Documentation 2FA

BYPASS 1

1. Création de compte et connexion

#a Se rendre sur le site portswigger.net
#b Se créer un compte
#c Se connecter

2. Début du détournement

#a Accéder au Lab

Web Security Academy > Authentication vulnerabilities > Multi-factor > Lab

Lab: 2FA simple bypass

APPRENTICE

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`

ACCESS THE LAB

💡 Solution

💡 Community solutions

#b Se connecter avec les identifiants

```
wienner
peter
```

Accéder au boîte mail et rentrer le code à double authentification

Congratulations, you solved the lab!   Share your skills!   𝕏   in   Continue learning »

Your email address is wiener@exploit-0a74008b035a83ef82dd507601a5007f.exploit-server.net

Displaying all emails @exploit-0a74008b035a83ef82dd507601a5007f.exploit-server.net and all subdomains

| Sent	To	From	Subject	Body	
2025-03-26 13:18:56 +0000	wiener@exploit-0a74008b035a83ef82dd507601a5007f.exploit-server.net	no-reply@0a53004c038083d282a851f200c90066.web-security-academy.net	Security code	Hello! Your security code is 0840. Please enter this in the app to continue. Thanks, Support team	View raw

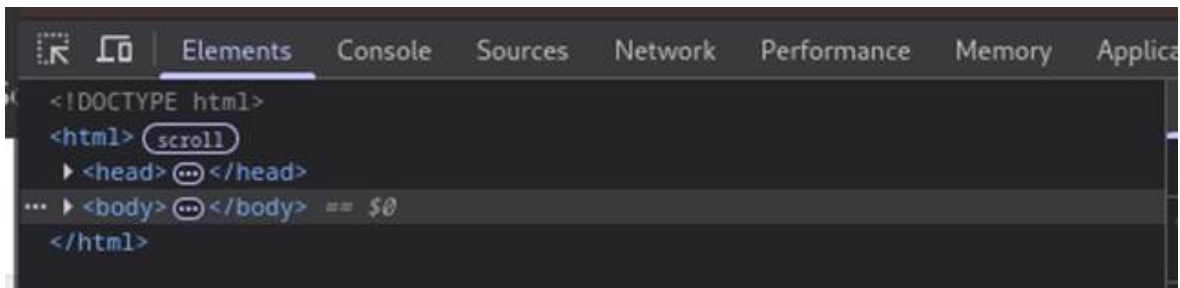Se deconnecter et changer de compte avec les identifiants

```
carlos
montoya
```
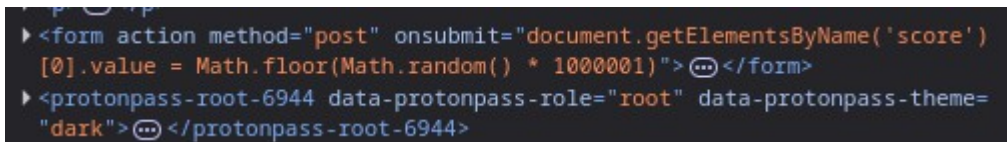
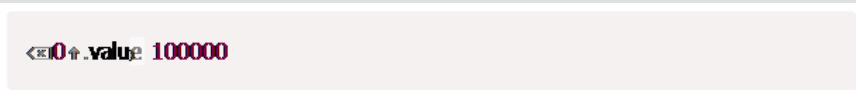# BURPSUITE - HTTP – POST

##1. D'abord on ouvre la console avec F12 du clavier
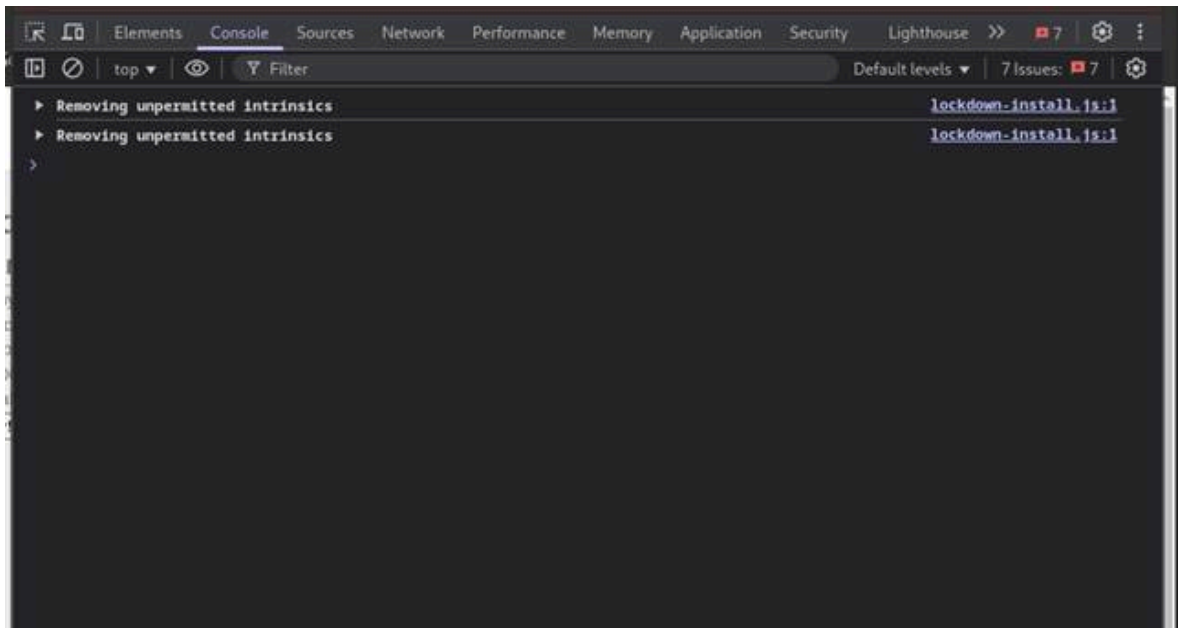
##2. Une fenêtre comme ceci apparaîtra aller dans la rubrique 'Elements' puis cliquer sur body

##3. Cliquer sur le dépliant de body


```
<form action method="post" onsubmit="document.getElementsByName('score')
[0].value = Math.floor(Math.random() * 1000001)"> </form>
<protonpass-root-6944 data-protonpass-role="root" data-protonpass-theme=
"dark"> </protonpass-root-6944>
```

##4. On va modifier la ligne et on va mettre ceci:

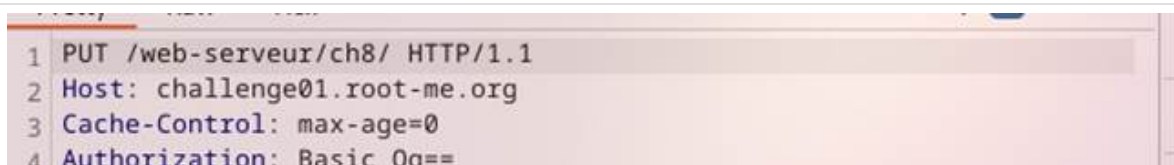0 .value 100000
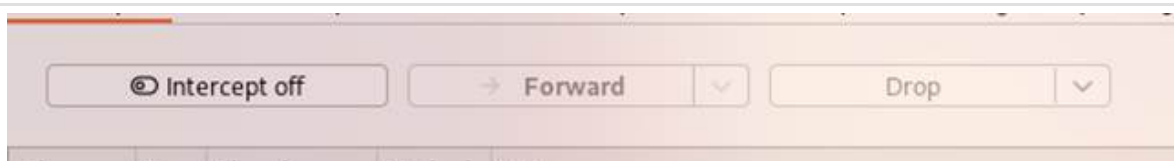
BURPSUITE - HTTP – Verb Tampering

##1. On s'y rend dans la rubrique proxy

##2. On clique sur open browser

On copie le lien du challenge root me on met sur burp browser

On active Interception


```
1 PUT /web-serveur/ch8/ HTTP/1.1
2 Host: challenge01.root-me.org
3 Cache-Control: max-age=0
4 Authorization: Basic 0g==
```

##3. On replace GET par PUT puis on clique sur 'Forwad' et le mot de passe s'affiche

Mot de passe / password : a23e$dme96d3saez$$prap