PLOUZENNEC Eliaz

CTF : trouver login et mot de passe
Wordpress, smb

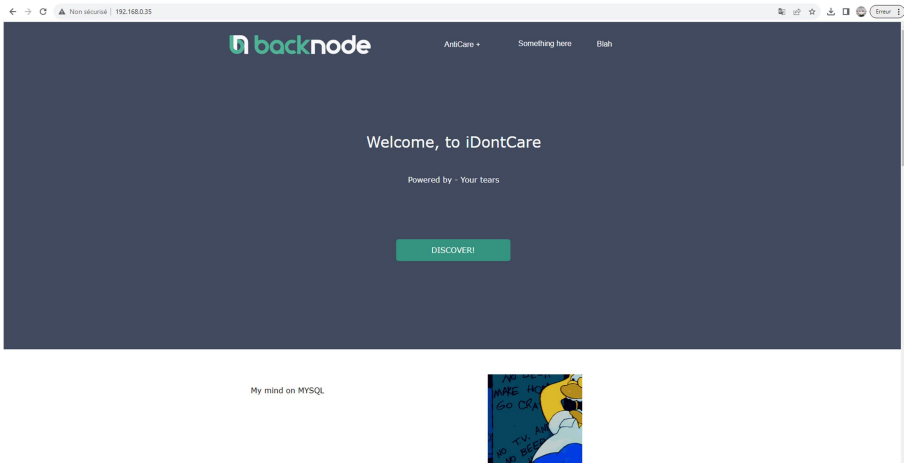
16/02/24

Contenu

Introduction :

Nous avons à notre disposition une machine avec une adresse IP : 192.168.0.35, nous devons retrouver un mot de passe et un login du wordpress 192.168.0.35/wordpress

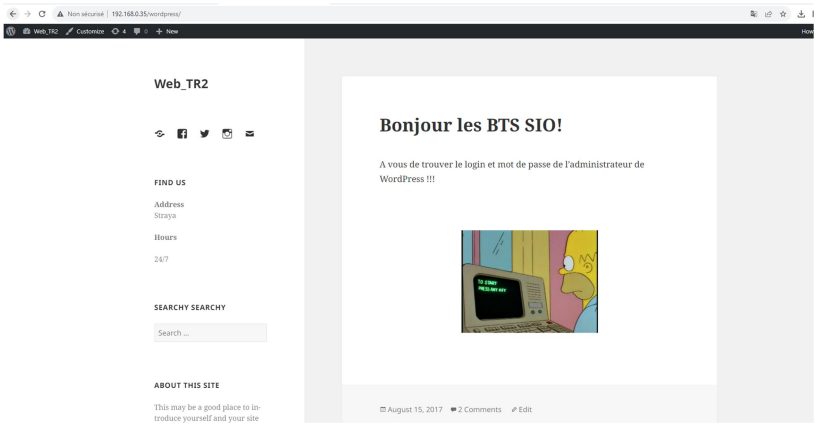
Etape 1 : Etudier la machine



Si on entre juste l'adresse IP on tombe sur ça. On peut donc rechercher avec dirb les autres pages disponibles.

```
┌──(root㉿plouzennec)-[~]
└─# dirb http://192.168.0.35/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Feb 16 11:47:44 2024
URL_BASE: http://192.168.0.35/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.35/ ----
==> DIRECTORY: http://192.168.0.35/apache/
+ http://192.168.0.35/index.html (CODE:200|SIZE:36072)
+ http://192.168.0.35/info.php (CODE:200|SIZE:77252)
==> DIRECTORY: http://192.168.0.35/javascript/
==> DIRECTORY: http://192.168.0.35/old/
==> DIRECTORY: http://192.168.0.35/phpmyadmin/
+ http://192.168.0.35/robots.txt (CODE:200|SIZE:92)
+ http://192.168.0.35/server-status (CODE:403|SIZE:292)
==> DIRECTORY: http://192.168.0.35/test/
==> DIRECTORY: http://192.168.0.35/wordpress/
==> DIRECTORY: http://192.168.0.35/wp/
```

Ainsi dirb http://192.168.0.35/ on trouve un lien vers un wordpress.

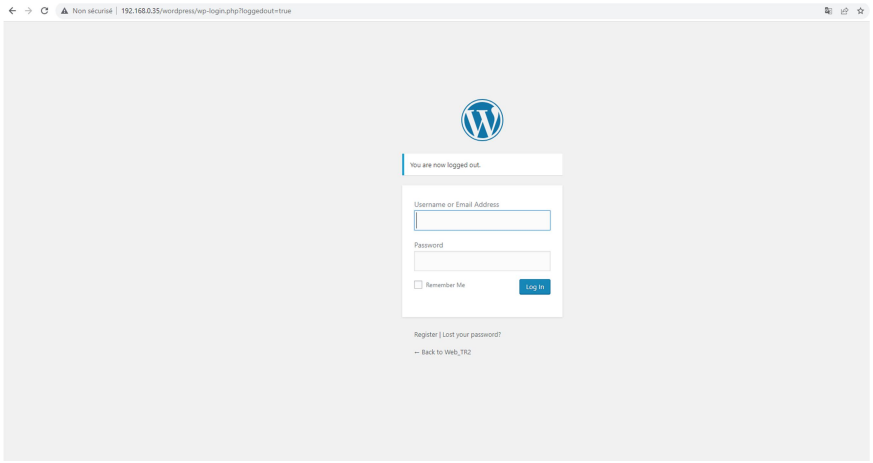


Qui ressemble à ça.

Ainsi on continue le dirb pour trouver la page de connexion au wordpress :

```
+ http://192.168.0.35/wordpress/index.php (CODE:301|SIZE:0)
==> DIRECTORY: http://192.168.0.35/wordpress/wp-admin/
==> DIRECTORY: http://192.168.0.35/wordpress/wp-content/
==> DIRECTORY: http://192.168.0.35/wordpress/wp-includes/
+ http://192.168.0.35/wordpress/xmlrpc.php (CODE:405|SIZE:42)
```

On trouve /wp-admin/, qui redirect vers wp-login.php



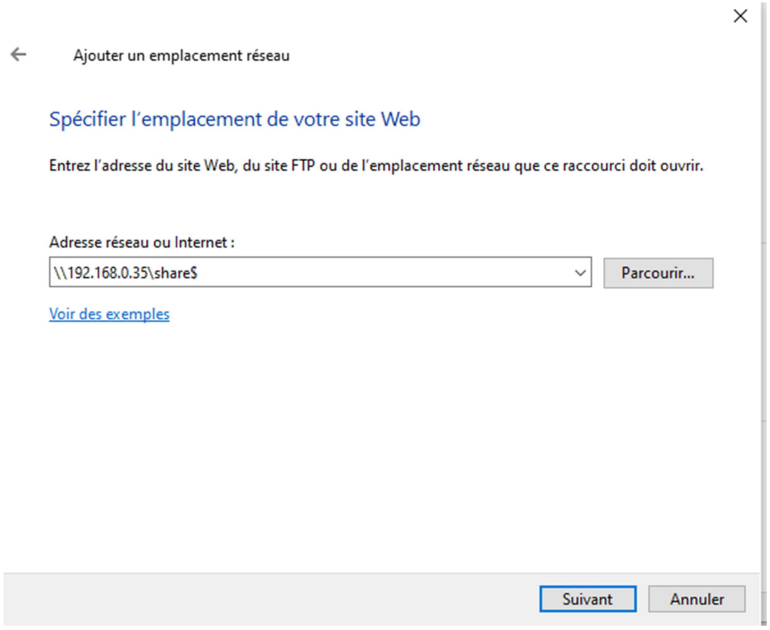
Etape 2 : Rentrer dans la machine

Connaissant le chemin vers la page de connexion, on peut desormais aller dans la machine pour trouver les fichier wordpress.

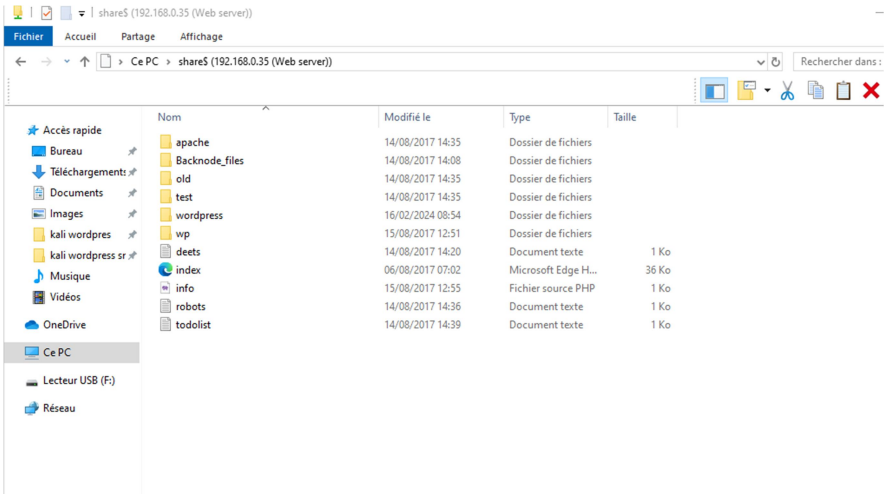
```
┌──(root㉿plouzennec)-[~]
└─# nmap -p 445 --script smb-enum-shares 192.168.0.35
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-16 11:55 CET
Nmap scan report for 192.168.0.35
Host is up (0.10s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: CC:47:40:BD:E2:06 (Unknown)

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\192.168.0.35\IPC$:
|     Type: STYPE_IPC_HIDDEN
|     Comment: IPC Service (Web server)
|     Users: 2
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\192.168.0.35\print$:
|     Type: STYPE_DISKTREE
|     Comment: Printer Drivers
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\lib\samba\printers
|     Anonymous access: <none>
|     Current user access: <none>
|   \\192.168.0.35\share$:
|     Type: STYPE_DISKTREE
|     Comment: Sumshare
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\var\www\html\
|     Anonymous access: READ/WRITE
|_    Current user access: READ/WRITE

Nmap done: 1 IP address (1 host up) scanned in 1.17 seconds
```

En rentrant cette commande, on trouve les faille de la machine smb, et dans le 3eme paragraphe on y trouve « \\192.168.0.35\share$ » avec ensuite Anonymous access : READ/WRITE , ce qui signifie qu'à ce chemin de partage sur l'adresse IP on peut trouver les dissier wordpress, sans connexion, et en libre accès.

On peut donc rentrer ce chemin dans rajouter un emplacement reseau sur un autre pc, ce qui donne :



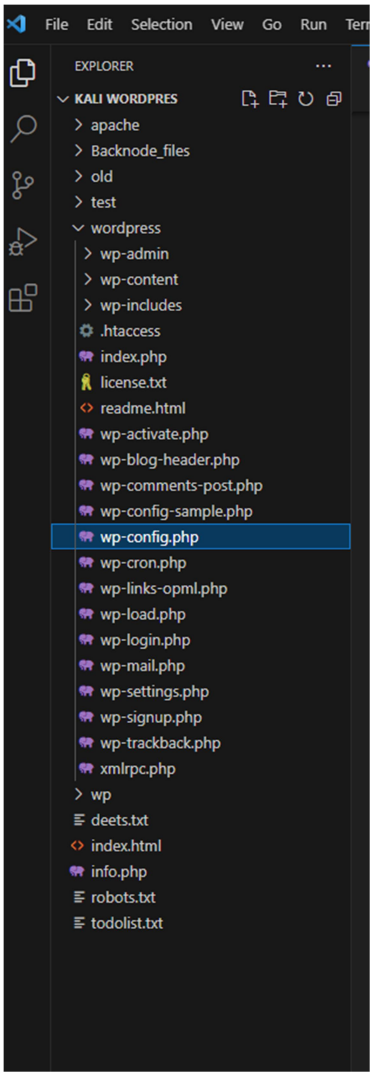
On a ensuite acces à cette page :



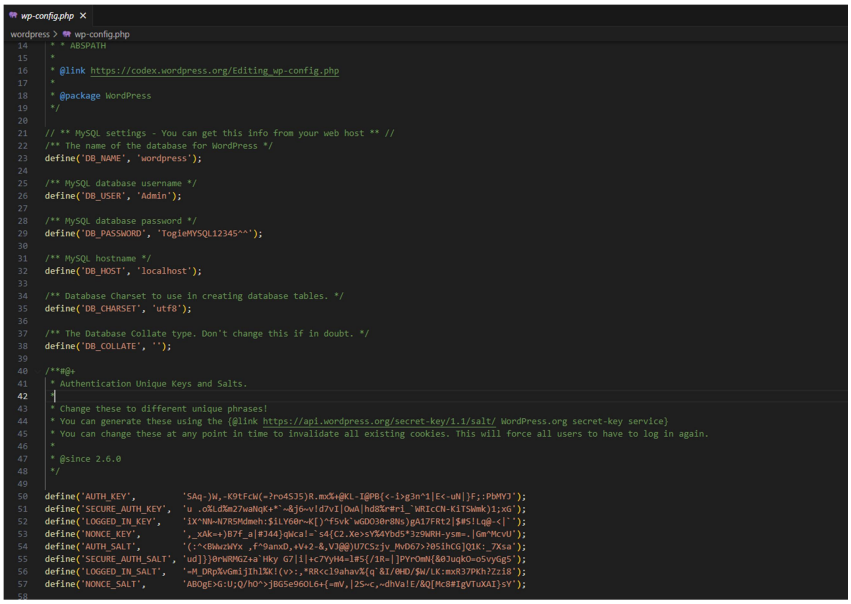
On y trouve tous les fichier wordpress.

Etape 3 : Exploiter les fichiers WordPress

Il ne reste plus qu'à mettre les fichier dans visual studio code pour les examiner, et aller à ce chemin, parce que c'est l'endroit où les identifiants et mot de passe sont stockés :

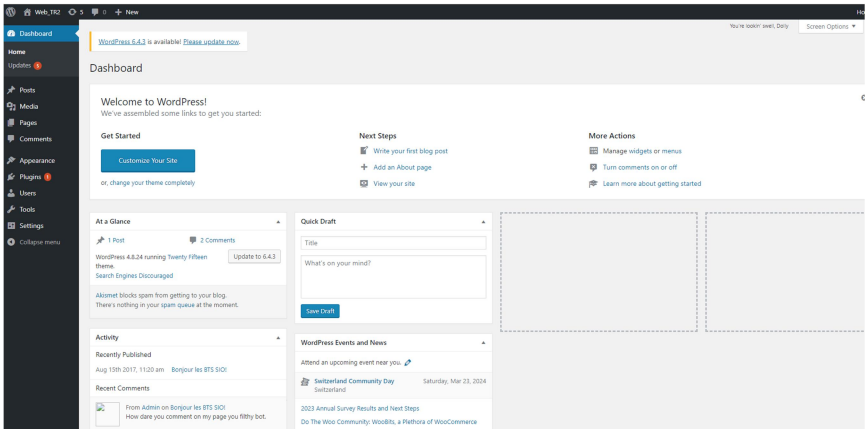


Pour trouver cette page :



Qui repertorie le login et mot de passe d'Admin, ici le mot de passe est TogieMYSQL12345^^

Plus qu'à rentrer le ça dans l'identification Wordpress :



Et accéder à Wordpress.