

Campos invisibles

Al acceder al directorio del reto, se observa un proyecto web desplegado con Docker, que incluye un Dockerfile, docker-compose.yml y un formulario web accesible desde un servicio Flask.

```
└$ ll
total 20
drwxrwxr-x 2 vfric vfric 4096 Dec 20 09:57 app
-rw-r--r-- 1 vfric vfric    77 Dec 12 22:45 docker-compose.yml
-rw-r--r-- 1 vfric vfric   101 Dec 12 22:45 Dockerfile
-rw-rw-r-- 1 vfric vfric 1177 Dec 20 09:56 formulario-curioso.zip
-rw-r--r-- 1 vfric vfric   162 Dec 12 22:45 README.md

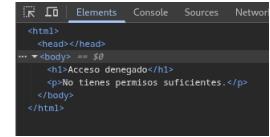
[(vfric@vfric)-[~/.../CTF-cyberminds-1er-Edici-n/Web/Campos invisibles/Solucion]
└$ docker-compose up
WARN[0000] /home/vfric/Desktop/CTF-cyberminds-1er-Edici-n/Web/Campos invisibles/Solucion/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion
unable to get image 'solucion-web': permission denied while trying to connect to the Docker daemon socket at unix://var/run/docker.sock: Get "http://%2Fvar%2Frun%2Fdocker.sock/v1.47/images/solucion-web/json": dial unix /var/run/docker.sock: connect: permission denied

[(vfric@vfric)-[~/.../CTF-cyberminds-1er-Edici-n/Web/Campos invisibles/Solucion]
└$ sudo docker-compose up
[sudo] password for vfric:
WARN[0000] /home/vfric/Desktop/CTF-cyberminds-1er-Edici-n/Web/Campos invisibles/Solucion/docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion
[+] Building 1.3s (10/10) FINISHED
  ⇒ [web internal] load build definition from Dockerfile                               docker:default
  ⇒ → transferring dockerfile: 138B                                                 0.0s
  ⇒ [web internal] load metadata for docker.io/library/python:3.11-slim               1.1s
  ⇒ [web internal] load .dockerignore                                              0.0s
  ⇒ → transferring context: 2B                                                 0.0s
  ⇒ [web 1/4] FROM docker.io/library/python:3.11-slim@sha256:158caf0e080e2cd74ef2879ed3c4e697792ee65251c8208b7af 0.0s
  ⇒ → resolve docker.io/library/python:3.11-slim@sha256:158caf0e080e2cd74ef2879ed3c4e697792ee65251c8208b7af 0.0s
  ⇒ [web internal] load build context                                              0.0s
  ⇒ → transferring context: 976B                                              0.0s
  ⇒ CACHED [web 2/4] WORKDIR /app                                              0.0s
  ⇒ CACHED [web 3/4] COPY app/ /app/                                             0.0s
  ⇒ CACHED [web 4/4] RUN pip install flask                                         0.0s
  ⇒ [web] exporting to image                                              0.0s
  ⇒ → exporting layers                                              0.0s
  ⇒ → writing image sha256:4adf6dbfad59a701dbf6c5626d67c5cad2ac376d6cc3453c9395f750b33413b3 0.0s
  ⇒ → naming to docker.io/library/solucion-web                                0.0s
  ⇒ [web] resolving provenance for metadata file                            0.0s
[+] Running 3/3
  ✓ web                                Built                                              0.0s
  ✓ Network solucion_default  Created                                         0.2s
  ✓ Container solucion-web-1  Created                                         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 server 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 14:57:55] "GET / HTTP/1.1" 200 -
web-1 | 172.23.0.1 - - [20/Dec/2025 14:57:56] "GET /favicon.ico HTTP/1.1" 404 -
web-1 | 172.23.0.1 - - [20/Dec/2025 14:58:12] "POST / HTTP/1.1" 200 -
web-1 | 172.23.0.1 - - [20/Dec/2025 14:58:13] "GET / HTTP/1.1" 200 -
web-1 | 172.23.0.1 - - [20/Dec/2025 14:58:17] "POST / HTTP/1.1" 200 -
web-1 | 172.23.0.1 - - [20/Dec/2025 14:58:18] "GET / HTTP/1.1" 200 -
█
W Enable Watch
```

Al ingresar a la aplicación web, se muestra un formulario simple. Al enviar el formulario con datos normales, el sistema responde con un mensaje de “Acceso denegado”, indicando que no existen permisos suficientes.

Acceso denegado

No tienes permisos suficientes.



```
<html>
  <head></head>
  <body> ...
    <h1>Acceso denegado</h1>
    <p>No tienes permisos suficientes.</p>
  </body>
</html>
```

Utilizando las DevTools, se inspecciona el formulario HTML. Aquí se detecta un detalle clave, existen campos ocultos (hidden) dentro del formulario, los cuales no son visibles para el usuario, pero sí son enviados al servidor. Estos campos invisibles contienen valores que determinan si el acceso es normal o privilegiado.



The screenshot shows a browser window with a simple form titled "Formulario". It has a text input field labeled "Nombre:" and a submit button labeled "Enviar". Below the browser is the browser's developer tools, specifically the "Elements" tab, displaying the generated HTML code:

```
<html>
  <head></head>
  <body>
    <h1>Formulario</h1>
    <form method="POST">
      ...
      <input type="hidden" name="isAdmin" value="false"> == $0
      <label>Nombre:</label>
      <input type="text" name="name">
      <button type="submit">Enviar</button>
    </form>
  </body>
</html>
```

Modificando manualmente los valores de los campos ocultos desde el HTML, se altera el contenido que se envía al backend.



The screenshot shows the same browser and developer tools setup. The "name" field now contains "flag" and the "isAdmin" field has been manually modified to "true". The developer tools show the updated HTML code:

```
<html>
  <head></head>
  <body>
    <h1>Formulario</h1>
    <form method="POST">
      ...
      <input type="hidden" name="isAdmin" value="true"> == $0
      <label>Nombre:</label>
      <input type="text" name="name">
      <button type="submit">Enviar</button>
    </form>
  </body>
</html>
```

Tras reenviar el formulario con los valores modificados, el servidor ya no responde con “Acceso denegado”, sino con un mensaje de “Acceso privilegiado”, confirmando que la validación del lado servidor es débil y confía en datos enviados por el cliente

Acceso privilegiado

Has modificado datos del formulario.

FIS{L0_0CULt0_NO_3S_S3GURO}

FIS{L0_0CULt0_NO_3S_S3GURO}