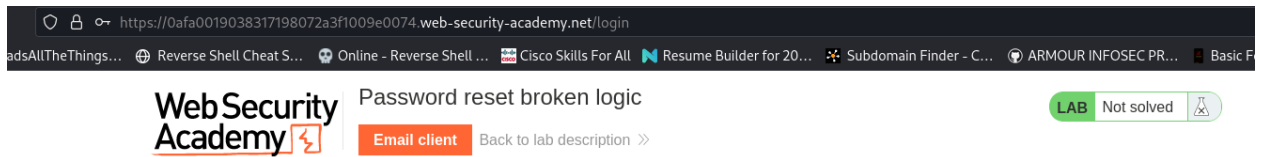


Authentication Lab3:- Password Reset Broken logic.

- Now, it's time to solve another lab let's do it.



Login

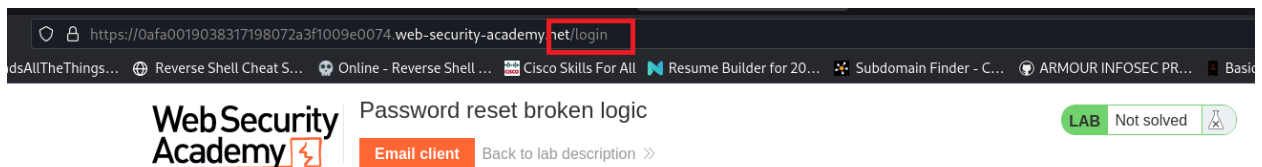
Username
wiener

Password
.....

[Forgot password?](#)

[Log in](#)

- Here, I tried with a random password but was unable to log in then I click on forgot password.



Login

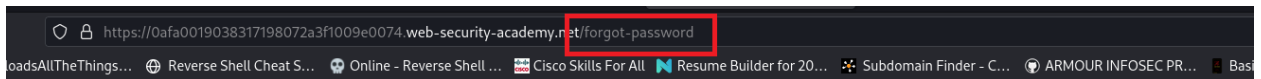
Username
wiener

Password

[Forgot password?](#)

[Log in](#)

- Now, a window appears and shows forgot password window which required user and or email in the given field where I enter (wiener).



Password reset broken logic

LAB Not solved

[Back to lab home](#)

[Email client](#)

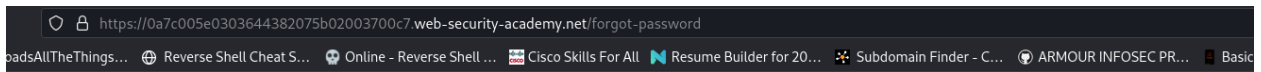
[Back to lab description >>](#)

Please enter your username or email

Submit

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

- Now, you have to check your email for a password reset link.



Password reset broken logic

LAB Not solved

[Back to lab home](#)

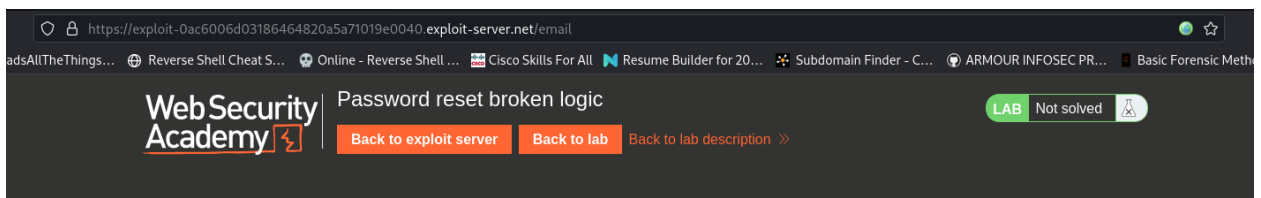
[Email client](#)

[Back to lab description >>](#)

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

Please check your email for a reset password link.

- Here, you found email reset link.



Your email address is wiener@exploit-0ac6006d03186464820a5a71019e0040.exploit-server.net

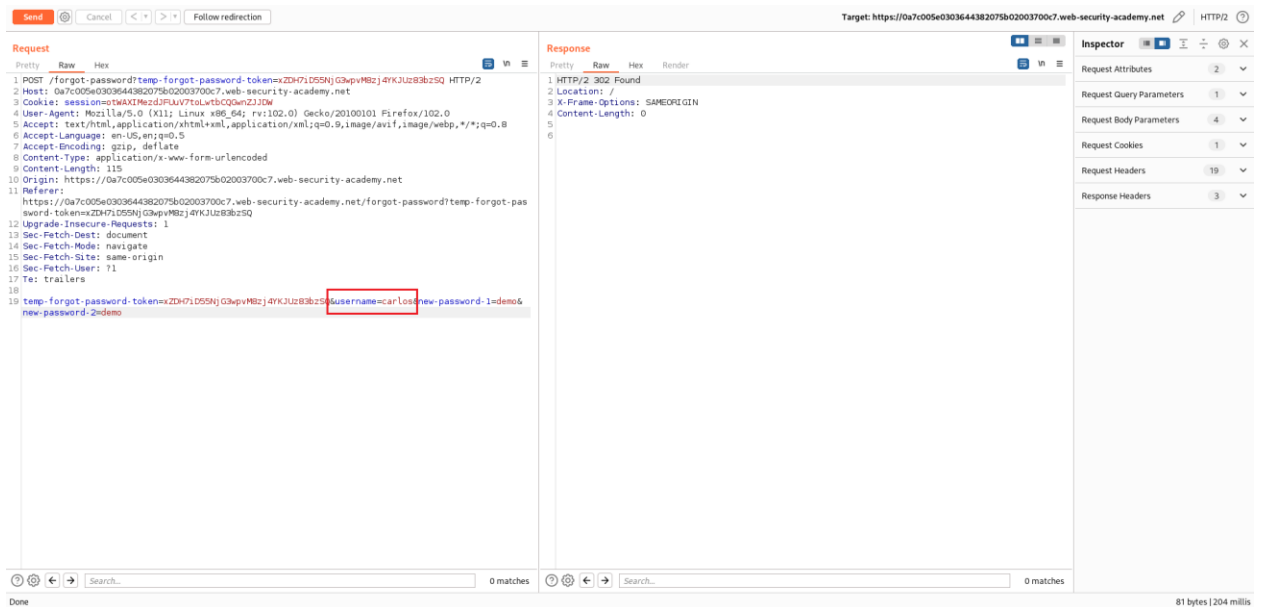
Displaying all emails @exploit-0ac6006d03186464820a5a71019e0040.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
				Hello!
				Please follow the link below to reset your password.
2023-03-30 13:56:42 +0000	wiener@exploit-0ac6006d03186464820a5a71019e0040.exploit-server.net	no-reply@0a7c005e0303644382075b02003700c7.web-security-academy.net	Account recovery	https://0a7c005e0303644382075b02003700c7.web-security-academy.net/forgot-password?temp-forgot-password-token=xZDH7iD55NjG3wpm8zj4YKJUz83bzSQ View raw
				Thanks, Support team

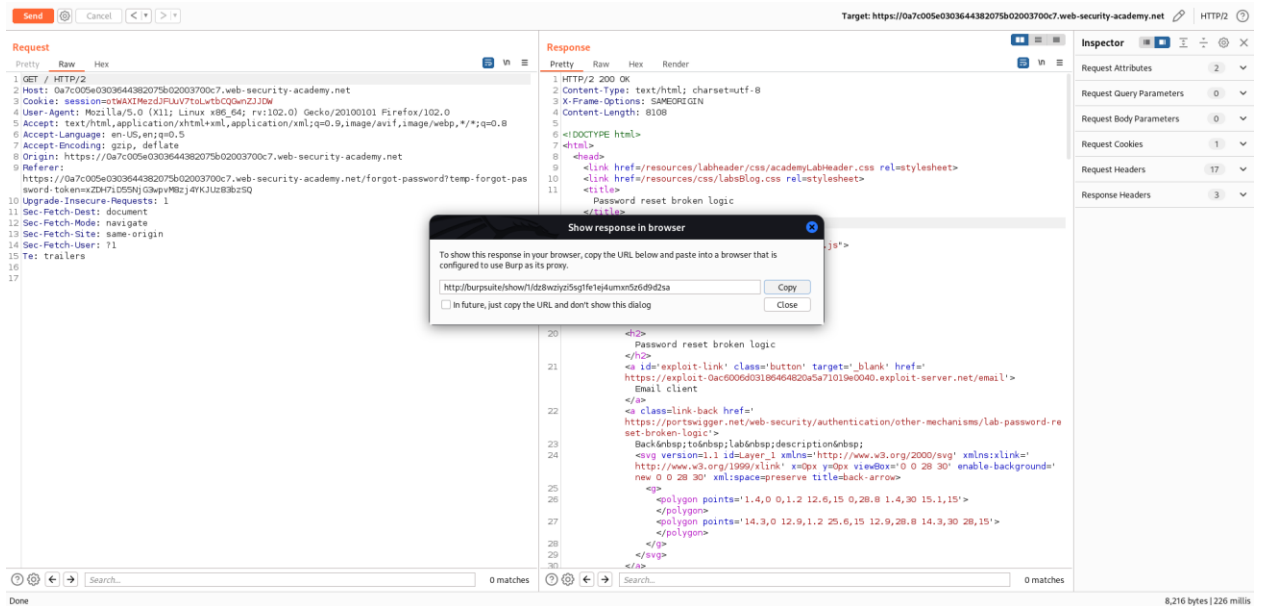
- Now, change the password of the wiener that is “demo” and capture the request in burp suite.

- Now send the request to a repeater and analyze it.

- Now here, in this request I change the username from Wiener to Carlos you found that on sending the request is redirects to another page then follow the redirect.



- Copy the link of the response and paste in browser as shown below.



- Here, you found on paste copied a link to the browser a login page appears.

Login

Username
carlos

Password
....

[Forgot password?](#)

Log in

- Now, enter the password because, in the above request, I captured only change the username and password is the same that is “demo”.

Login

Username
carlos

Password
....

[Forgot password?](#)

Log in

- Boom, here I receive a pop-up of the hard work, I solved this lab.



Password reset broken logic

LAB Solved



[Back to lab description >>](#)

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

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

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

[Update email](#)