Authentication

Refer for theory: https://portswigger.net/web-security/authentication

Vulnerability Labs(apprentice):

1. Username enumeration via different responses.

This lab is vulnerable to username enumeration and password brute-force attacks. It has an account with a predictable username and password, which can be found in the following wordlists:

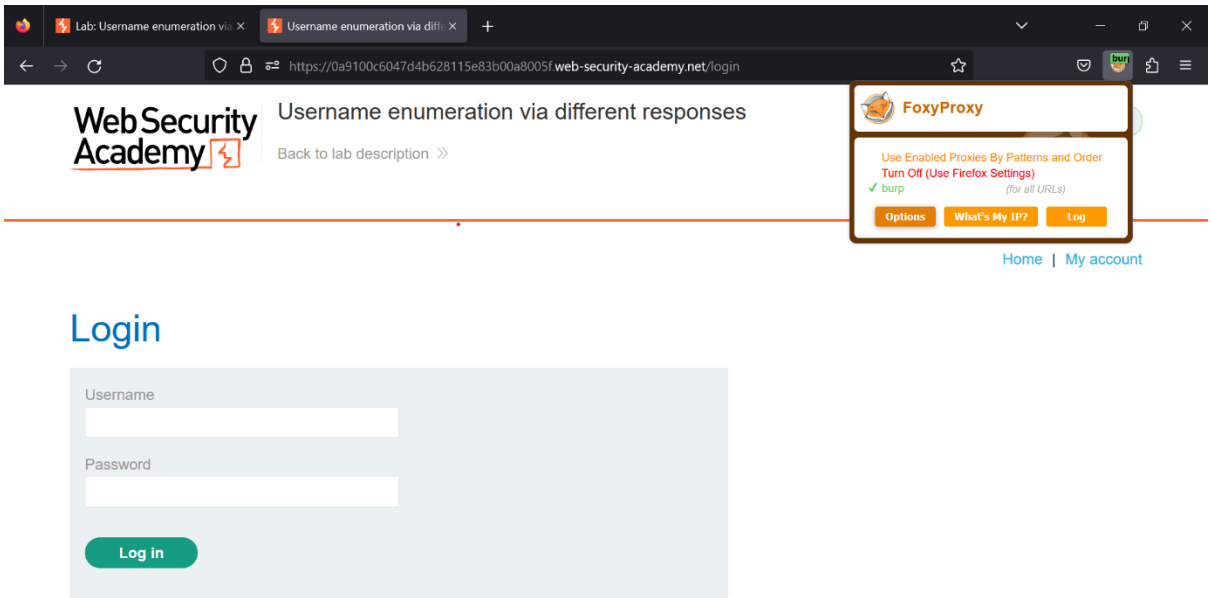
https://portswigger.net/web-security/authentication/auth-lab-usernames

https://portswigger.net/web-security/authentication/auth-lab-passwords

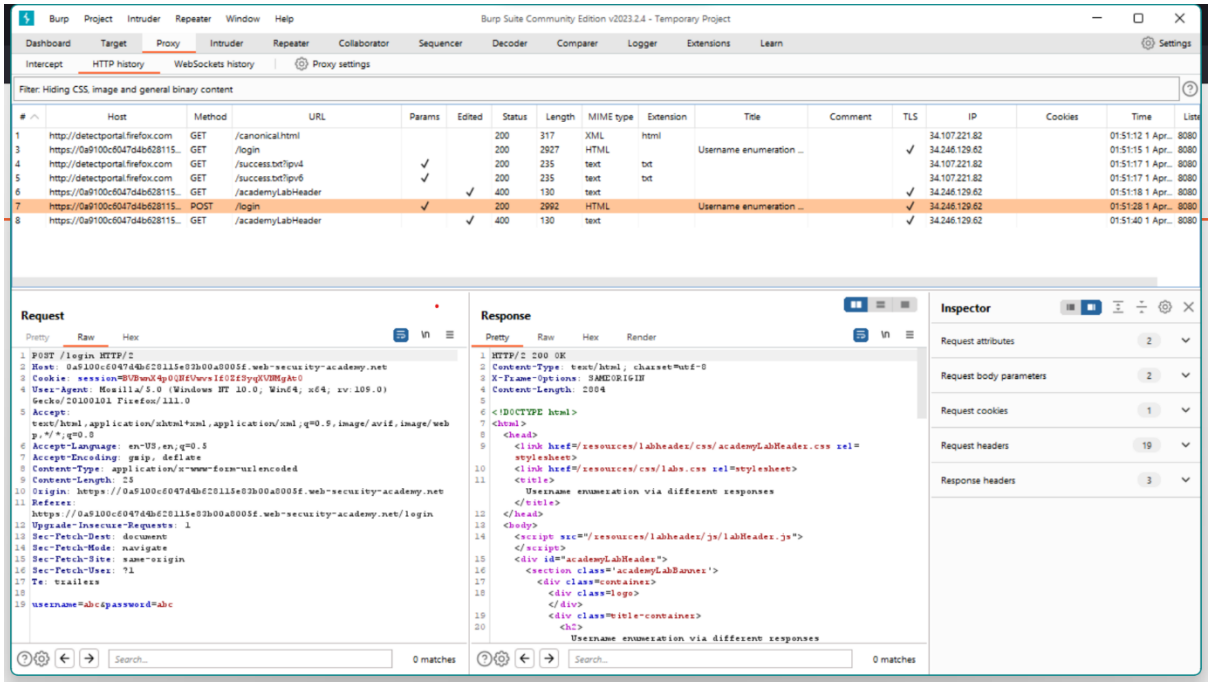
To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Solution:

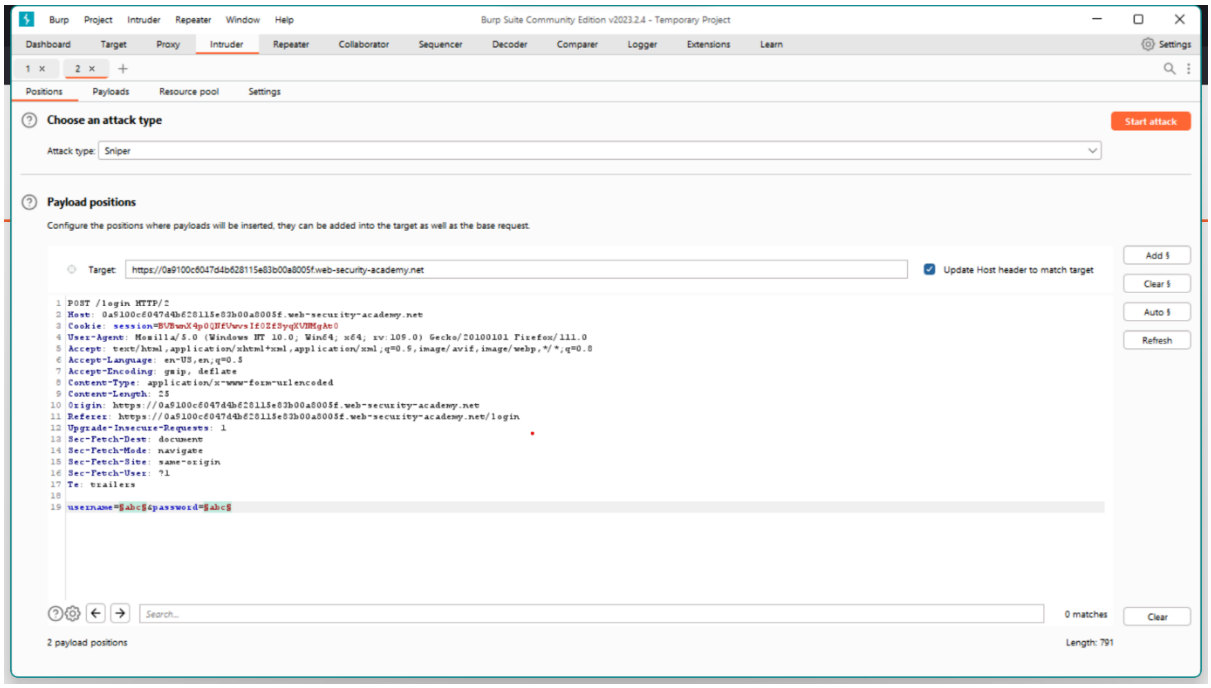
- We will be using the burp intruder for this lab.
- Once you access the lab, click on my account. Turn on your foxy proxy and intercept on burp suite.



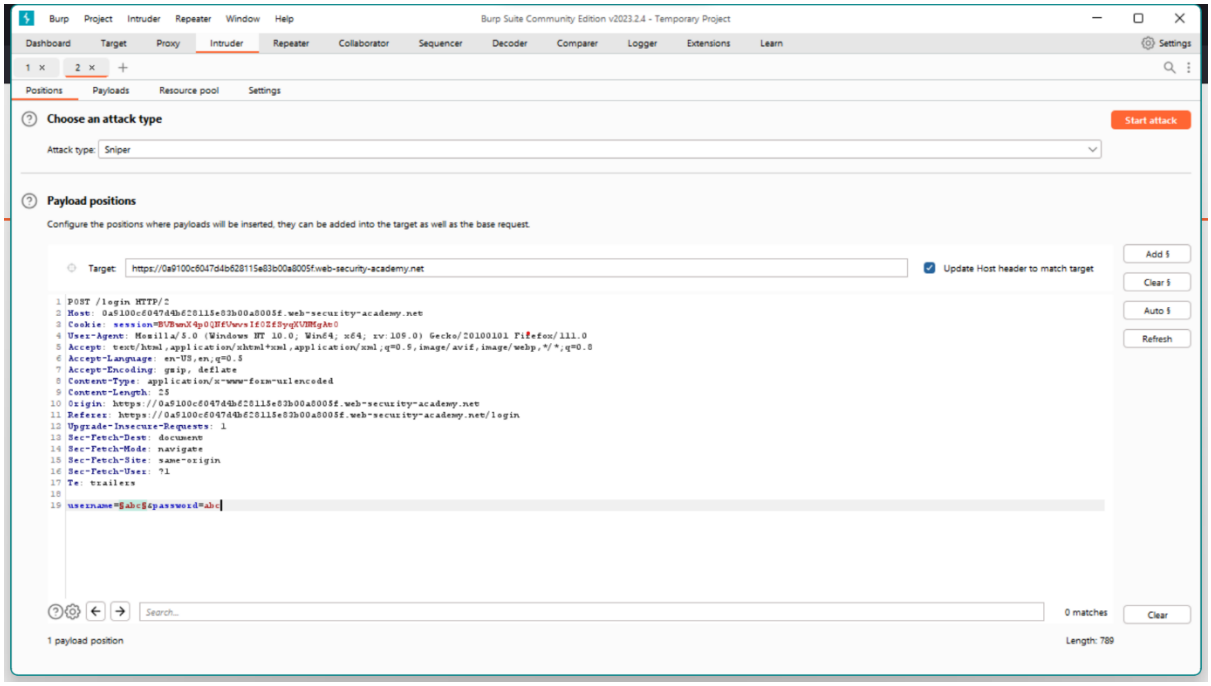
- Enter any invalid username and password and click on log in.
- Go to burp suite and forward all the packets.
- Open your HTTP History and look for a POST method with /login.



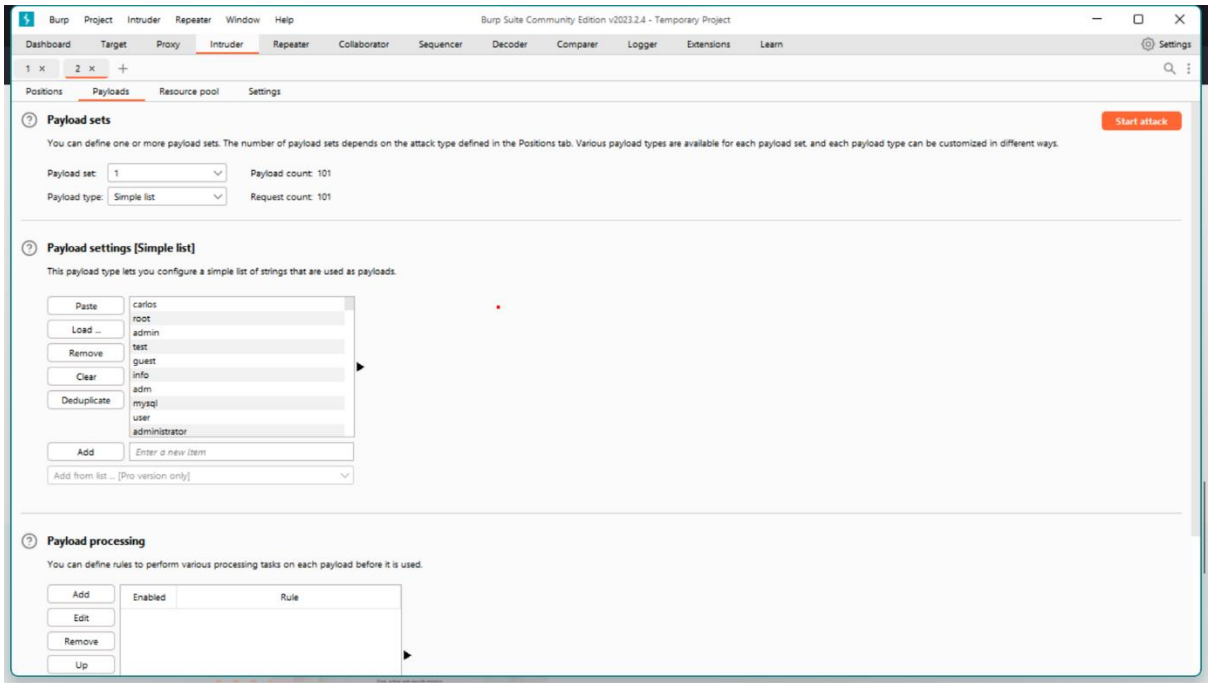
- Send that particular packet to intruder by right clicking on it and send to intruder.



- Make sure that the attack type is set to sniper.
- On the right side click on clear payload option as we only need to select one payload at a time.

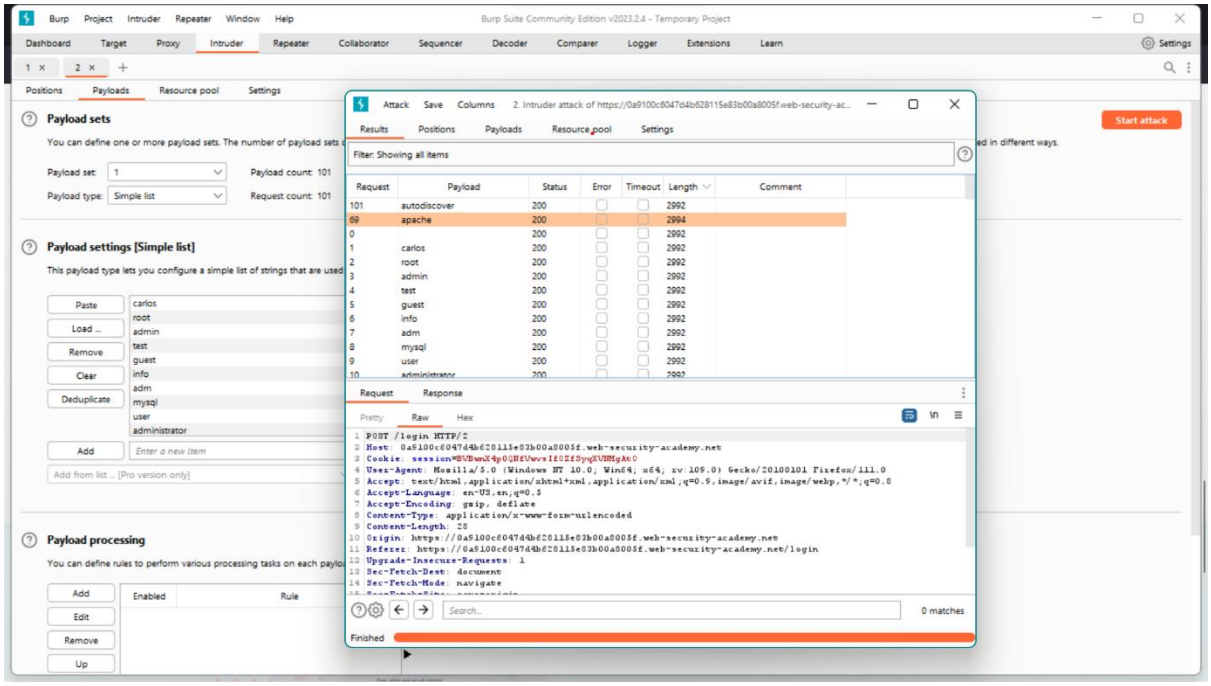


- You'll need to select the value of the username parameter and click on Add to add it as a payload.
- Open the payloads tab and make sure the type is set to simple list.
- Copy all the usernames from the link provided in the problem statement and paste them in the Payload setting(Simple list) by clicking on the paste option.
- Click on start attack.



- Wait till all the usernames have been processed.

- Once completed you'll see that one of the usernames will have the length different to the others. That is an indication that it might be a valid username.



- Send this packet to the repeater to confirm that the username is valid.
- In the burp repeater, change the username to the one that we assume is valid and send the packet to get the response.
- Analyze the response to see whether you find a text saying "Incorrect password". If yes then the username is correct else the username is different.
- Do the same process to get the password by changing the payload settings. Enter the obtained username and password to solve the lab.

2. <u>2FA simple bypass.</u>

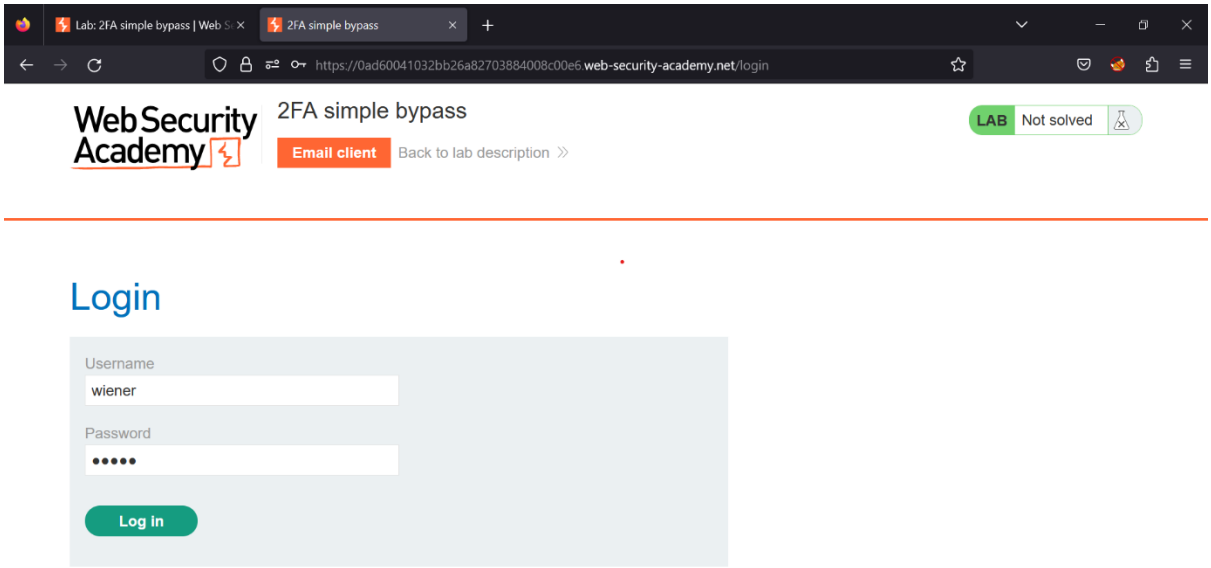
This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

Your credentials: wiener: Peter

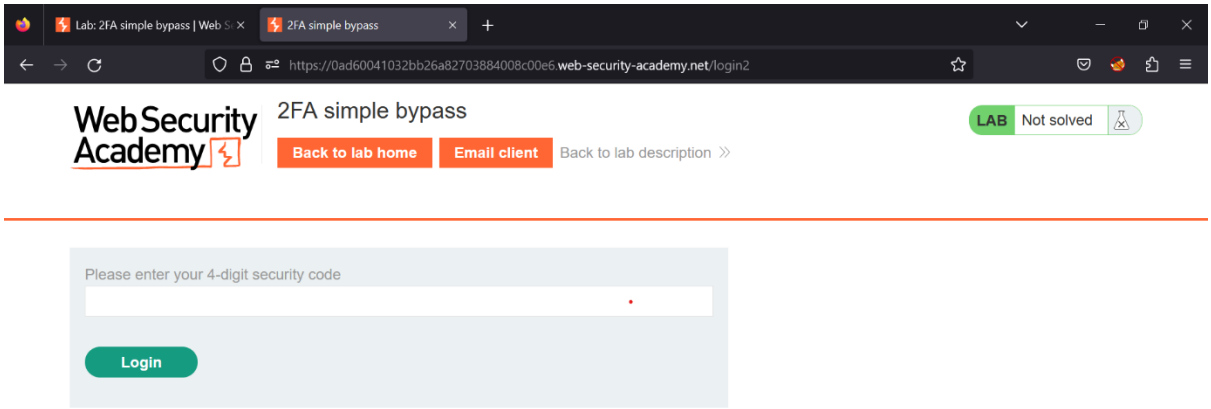
Victim's credentials Carlos: Montoya

Solution:

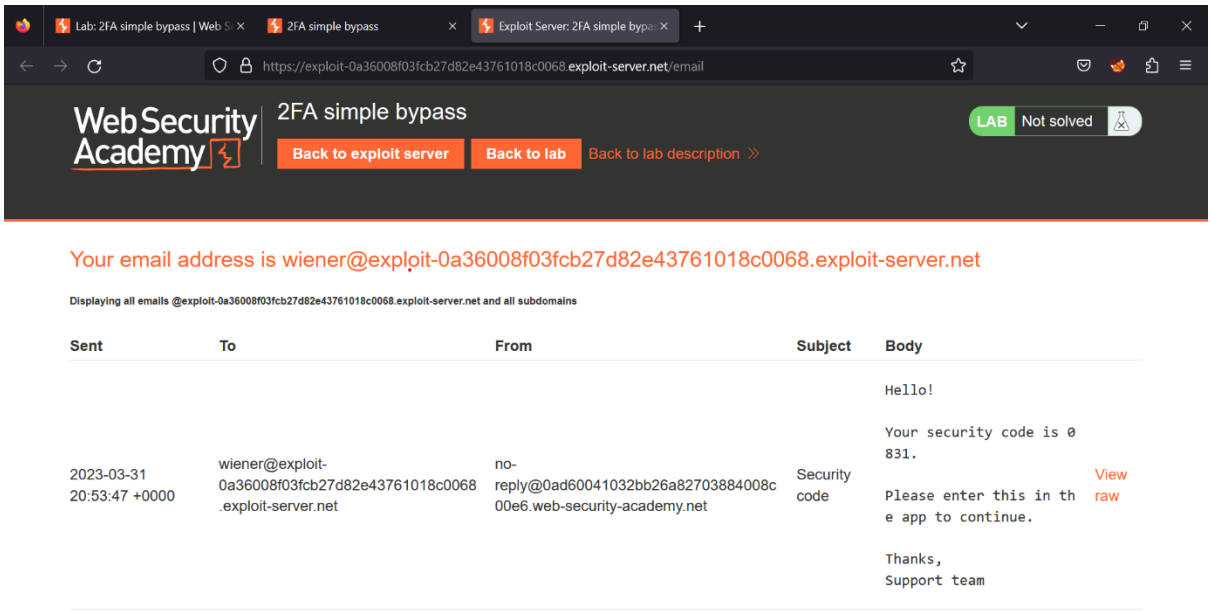
- Once you access the lab go to my account and enter your credentials.



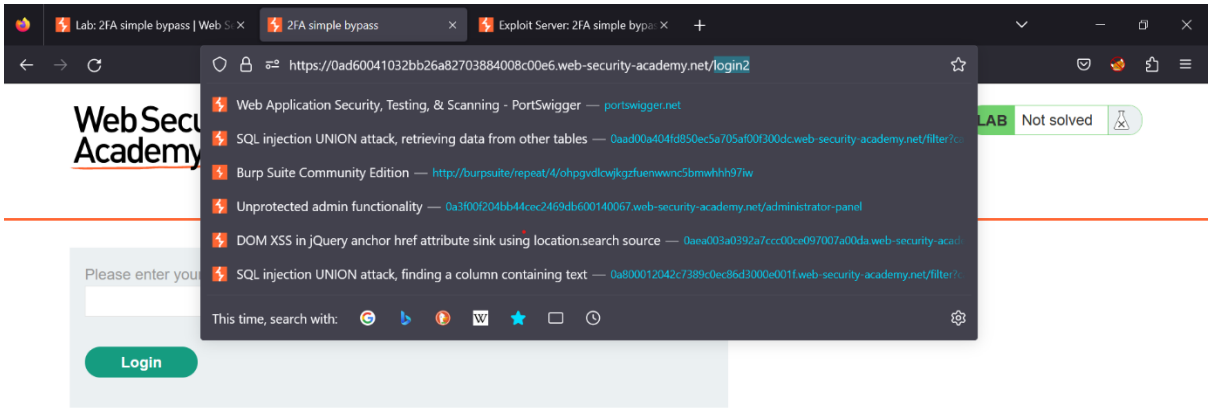
- Once you log in, you will have to put your verification code to very your account. For this click on the email client given above.

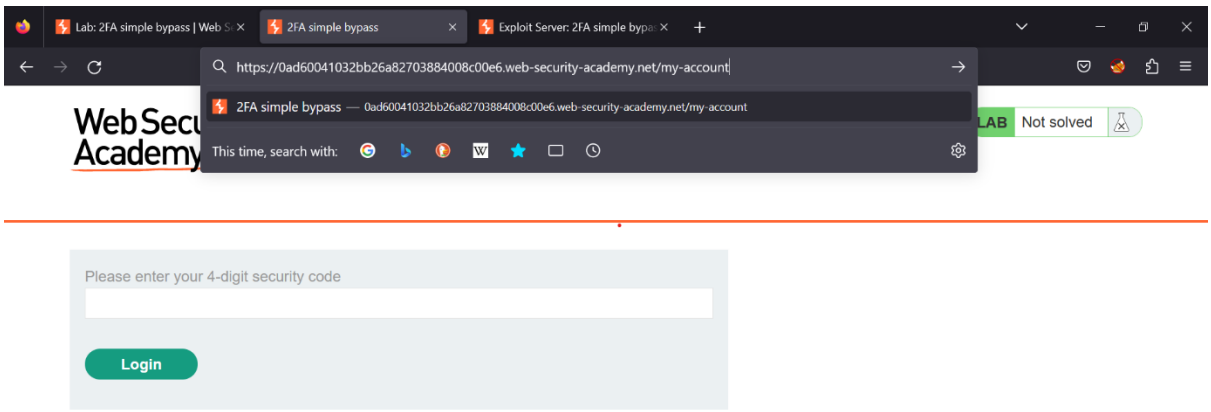


- Copy the verification code and paste it in the text field.



- Log out from your account and now log in again using the victim's credentials.
- On the page where it is asking for the verification code, open the URL and replace the end with /my-account.





- Once you click enter, the verification will be skipped and your lab will be completed.

3. <u>Password reset broken logic.</u>

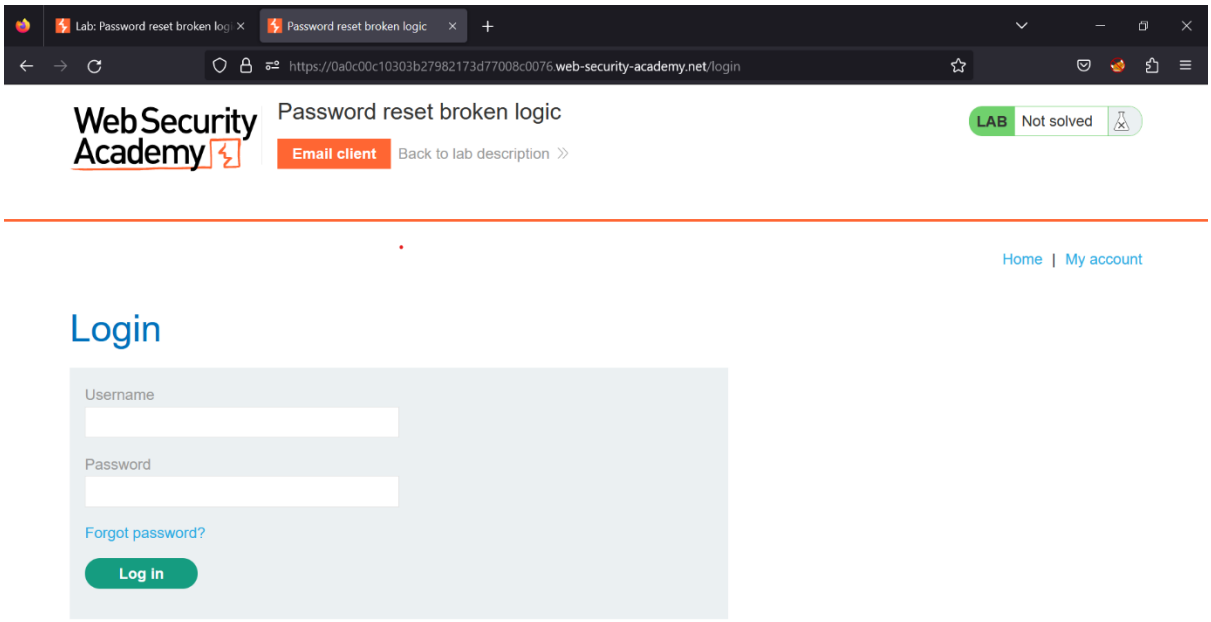
This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

Your credentials: wiener:peter

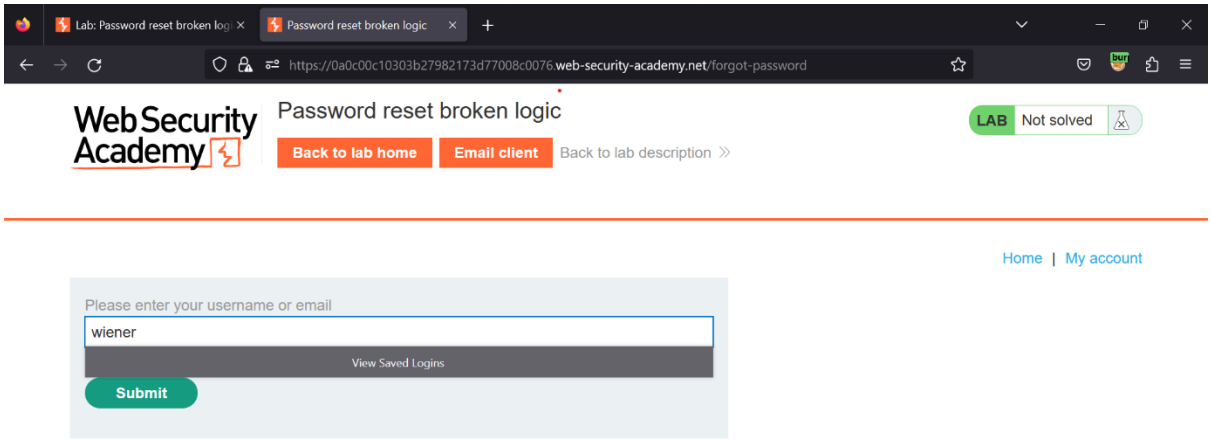
Victim's username: carlos

Solution:

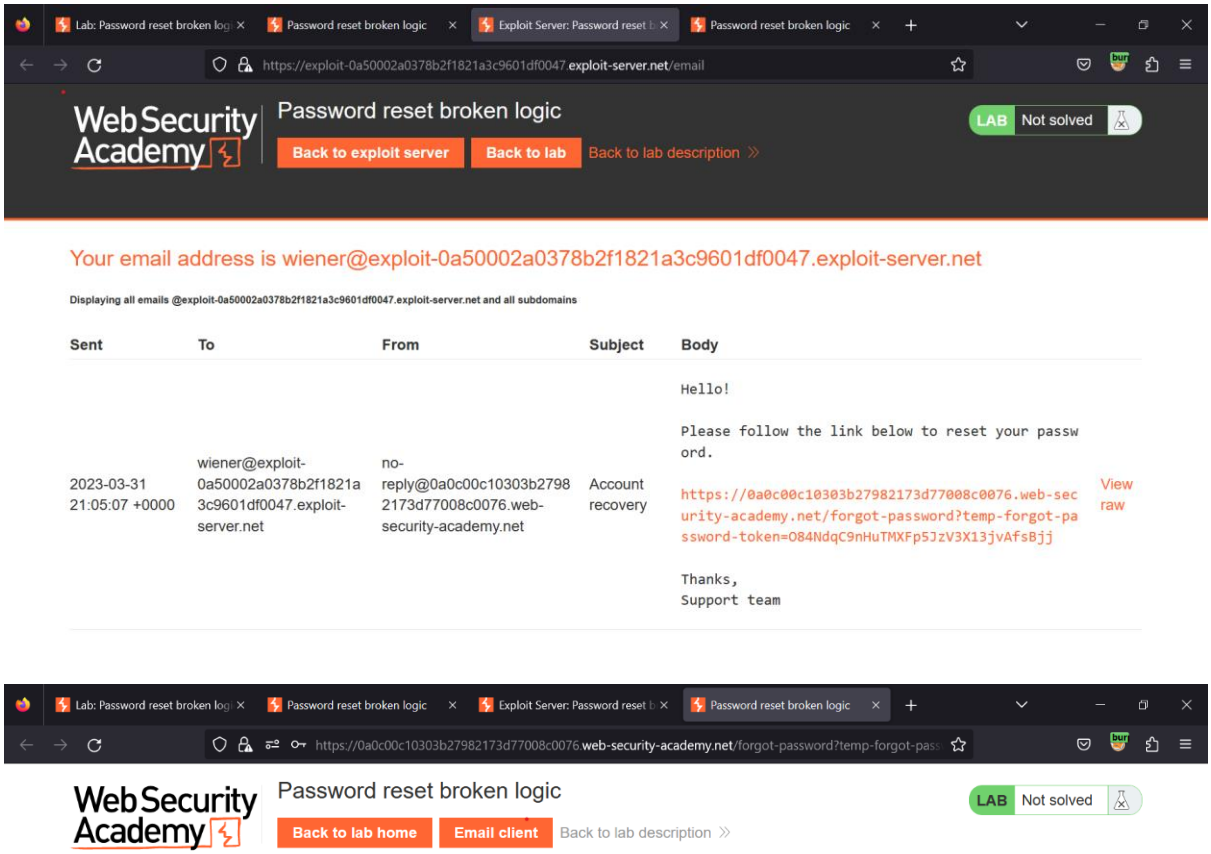
- Access the lab and go to my account tab.

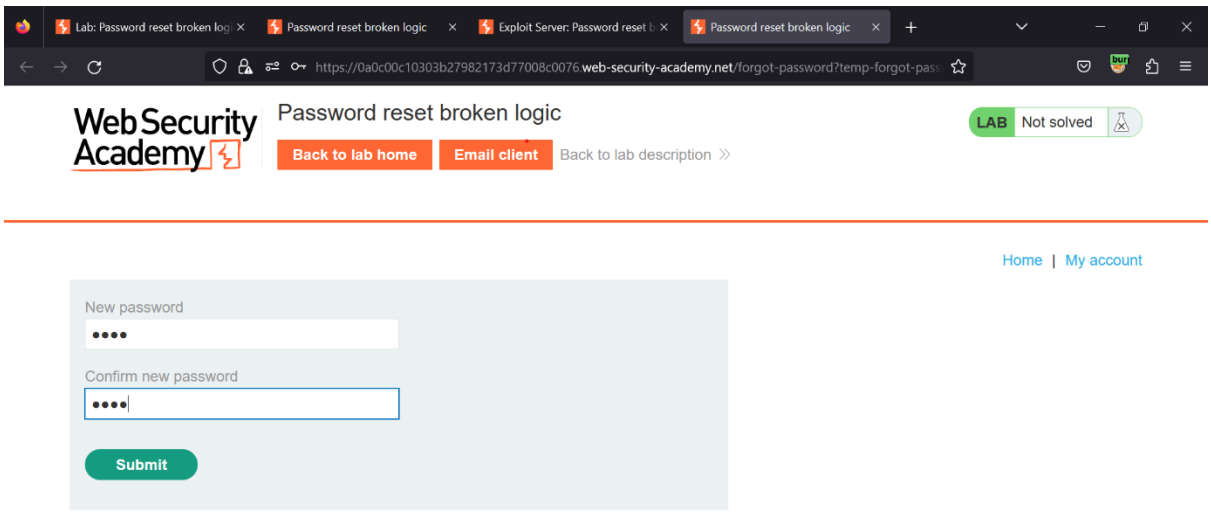


- With Burp running, click the Forgot your password? link and enter your own username.

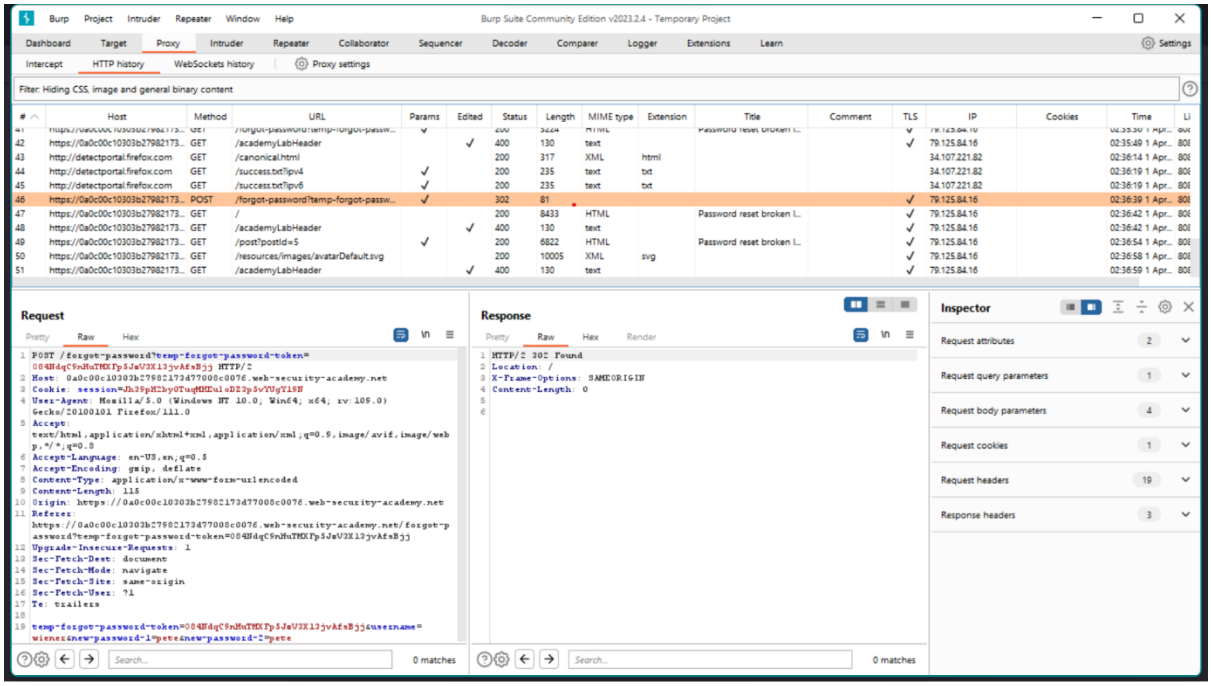


- Click the Email client button to view the password reset email that was sent. Click the link in the email and reset your password to whatever you want.

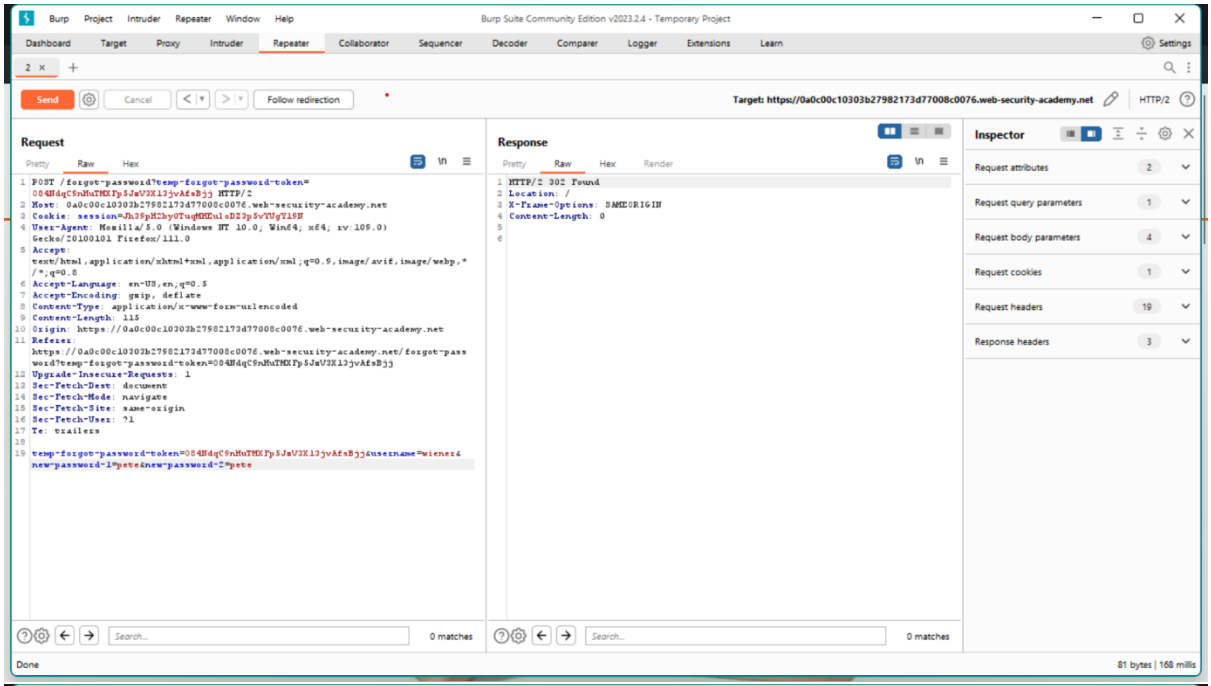


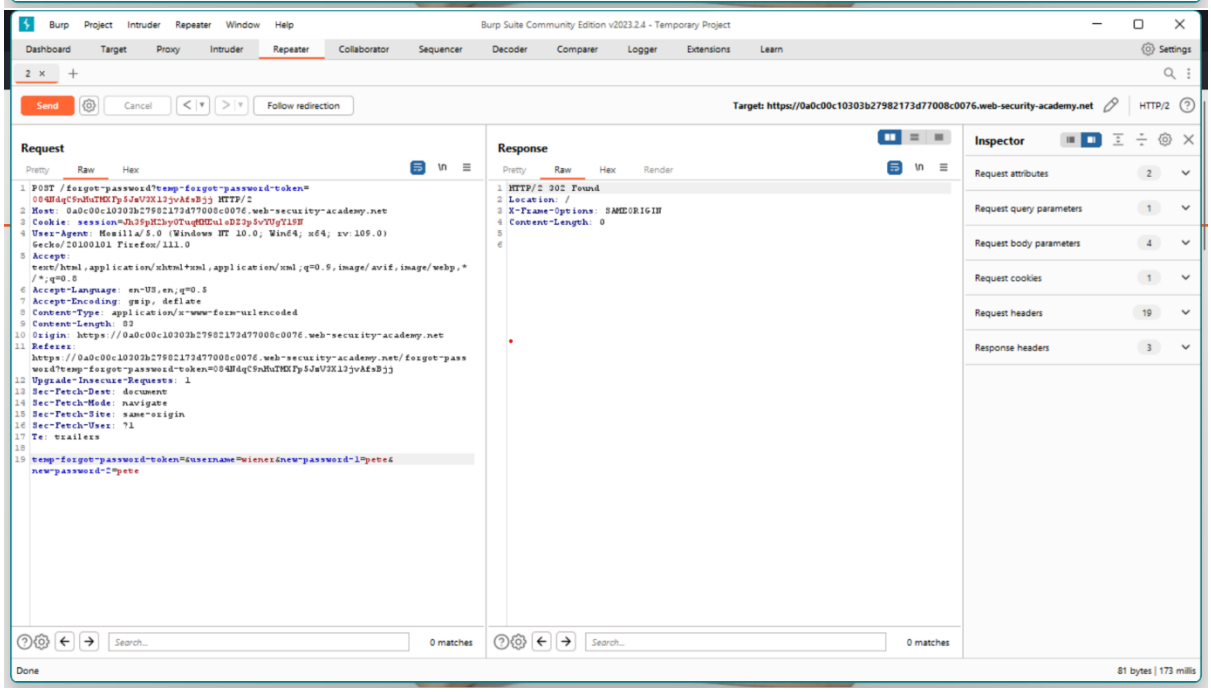


- In Burp, go to Proxy > HTTP history and study the requests and responses for the password reset functionality. Observe that the reset token is provided as a URL query parameter in the reset email. Notice that when you submit your new password, the POST /forgot-password?temp-forgot-password-token request contains the username as hidden input. Send this request to Burp Repeater.



- In Burp Repeater, observe that the password reset functionality still works even if you delete the value of the temp-forgot-password-token parameter in both the URL and request body. This confirms that the token is not being checked when you submit the new password.





- In the browser, request a new password reset and change your password again. Send the POST /forgot-password?temp-forgot-password-token request to Burp Repeater again.
- In Burp Repeater, delete the value of the temp-forgot-password-token parameter in both the URL and request body. Change the username parameter to carlos. Set the new password to whatever you want and send the request.
- In the browser, log in to Carlos's account using the new password you just set. Click My account to solve the lab.