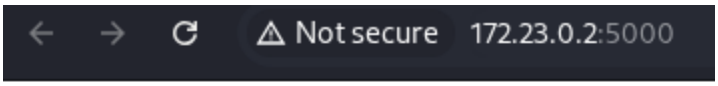
Confianza excesiva

Al descomprimir el archivo del reto, se observa un proyecto web desplegado mediante Docker, el cual incluye un Dockerfile y un docker-compose.yml. La instancia se levanta correctamente utilizando docker-compose up.

```
└─$ ll
total 20
drwxrwxr-x 2 vfric vfric 4096 Dec 20 10:12 app
-rw-rw-r-- 1 vfric vfric 1125 Dec 20 10:11 confianza-cliente.zip
-rw-r--r-- 1 vfric vfric   77 Dec 12 22:04 docker-compose.yml
-rw-r--r-- 1 vfric vfric  101 Dec 12 22:04 Dockerfile
-rw-r--r-- 1 vfric vfric  163 Dec 12 22:04 README.md

┌──(vfric㉿vfric)-[~/…/CTF-cyberminds-1er-Edici-n/Web/Confianza excesiva/Solucion]
└─$ sudo docker-compose up
[sudo] password for vfric:
WARN[0000] /home/vfric/Desktop/CTF-cyberminds-1er-Edici-n/Web/Confianza excesiva/Solucion/docker-compose.yml: the a
ttribute `version` is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Running 1/1
 ✔ Container solucion-web-1  Recreated                                                                    0.0s
Attaching to web-1
web-1  |  * Serving Flask app 'app'
web-1  |  * Debug mode: off
web-1  | WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI ser
ver instead.
web-1  |  * Running on all addresses (0.0.0.0)
web-1  |  * Running on http://127.0.0.1:5000
web-1  |  * Running on http://172.23.0.2:5000
web-1  | Press CTRL+C to quit
web-1  | 172.23.0.1 - - [20/Dec/2025 15:12:26] "GET / HTTP/1.1" 200 -
```

Al acceder a la aplicación web (http://<IP>:5000), se muestra la página principal.



Bienvenido

Acceso estándar.

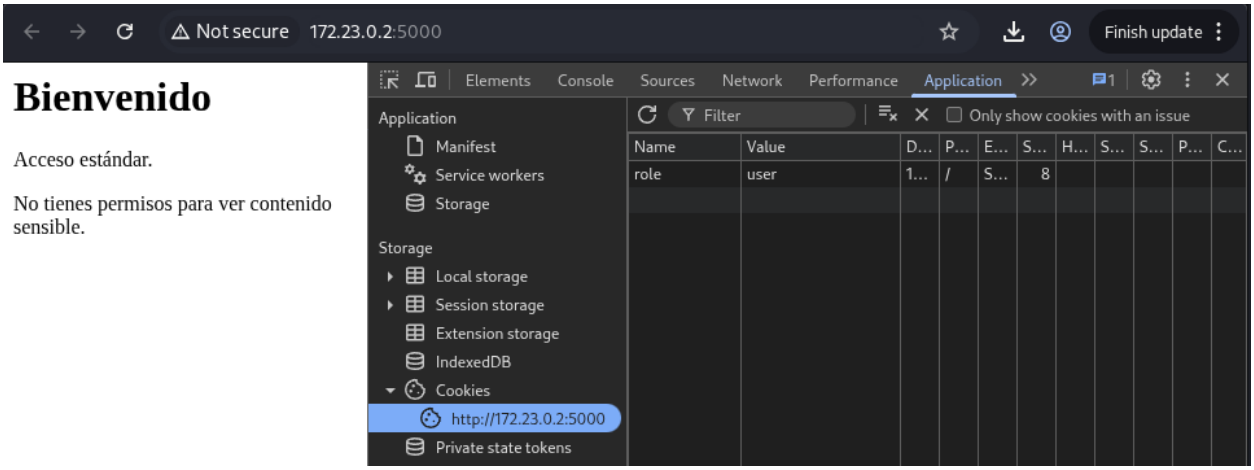
No tienes permisos para ver contenido sensible.

Al inspeccionar el código HTML de la página, se observa que no existe ningún control visible de autenticación, ni verificación explícita del usuario en el frontend.

Esto sugiere que el control de acceso podría depender de datos del lado cliente, como cookies o almacenamiento local.

```
<html>
  <head></head>
  <body> == $0
    <h1>Bienvenido</h1>
    <p>Acceso estándar.</p>
    <p>No tienes permisos para ver contenido sensible.</p>
  </body>
</html>
```

Utilizando las DevTools, en la sección Application → Cookies, se identifica una cookie asociada al sitio.



Esta cookie define el rol del usuario y es utilizada por la aplicación para determinar el nivel de acceso. Tras la modificación del valor de la cookie, se obtiene acceso al Panel de administración, donde el sistema confirma que se ha accedido con privilegios elevados y revela directamente la flag del reto.

NOTA: Si al acceder a la instanica vez una anterior usa:
sudo docker-compose down

sudo docker-compose build --no-cache

sudo docker-compose up