TryHackMe Room Write-up

Title: Hidden Deep Into My Heart

Description: Find what's hidden deep inside this website.

Author: Igor Buszta

Deep Into My Heart

Description: My Dearest Hacker,

Cupid's Vault was designed to protect secrets meant to stay hidden forever. Unfortunately, Cupid underestimated how determined attackers can be.

Intelligence indicates that Cupid may have unintentionally left vulnerabilities in the system. With the holiday deadline approaching, you've been tasked with uncovering what's hidden inside the vault before it's too late.

You can find the web application here: http://MACHINE_IP:5000

Objective: What is the flag?

Tools: macOS, nmap, ffuf

Let’s not waste our time on main page, because there’s nothing interesting. Let’s head straight into scanning the server and revealing any vulnerabilities.

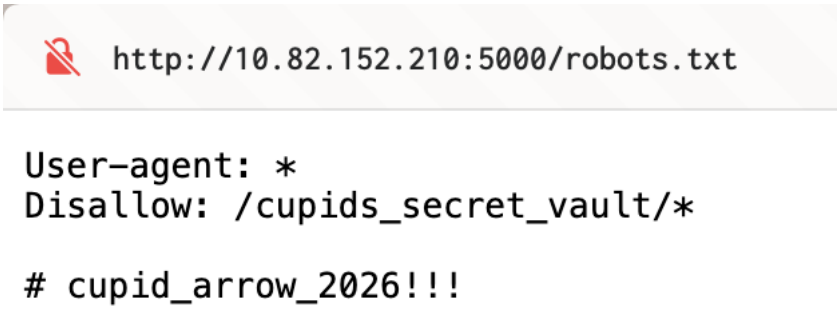
```
> sudo nmap -sC -sV 10.82.152.210
Starting Nmap 7.97 ( https://nmap.org ) at 2026-02-15 15:35 +0100
Nmap scan report for 10.82.152.210
Host is up (0.091s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   256 b9:55:a7:96:93:63:c6:ef:d4:67:32:1e:fe:06:d1:a3 (ECDSA)
|_  256 06:fd:53:03:44:1f:aa:c2:ed:0a:4f:88:1d:7b:44:ae (ED25519)
5000/tcp open  http    Werkzeug httpd 3.1.5 (Python 3.10.12)
| http-robots.txt: 1 disallowed entry
|_/cupids_secret_vault/*
|_http-title: Love Letters Anonymous
|_http-server-header: Werkzeug/3.1.5 Python/3.10.12
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.84 seconds
```

Picture 1: nmap results.

We can see that port 22 on quite new version OpenSSH 8.9p1 is open.

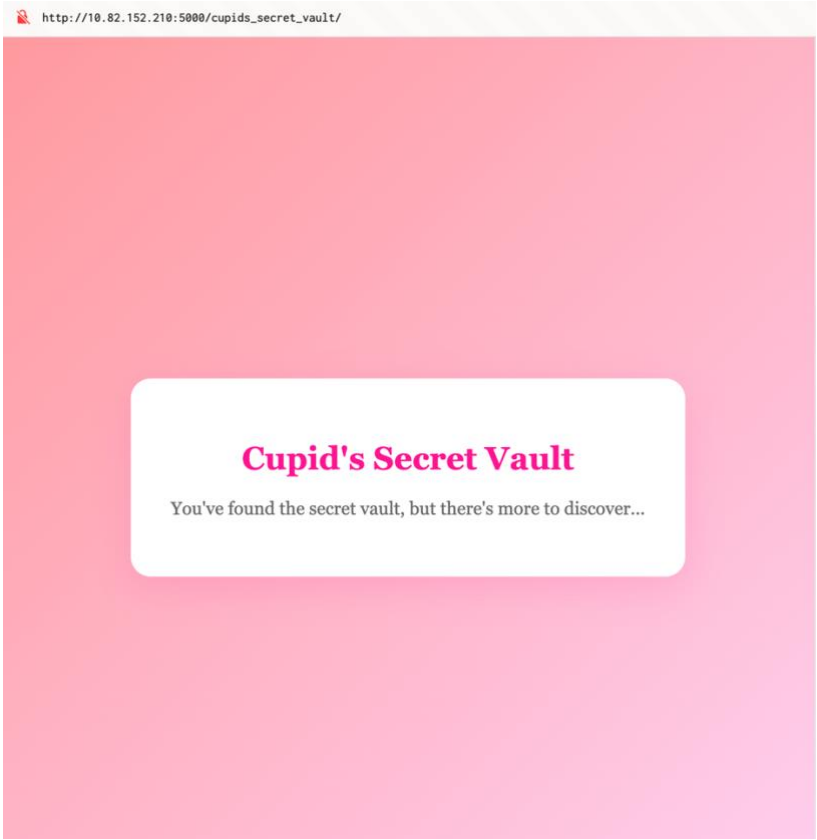
I tried looking for vulnerabilities there using ssh-audit and using different nmap scripts, but found nothing.

We should expect logging in at some point. Ssh-hostkeys are no use for us. Below is the meat. We can see that there's a robots.txt with informations.



Picture 2: robots.txt contents.

We have what looks like a password for expected logging in. Let's see what's in the restricted directory.



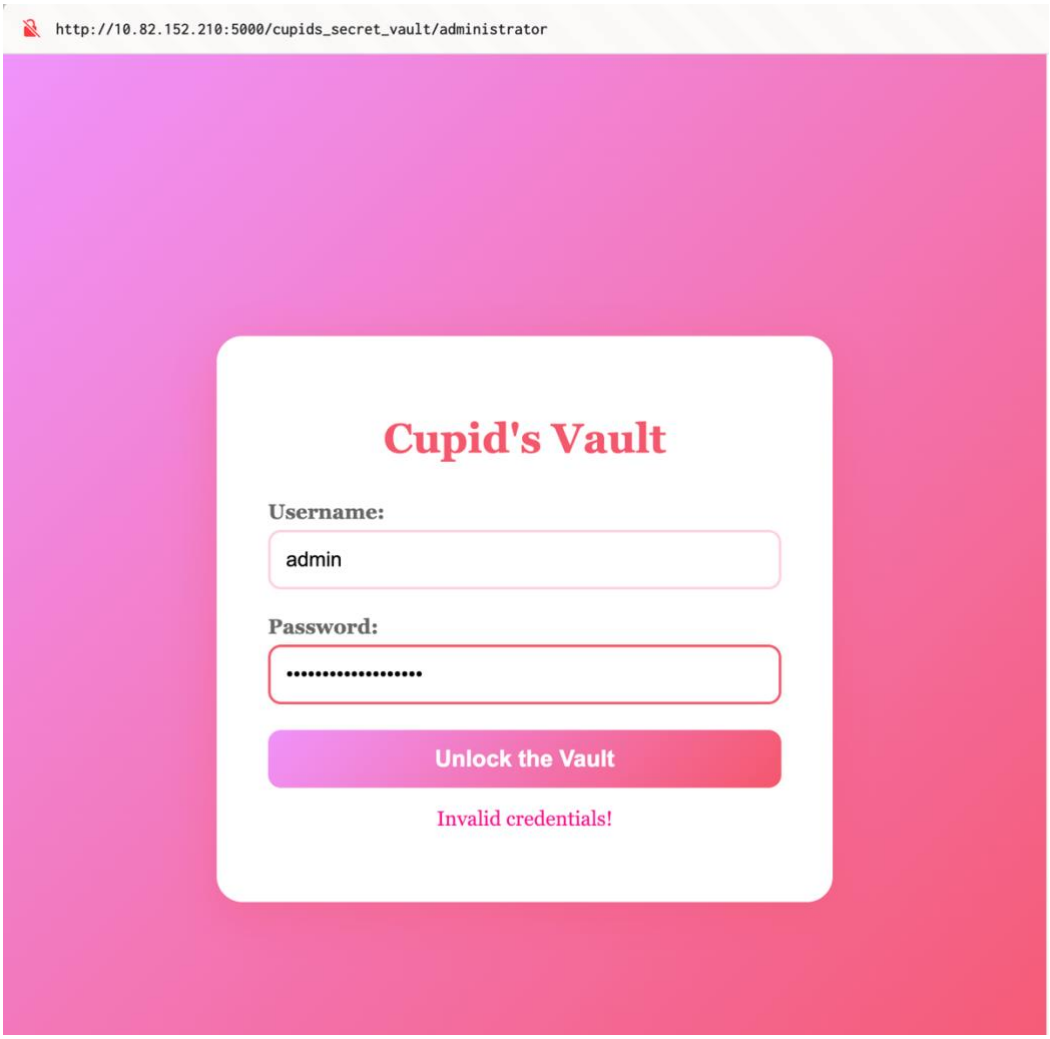
Picture 3: /cupids_secret_vault/ contents.

After finding this hidden page, we should try to find another ones. We have gobuster or ffuf available. I used ffuf because of speed and thoroughness.

```
:: Progress: [3755/220560] :: Job [1/1] :: 178 req/sec :: Duration: [0:00:17] :: Errors
:: Progress: [3774/220560] :: Job [1/1] :: 175 req/sec :: Duration: [0:00:17] :: Errors
administrator           [Status: 200, Size: 2381, Words: 956, Lines: 90, Duration: 55ms]
:: Progress: [12708/220560] :: Job [1/1] :: 2 req/sec :: Duration: [0:03:08] :: Errors: 205 ::
[INFO] ------ PAUSING ------

entering interactive mode
type "help" for a list of commands, or ENTER to resume.
```

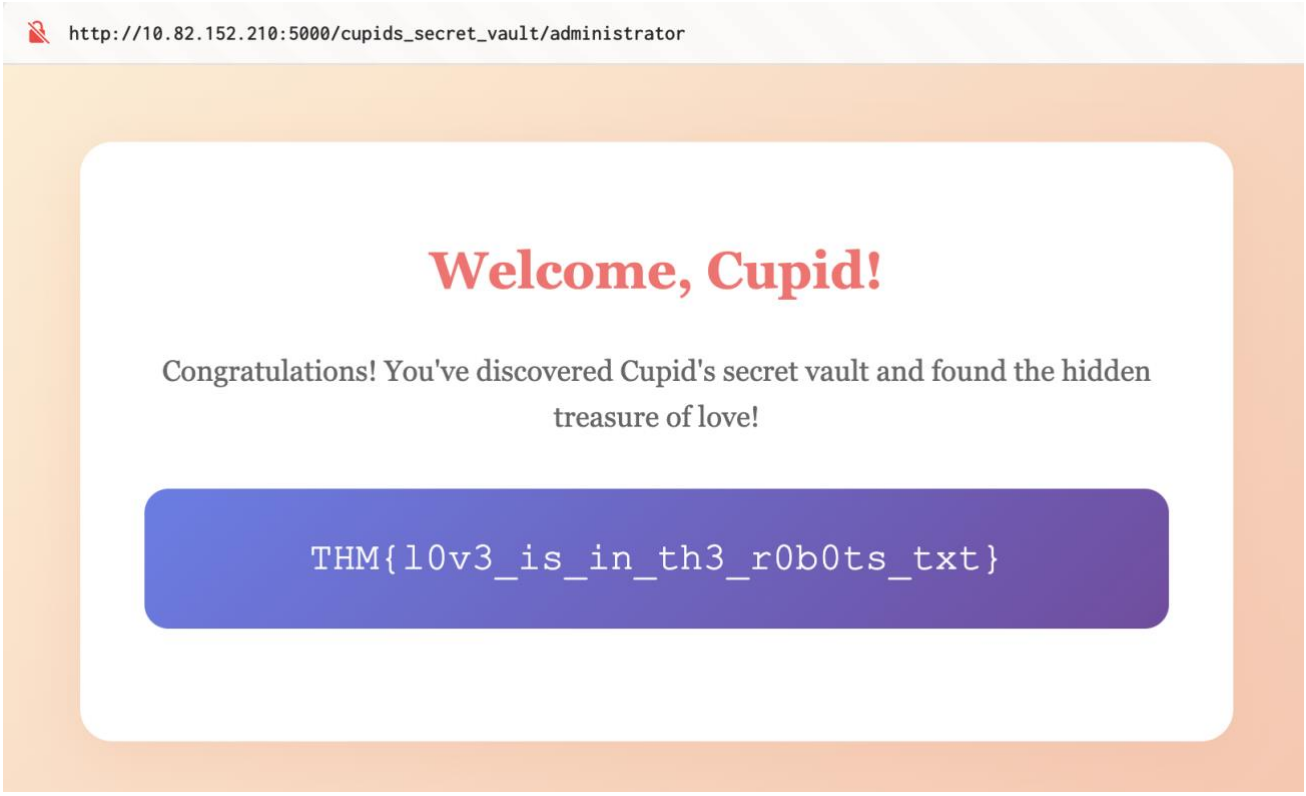
Picture 4: ffuf selected results.

Bingo! Let's go and see what's on the administrator page.



Picture 5: /cupids_secret_vault/administrator page contents.

I went ahead and filled the credentials. I used the password found in robots.txt and tried the possible usernames without any tools. First guess was *cupid* and then *admin*.



Picture 6: Successful login and found flag.