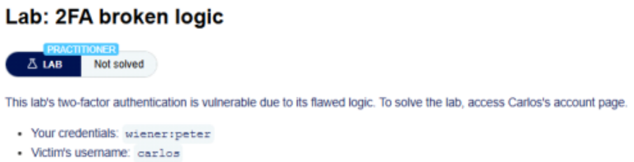
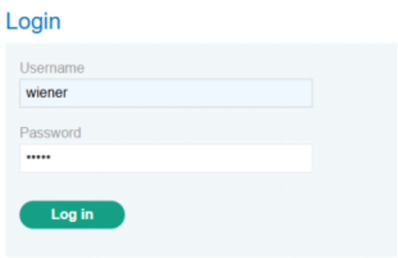
Lab- 2FA broken logic

lundi 4 août 2025 22:13

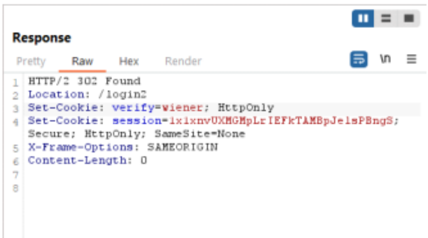


Le but de ce lab est d'utiliser la vulnérabilité du cookie pour se connecter sur le compte d'un autre user.



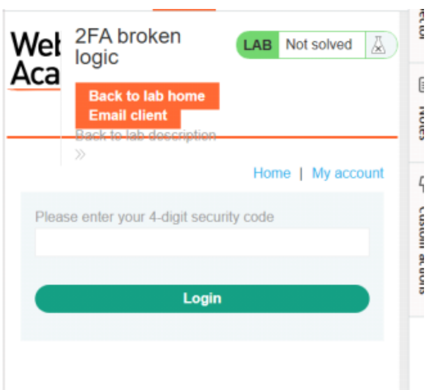

```
POST /login HTTP/2
Host:
0ac700b6043aa55083ca41890058000б.web-security-academy.
net
Cookie: verify=wiener; session=
OkpsVYCBAdOVjsBYRo21NgjZvdiE1CVw
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: fr-FR,fr;q=0.9
Origin:
https://0ac700b6043aa55083ca418900580006.web-security-
academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 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://0ac700b6043aa55083ca418900580006.web-security-
academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=wiener&password=peter
```

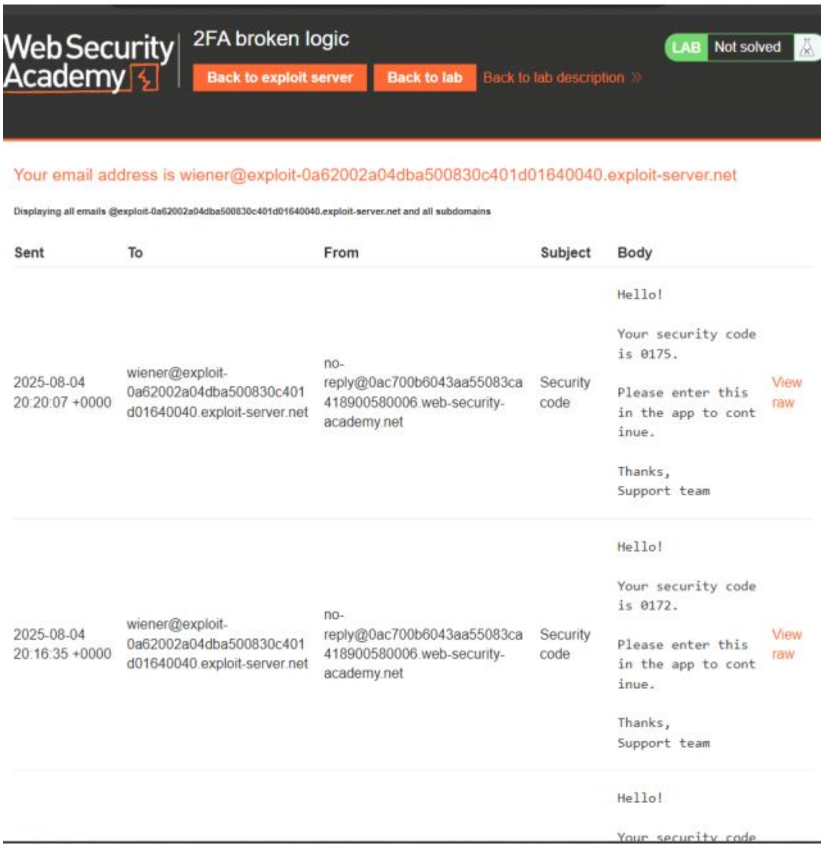



```
HTTP/2 302 Found
Location: /login2
Set-Cookie: verify=wiener; HttpOnly
Set-Cookie: session=1x1xnvUXMGMpLrIEFkTAMBpJelsPBngS;
Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

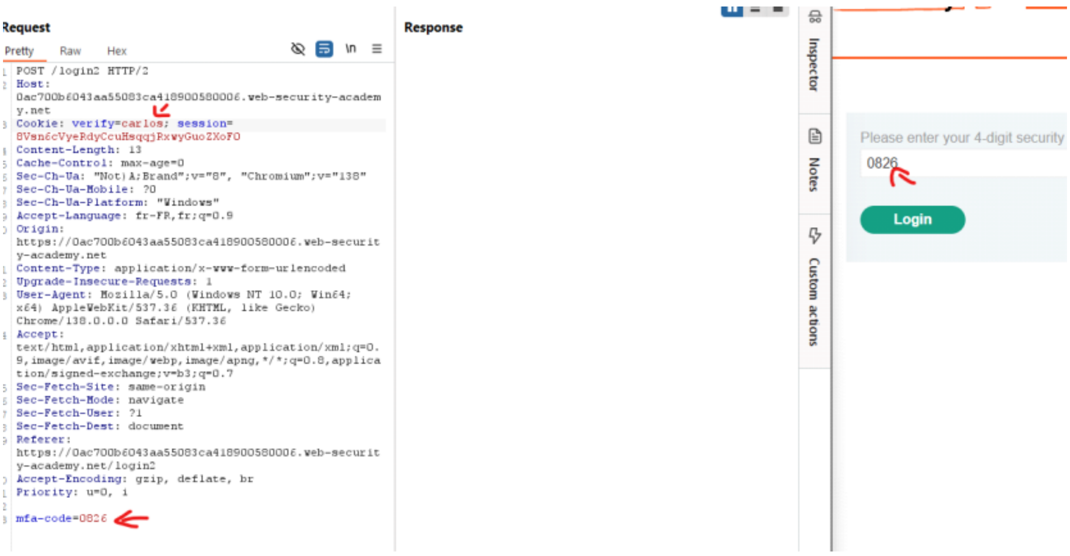
On arrive sur la page qui nous demande de rentrer le code de vérification :

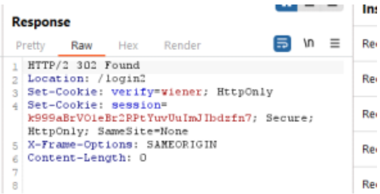


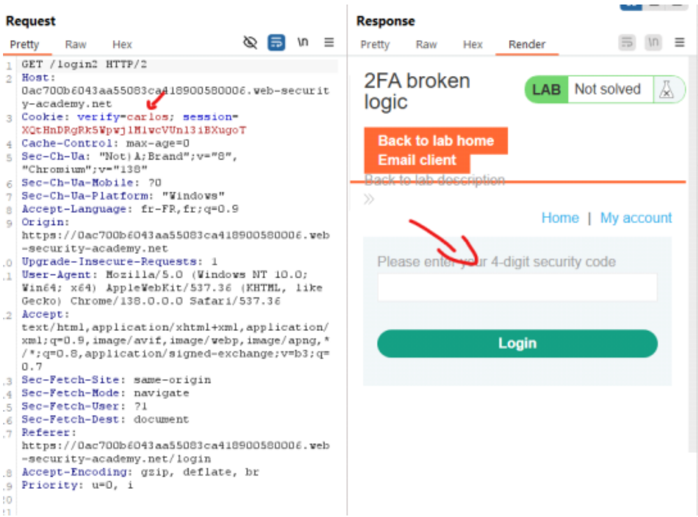
On va sur notre mail :



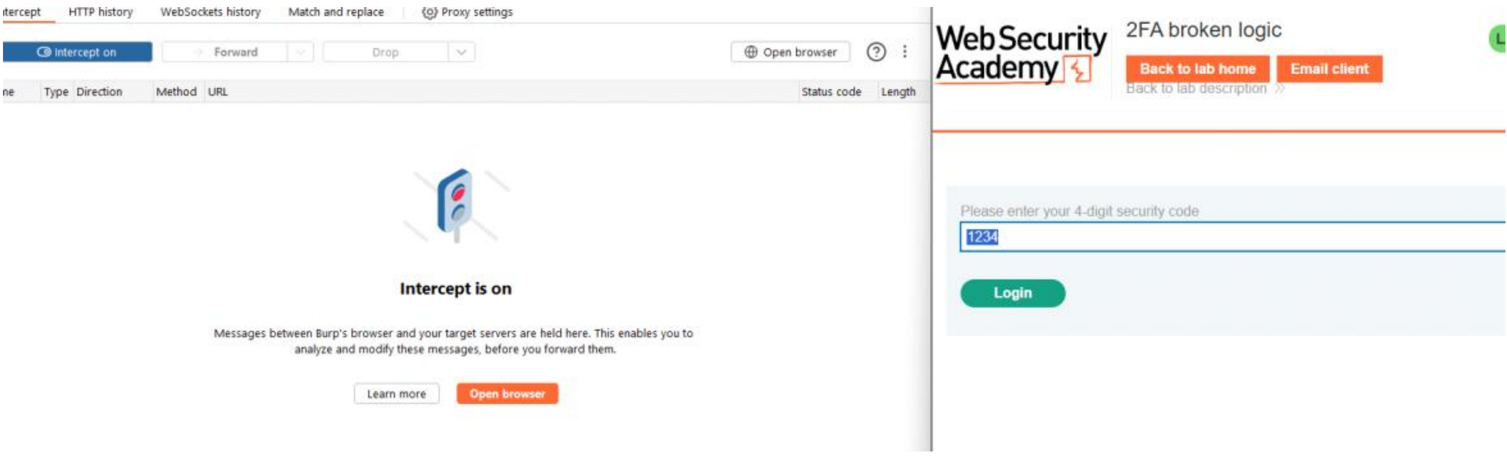
Et c'est là où la magie commence :

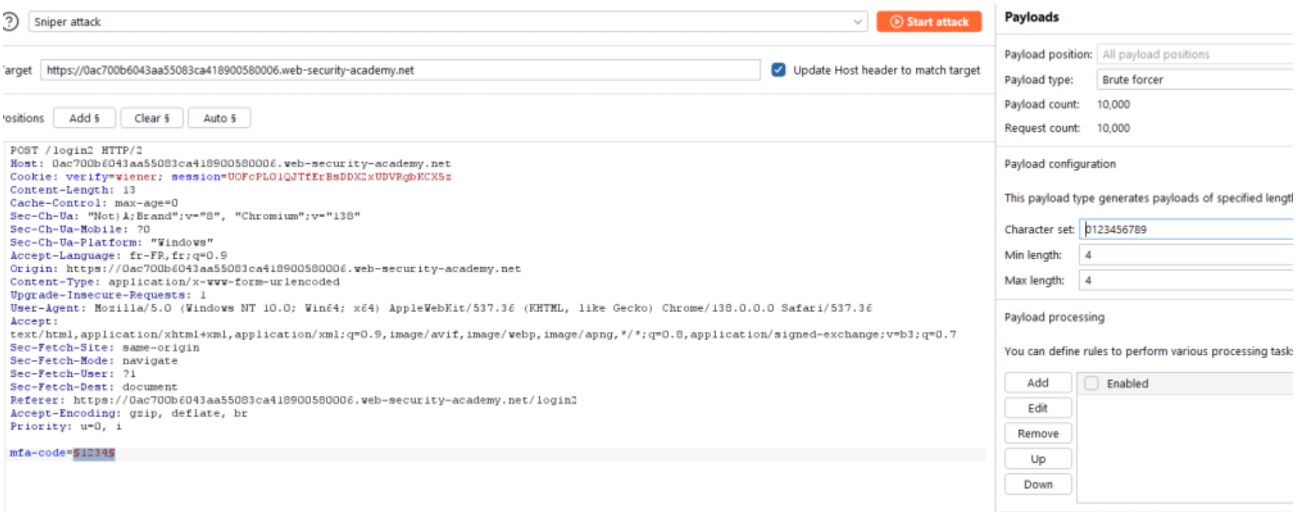






Bon ici on a pu accéder à la demande de vérification avec le code donc ça veut dire qu'on a envoyé un mail avec un code au user Carlos. On peut essayer de brute forcer vu qu'on a pas accès à son mail.





Idem vu que je n'ai pas burpsuite pro c'est juste galère à résoudre ce chall donc go le refaire plus tard, un jour.