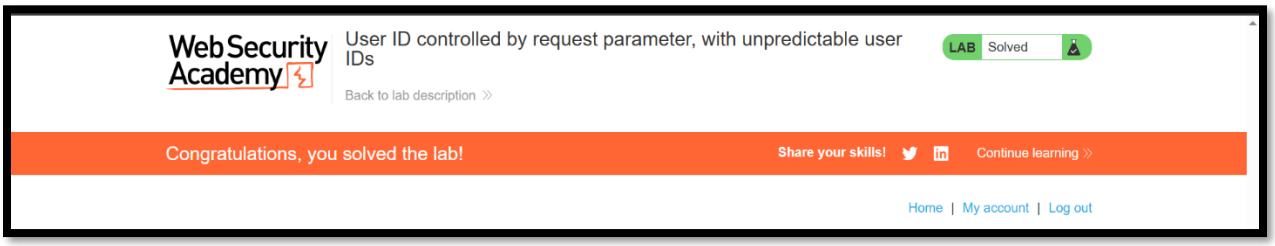
After that,Log into your account with the given credentials.



Change the id parameter in the URL to the one we got from Carlos's blog post.



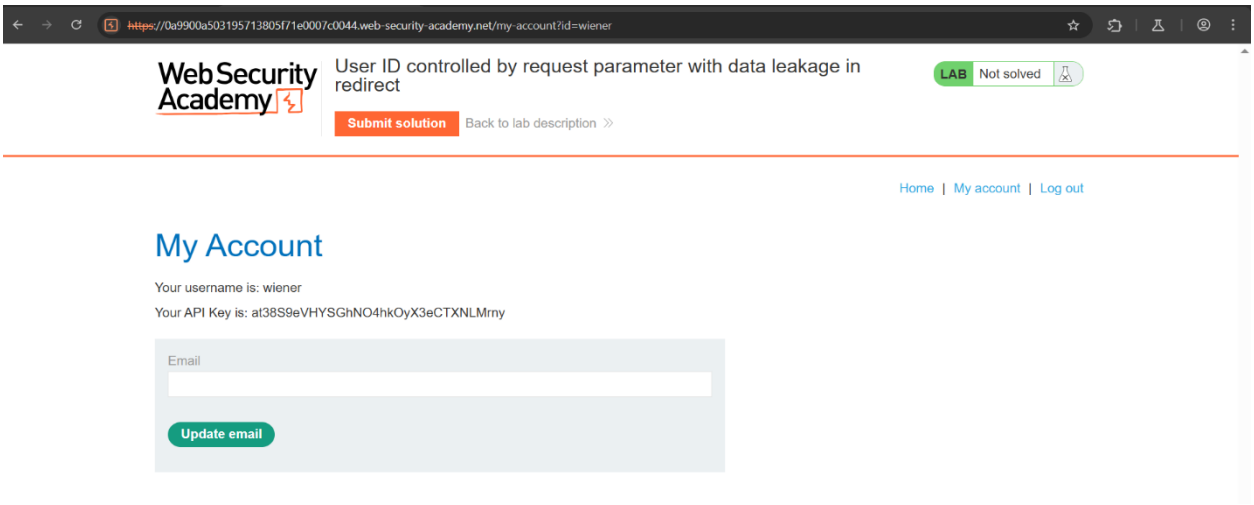
Submit the carlos' API key as the solution.



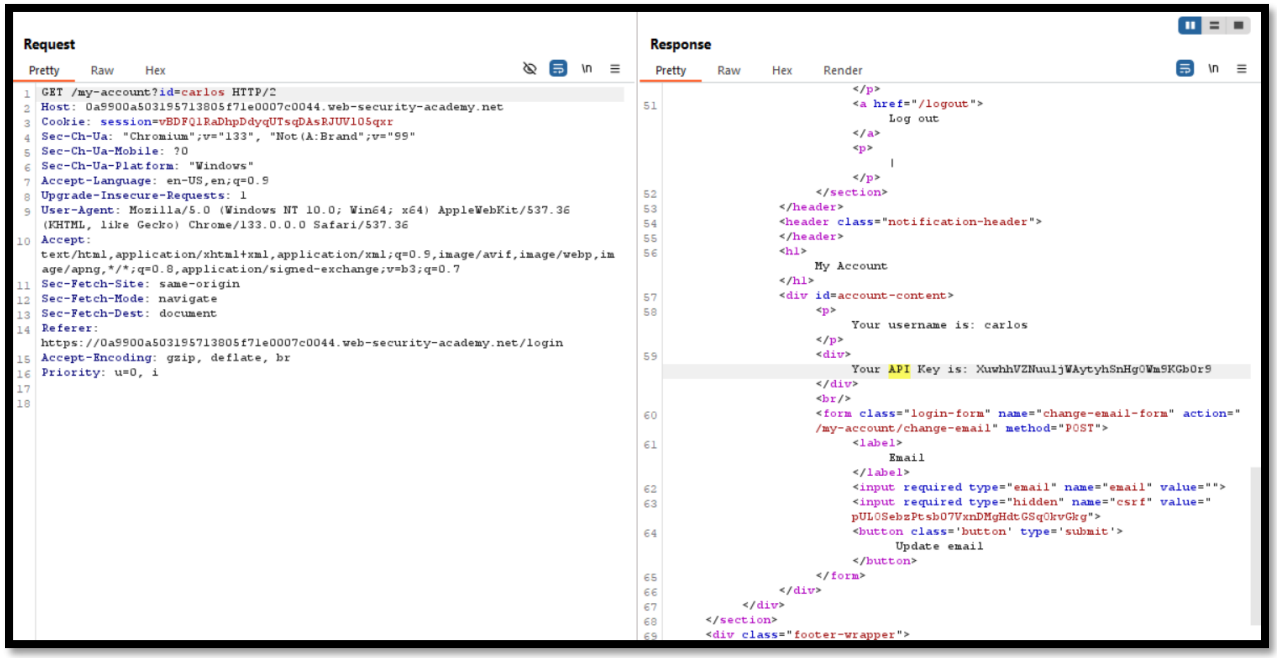
Lab 7

User ID controlled by request parameter with data leakage in redirect.

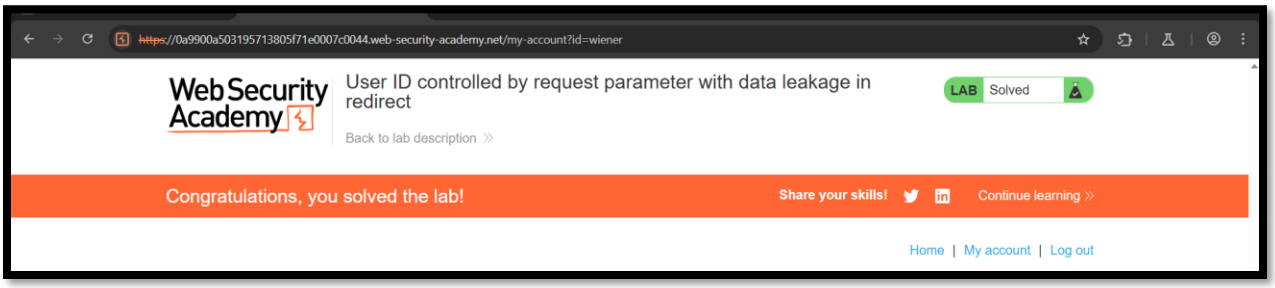
Start off by logging into your account using the given credentials and send the request to burp suite.



Change the id parameter to carlos and send the request.



Submit the API key as the solution.

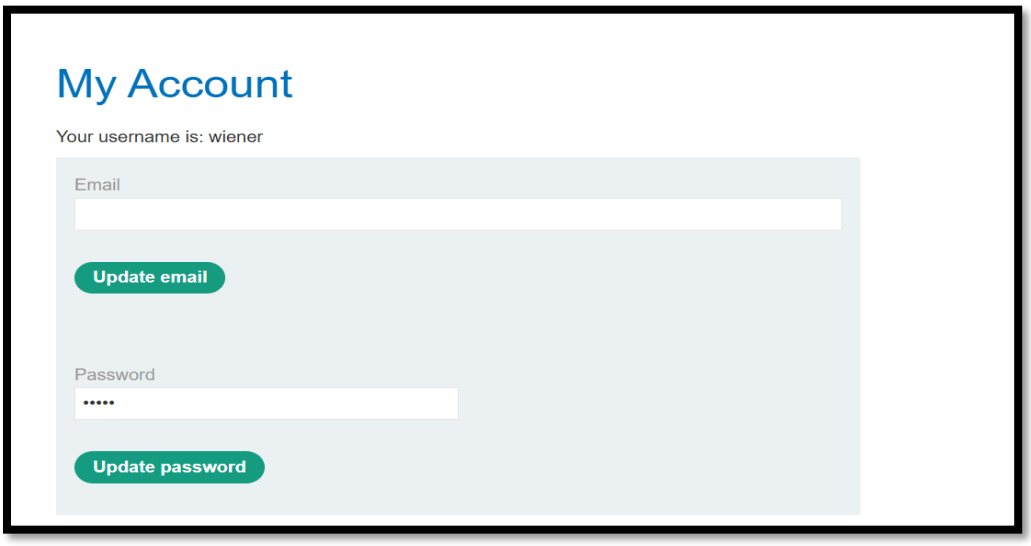


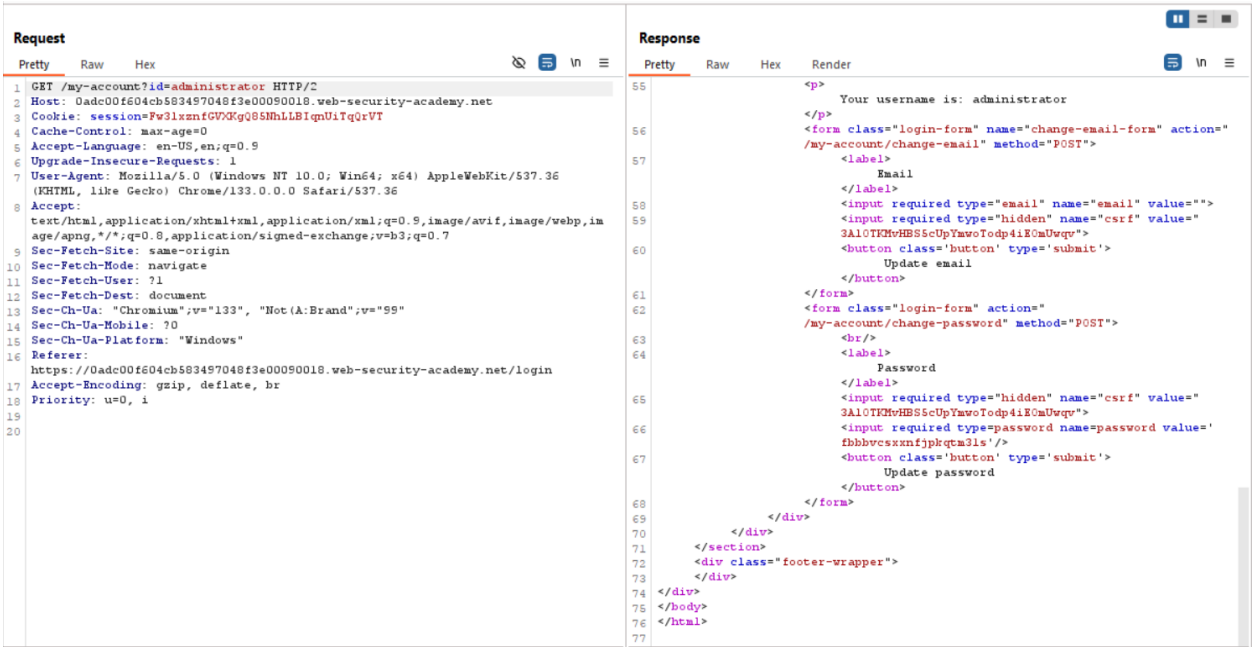
Lab 8

User ID controlled by request parameter with password disclosure.

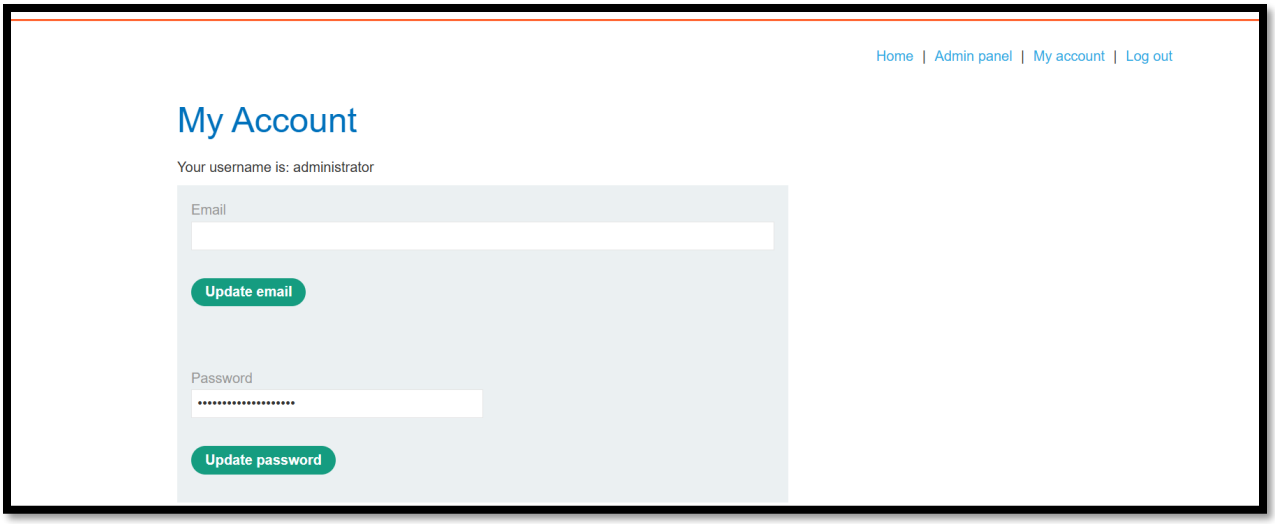
First log in using the provided credentials.

Intercept the request in burp suite.

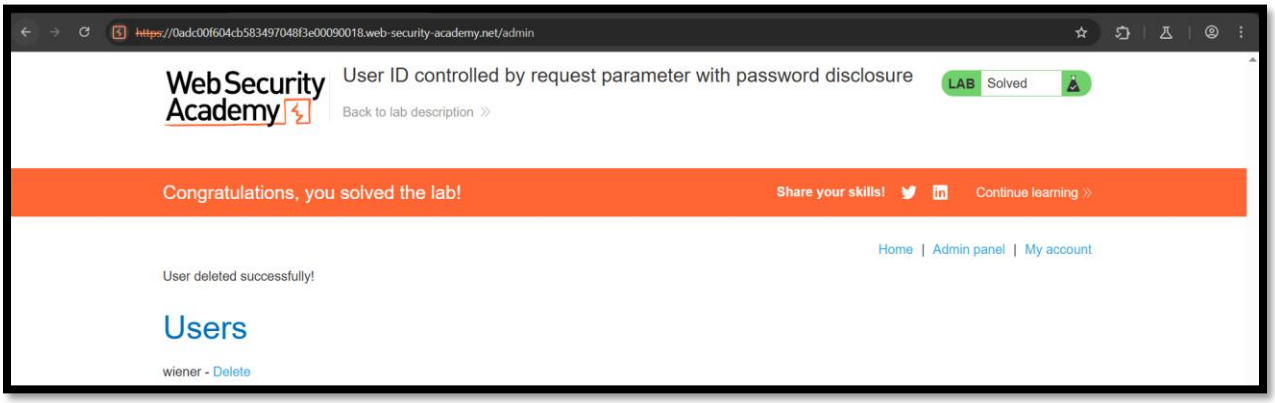




Change the id to administrator. And we will get the password for admin.



Now login as an administrator using obtained password and delete user carlos.



Lab 9

Insecure direct object references.

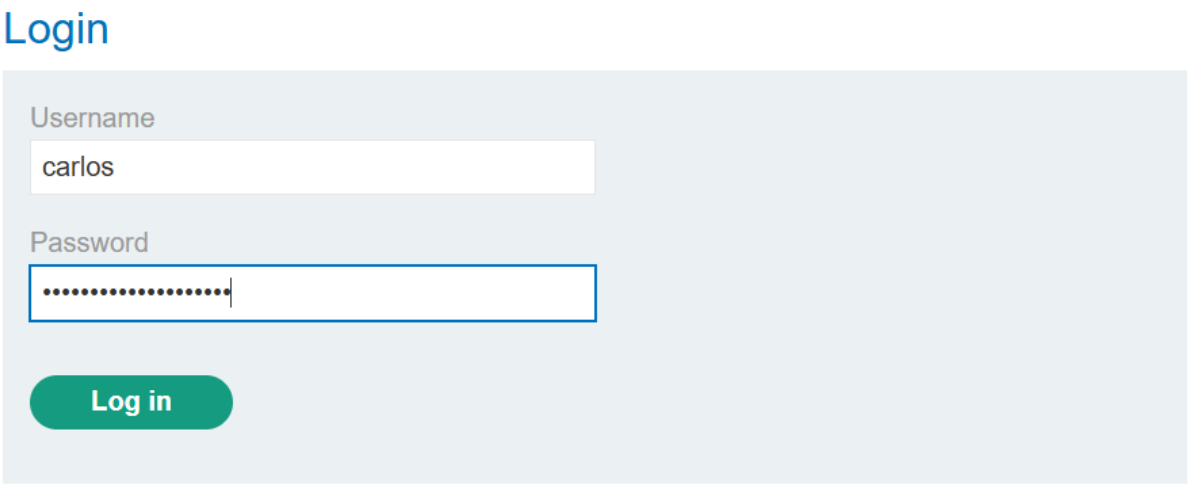
Select the live chat feature.

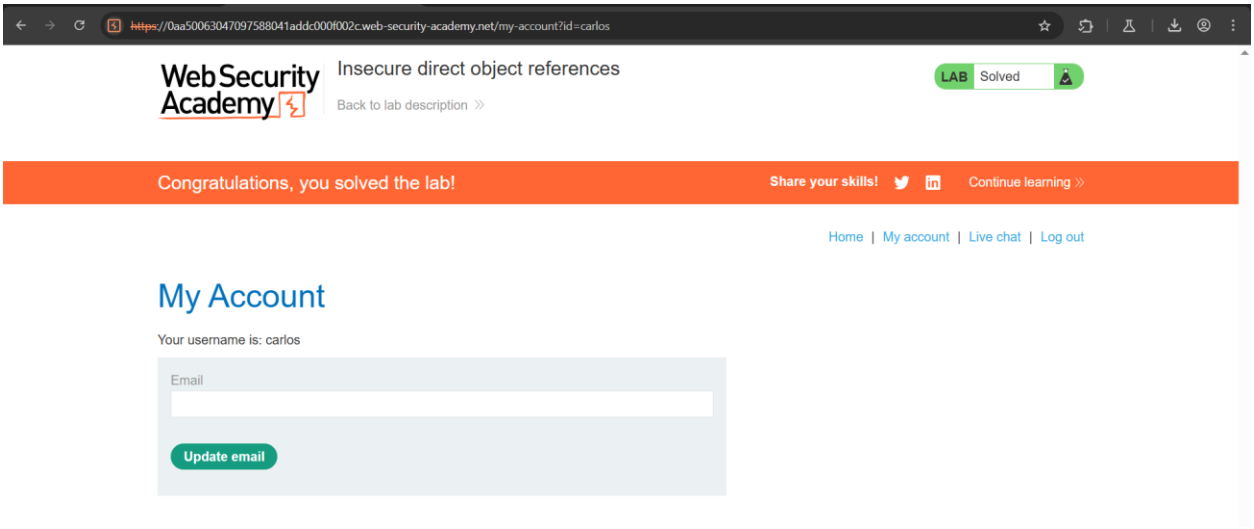
Once we send a message and click on view transcript, it outputs a downloadable file that contains the messages.

We can capture the download request in burpsuite and change the filename to 1.txt, to view all past messages.

In that we will find the password.

We can log in using the stolen credentials to solve the lab.




https://0aa50063047097588041addc000f002c.web-security-academy.net/my-account?id=carlos
Web Security Academy
Insecure direct object references
Back to lab description
LAB Solved
Congratulations, you solved the lab!
Share your skills!
Continue learning
Home | My account | Live chat | Log out
My Account
Your username is: carlos
Email
Update email

Lab 10

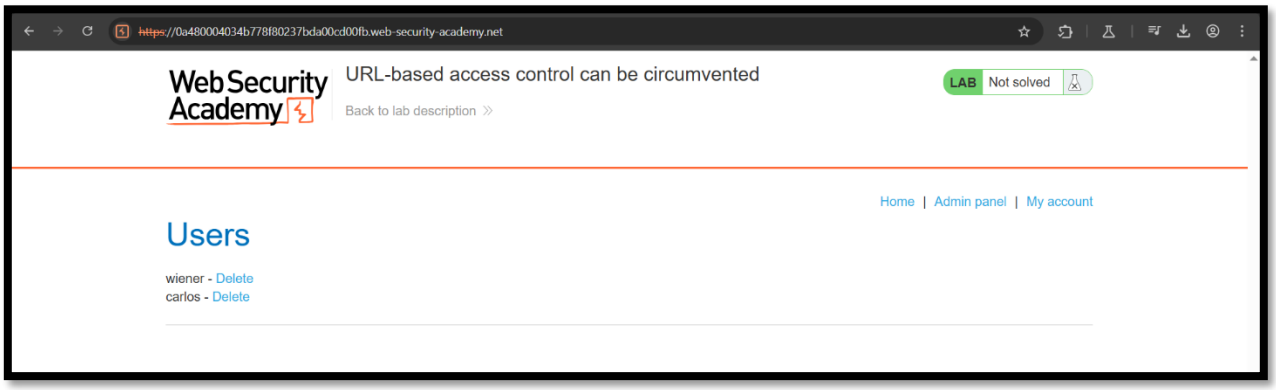
URL-based access control can be circumvented.

Try to load /admin and observe that I get blocked.

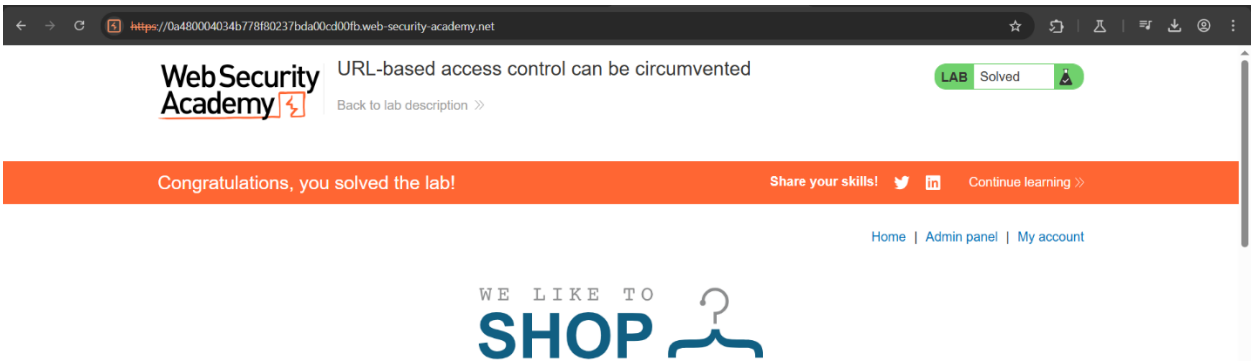
Need to intercept the request and add the HTTP header **X-Original-URL: /invalid.** It returns a "not found" response. This indicates that the back-end system is processing the URL from the X-Original-URL header.

Changed the value of the X-Original-URL header to /admin. And I could access the admin page.

By clicking the delete button we can't delete the user.



To delete carlos, add **?username=carlos** to the real query string, and change the X-Original-URL path to **/admin/delete**.



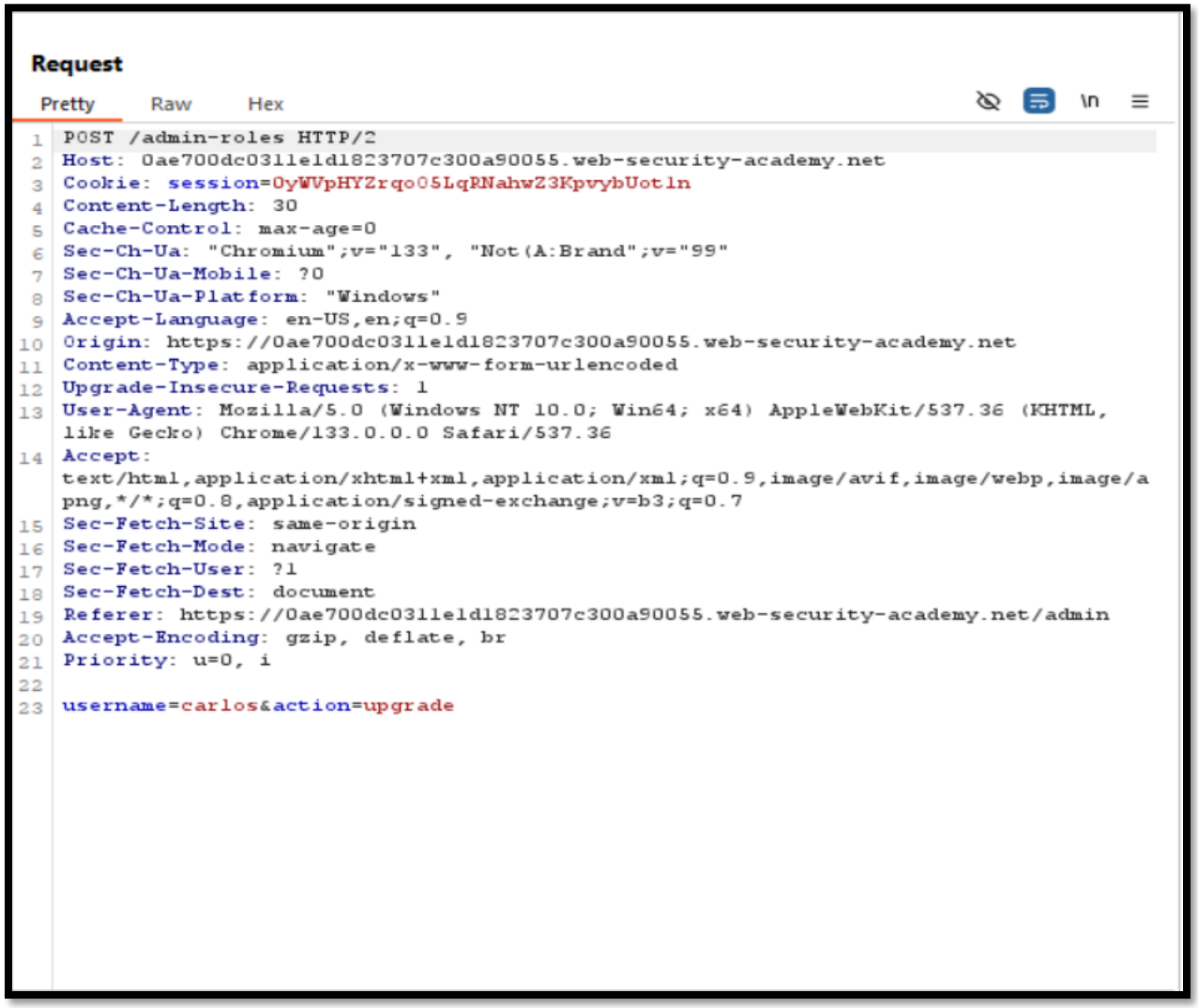
Lab 11

Method-based access control can be circumvented.

Enter the admin credentials and log in.

In the admin panel, find the option to promote user "carlos" to an elevated role.

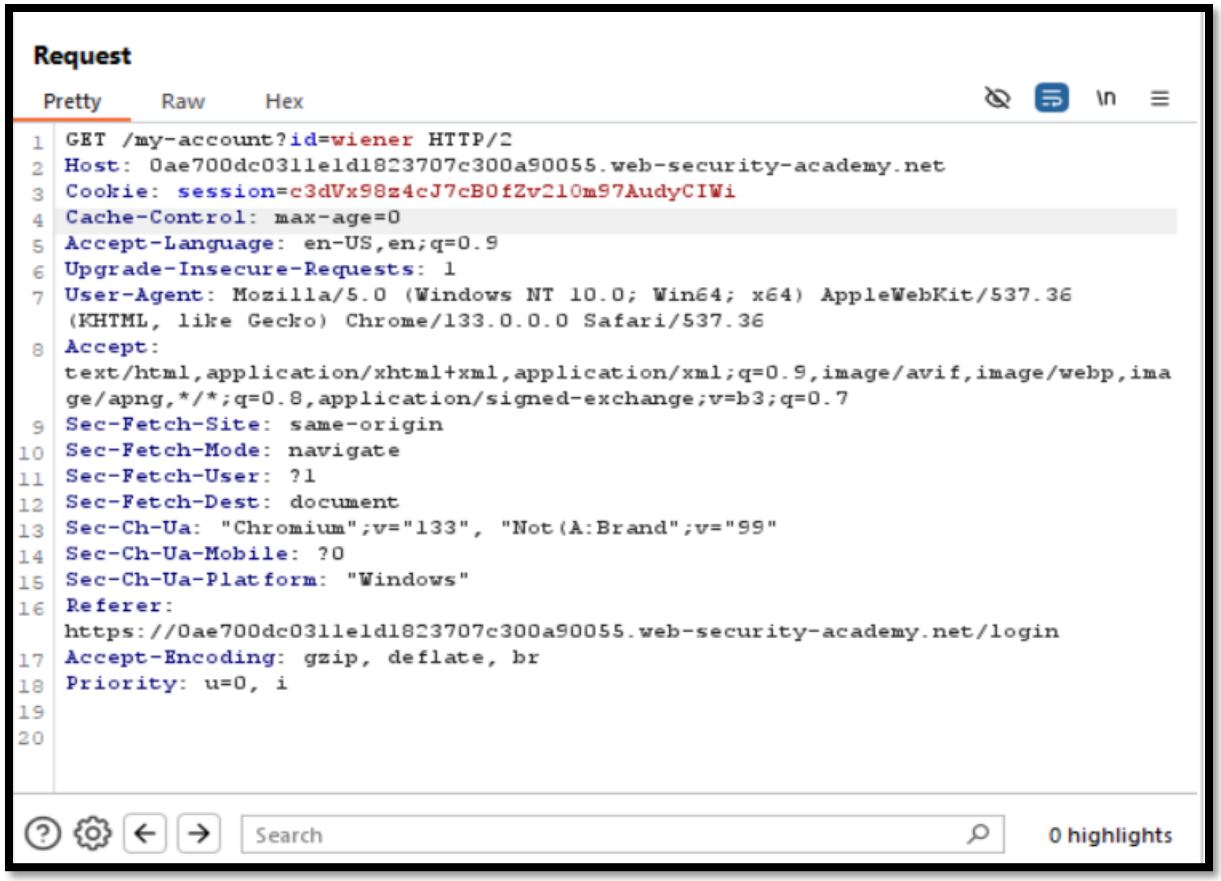
Capture the Promotion Request in Burp Suite



After that,

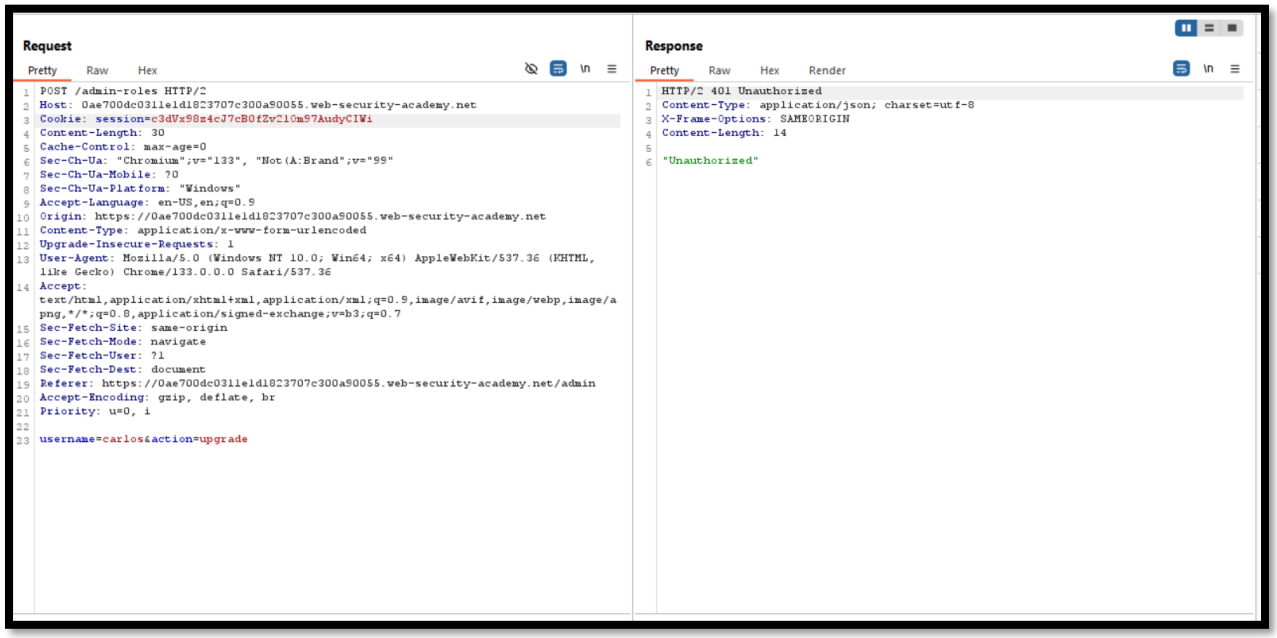
Log in using the non-admin credentials.

Copy the session cookie of this non-admin user.(wiener)



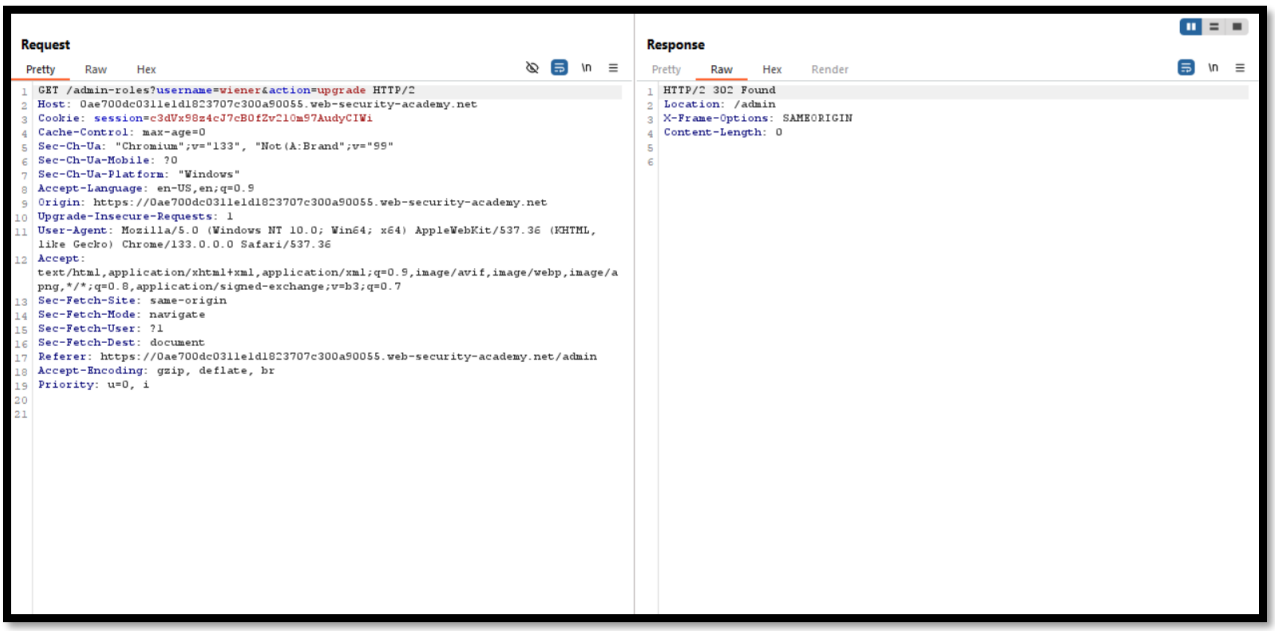
Replace the admin session cookie with the non-admin user's session cookie.

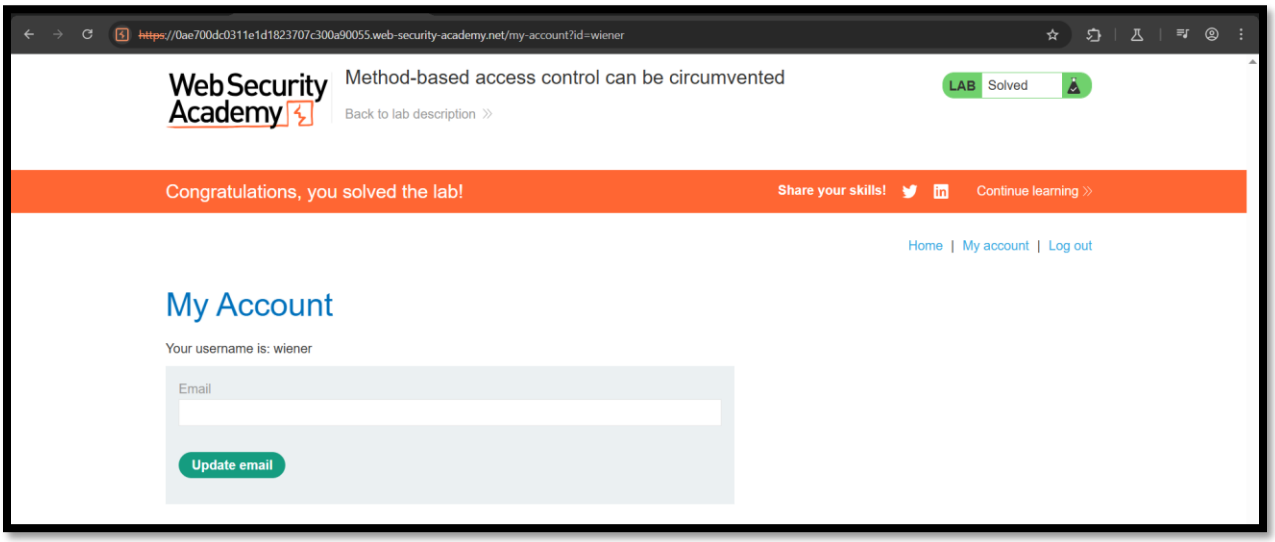
Resend the request and observe that the response states "Unauthorized".



Right-click the request in Burp Repeater. Select "Change request method" and set it to GET.

Modify the username parameter in the request to wiener.





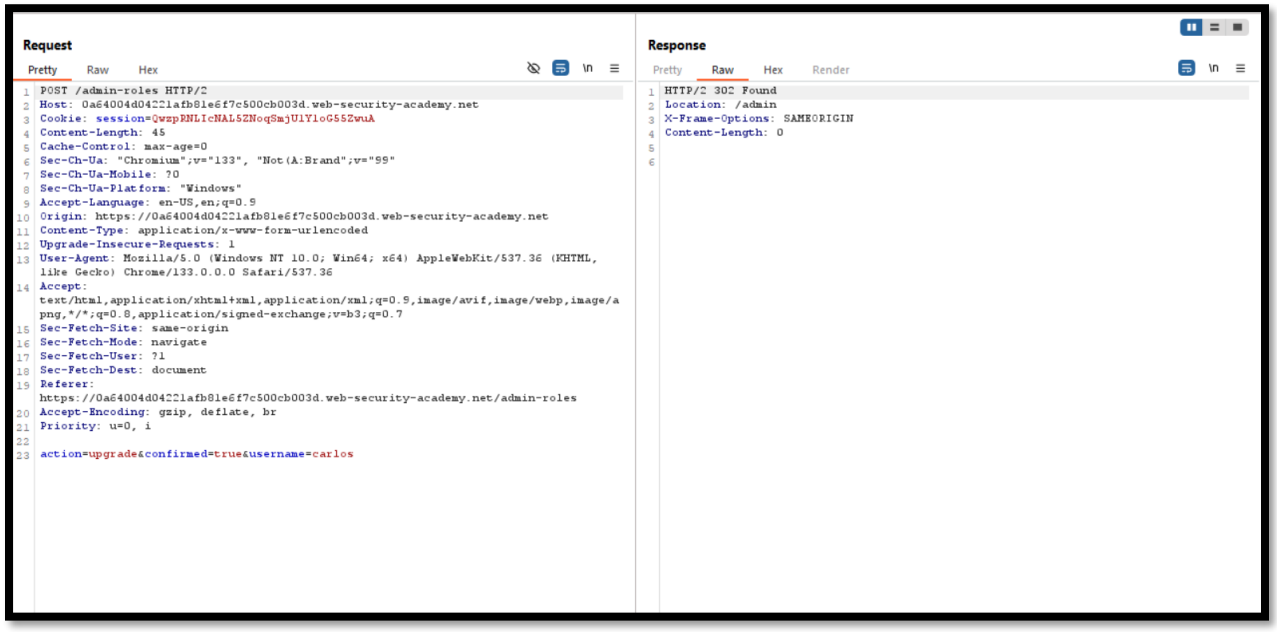
Lab 12

Multi-step process with no access control on one step.

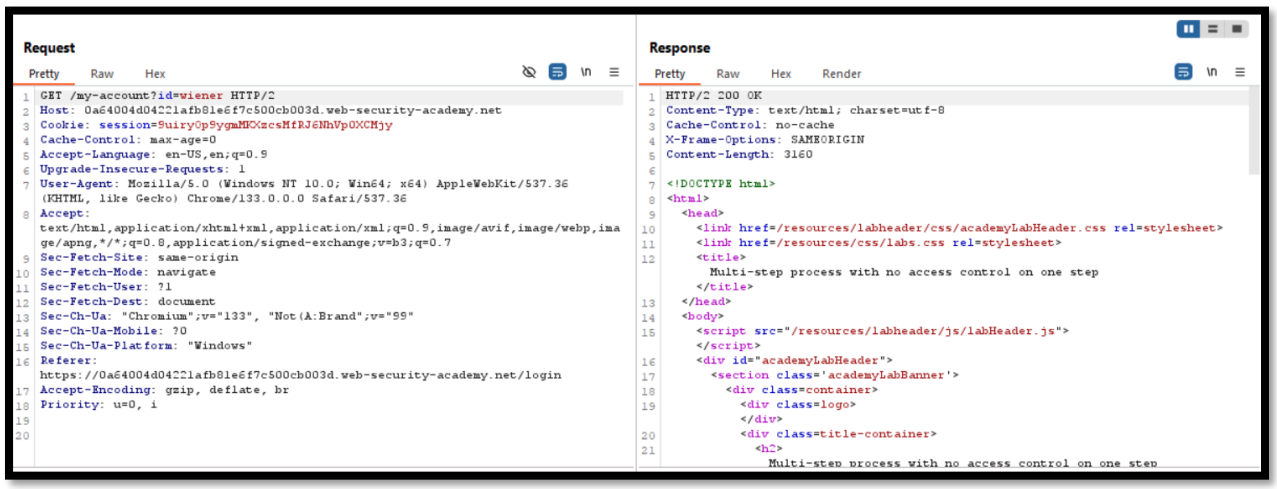
Enter the admin credentials provided for the challenge.

Click Login and proceed to the admin panel.

Promote Carlos and Capture the Request. And sent it to the repeater.

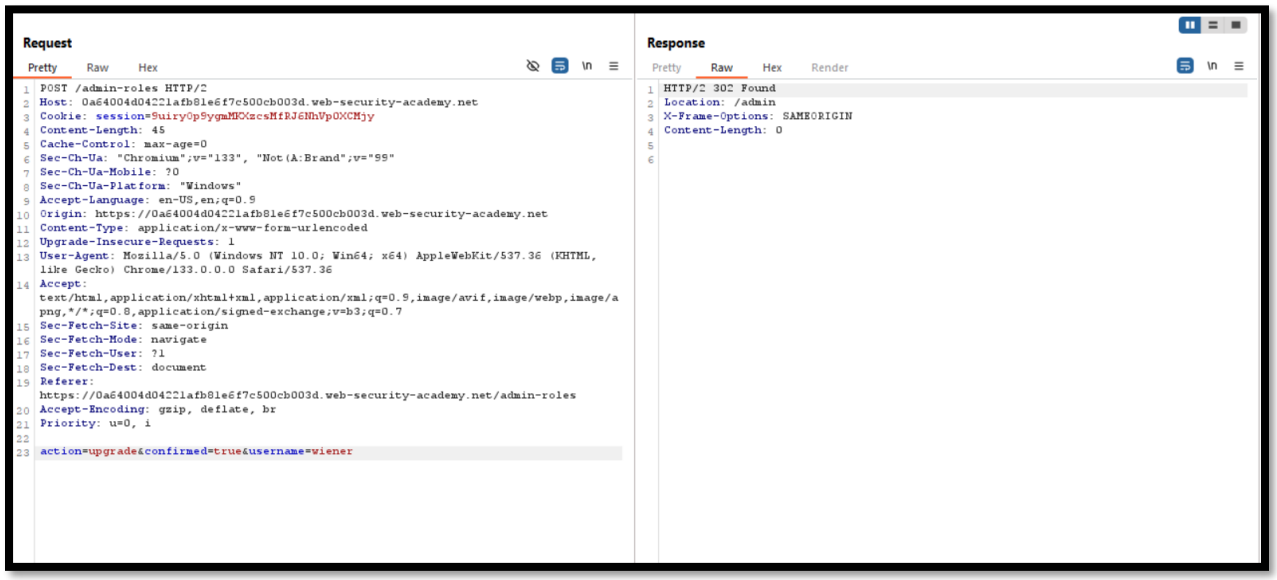


Now, Log in using non-admin credentials provided in the challenge. copy the session cookie of the non-admin user.



Replace the admin session cookie in the previously captured request with the non-admin session cookie.

Modify the username parameter in the request to your wiener.

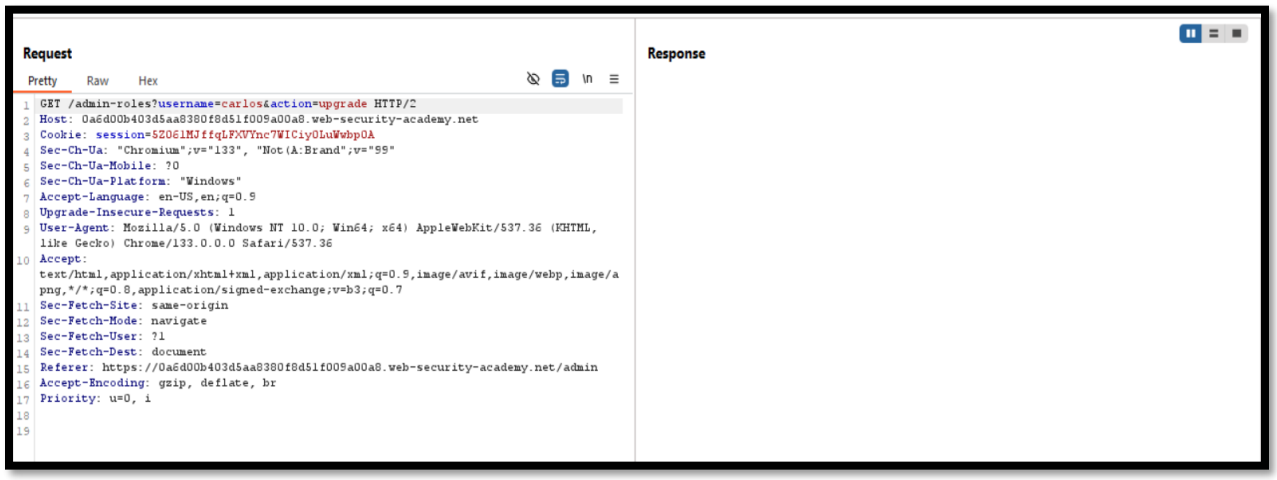


Lab 13

Referer-based access control.

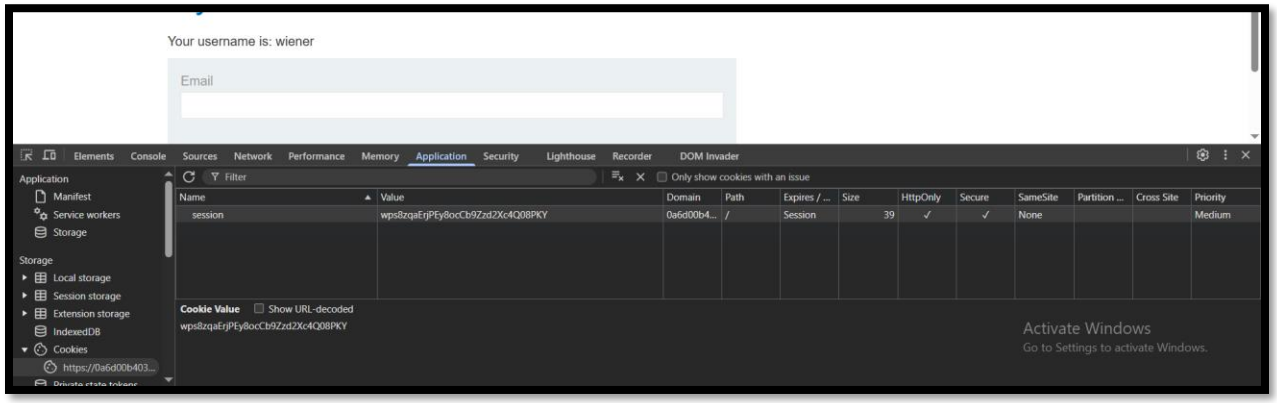
To solve this lab first we need to Log in as an Admin.

Promote user Carlos to and Capture the Request. And send it to the repeater.



Now, Log in as a Non-Admin User. Attempt unauthorized access. The request is unauthorized due to the missing **Referer** header.

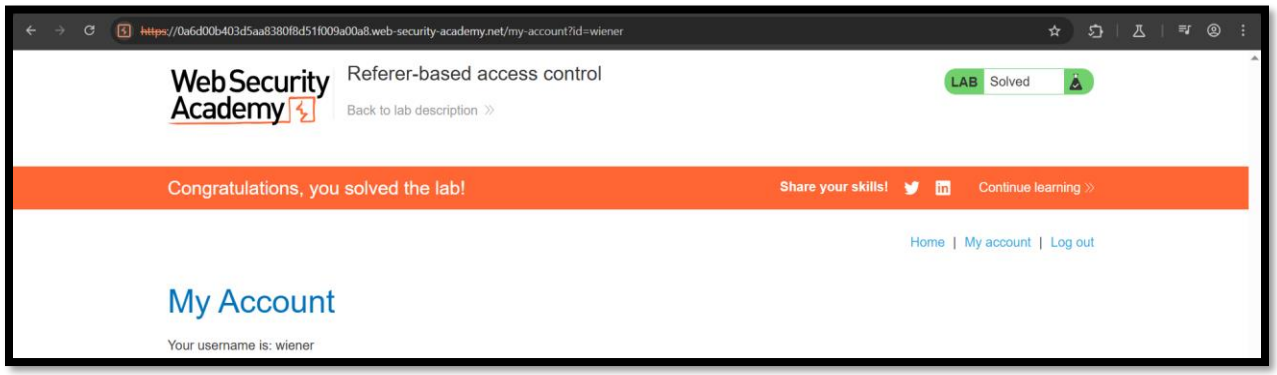
Now copy the session-cookie of Non-admin user.



Replace the **admin session cookie** in the previously captured request with the **non-admin session cookie**.

Modify the **username** parameter in the request to wiener.


Request
Pretty
Raw
Hex
GET /admin-roles?username=wiener&action=upgrade HTTP/2
Host: 0a6d00b403d5aa8380f8d51f009a00a8.web-security-academy.net
Cookie: session=wps8zqaErjPEy8ocCb9ZzdZXc4Q08PKY
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
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://0a6d00b403d5aa8380f8d51f009a00a8.web-security-academy.net/admin
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Response
Pretty
Raw
Hex
Render
HTTP/2 302 Found
Location: /admin
X-Frame-Options: SAMEORIGIN
Content-Length: 0


https://0a6d00b403d5aa8380f8d51f009a00a8.web-security-academy.net/my-account?id=wiener
Web Security Academy
Referer-based access control
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: wiener