PenTest 2

ROOM A

MODUS POTENT

Members:

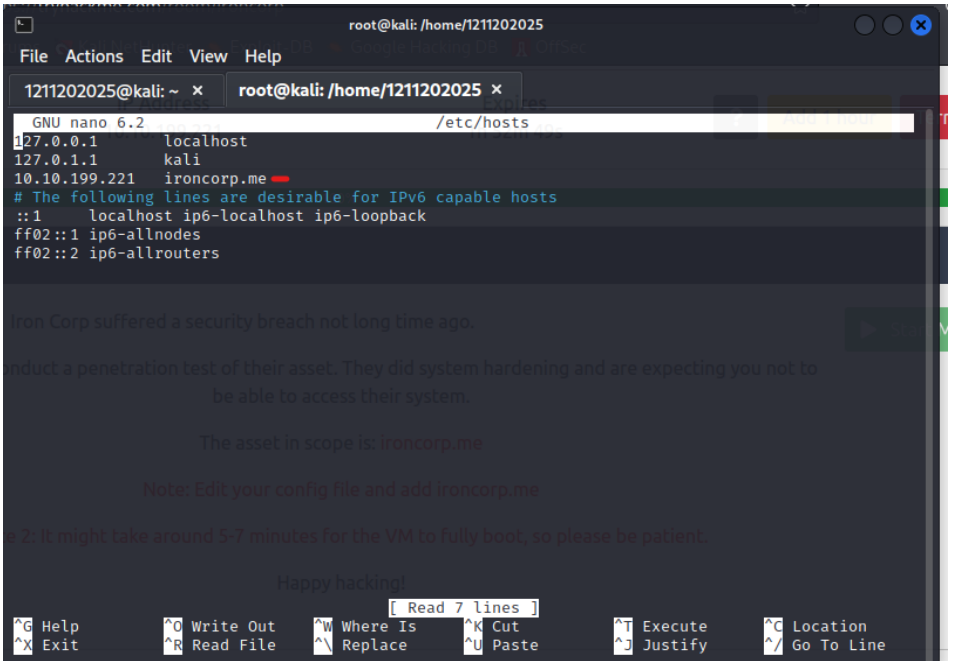
ID	NAME	ROLE
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Leader
1211202025	Abdullah Bin Kamaruddin	Member
1211103649	Nur Qistina Binti Roslan	Member

Recon and Enumeration

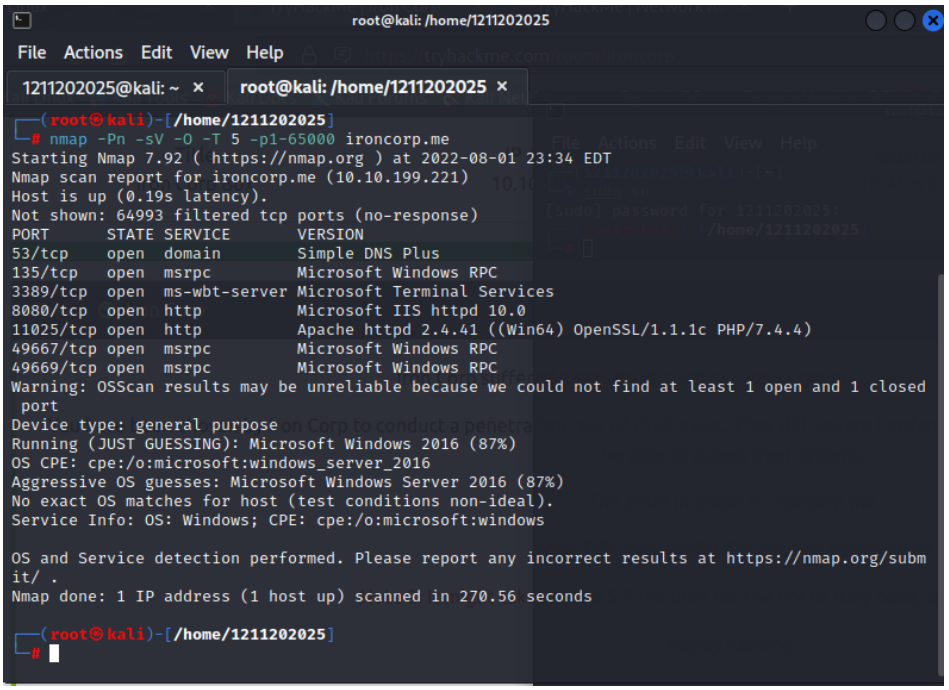
Members Involved: Abdullah

Tools Used: Kali Linux, Terminal, Firefox, nano, cat, Nmap, Hydra, Dig, Burp, OWASP, apache

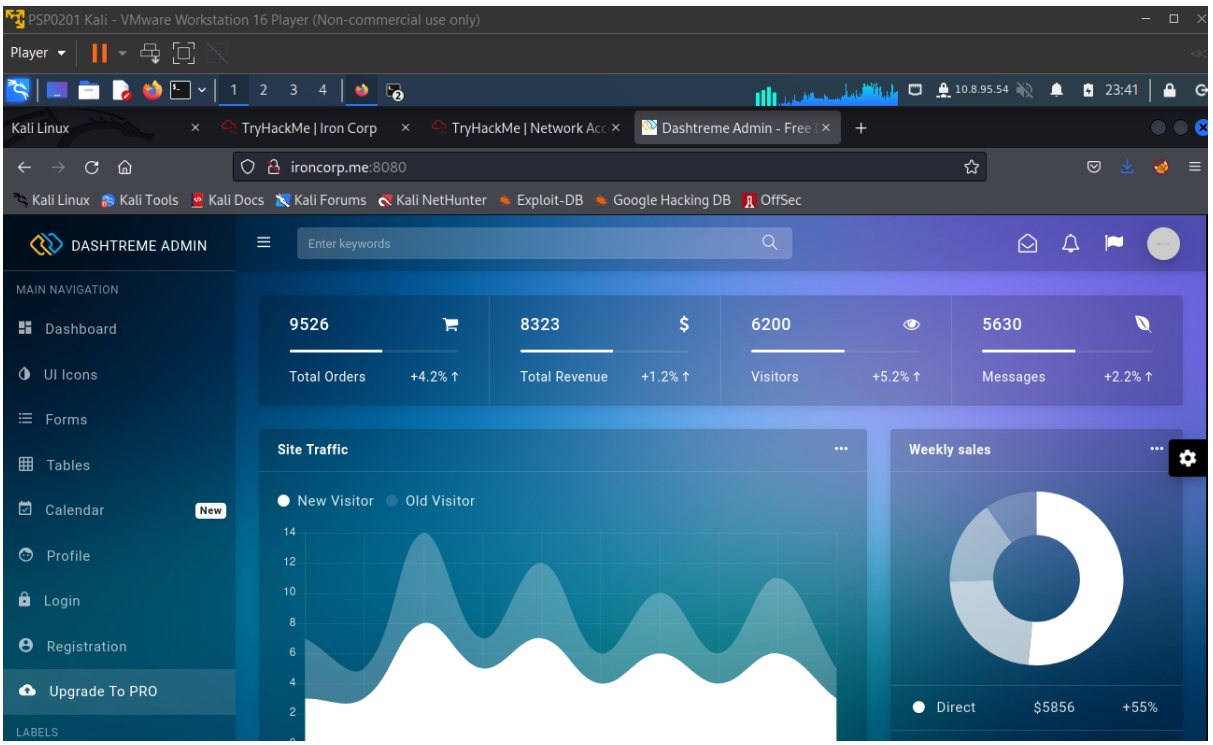
Firstly we will go onto the root kali and edit out the hosts by adding one more with the name ironcorp.me. We will set the IP Address with the newly made host, ironcorp.me.



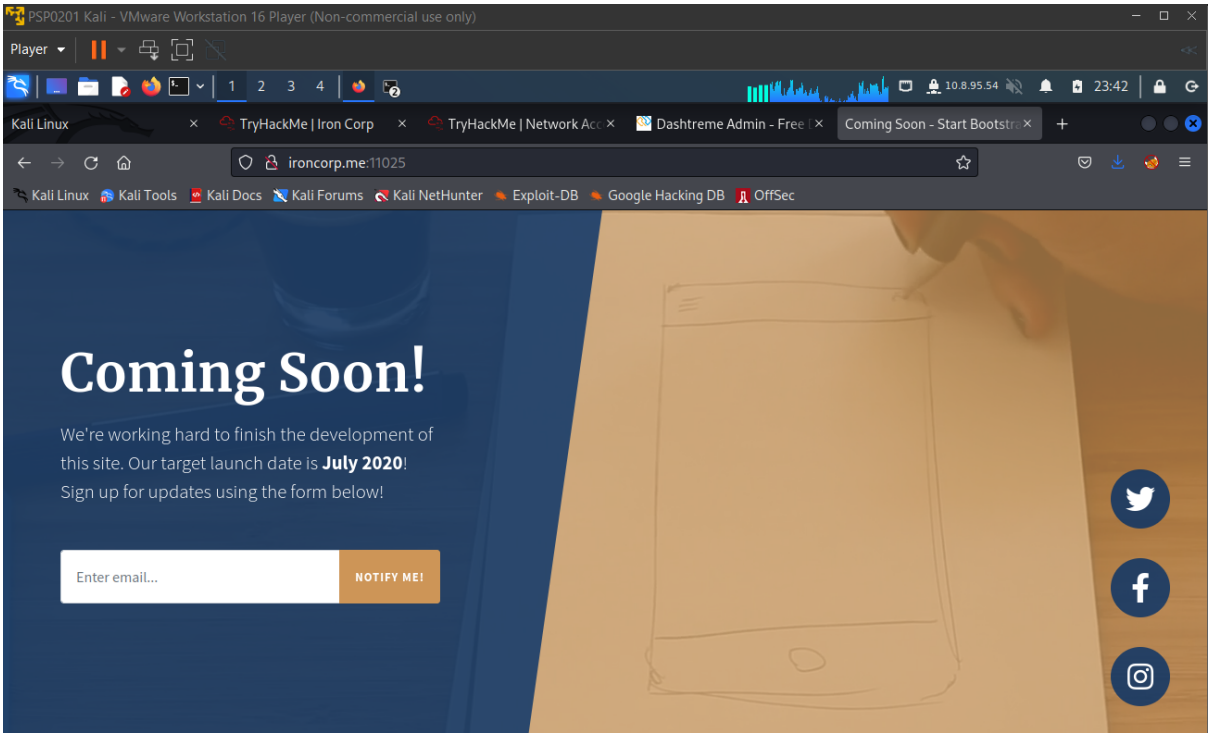
Then we will start an nmap of the ironcorp.me and find out that there are 7 open ports with 2 of them being http ports. We will check these two ports out on firefox



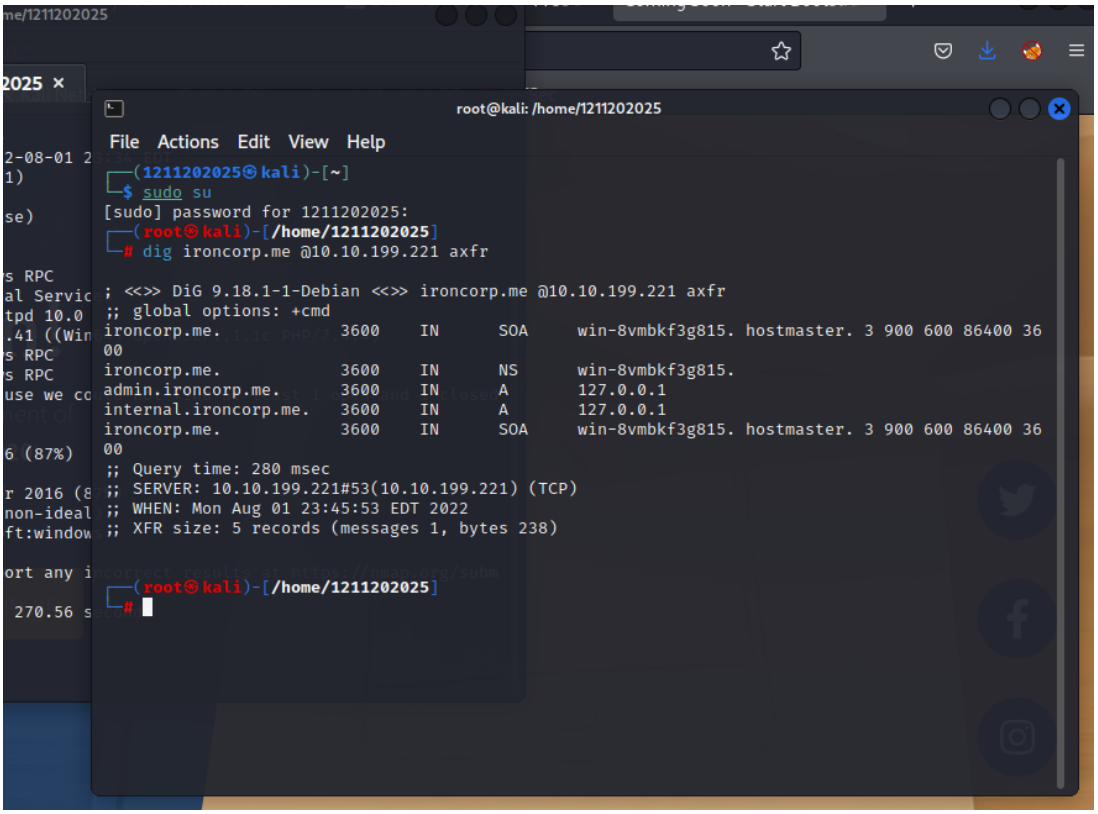
We opened the port 8080 first and we found out that the title of the website is called Dashtreme Admin. It shows multiple statistics and graphs of some sort of business. We will now check the other port and see what is on that port.



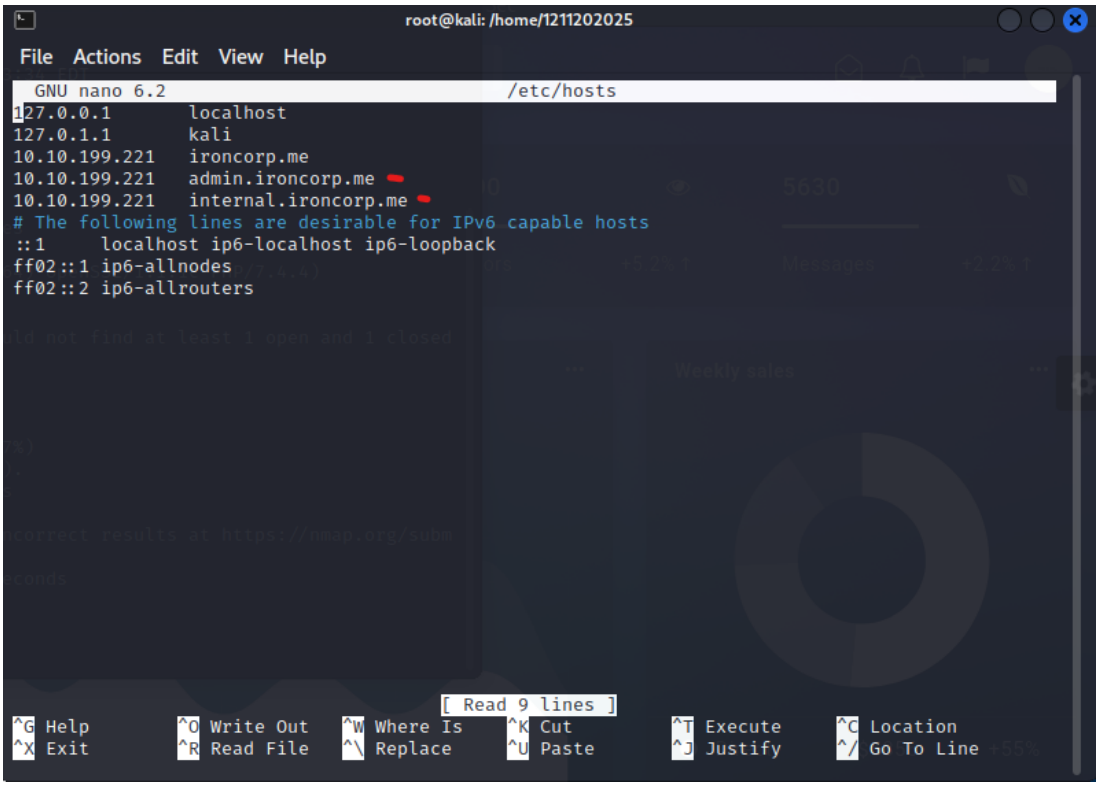
Opening port 11025, we get another page related to the business. This time it is like an enquiry page for customers to keep up to date with the business. Nothing really important as of now.



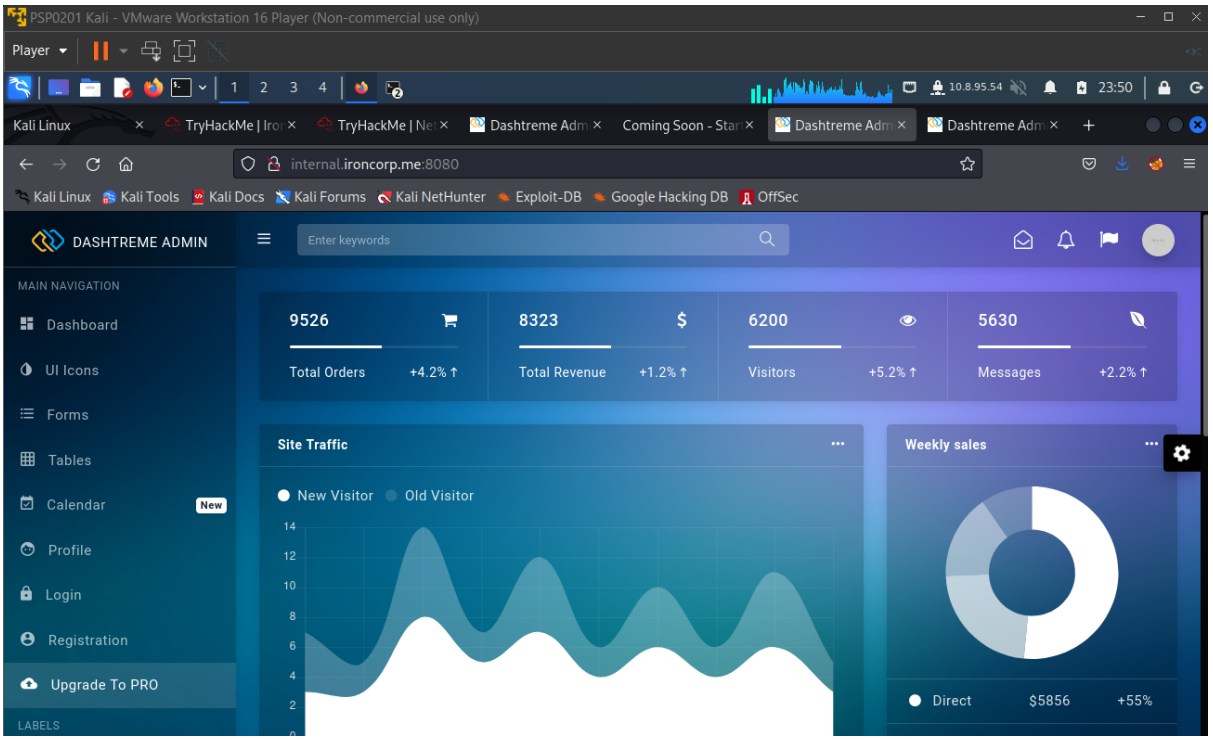
On the terminal, we will do the sudo su to switch user to root and we will dig ironcorp.me at 10.10.199.221. The “axfr” command reveals resource records including subdomain names for free.

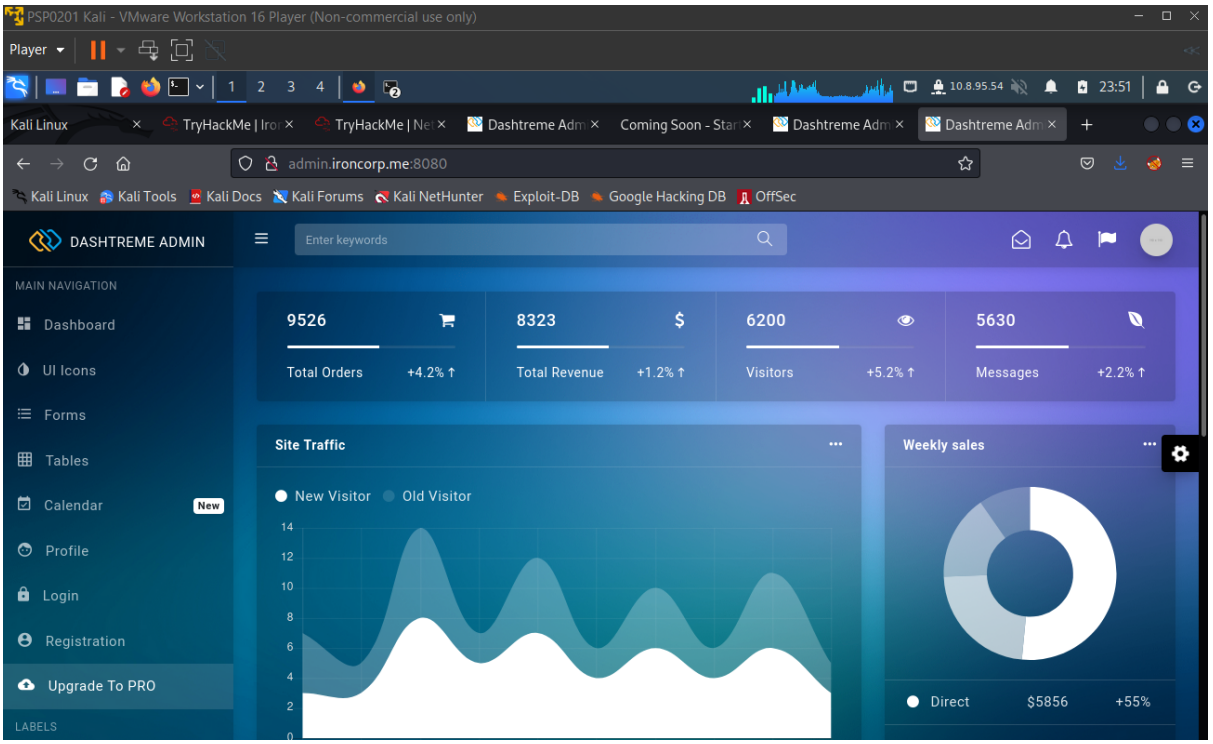


Knowing by the results of our digging in ironcorp, we put in the admin.ironcorp.me and the internal.ironcorp.me in the hosts file, along with the IP address.

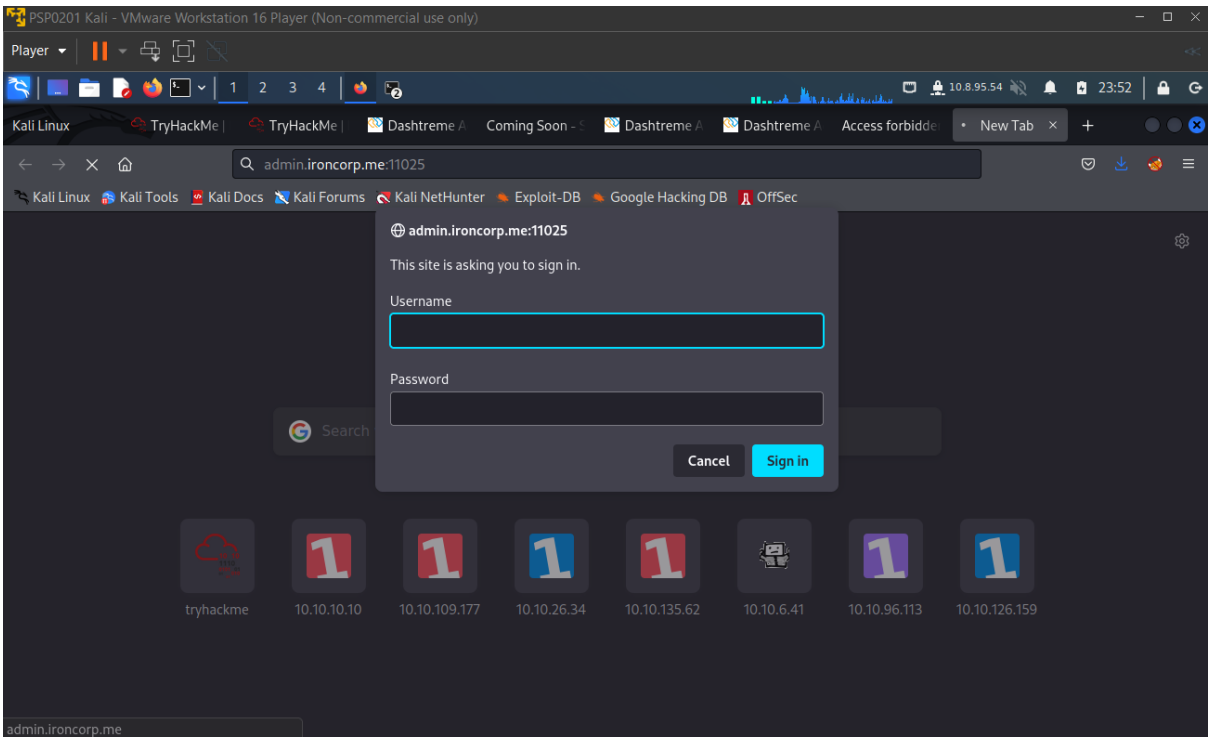


Checking each one of it with different portals; 8080 and 11025. Port 8080 is pretty much useless to our advantage.

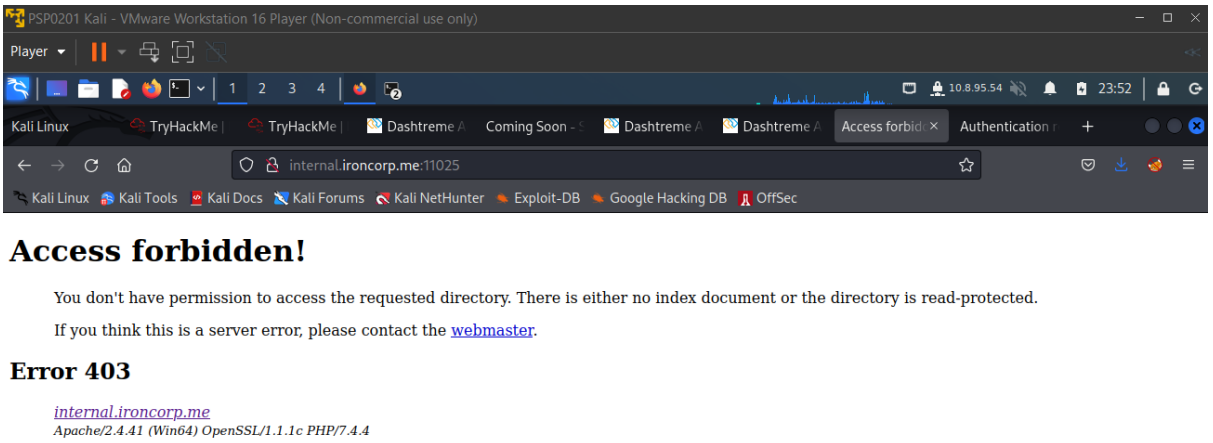




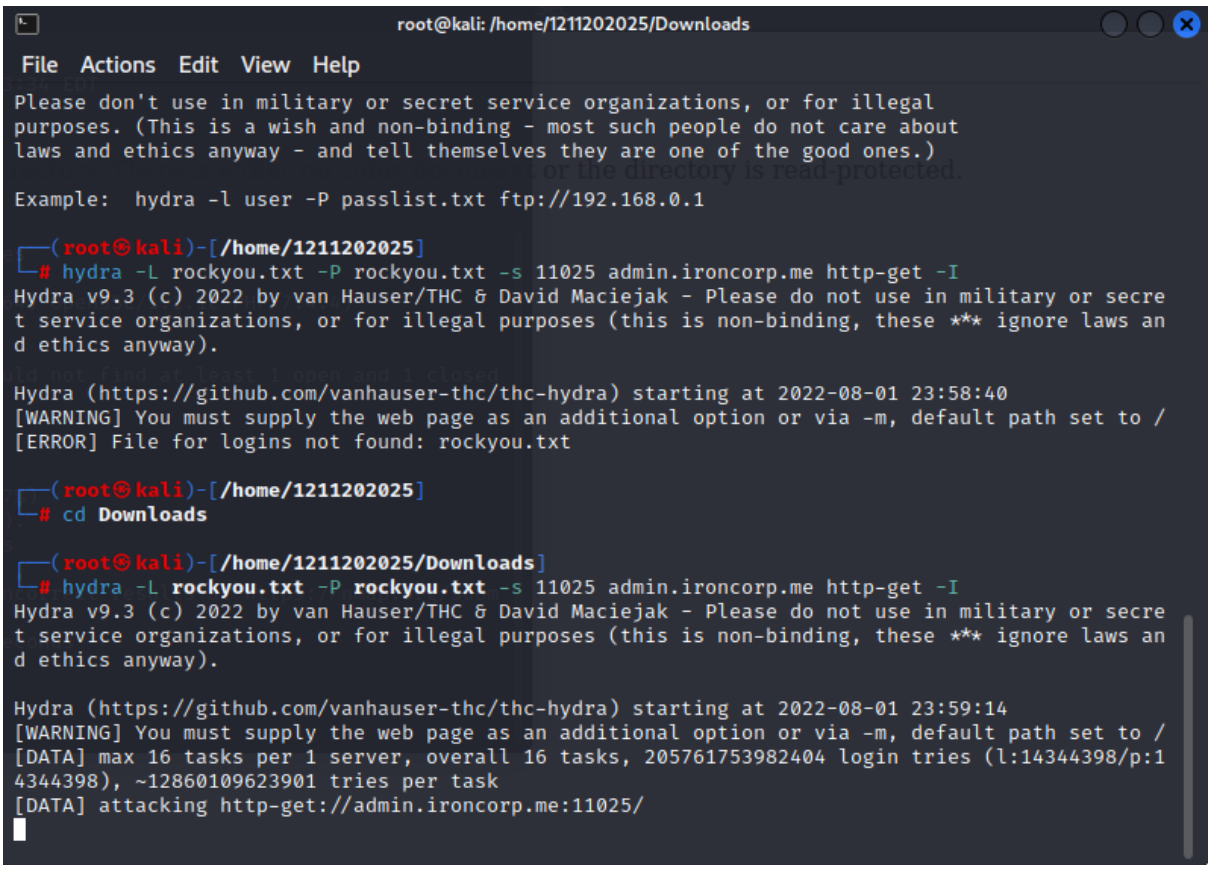
Port 11025 however we can see that admin.ironcorp.me port 11025 has a login function. With what we can observe the programme seems to be using the basic http authentication that allows us to perform using brute force for the login in order to gain the hidden content within.



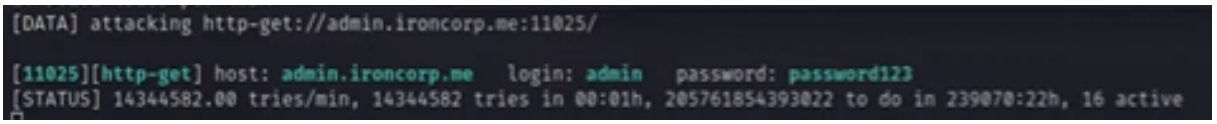
The internal.ironcorp.me port 11025 on the other hand is practically forbidden. But we just keep it in mind as it may be useful along the way.



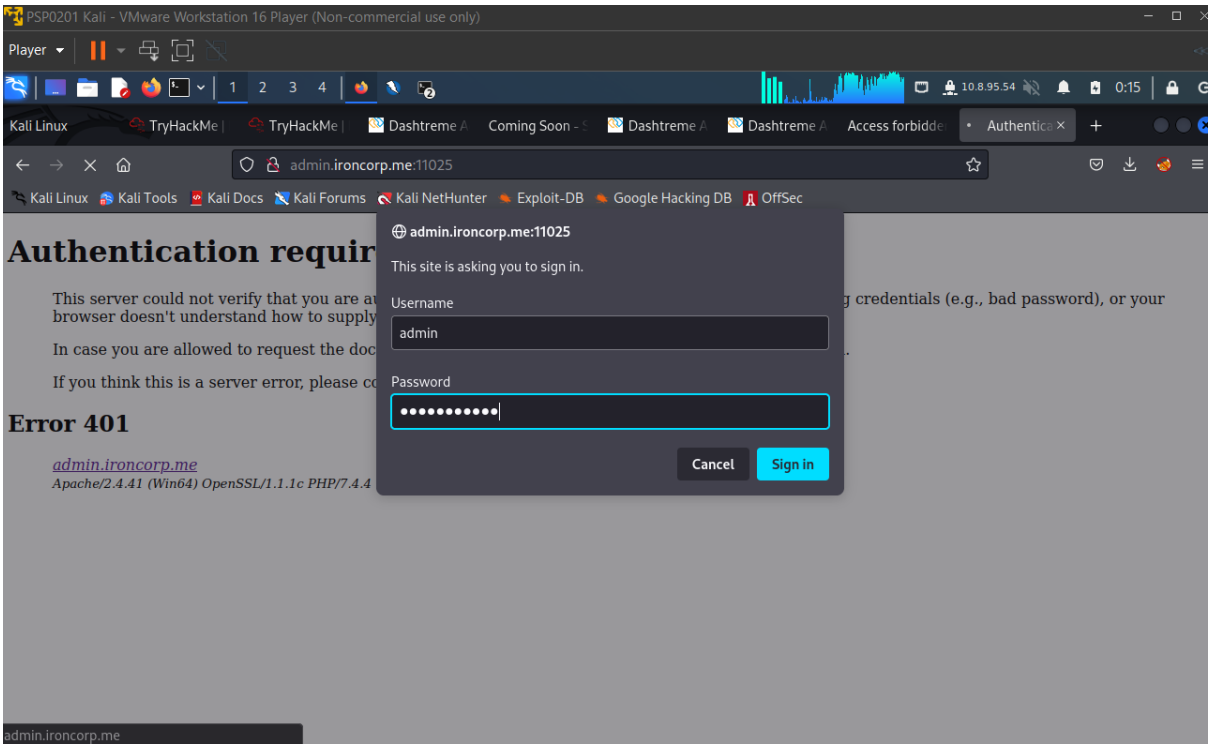
We use hydra to perform brute-force attacks in order to guess the right username and password combination for admin.ironcorp.me by checking the rockyou.txt file that we have (rockyou.txt file contains most common passwords in the world).



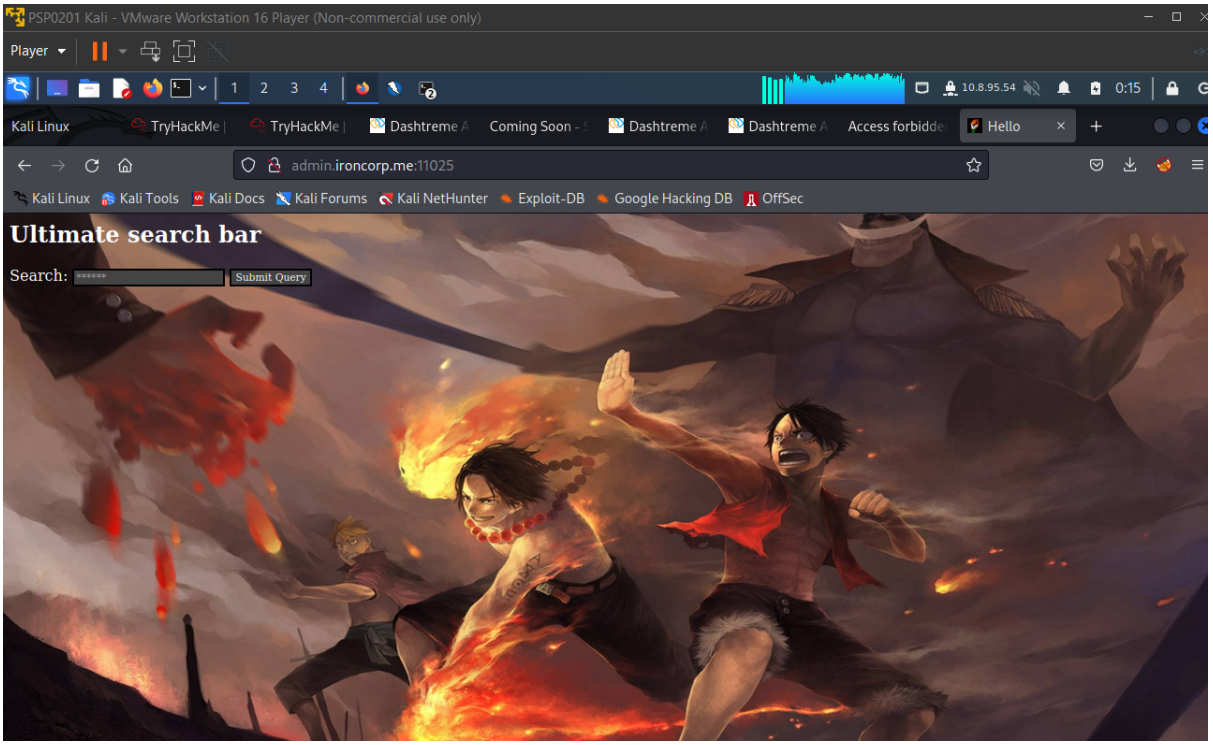
Waiting for a while, we successfully got the credentials, admin as the username and password123 as the password.



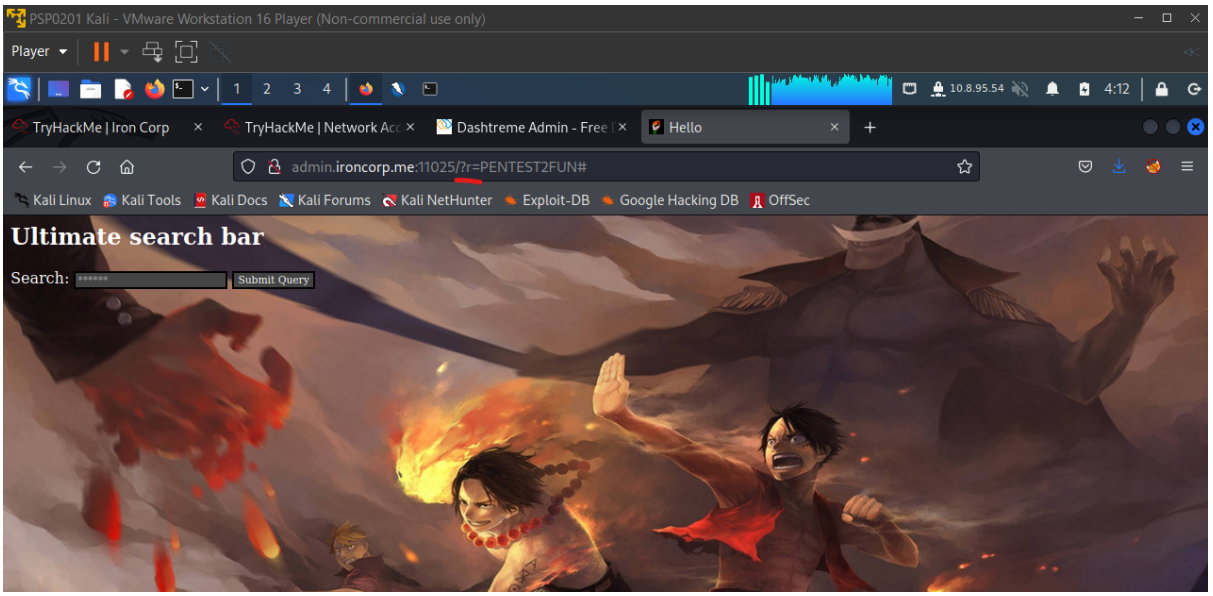
Putting in the credentials in the authentication required site,



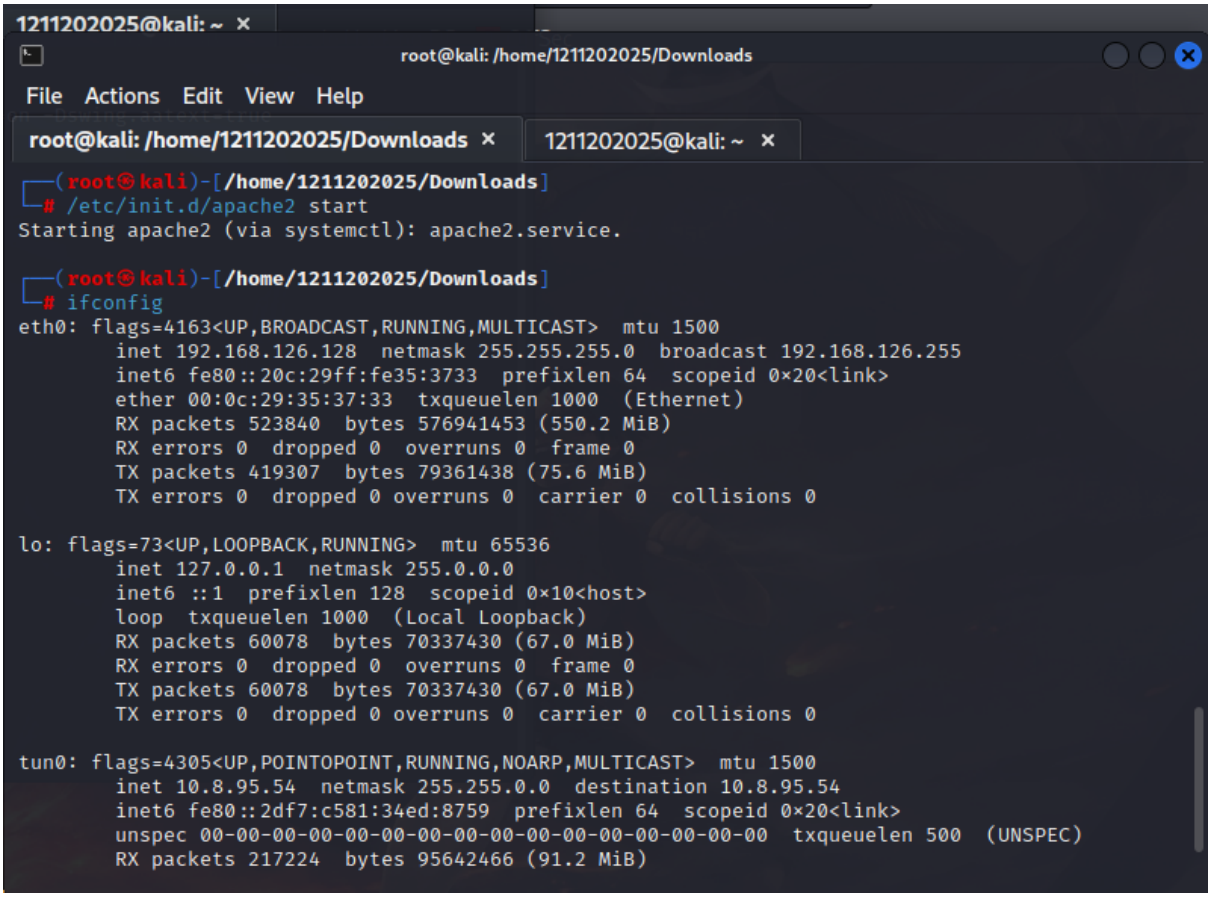
we were able to log in. The first thing that we encountered is the ultimate search bar where we will be able to send queries, with one piece as the background.



We put in random things like PENTEST2FUN just to see anything like the parameter used, and the parameter r popped out in the URL.

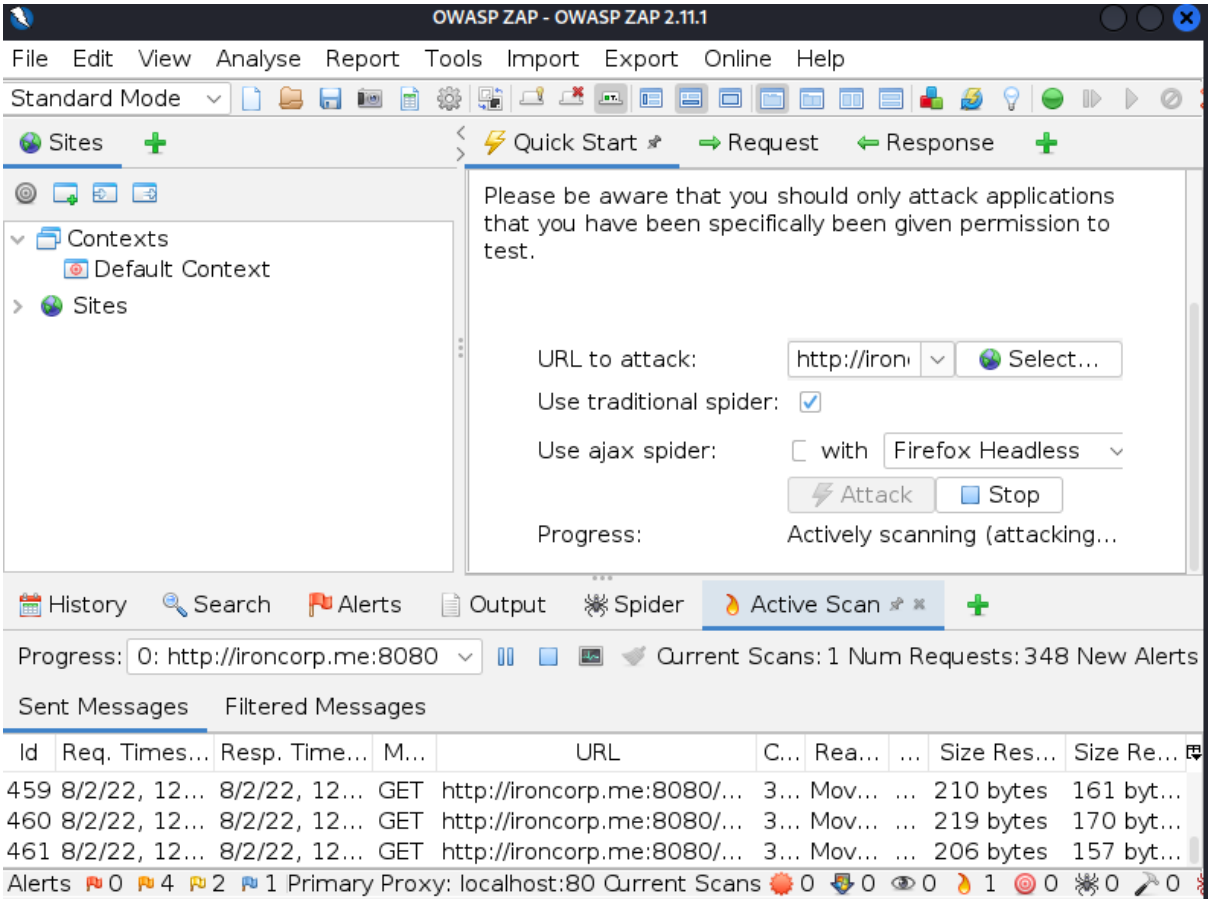


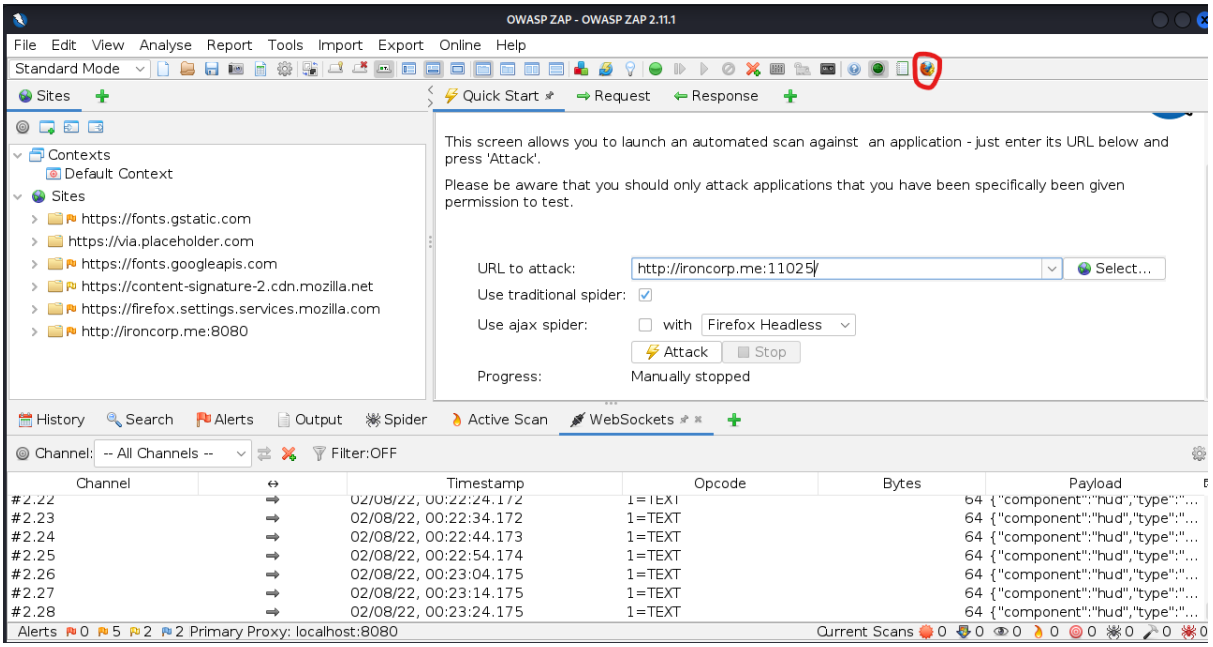
Starting apache and ifconfig to check our inet 10.8.95.54.



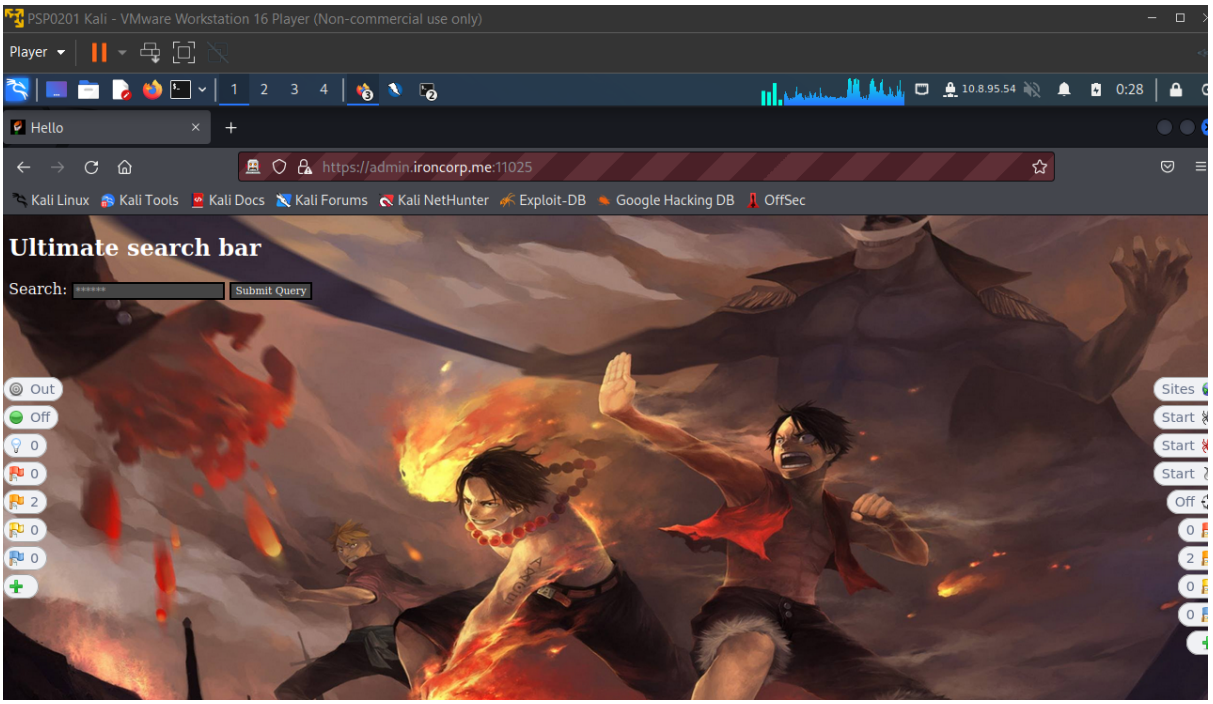
Owasp - Failure

We started using OWASP and attacked the ironcorp.me port 8080 for example to get any useful information out of it.

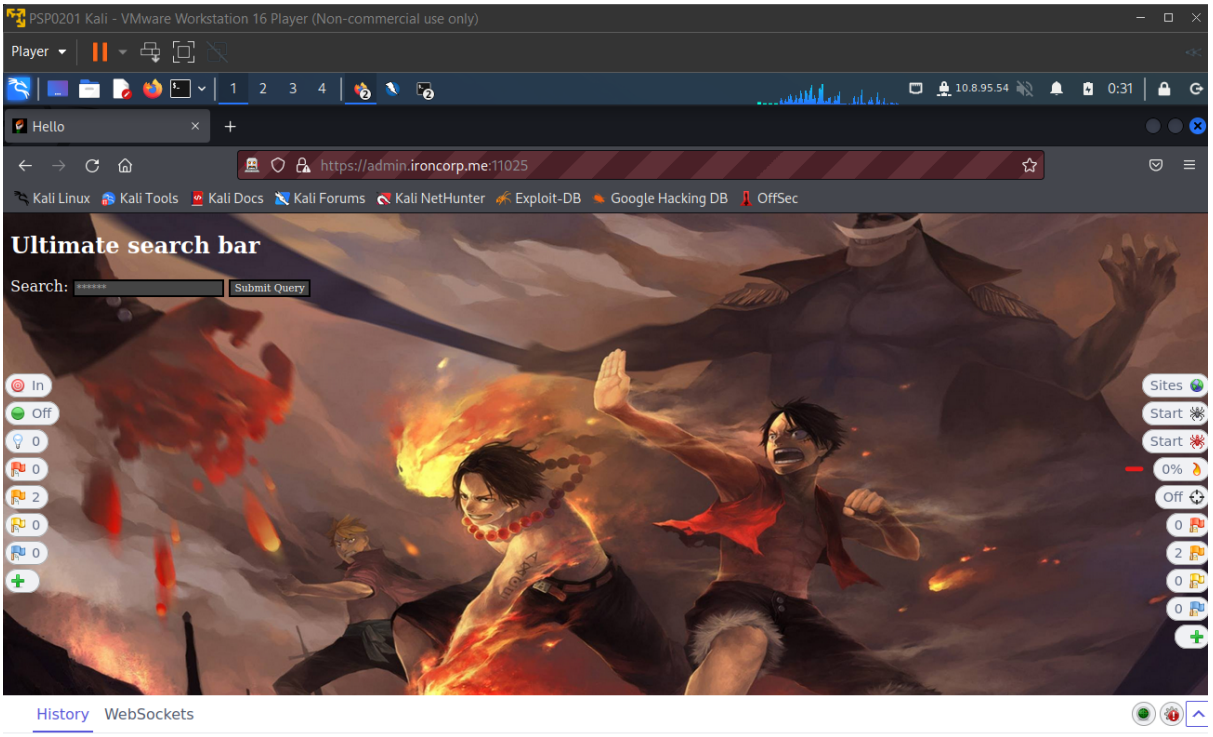




Going to the OWASP browser itself, we went to the admin.ironcorp.me port 11025 and started active scanning it.

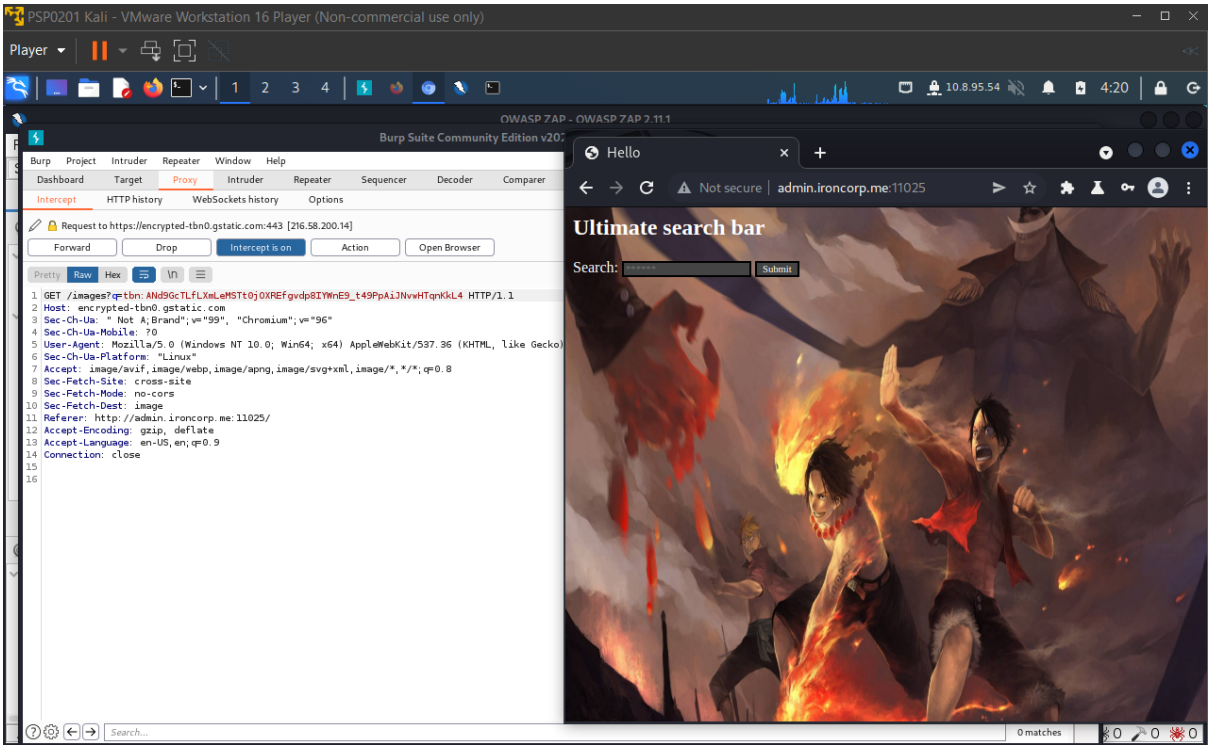


But yeah, to no avail.

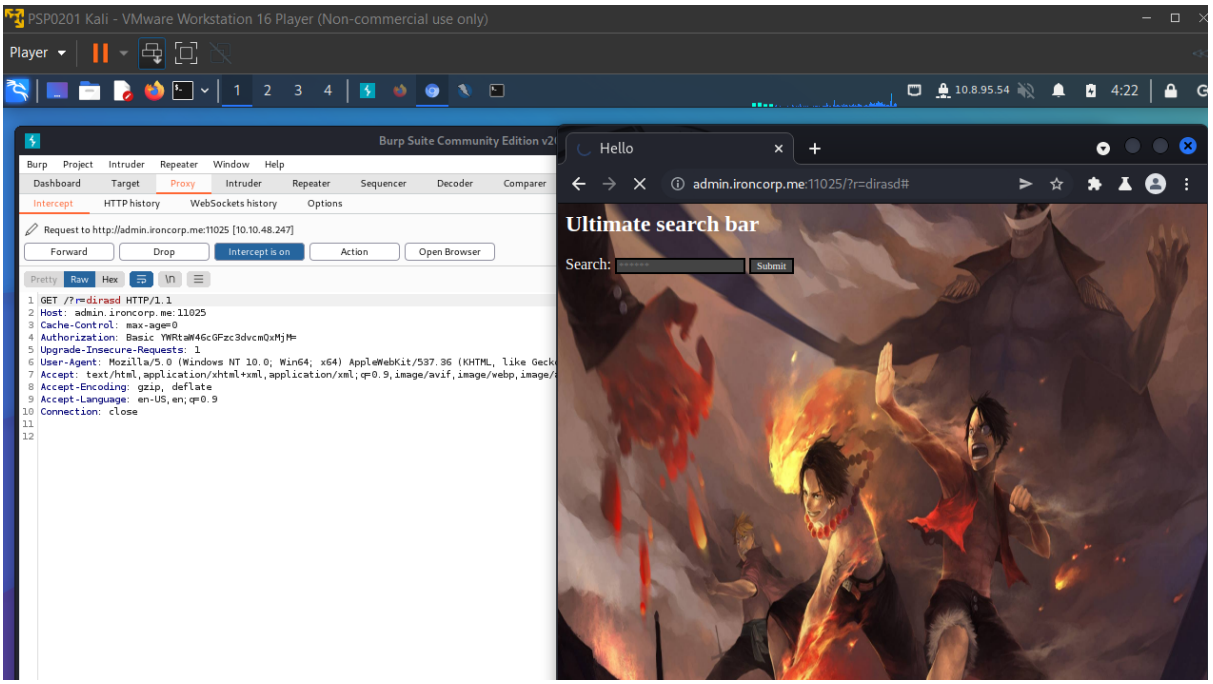


Start using Burp

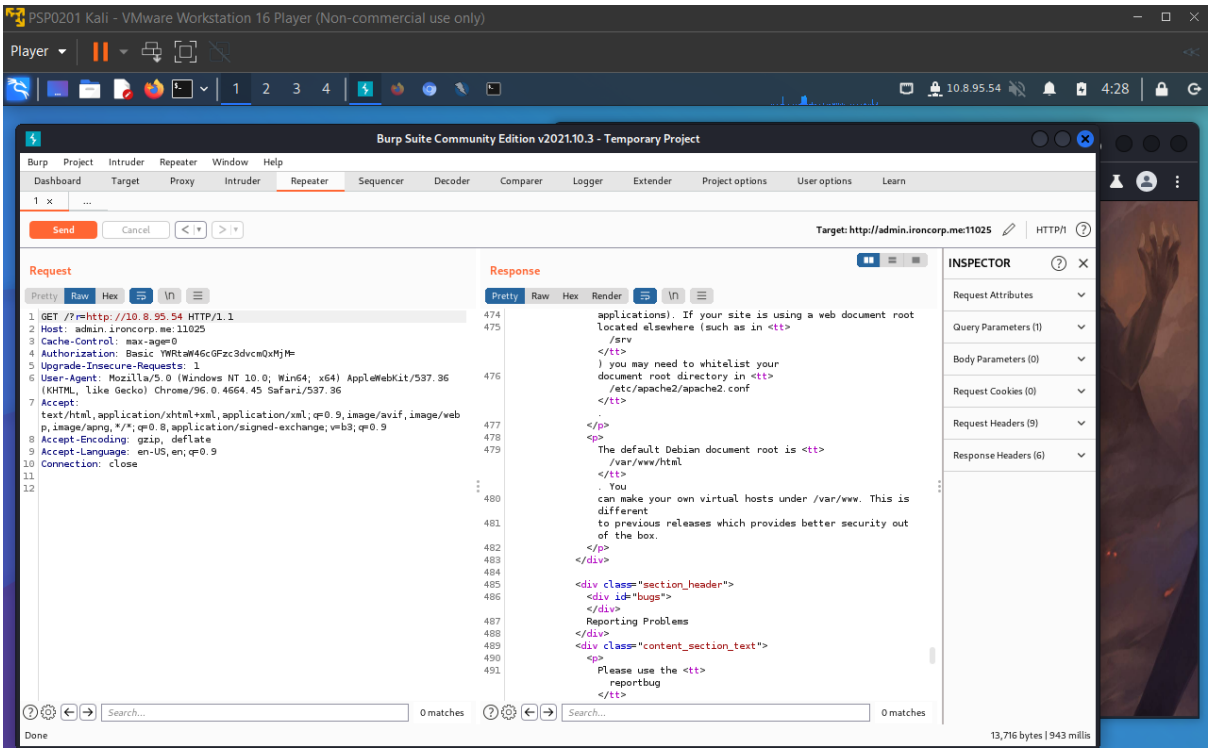
Using Burp and its built-in browser, we went to the same one piece site, but this time with intercept on in Burp Suite.



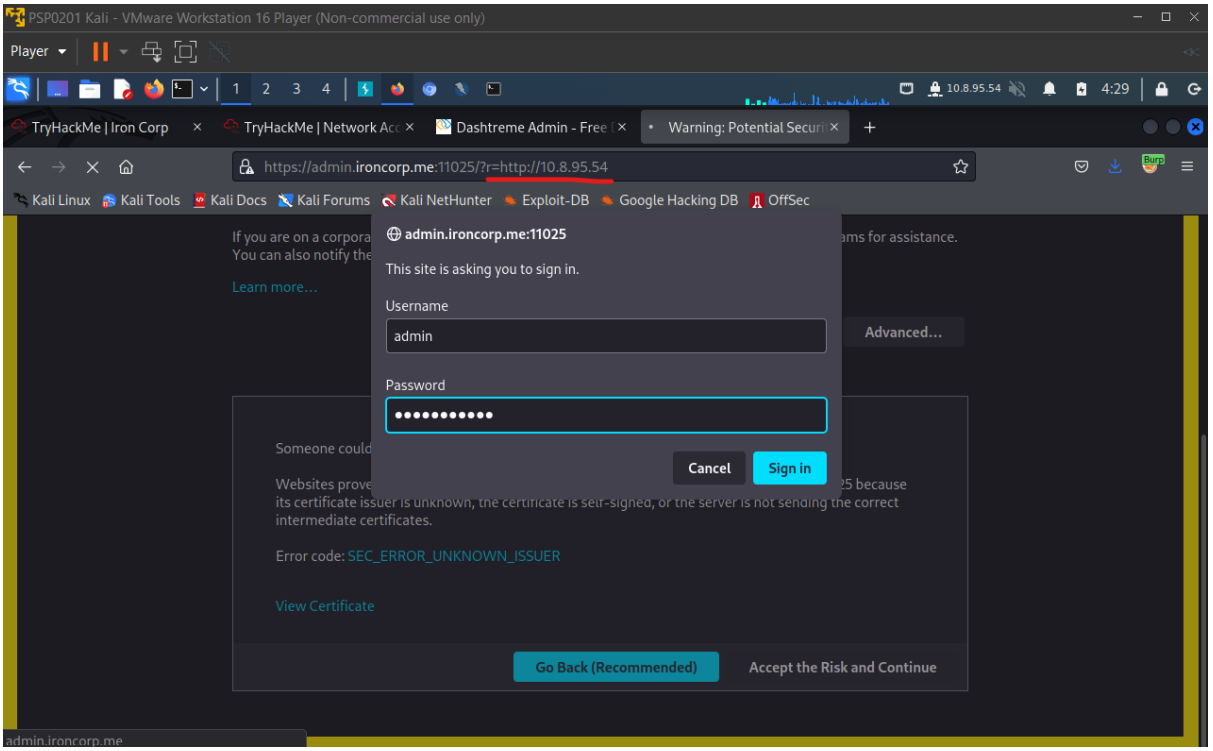
We send the intercept to Repeater.



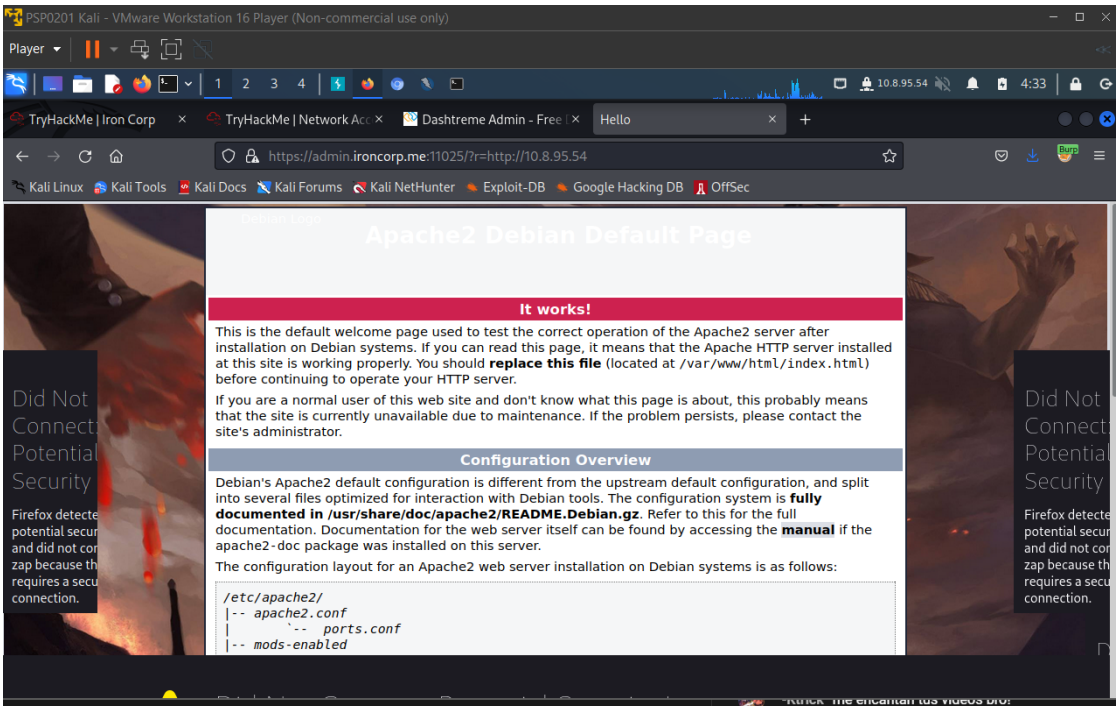
And then by editing in the Repeater, we put in our IP address (the inet) that we got in apache ifconfig, which is 10.8.95.54. We click send to see anything useful.



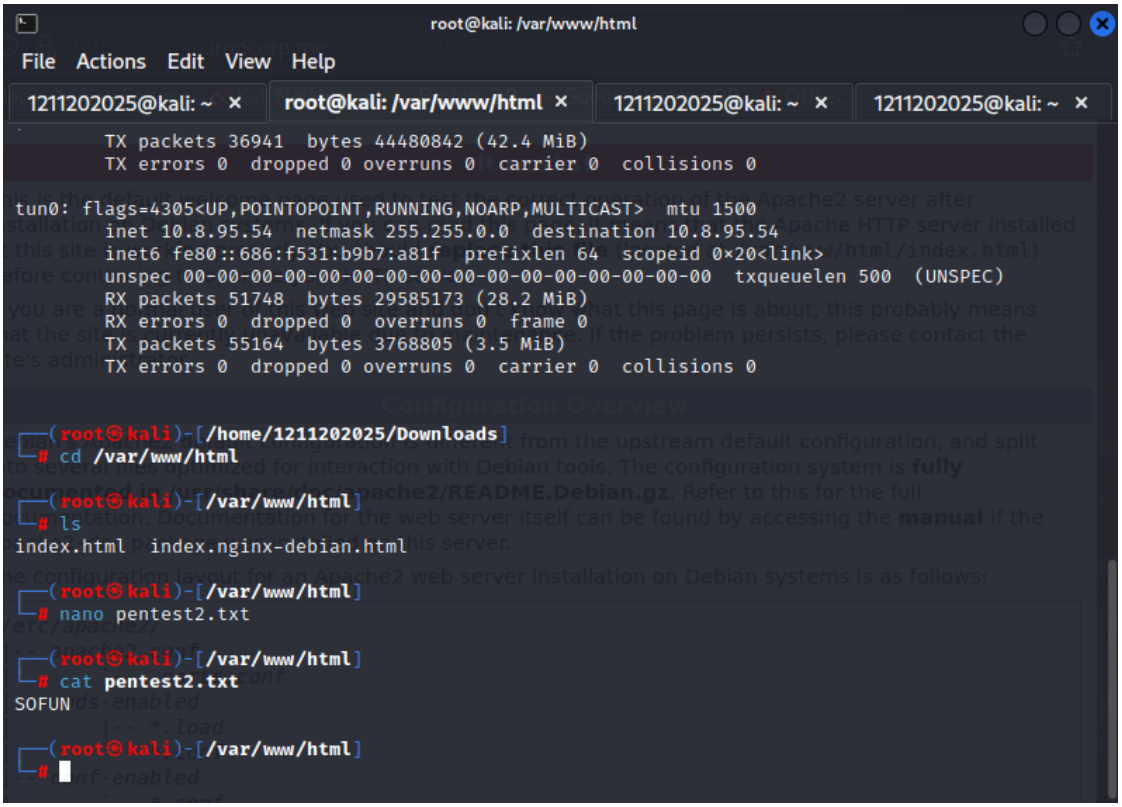
After that, we decided to put in that IP address of ours in the one piece URL itself. Putting in the asked credentials,



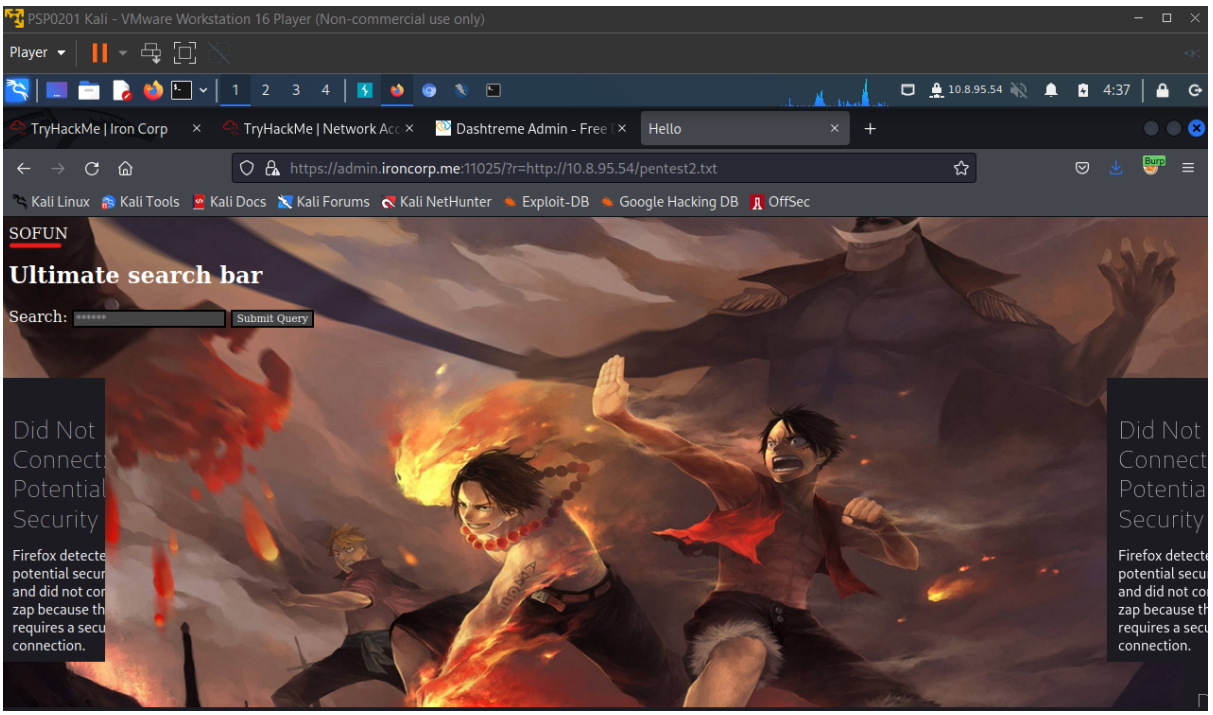
we were brought to a weird-looking one piece site again, this time showing a large screen of Apache2 Debian Default page, saying that the Apache HTTP server installed is working properly.



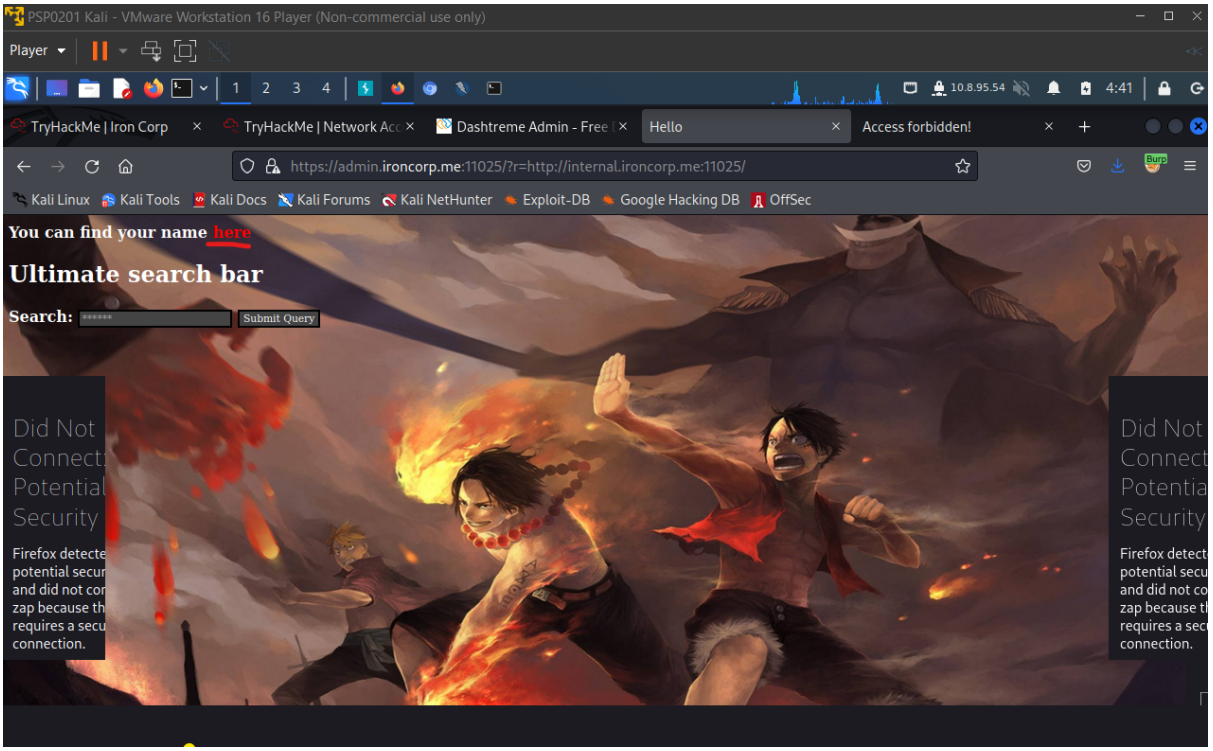
Taking advantage of what they said, saying we should replace the index.html file located at /var/www/html, we created a file and named it pentest2.txt. We also put in SOFUN as its content.



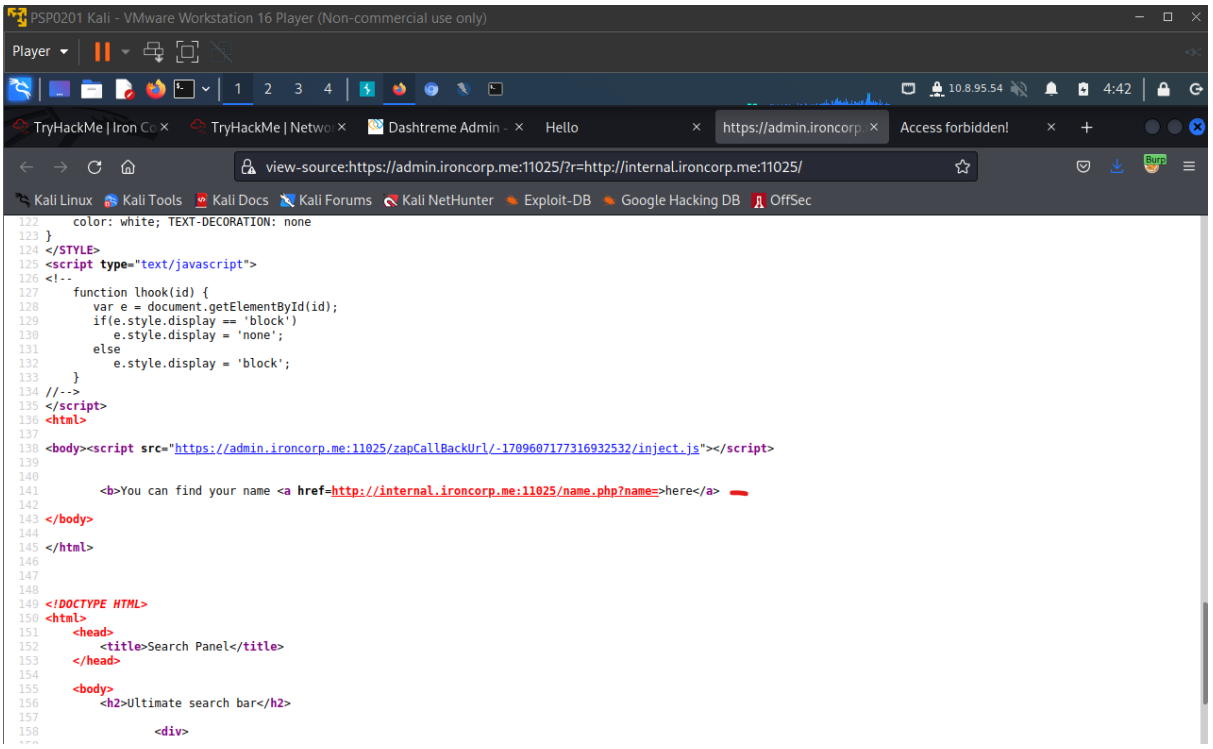
After all the process, by putting pentest2.txt in the URL, we were able to make sure that the site is vulnerable to SSRF attacks, a vulnerability where an attacker has full or partial control of the request sent by the web application.



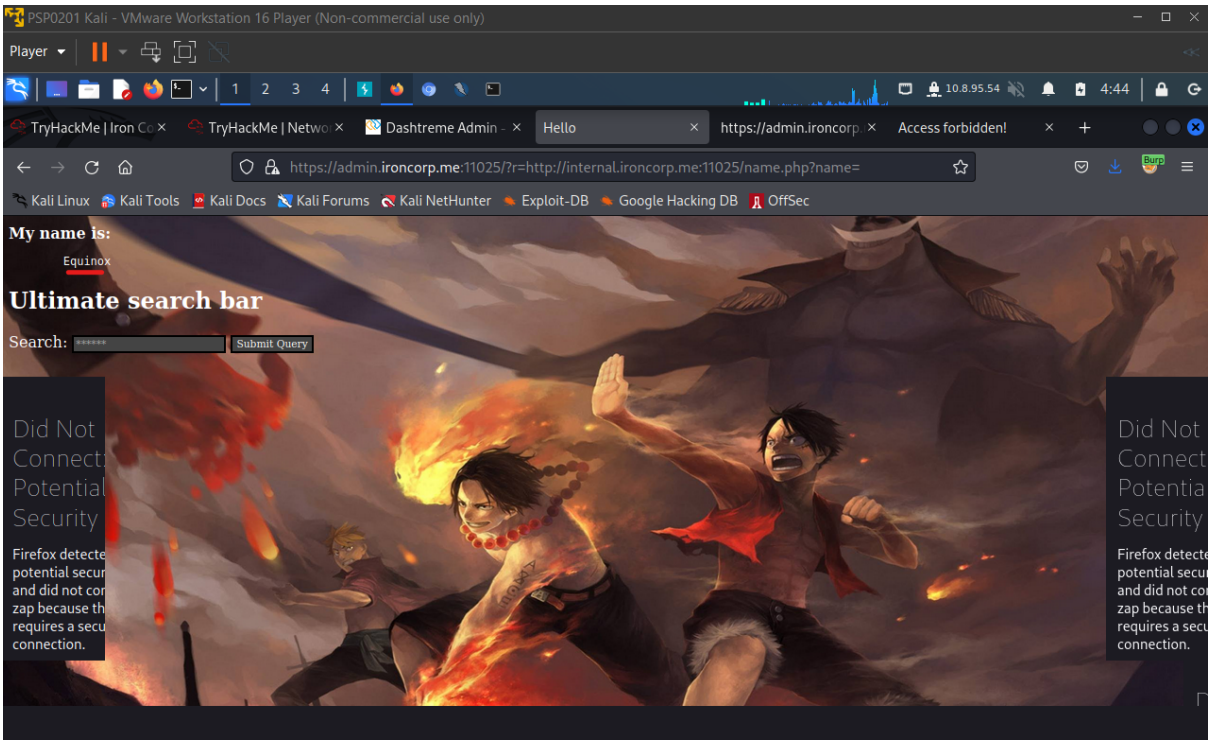
Taking advantage of the vulnerability, we loaded the internal.ironcorp, a forbidden subdomain that we couldn't access earlier. But now, it works. The site also stated “You can find your name here”.



We went ahead and viewed its page source, and fair enough, we can see the URL needed to see the name.



Putting that particular URL in the site's URL, we got to see the name Equinox stated.

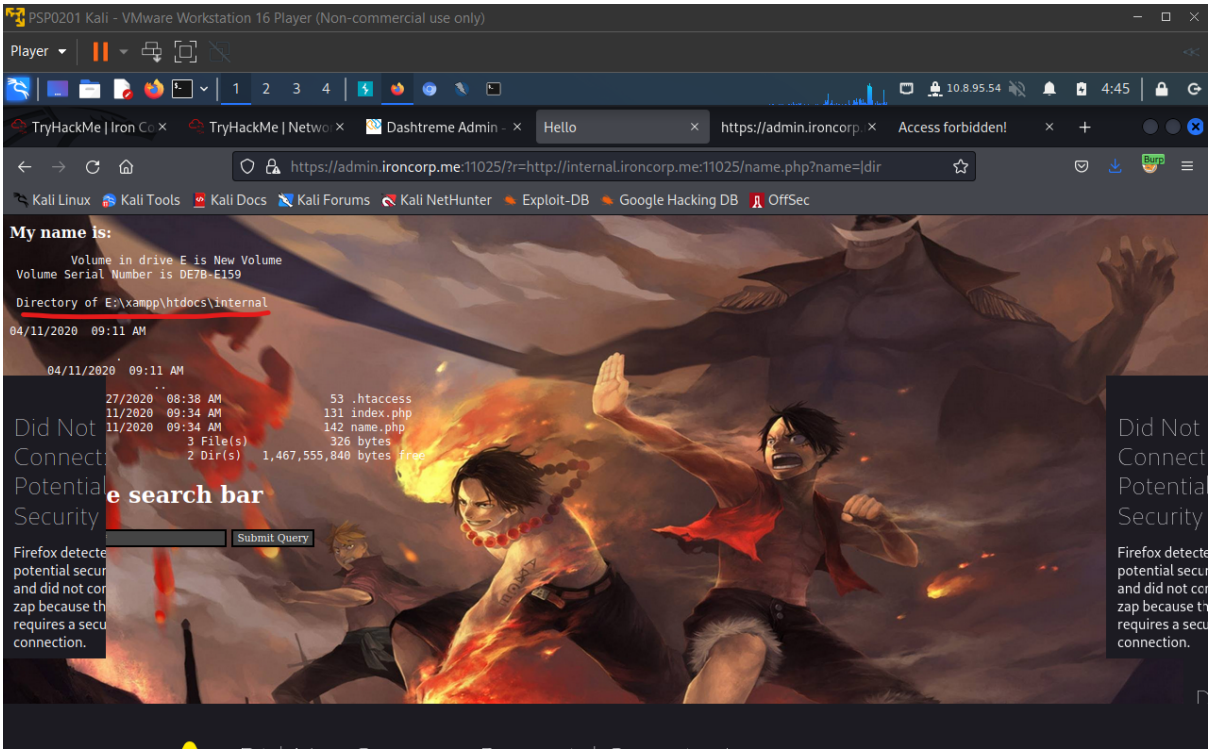


Initial Foothold (Reverse Shell)

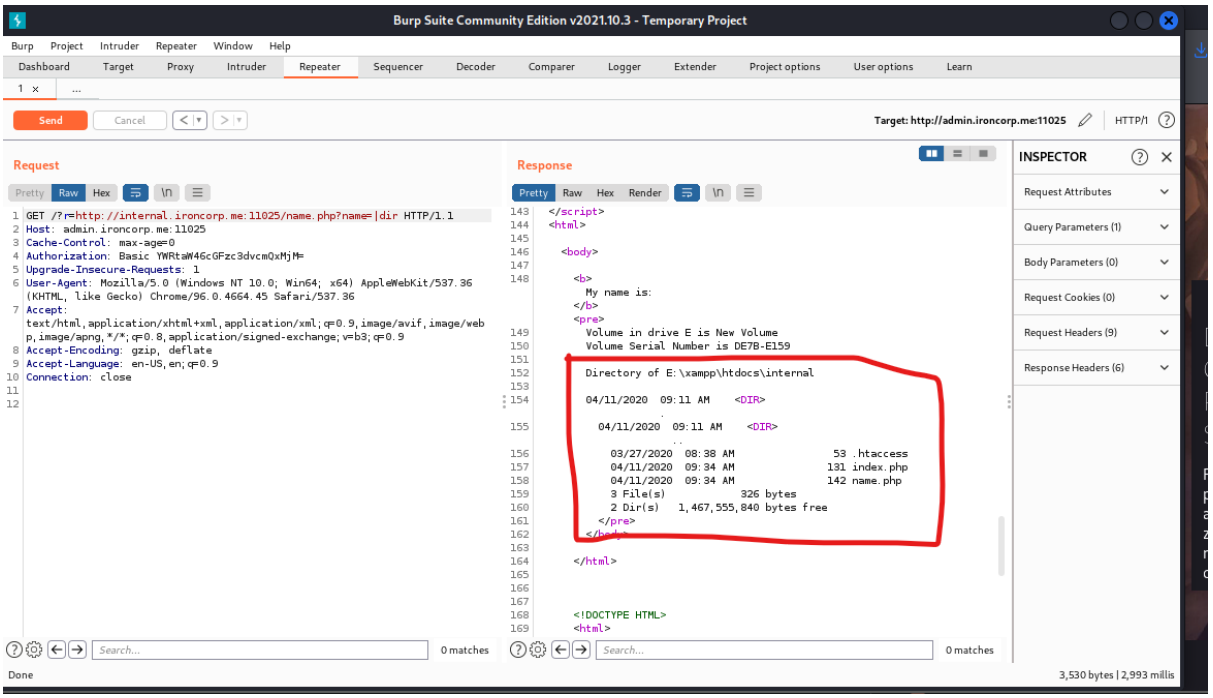
Members Involved: Abdullah

Tools Used: Burp, powershell, Firefox, Kali, Terminal, nano, cat, netcat

Adding a pipe and then dir in the URL, we were also able to see the directory of E:\xampp\htdocs\internal stated.

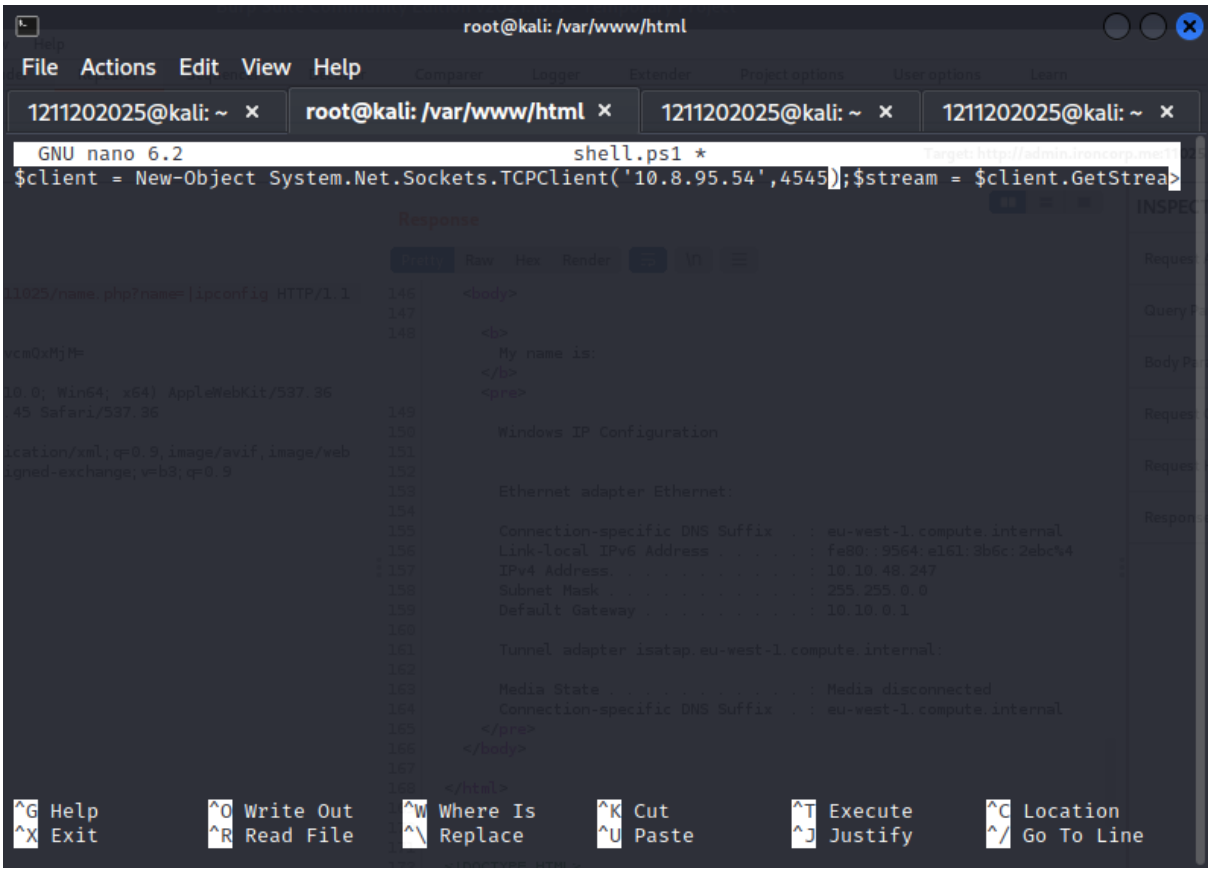


Making sure of it we send it to Repeater in Burp Suite and click Send to make sure, and see it is the same, stating that there is .htaccess, index.php and name.php in that particular directory.

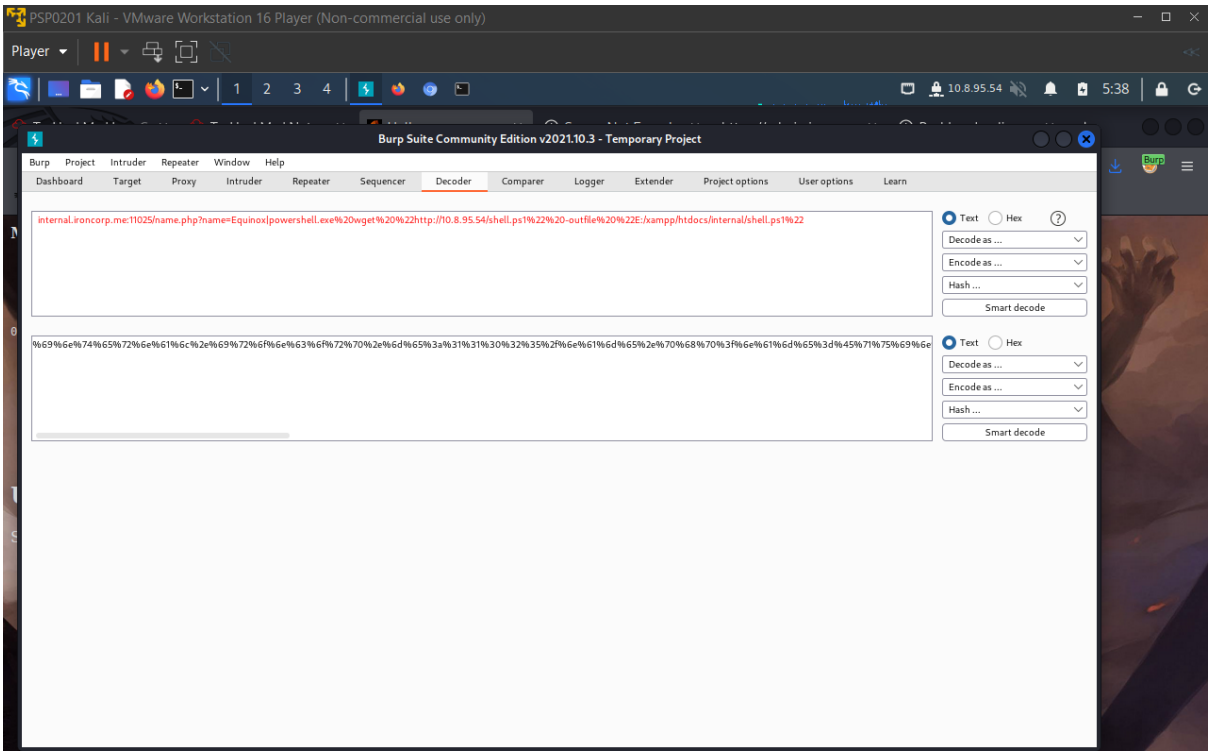


Moving on, we went to our kali machine and created a file named shell.ps1.

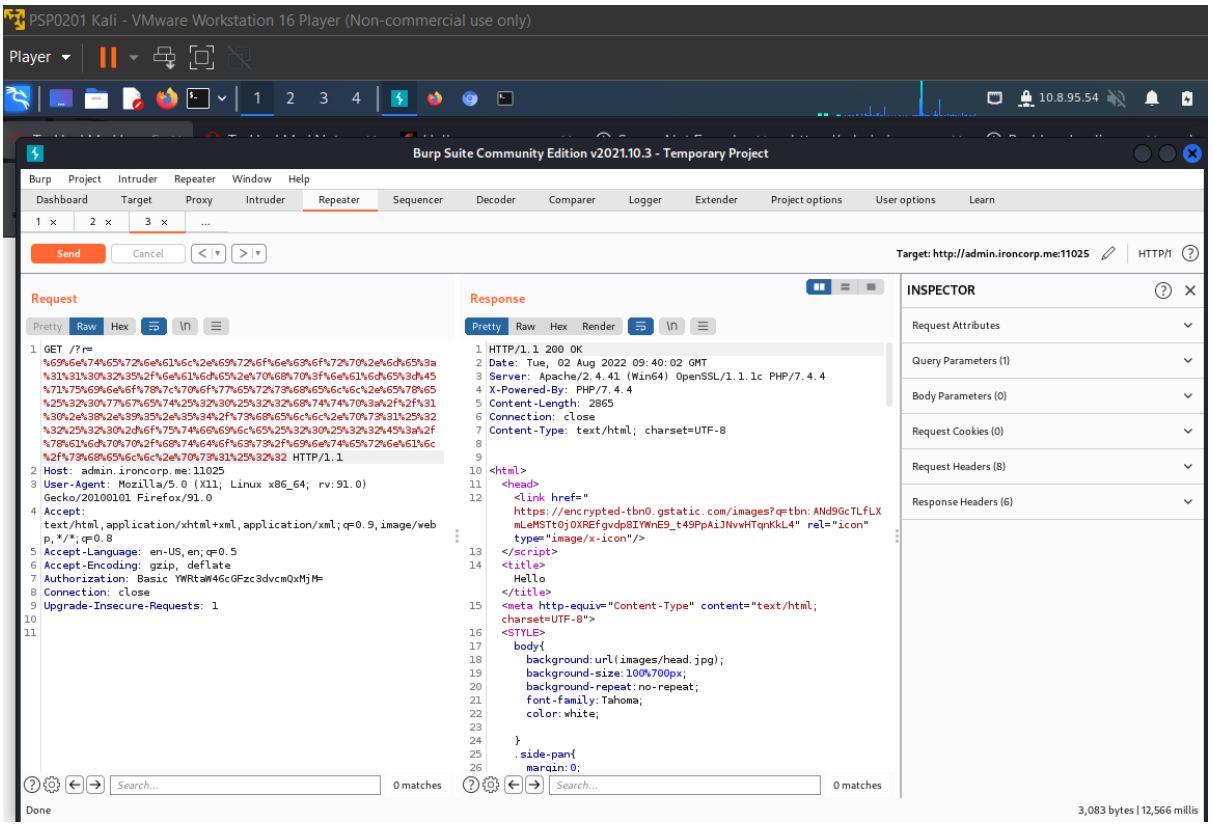
and we put the powershell reverse shell code in the file shell.ps1 that we created.



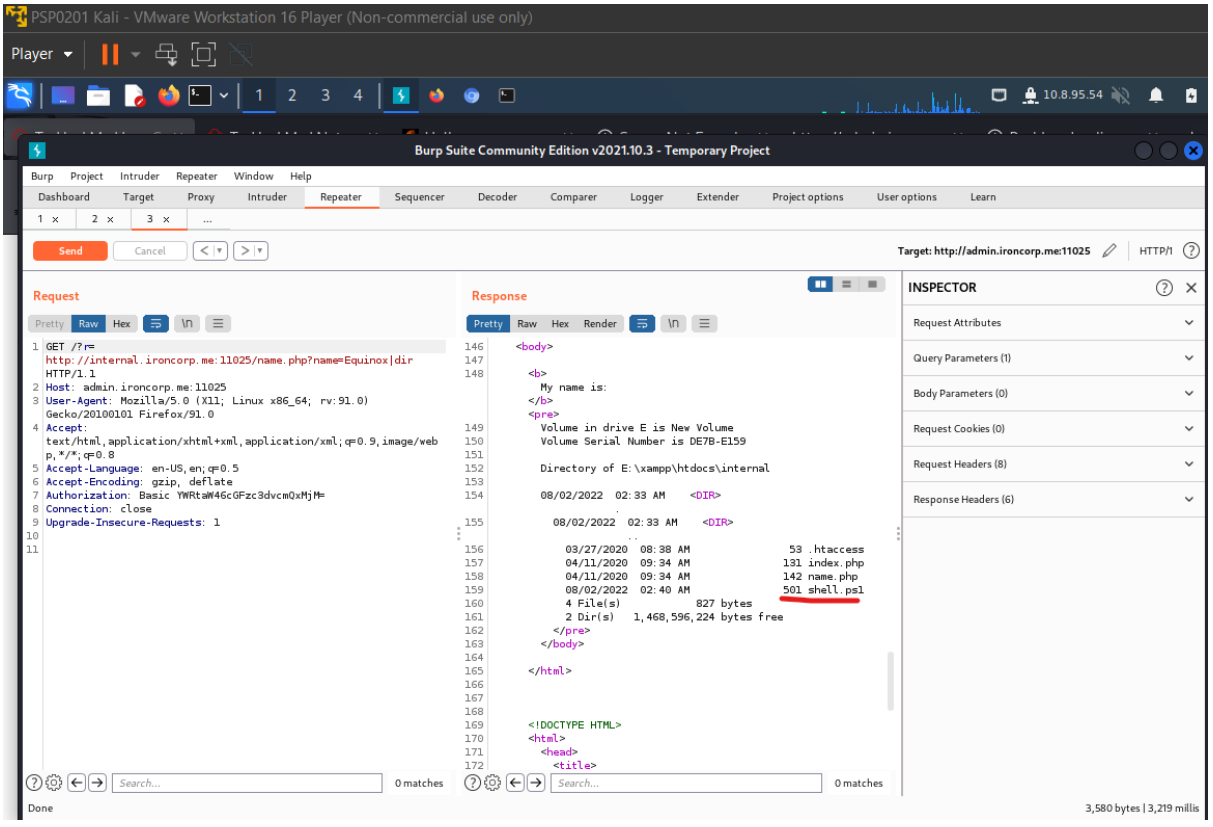
We then encode the below powershell to URL to add the shell.ps1 that we created in the E: drive.



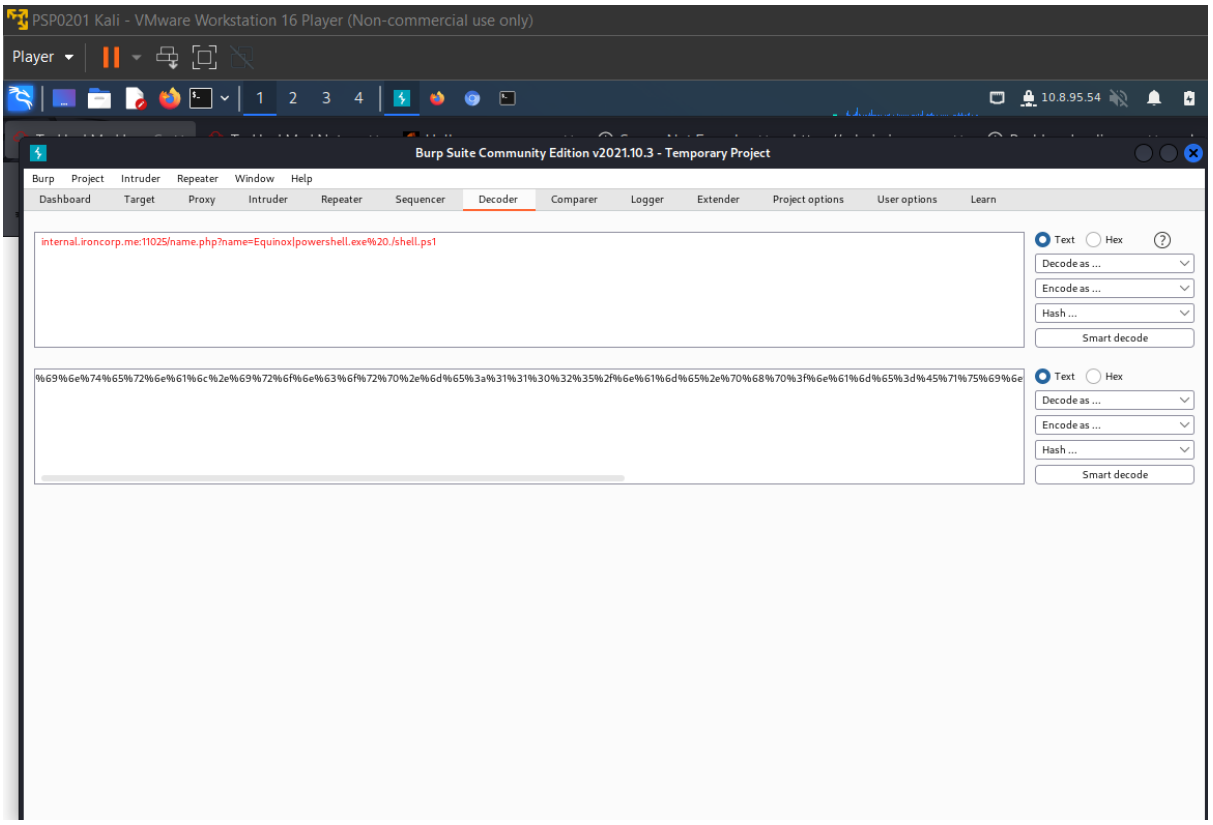
We copied the whole URL and pasted it in Repeater and Send.



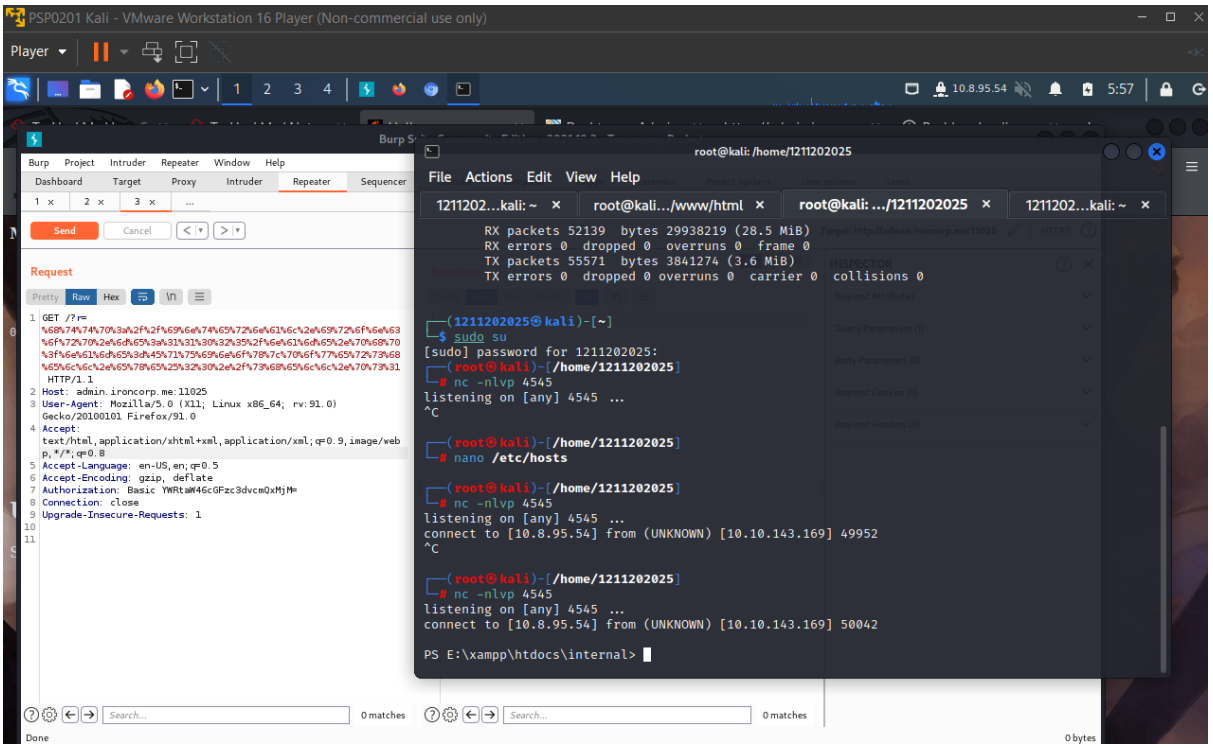
Checking back in the original directory, it seems that the shell.ps1 is successfully added into it.



Now encoding the below powershell with the shell.ps1 in it to URL,



We started listening in our Kali machine using netcat and at the same time pasting the URL in the Repeater. After that by clicking Send, we were able to connect to the E:\xampp\htdocs\internal



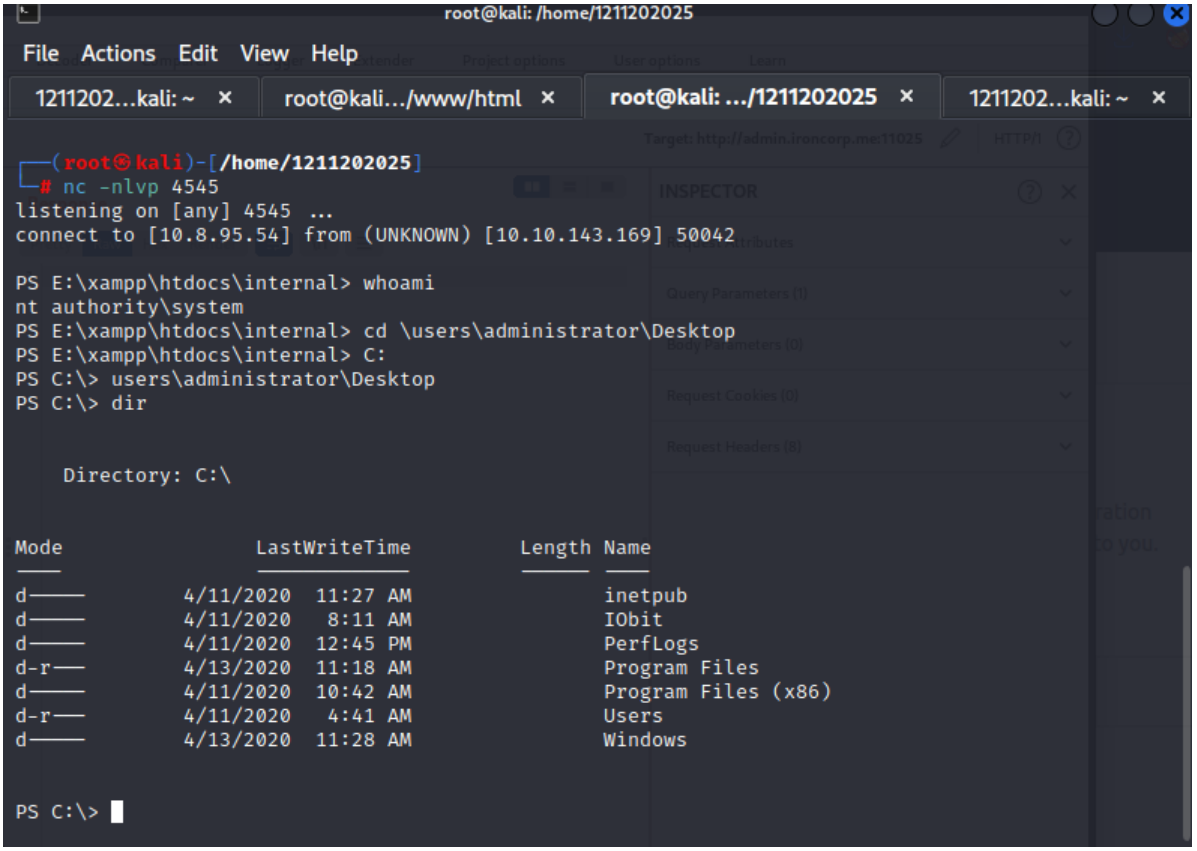
Horizontal Privilege Escalation

Members Involved:

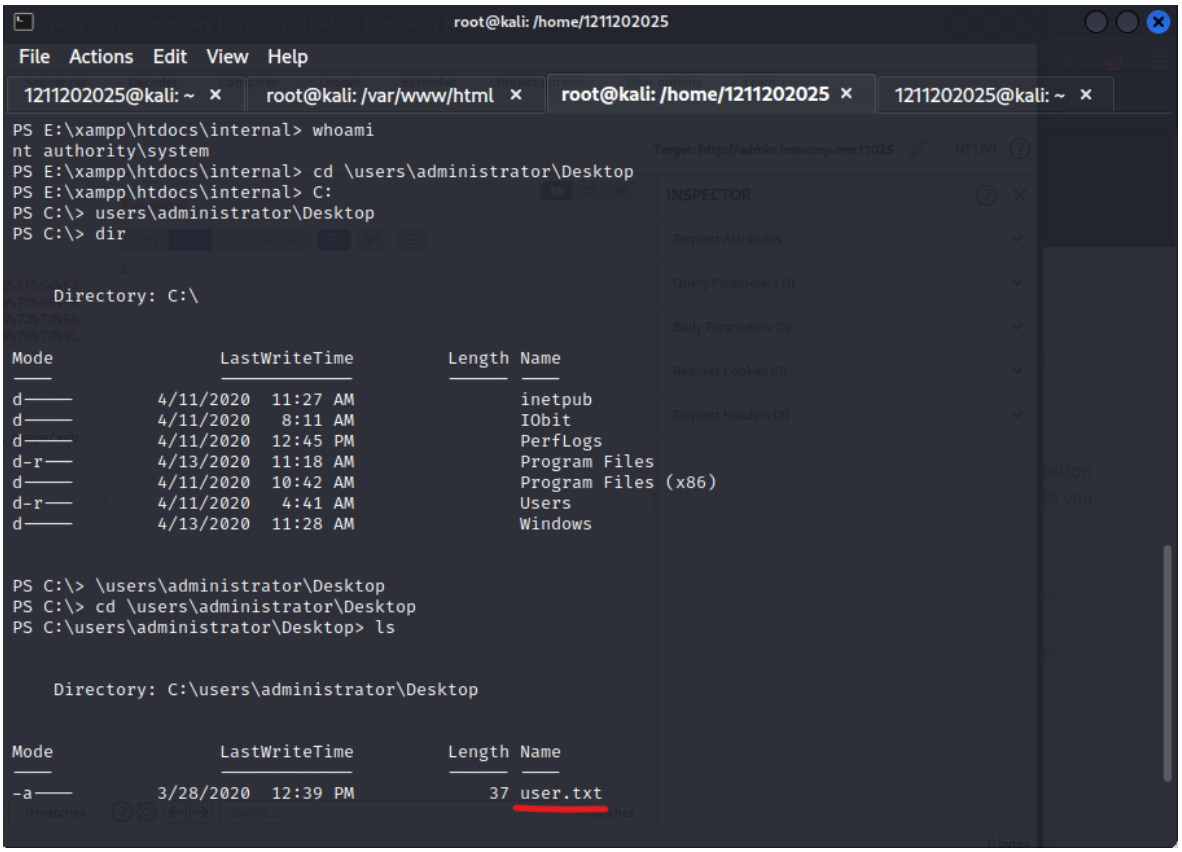
Tools Used: Kali, Terminal, dir, ls

E: > C:\administrator

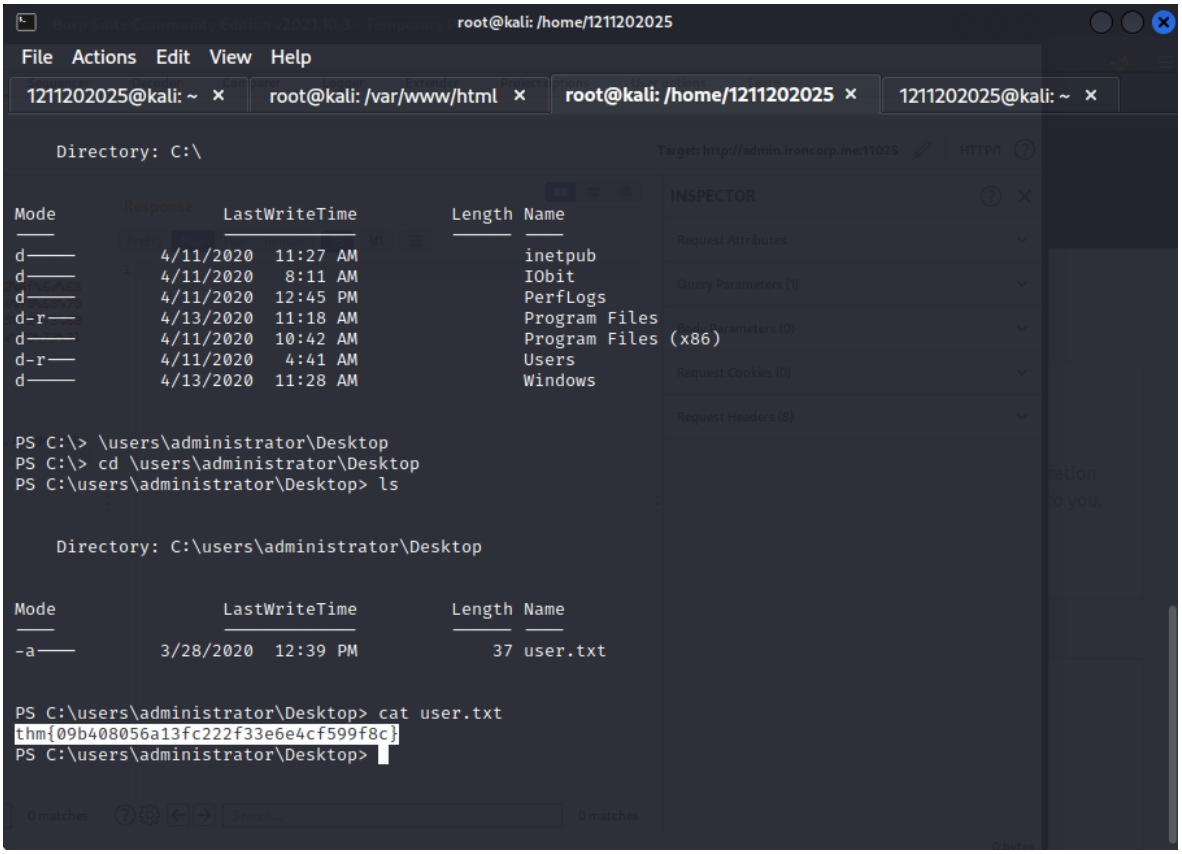
We went from E: drive to C: drive by using the change directory to \users\administrator\Desktop. Then we use dir to find any information on existing directories there.



Nothing, we decided to use ls to list out any file and fair enough, there is one, that is the user.txt.



Using cat command to check its contents, we were able to capture the first flag.

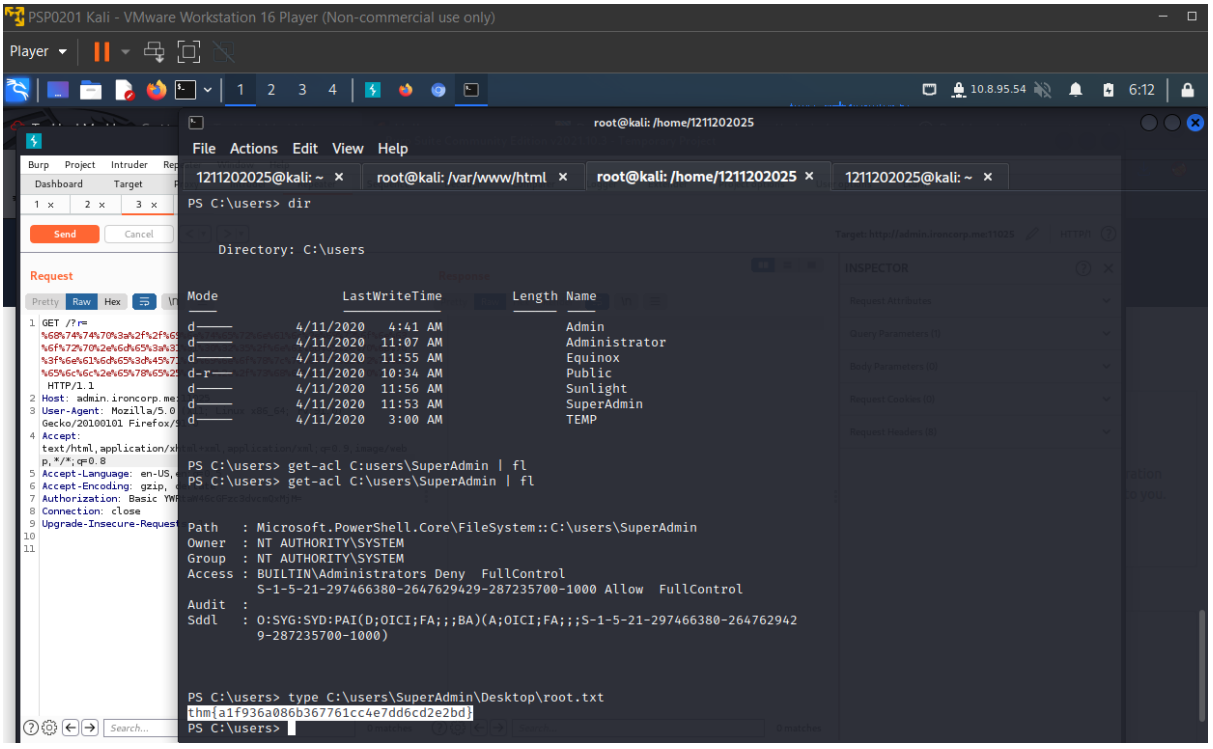


Root Privilege Escalation

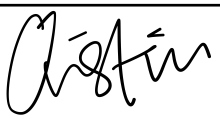
Members Involved: Abdullah

Tools Used: Kali, Terminal, get-acl, fl, type

Using dir to check the directories, we found SuperAdmin. Using get-acl to check the permissions that we have on that particular directory, in this case SuperAdmin, we can see that it Deny FullControl as Administrator (the fl cmdlet is just to format the output of our command as a list of properties in which each property is displayed on a separate line). But we found that by trying to read the file directly in SuperAdmin without being in SuperAdmin, we were able to get the root.txt, which allows us to capture the second flag.



Contributions

ID	Name	Contribution	Signatures
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Did Recon and Enum but failed at hydra, so just helped recording	
1211202025	Abdullah Bin Kamaruddin	Did the recon and enum, initial foothold and both horizontal and root privilege escalation. Everything.	
1211103649	Nur Qistina Binti Roslan	Did the write up	

VIDEO LINK: https://youtu.be/rKnE8Cf0pSI