PenTest 2
Iron Corp
GOLD

Members:

ID	Name	Role
1211101707	Nur’aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

Step1: Recon and Enumeration

Members Involved: Aina, Afreen, Hanisah, Aisyah

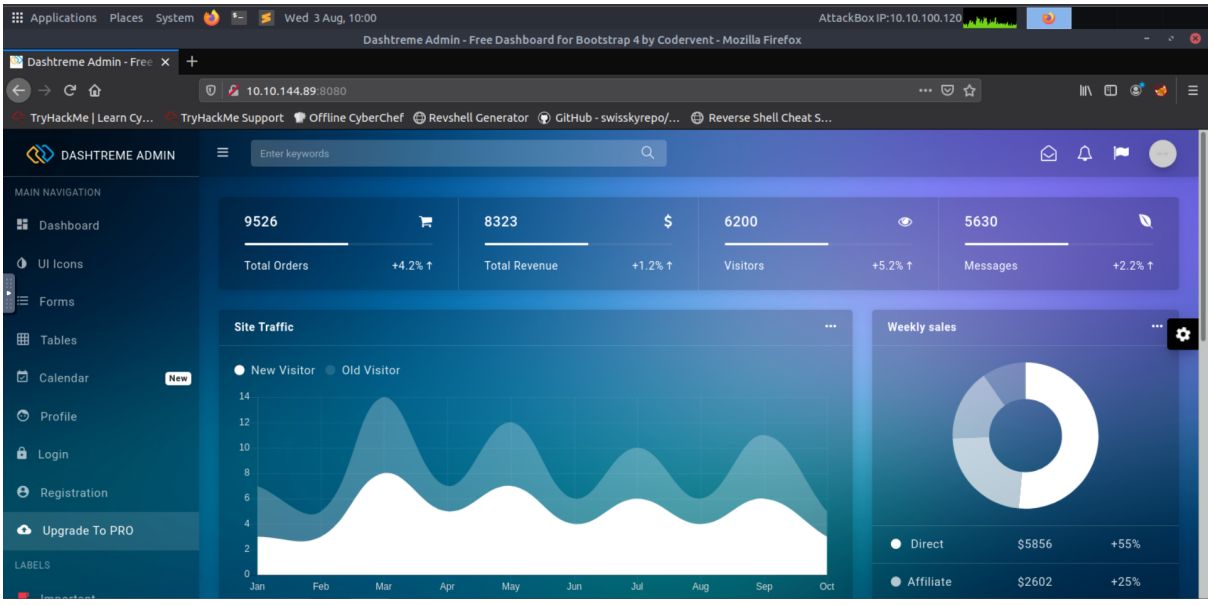
Tools used: Nmap, Dig, Hydra

Thought Process and Methodology and Attempts:

First, I'm using nmap to scan all the tcp ports. It shows the open ports.

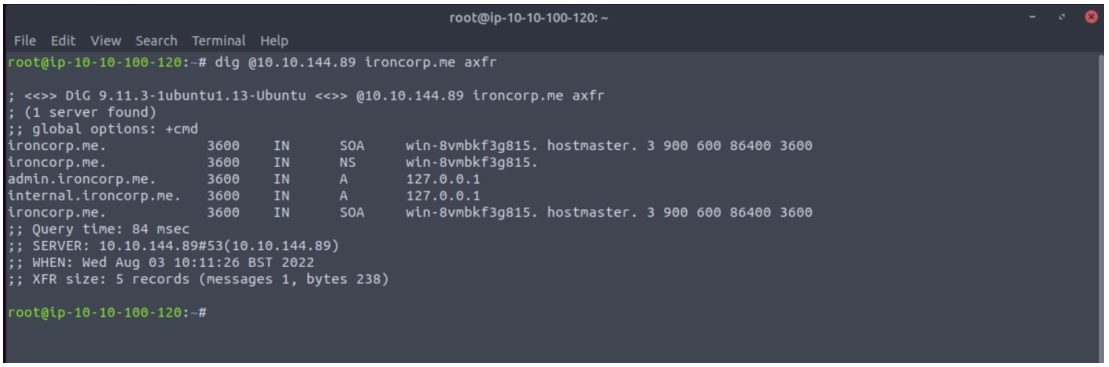
```
root@ip-10-10-100-120:~# nmap -n -Pn -sV -sC 10.10.144.89

Starting Nmap 7.60 ( https://nmap.org ) at 2022-08-03 09:54 BST
Nmap scan report for 10.10.144.89
Host is up (0.0053s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-02T08:48:36
|_Not valid after:  2023-02-01T08:48:36
|_ssl-date: 2022-08-03T08:54:29+00:00; 0s from scanner time.
8080/tcp open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
MAC Address: 02:02:19:62:CE:FD (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.33 seconds
root@ip-10-10-100-120:~#
```

Using the port I've got earlier which is 8080, I look for it in the browser by entering ironcorp.me:8080 but the page won't reload so I tried by entering my machine ip address followed by the port number, and here is how the page for port 8080 look like.

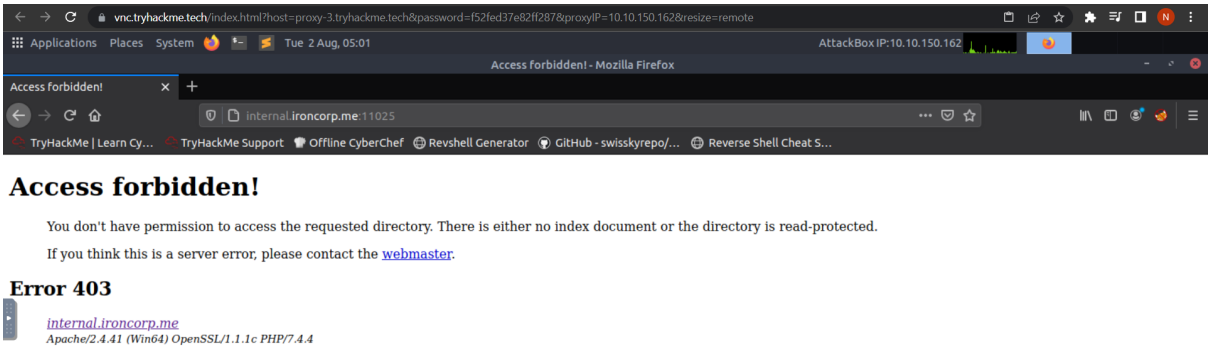


I tried multiple times with the other port numbers, but I gain nothing.

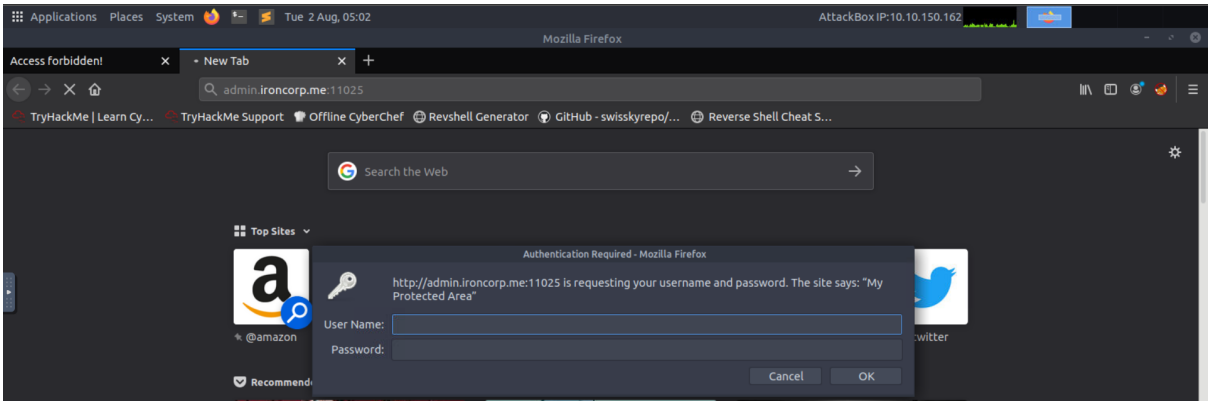
Then, I tried using dig to look for any information. Here I found two subdomains that are running internally, **admin.ironcorp.me** and **internal.ironcorp.me**



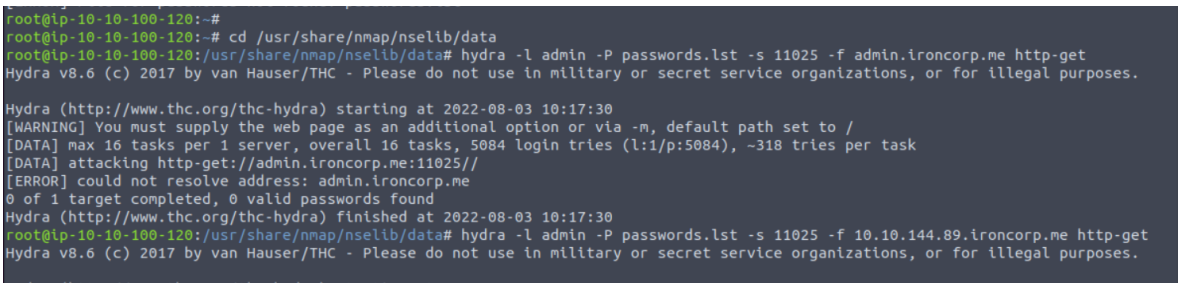
I tried to search the subdomains I've found earlier in the web browser. For the first page it state that access forbidden.



I tried with the second one, now they ask for user name and password.



To get the username and password I tried using hydra.



But unfortunately, after so many attempts I couldn't find it so I ask my friend for the username and password instead.

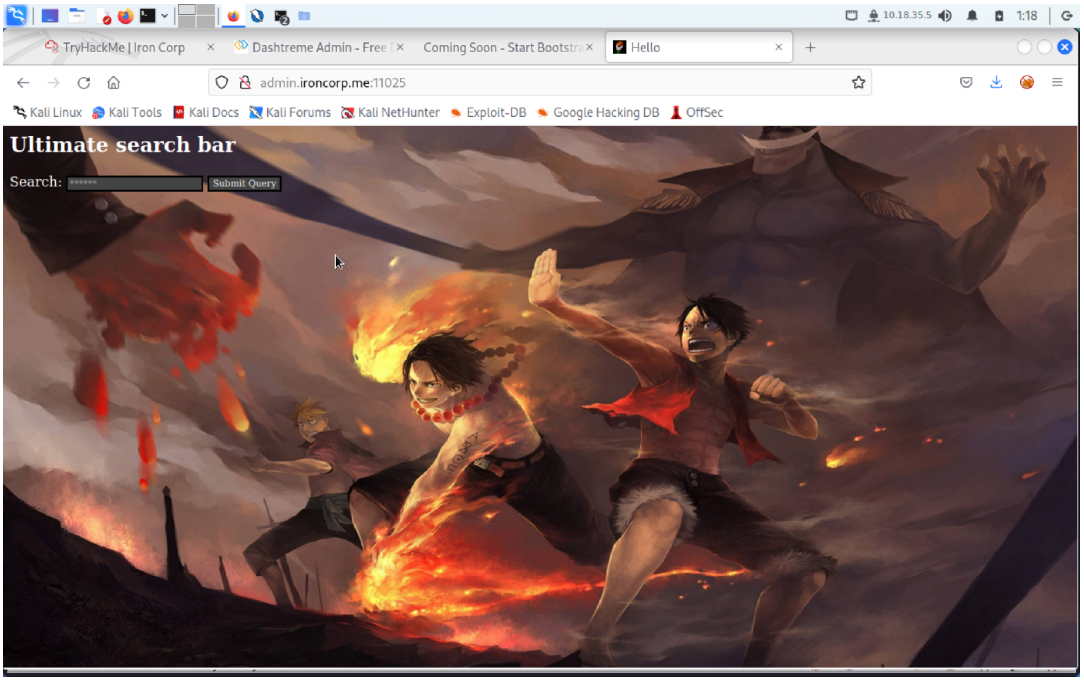
Step 2: Initial Foothold

Members Involved: Aisyah

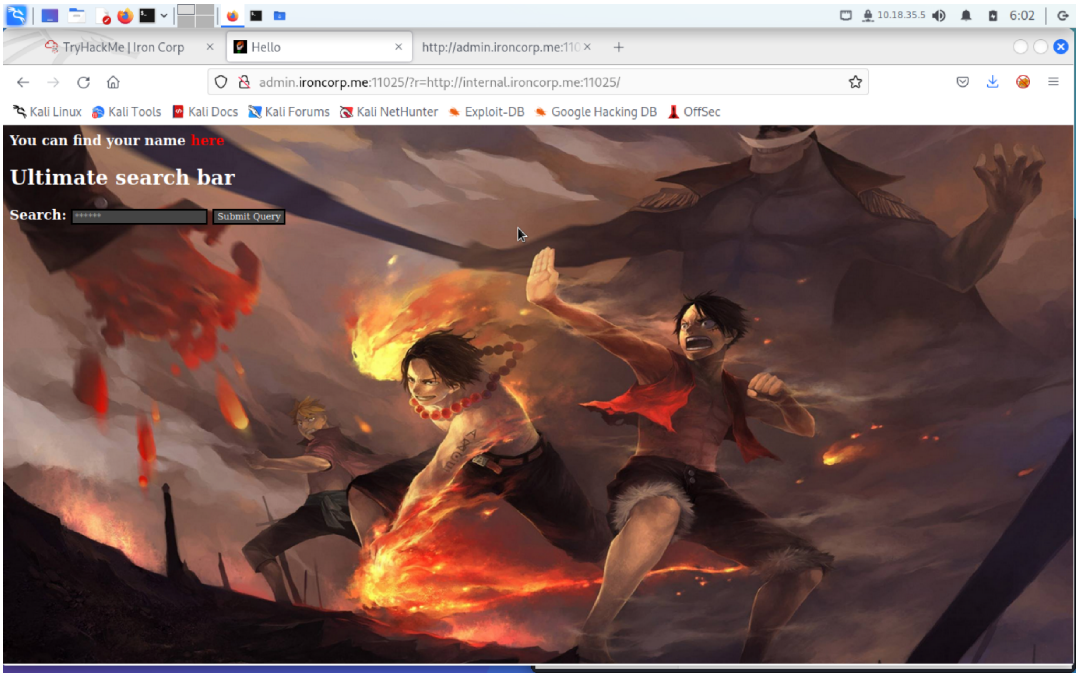
Tools used: chrome,

Thought Process and Methodology and Attempts:

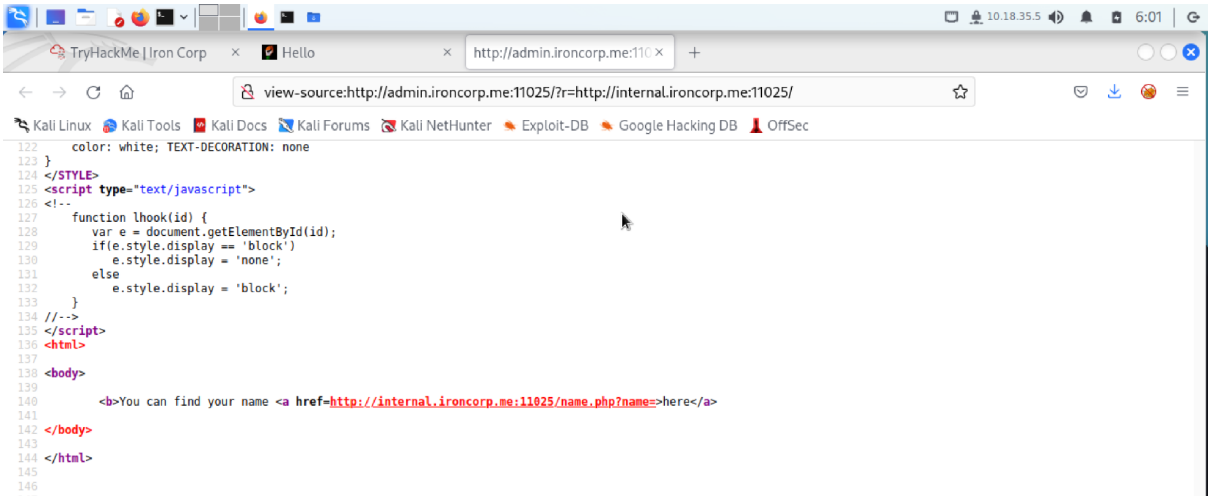
After we input the name and password we'll get into this page



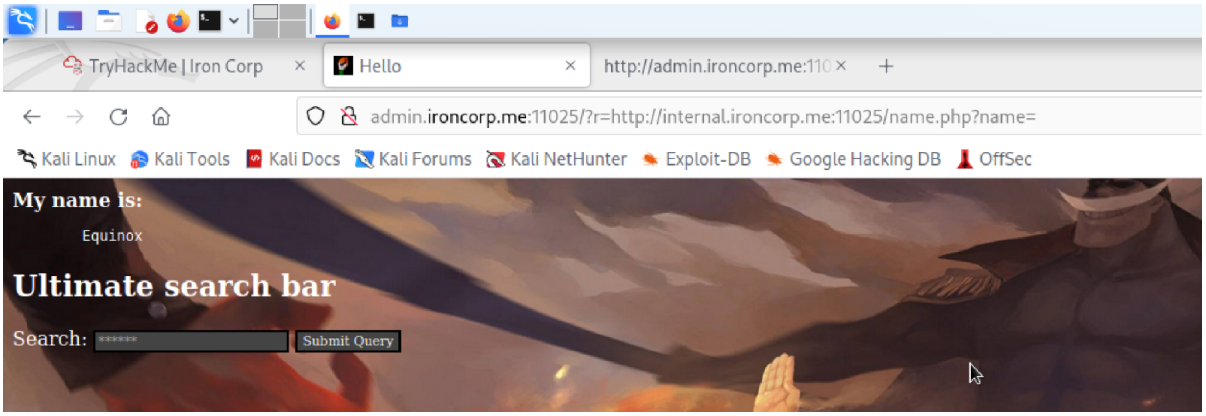
When we input http://internal.ironcorp.me:11025 in the search bar, this is what we'll get.



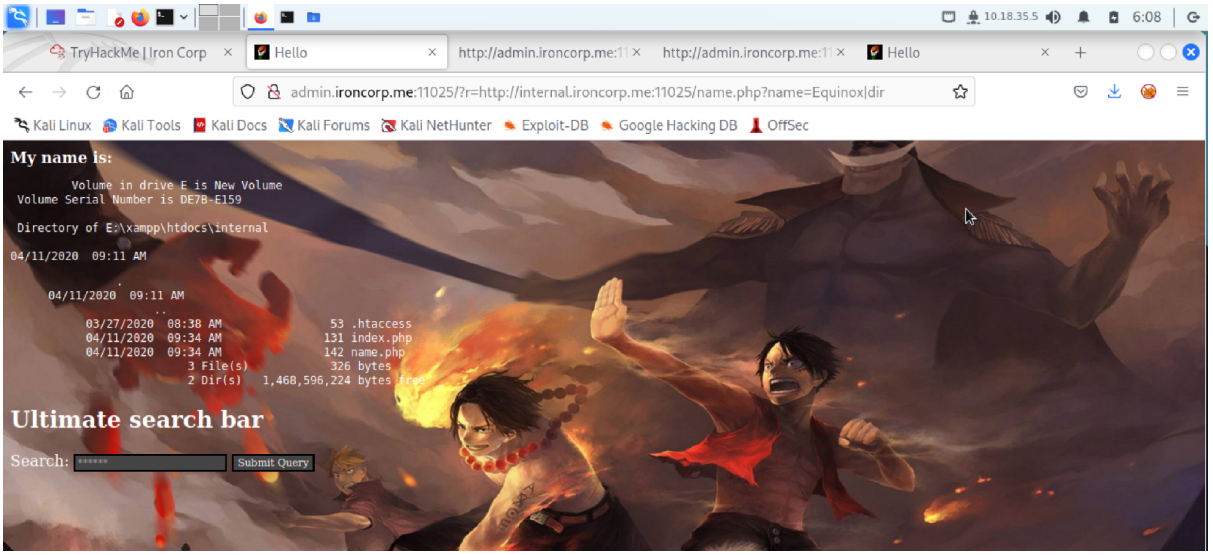
And if we look in the source page, we'll get a clue on how to gain the name.



Once we input the link in the search tab, this is what we'll get. The name is Equinox.



We can also look at the directory by entering |dir.



After the attacking process, the website displays this.

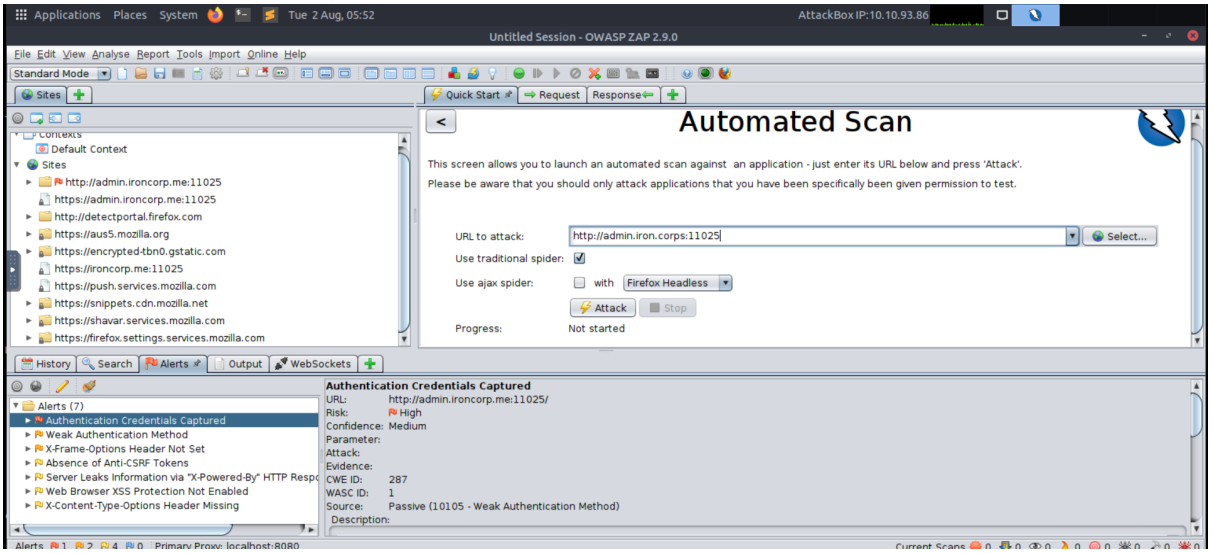
Step 3: Horizontal Privilege Escalation

Members Involved: Afreen, Aina

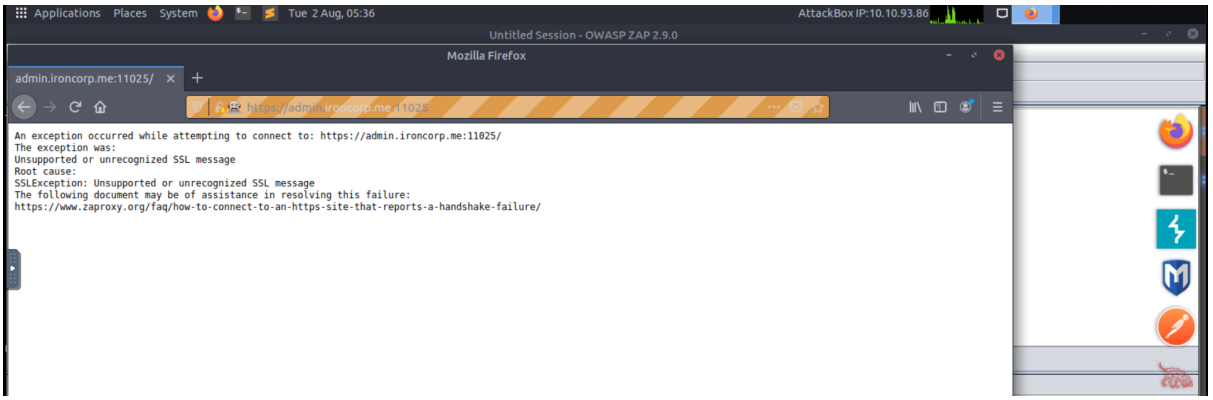
Tools used: nmap, BurpSuite, github, owasp, firefox, powershell

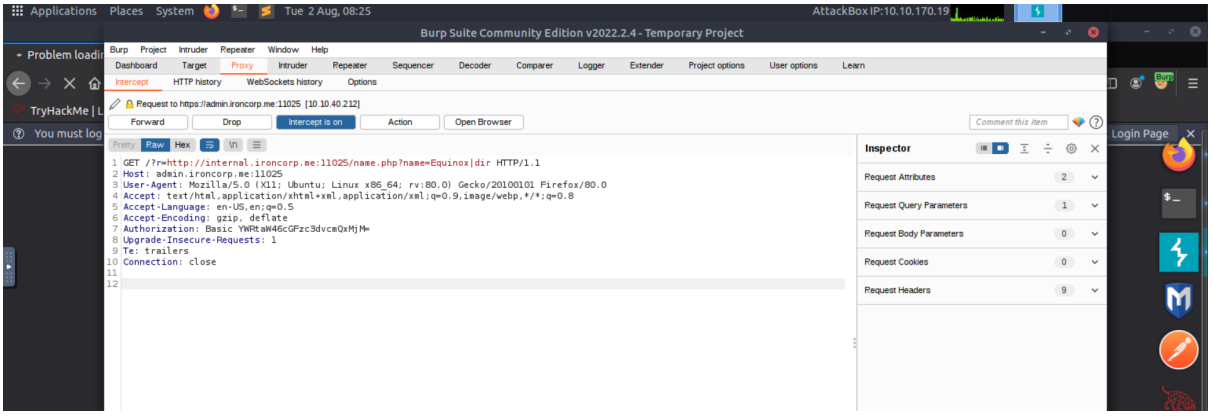
Thought Process and Methodology and Attempts:

Then, we open owasp to attack the website in order to reverse the shell and run powershell.

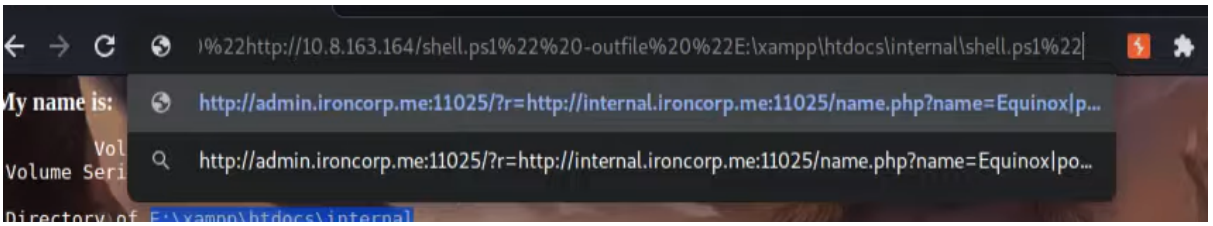


After the attacking process, the website displays this.

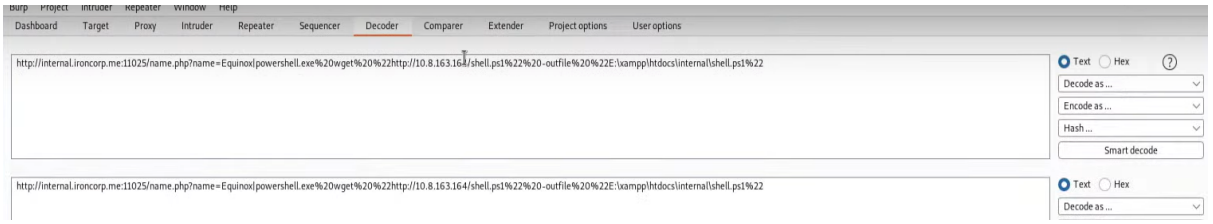




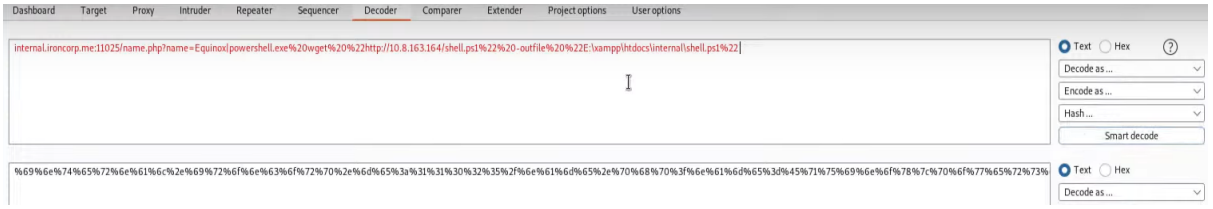
Then, we add this URL into the URL bar



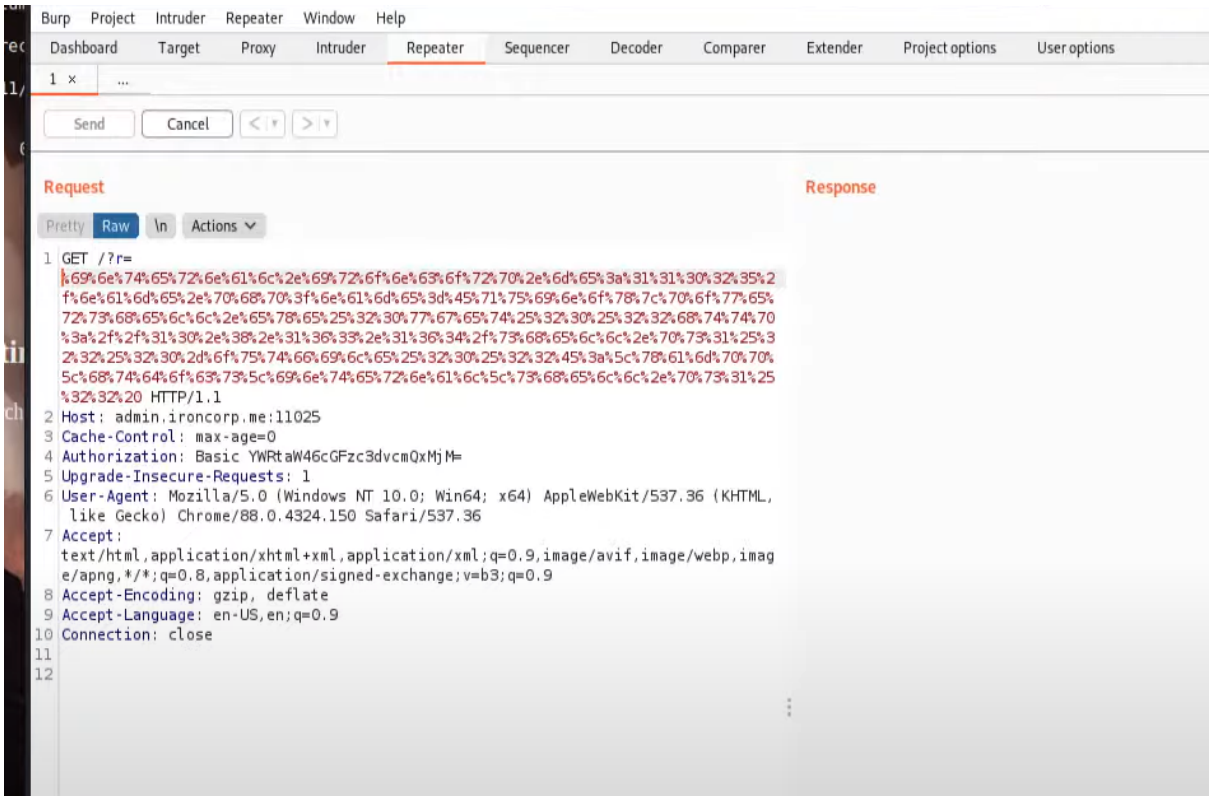
After that we decode that URL and change the encode as to URL



Where we will get this.

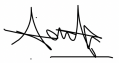


We then paste that into the first page.



End of progress.

Contributions:

ID	Name	Contribution	Signatures
1211101707	Nur'aina Binti Ikhwan Moeid	Do the reconnaissance and enumeration, the horizontal privilege escalation and presentation video editing.	
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Do the reconnaissance and enumeration and the horizontal privilege escalation.	
1211101519	Aisyah Binti Ahmad Komarolaili	Do the reconnaissance and enumeration. Find the name from the admin page.	
1211102590	Nur Hanisah Binti Mohd Pauzi	Do the reconnaissance and enumeration.	

Video link: https://youtu.be/bYF2gde6kn0