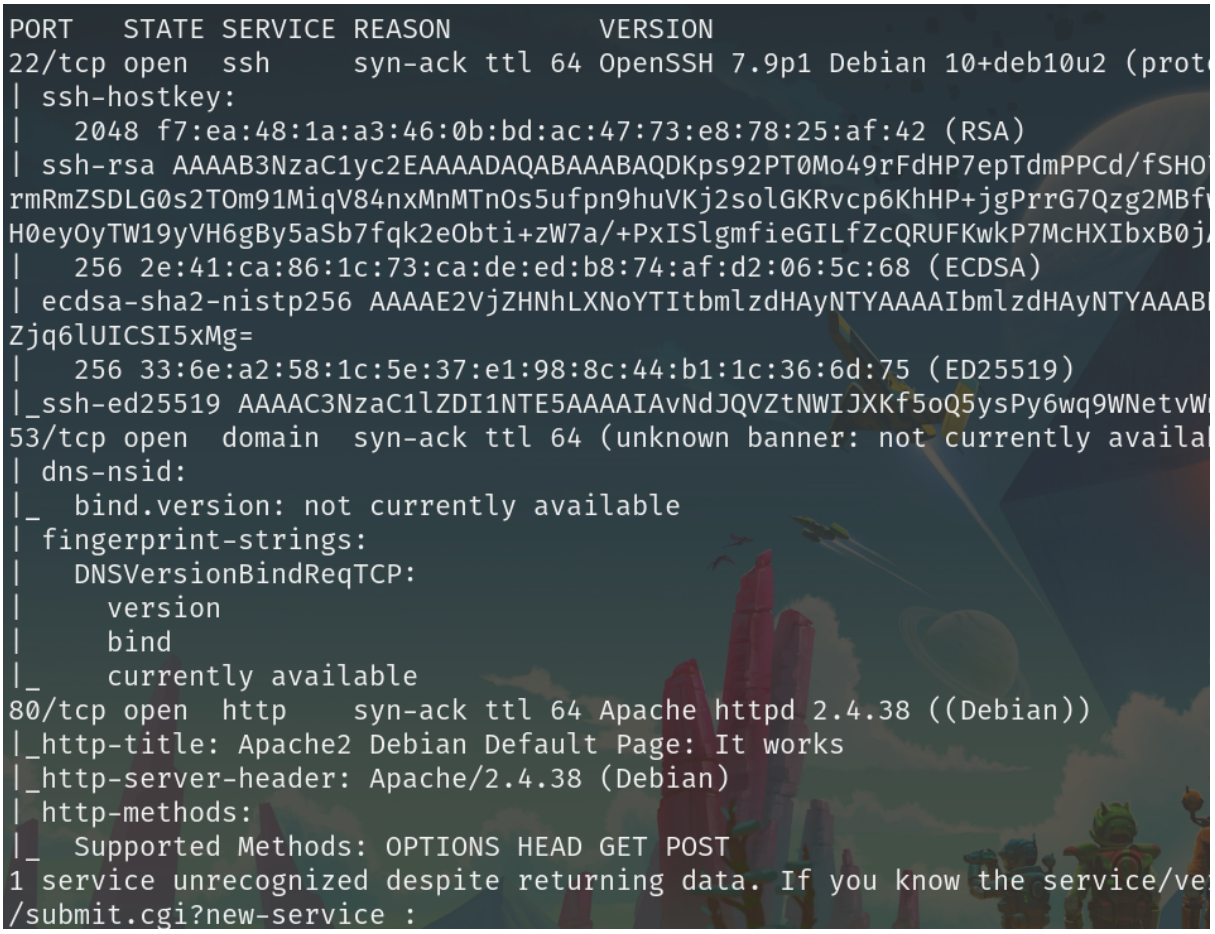
Zone

```
nmap -sS --open -p- -Pn -n -vvv 192.168.137.7
```

```
nmap -sCV -p22,53,80 -Pn -n -vvv 192.168.137.7
```

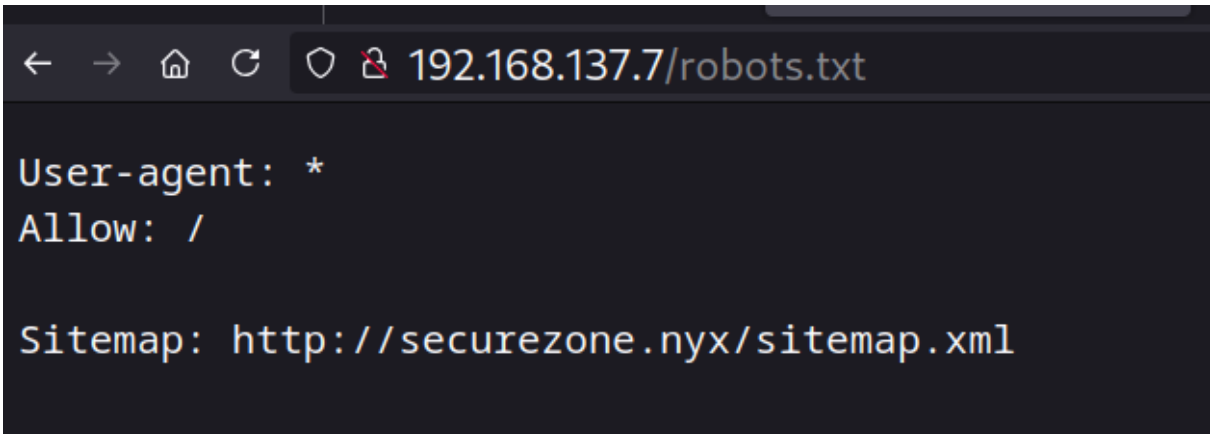



```
❯ whatweb 192.168.137.7
```

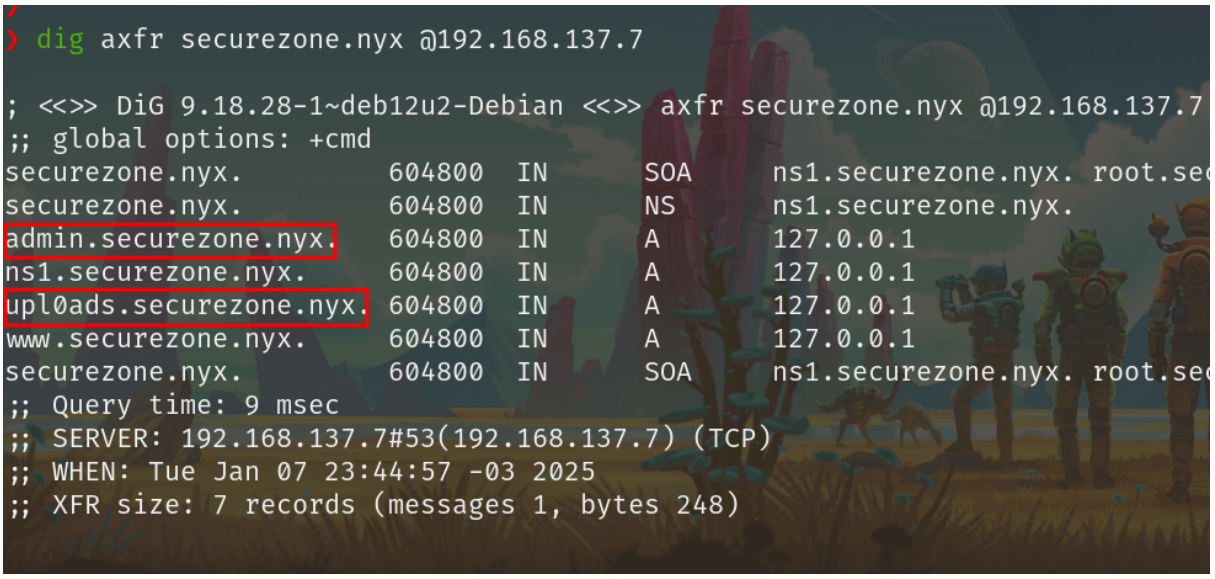
http://192.168.137.7 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.7], Title[Apache2 Debian Default Page: It works]

```
❯ gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.137.7/ -t 50 -x php,html,txt
```

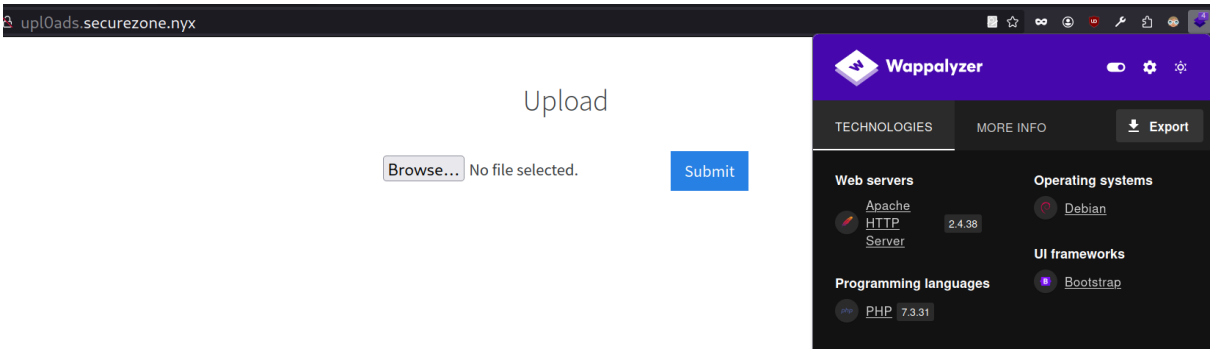
- incluimos en el /etc/hosts



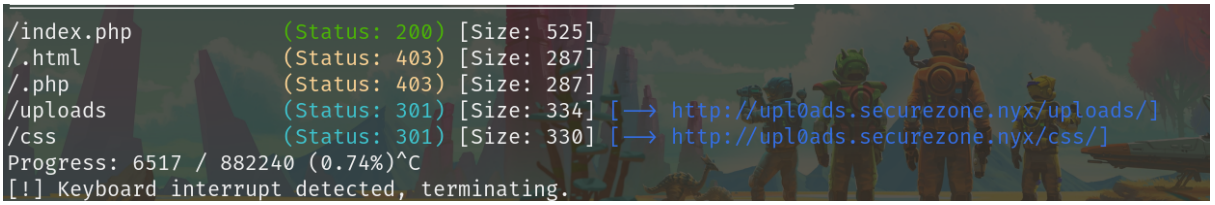
- no pasa nada si la fuzzeo por domnio, voy a intentar por suvdomnios

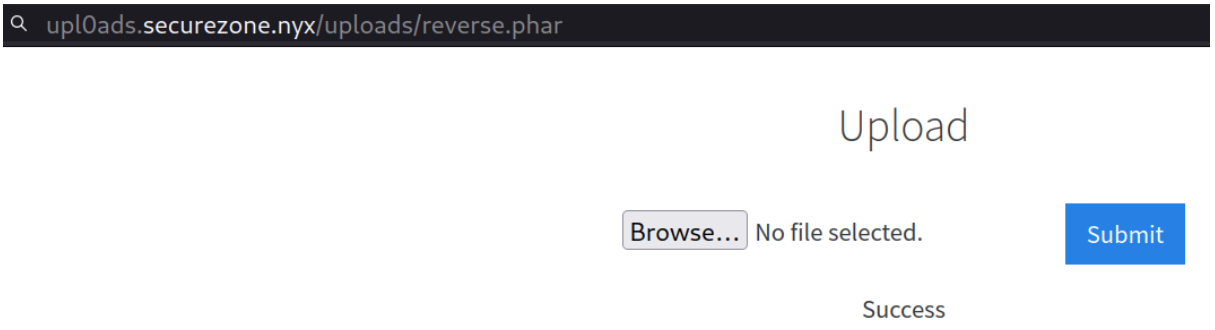


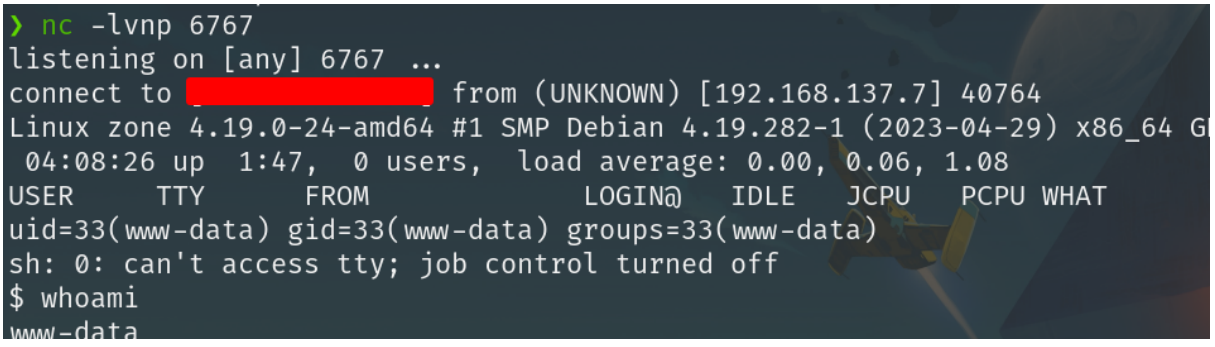
juicy...



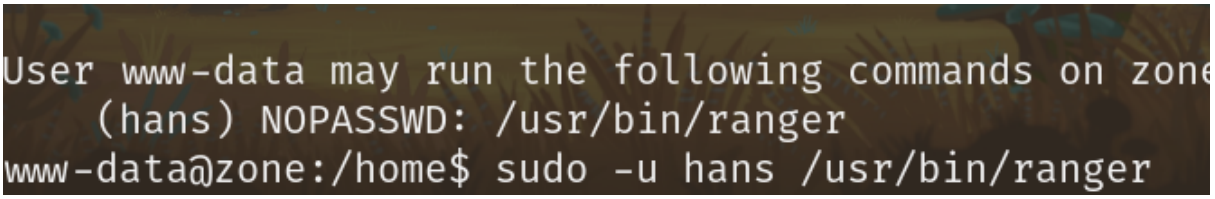

```
❯ gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u 'http://upl0ads.securezone.nyx/' -t 50 -x php,txt,html
```

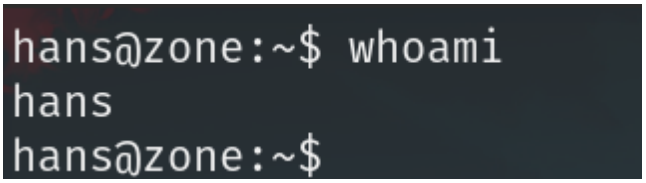


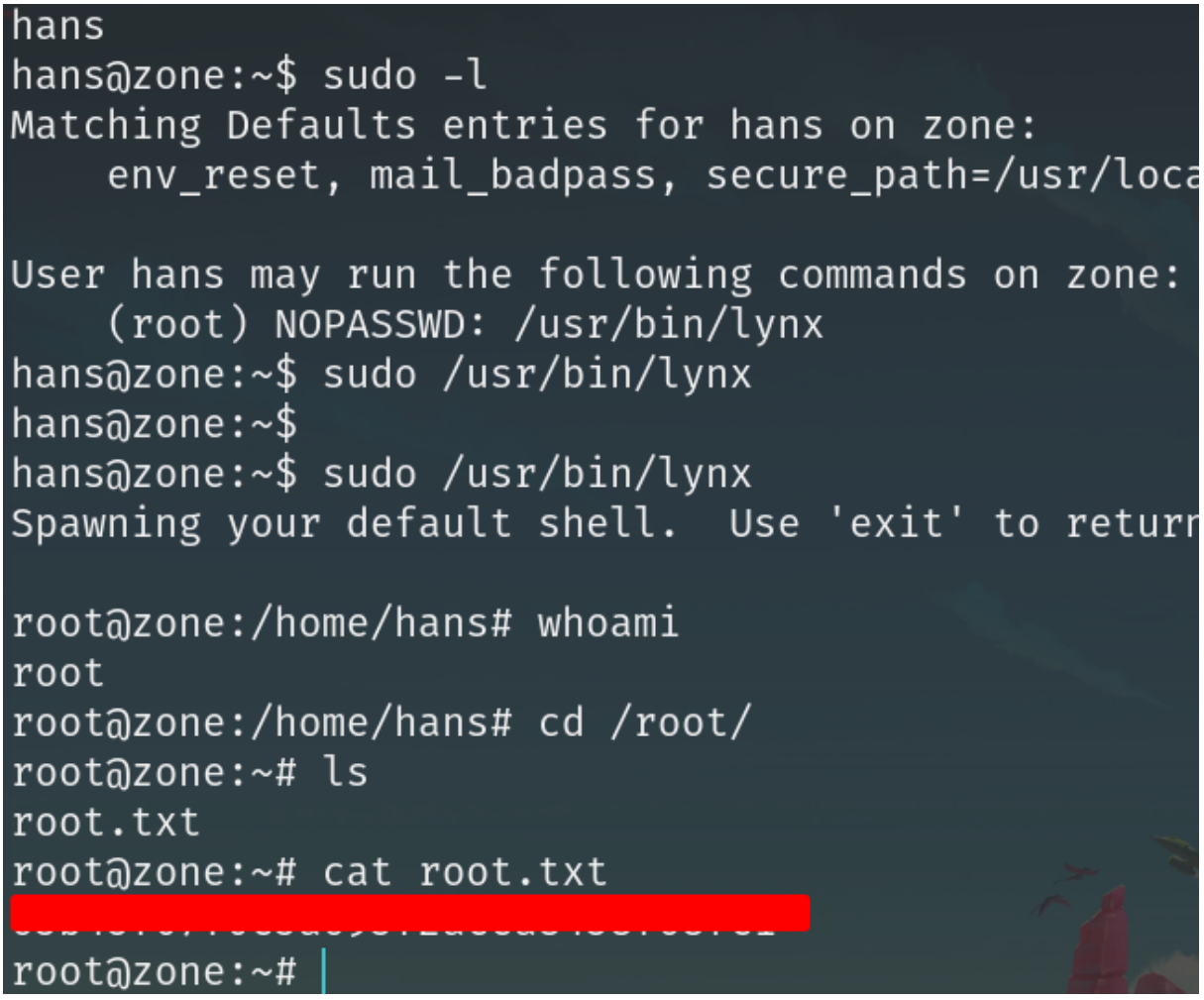




vemos q al ejecutarlo nos avre una consola, hacemos shift+1 y nos da una shell, /bin/bash y listo







lynx havre como si fuese un more, aprete shift+1 y sali como root