

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:

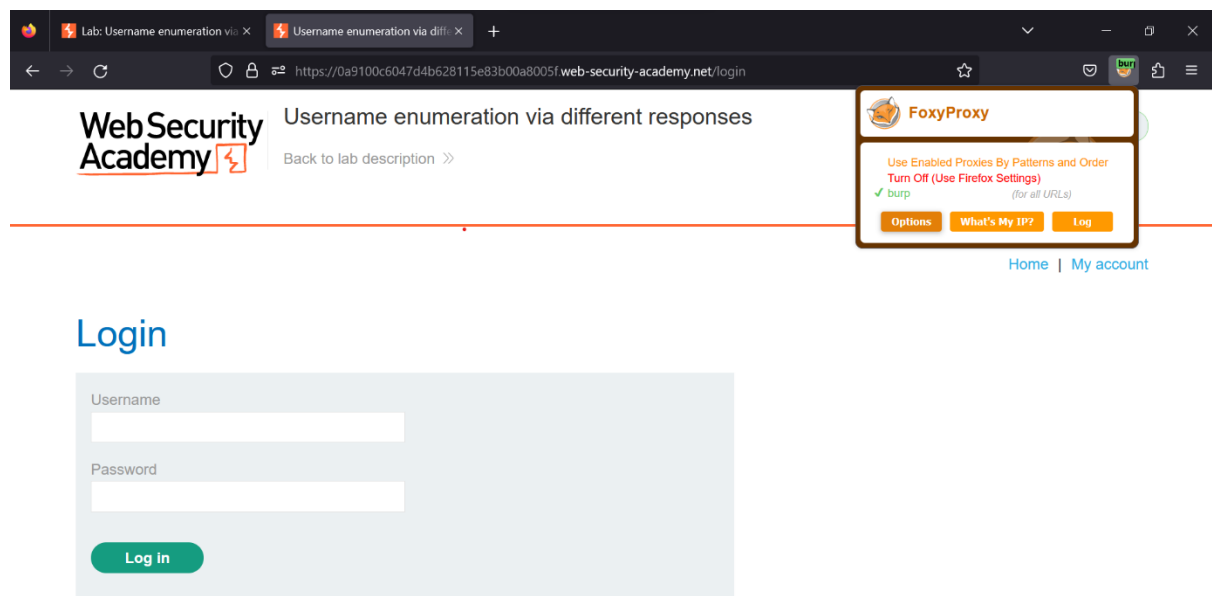
<https://portswigger.net/web-security/authentication/auth-lab-usernames>

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

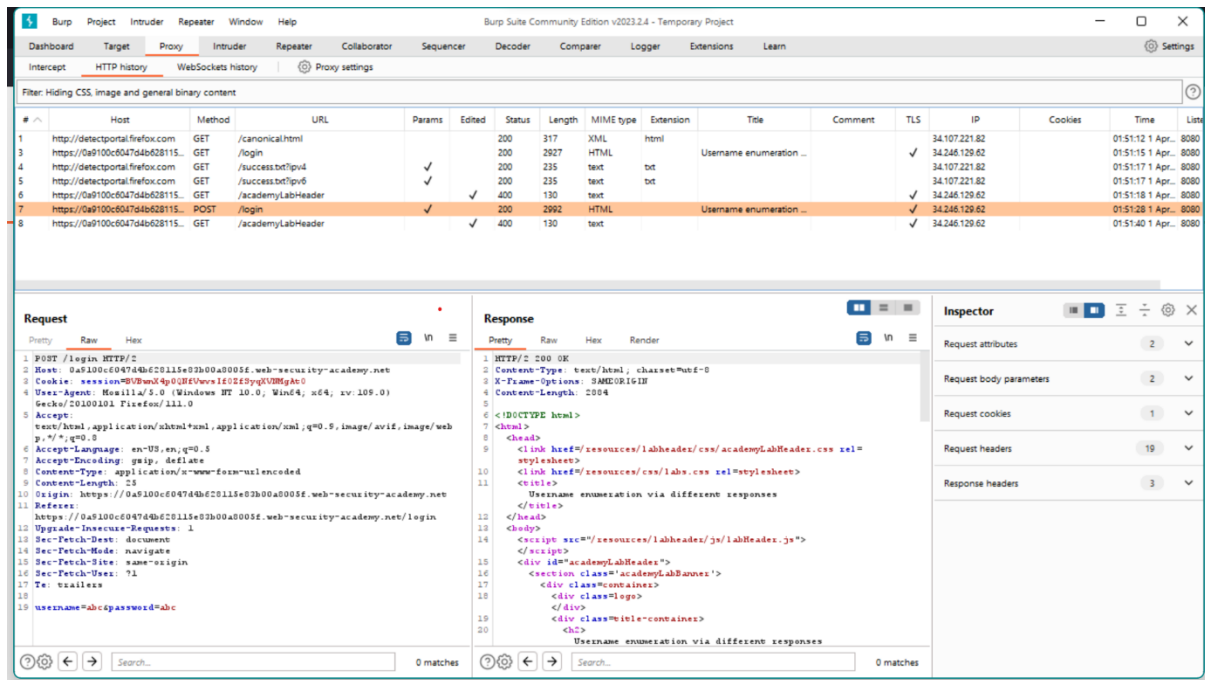
To solve the lab, enumerate a valid username, brute-force this user's password, then access their account page.

Solution:

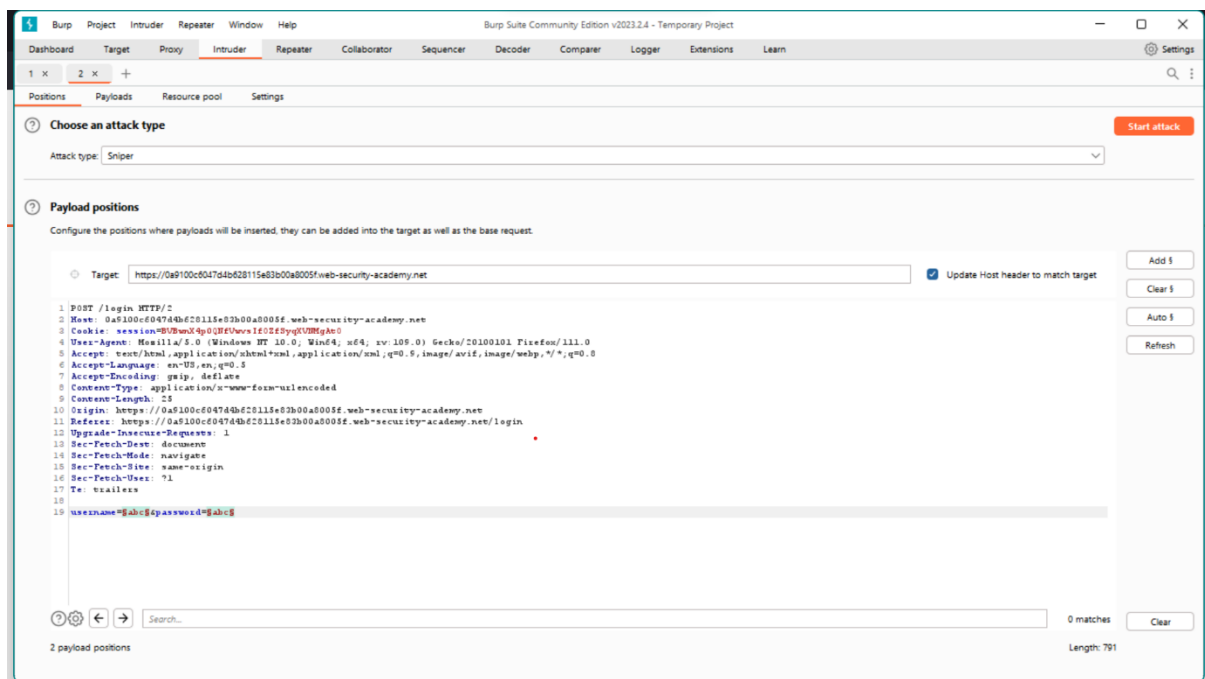
- We will be using the burp intruder for this lab.
- Once you access the lab, click on my account. Turn on your foxy proxy and intercept on burp suite.



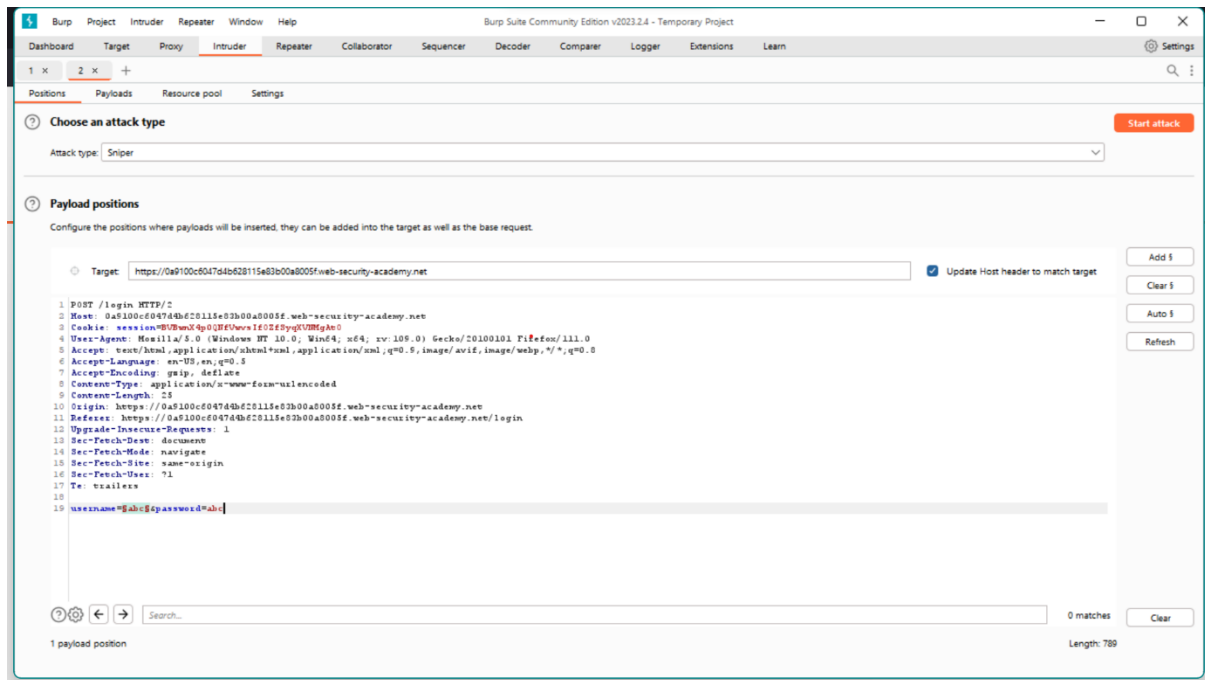
- Enter any invalid username and password and click on log in.
- Go to burp suite and forward all the packets.
- Open your HTTP History and look for a POST method with /login.



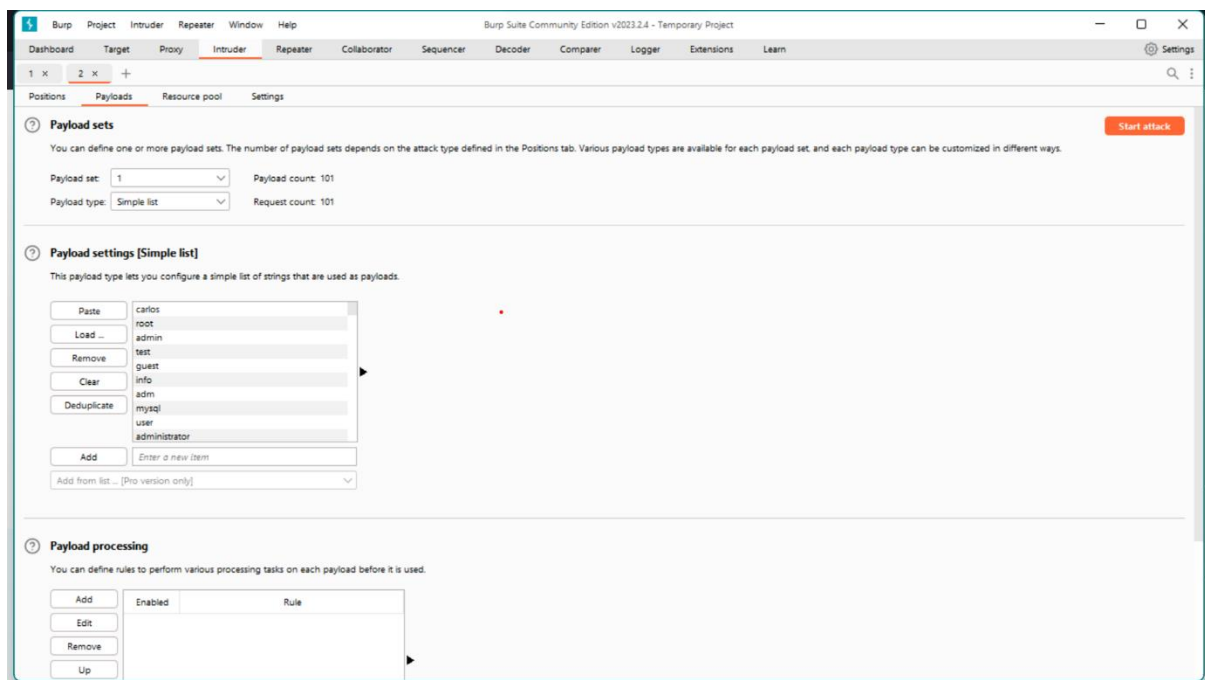
- Send that particular packet to intruder by right clicking on it and send to intruder.



- 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.

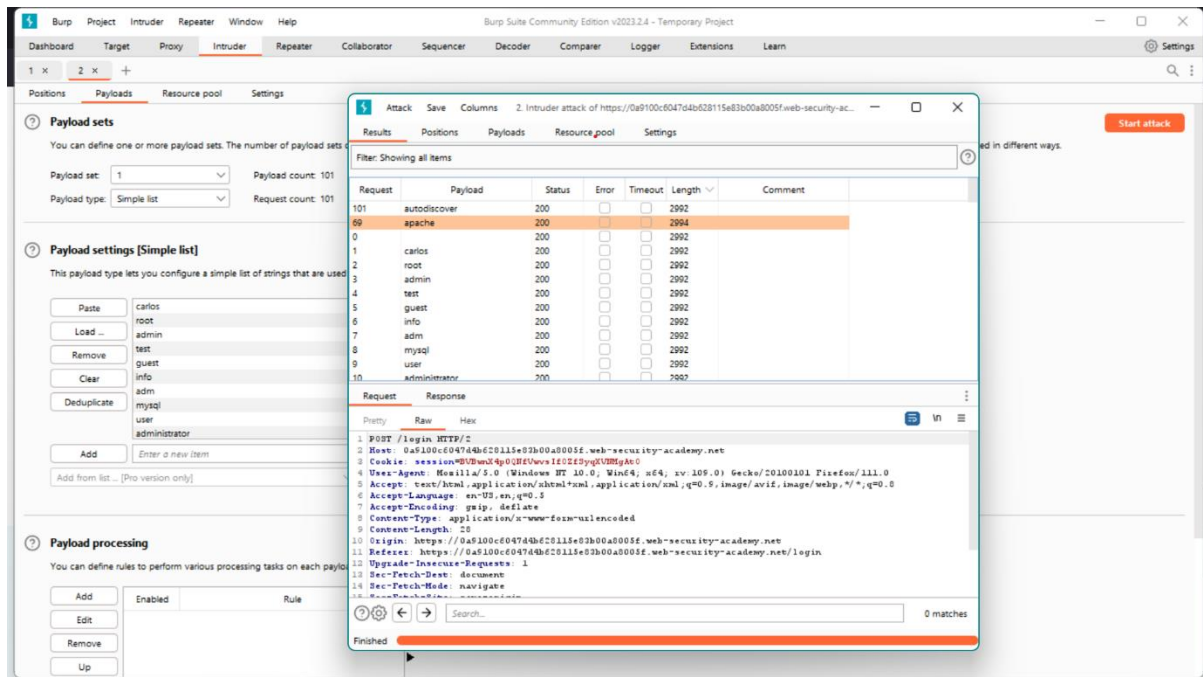


- You'll need to select the value of the username parameter and click on Add to add it as a payload.
- Open the payloads tab and make sure the type is set to simple list.
- Copy all the usernames from the link provided in the problem statement and paste them in the Payload setting(Simple list) by clicking 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. 2FA simple bypass.

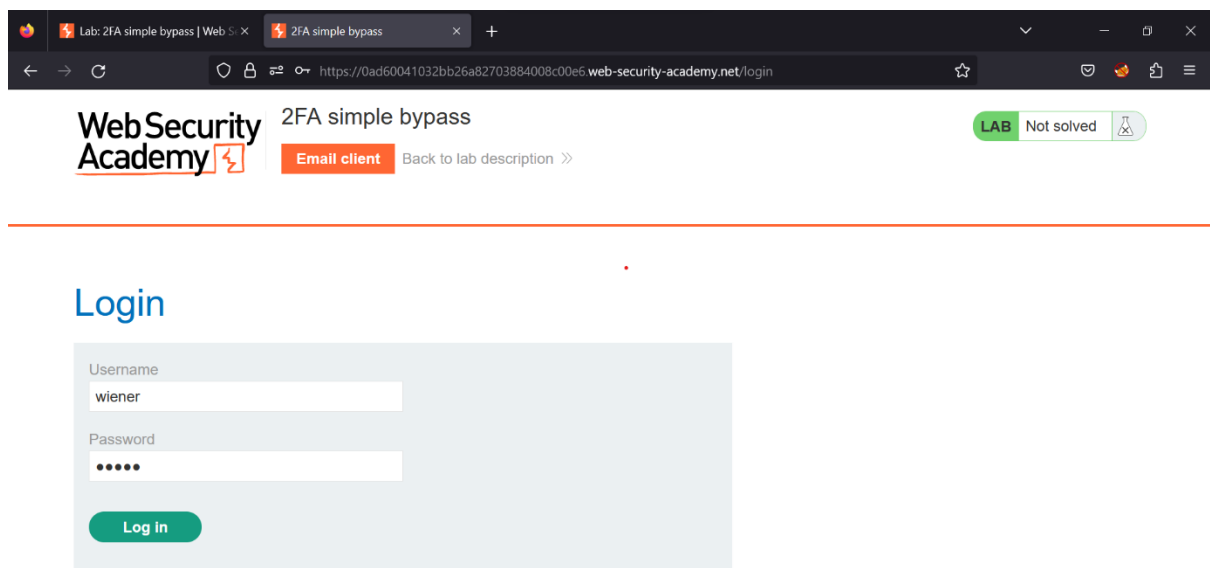
This lab's two-factor authentication can be bypassed. You have already obtained a valid username and password, but do not have access to the user's 2FA verification code. To solve the lab, access Carlos's account page.

Your credentials: wiener: Peter

Victim's credentials Carlos: Montoya

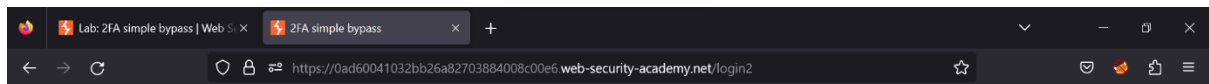
Solution:

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



The screenshot shows a web browser window with two tabs: 'Lab: 2FA simple bypass | Web Security Academy' and '2FA simple bypass'. The address bar shows the URL 'https://0ad60041032bb26a82703884008c00e6.web-security-academy.net/login'. The page header includes the 'Web Security Academy' logo, the title '2FA simple bypass', a green 'LAB' badge, and a 'Not solved' status. Below the header, there is a 'Login' section with a light blue background. It contains a 'Username' field with the value 'wiener', a 'Password' field with five dots, and a green 'Log in' button. To the right of the login fields, there is an orange 'Email client' button and a link 'Back to lab description >>'. A horizontal orange line is positioned below the login section.

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



WebSecurity Academy

2FA simple bypass

[Back to lab home](#)

[Email client](#)

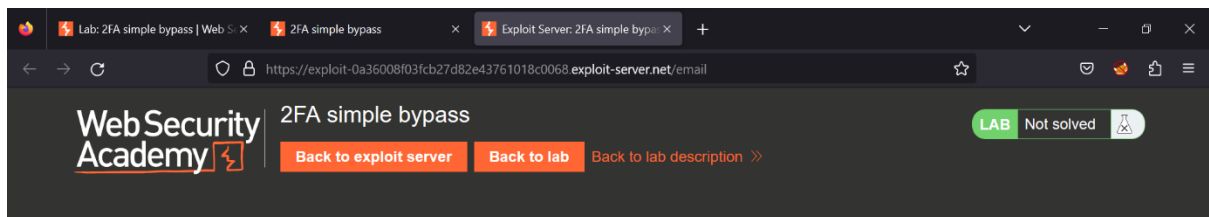
[Back to lab description >>](#)

LAB Not solved

Please enter your 4-digit security code

Login

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

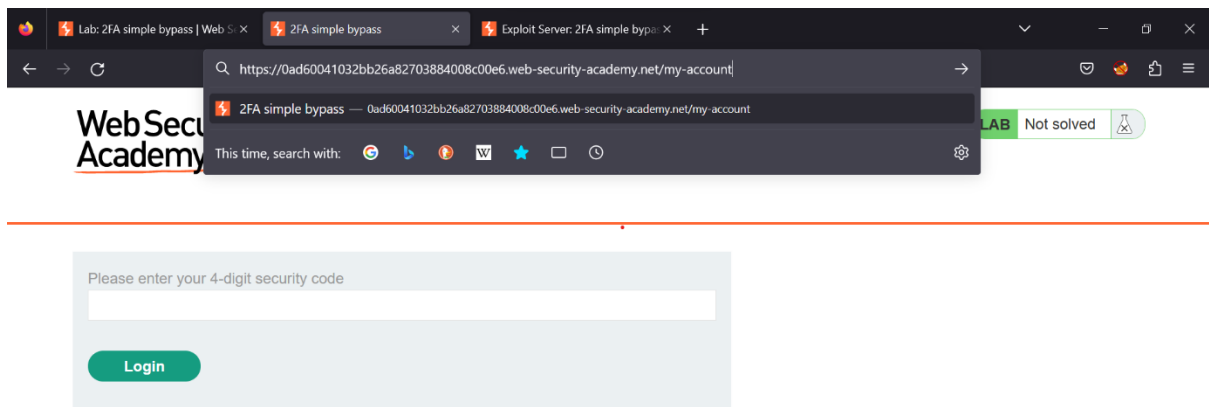
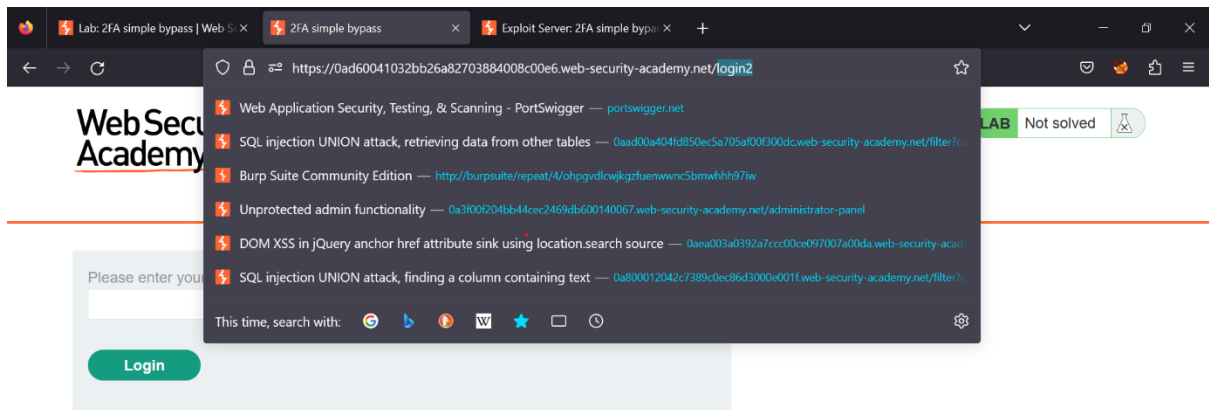


Your email address is wiener@exploit-0a36008f03fcb27d82e43761018c0068.exploit-server.net

Displaying all emails @exploit-0a36008f03fcb27d82e43761018c0068.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
				Hello!
				Your security code is 0831.
2023-03-31 20:53:47 +0000	wiener@exploit-0a36008f03fcb27d82e43761018c0068.exploit-server.net	no-reply@0ad60041032bb26a82703884008c00e6.web-security-academy.net	Security code	Please enter this in the app to continue. View raw
				Thanks, Support team

- 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. Password reset broken logic.

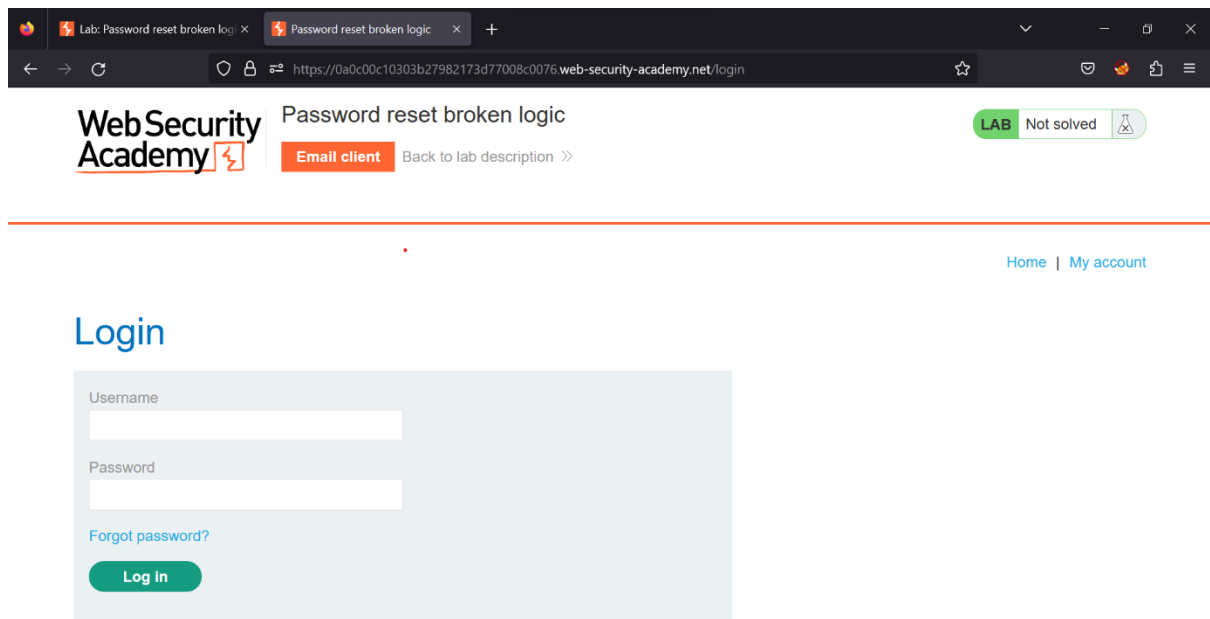
This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

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.

WebSecurity Academy Password reset broken logic LAB Not solved

[Back to lab home](#) [Email client](#) [Back to lab description](#)

Home | My account

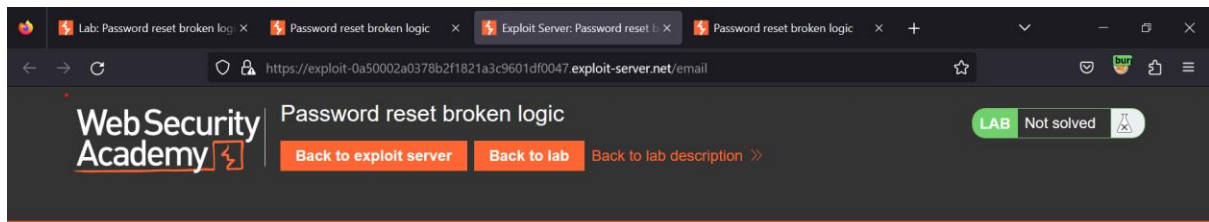
Please enter your username or email

wiener

[View Saved Logins](#)

Submit

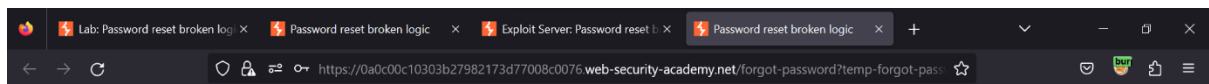
- Click the Email client button to view the password reset email that was sent. Click the link in the email and reset your password to whatever you want.



Your email address is `wiener@exploit-0a50002a0378b2f1821a3c9601df0047.exploit-server.net`

Displaying all emails @exploit-0a50002a0378b2f1821a3c9601df0047.exploit-server.net and all subdomains

Sent	To	From	Subject	Body	
2023-03-31 21:05:07 +0000	wiener@exploit-0a50002a0378b2f1821a3c9601df0047.exploit-server.net	no-reply@0a0c00c10303b27982173d77008c0076.web-security-academy.net	Account recovery	<p>Hello!</p> <p>Please follow the link below to reset your password.</p> <p>https://0a0c00c10303b27982173d77008c0076.web-security-academy.net/forgot-password?temp-forgot-password-token=084NdqC9nHuTMXfp5JzV3X13jvAFsBjj</p> <p>Thanks, Support team</p>	View raw



New password

Confirm new password

- 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.

The screenshot displays the Burp Suite interface. The top menu bar includes Dashboard, Project, Intruder, Repeater, Window, and Help. The main toolbar shows various tools like Intercept, HTTP history, WebSockets history, and Proxy settings. The HTTP history table lists several requests, with the selected request being a POST to /forgot-password/temp-forgot-password-token. The detailed view of this request shows the raw data in the Request tab, including headers like Host, User-Agent, and Content-Type, and the body containing a token and a new password. The Response tab shows the server's reply, which is an HTTP 200 OK with a Content-Type of text/html. The Inspector panel on the right provides a structured view of the request and response attributes, query parameters, body parameters, cookies, headers, and footers.

#	Host	Method	URL	Params	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Li
41	https://0a0c00c10303b27982173...	GET	/forgot-password/temp-forgot-passw...		200	3244	text/html		Password reset broken L...		✓	79.125.84.16		02:35:49 1 Apr...	806
42	https://0a0c00c10303b27982173...	GET	/academyLabHeader		200	130	text				✓	79.125.84.16		02:35:49 1 Apr...	806
43	https://0a0c00c10303b27982173...	GET	/canonical.html		200	317	XML	html			✓	34.107.221.82		02:36:14 1 Apr...	806
44	https://0a0c00c10303b27982173...	GET	/successbetipiv4		200	235	text	txt			✓	34.107.221.82		02:36:19 1 Apr...	806
45	https://0a0c00c10303b27982173...	GET	/successbetipiv4		200	235	text	txt			✓	34.107.221.82		02:36:19 1 Apr...	806
46	https://0a0c00c10303b27982173...	POST	/forgot-password/temp-forgot-passw...		200	81					✓	79.125.84.16		02:36:39 1 Apr...	806
47	https://0a0c00c10303b27982173...	GET	/		200	8433	HTML		Password reset broken L...		✓	79.125.84.16		02:36:42 1 Apr...	806
48	https://0a0c00c10303b27982173...	GET	/academyLabHeader		200	130	text				✓	79.125.84.16		02:36:42 1 Apr...	806
49	https://0a0c00c10303b27982173...	GET	/post/postid=5		200	6822	HTML		Password reset broken L...		✓	79.125.84.16		02:36:54 1 Apr...	806
50	https://0a0c00c10303b27982173...	GET	/resources/images/avatarDefault.svg		200	10005	XML	svg			✓	79.125.84.16		02:36:58 1 Apr...	806
51	https://0a0c00c10303b27982173...	GET	/academyLabHeader		200	130	text				✓	79.125.84.16		02:36:59 1 Apr...	806

```

Request
1 POST /forgot-password/temp-forgot-password-token=004B4qC6nHnTHKTP5JvU3K13jvAfeBj HTTP/2
2 Host: 0a0c00c10303b27982173d77008c0076.web-security-academy.net
3 Cookie: session=0a39gHtby0TqG0Dnlv0E3p3v00g715W
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 115
10 Origin: https://0a0c00c10303b27982173d77008c0076.web-security-academy.net
11 Referer: https://0a0c00c10303b27982173d77008c0076.web-security-academy.net/forgot-password/temp-forgot-password-token=004B4qC6nHnTHKTP5JvU3K13jvAfeBj
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 temp-forgot-password-token=004B4qC6nHnTHKTP5JvU3K13jvAfeBj&username=
20 w1ne3cnew&password=1m3te3cnew&password=2m3te3cnew

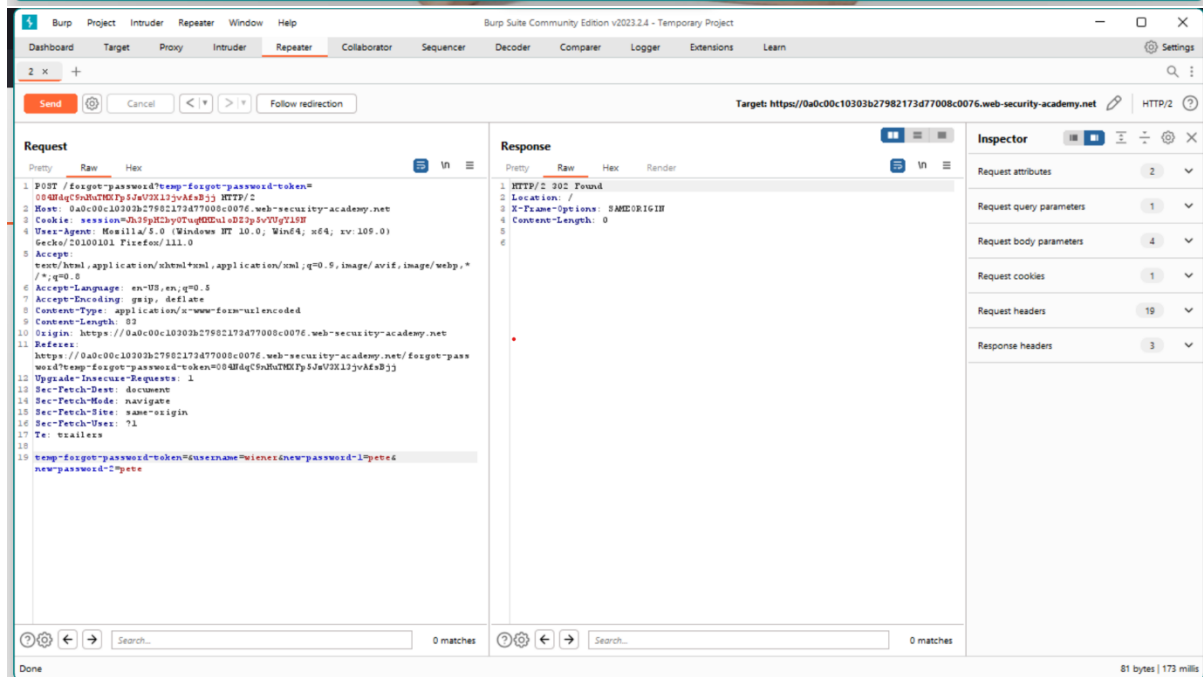
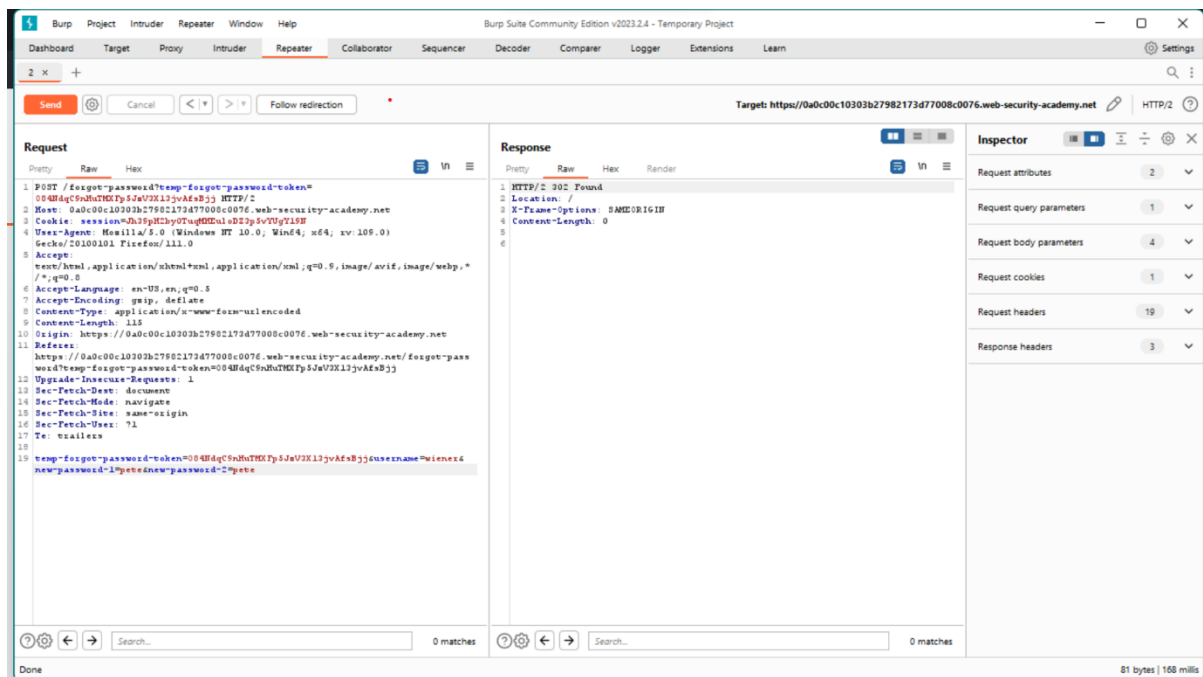
```

```

Response
1 HTTP/2 200 Found
2 Location: /
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 0
5
6

```

- 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.