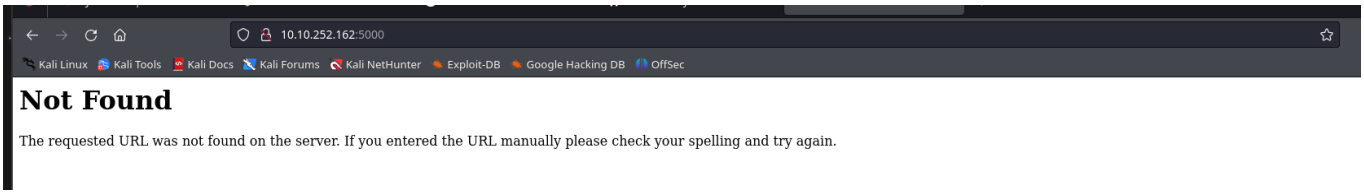
SSTI

Escaneo

```
❯ nmap -p- --open -sC -sV -sS --min-rate 5000 -n -Pn -vvv 10.10.252.162 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-05 12:32 CET
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
```

```
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 eb:36:ba:cc:38:7c:a3:72:74:0b:d0:ff:d6:22:c3:de (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC2SObkDbgtLAxFVw4BPY+ze/kkRxO5H09Zt6jTubH9N30ak8VJnqJoyPk93z17qlwZ9IBf5DeRT5jbtkRzal0A17+6wj+yC8UthgZYeWJFgGHWok/GOJj+cZEJbxpjoqmmb6C1Ec+2JP7Xgj
xJdfm5c0lbRRvOvO6K6rtl1UosCC3LLAkDg6J1BW6qIcc7Mp/i7KE2ueqYhyb7u6G+iwDnsCkYYNbLiVrkhAQ0bgSoD/Ob/t5FOu8LLdfm31WExikzmwzuadwMZZaPIIW934M9aV1LV3chnOg56dw6L3P0El2zK5ESIamzKysCfLZrsfMOh6BP2K
UvHwgOI/G9sOr1
|   256 ac:27:df:7b:bd:bd:db:27:72:8c:4d:3e:fe:37:ac:7c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH1xA4hSkWOkV3opulagt4TSUkiFY9HhG4lf2iMaxFk0sazNrz/X+Iv1Y+5InTNLvDfOmAA2KrgGMx6XM44nZ6Q=
|   256 bd:87:c7:fa:c7:0f:a4:fe:a6:0e:ad:58:ee:0e:31:10 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC9RJ1kEI05K1NmFn9XtREtPZeo6/Yl3NmWMdB3eEd8d
5000/tcp open  http    syn-ack ttl 63 Werkzeug httpd 1.0.1 (Python 3.6.9)
|_http-server-header: Werkzeug/1.0.1 Python/3.6.9
|_http-title: 404 Not Found
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Ahora nos dirigimos al puerto http que tiene que es 5000

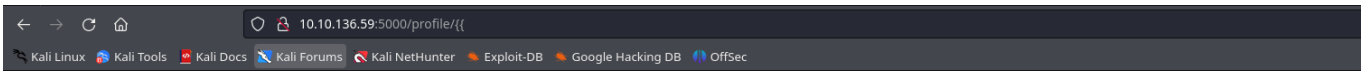


viendo esto lanzaremos un wfuzz

```
❯ wfuzz -c --hc=400 -t 200 --sc=200,301 -w /usr/share//wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.252.162:5000/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.252.162:5000/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
```

```
❯ wfuzz -c --hc=400 -t 200 --sc=200,301 -w /usr/share//wordlists/dirb/common.txt -u http://10.10.252.162:5000/FUZZ/aaa
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.252.162:5000/FUZZ/aaa
Total requests: 4614

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000003160:   200        0 L      6 W        39 Ch       "profile"

Total time: 0
Processed Requests: 4614
Filtered Requests: 4613
Requests/sec.: 0
```

Ahora probamos cual es la plantilla hasta el error



Internal Server Error

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there is an error in the application.

vnos da el error cuando ponemos dos llaves