OAuth2: Roles

Implementa la seguridad de tu API Rest con Spring Boot

Roles

- En OAuth2 Se definen varios roles
  - Dueño del recurso (*Owner*)
  - Cliente (*Client*)
  - Servidor de recursos protegidos (*Resource Server*)
  - Servidor de autorización (*Authorization Server*)

Dueño del recurso

- El propietario del recurso es el “usuario” que da la autorización a una aplicación, para acceder a su cuenta.
- El acceso de la aplicación a la cuenta del usuario se limita al “alcance” de la autorización otorgada (e.g. acceso de lectura o escritura).
- Se le llama el dueño de los recursos porque, si bien la API no es tuya los datos que maneja si lo son.

Cliente

- El cliente es la aplicación que desea acceder a la cuenta del usuario.
- Antes de que pueda hacerlo, debe ser autorizado por el usuario, y dicha autorización debe ser validada por la API.
- Este cliente puede ser una aplicación web, móvil, de escritorio, para Smart TV, un dispositivo IoT, **otra API**, etcétera.

Servidor de autorización

- Es el responsable de gestionar las peticiones de autorización.
- Verifica la identidad de los usuarios y emite *tokens de acceso* a la aplicación cliente.
- En muchas ocasiones, estará implementado por un tercero conocido (*Facebook*, *Twitter*, *Github*, *Google*, *Okta*, ….)
- Puede formar parte de la misma aplicación que el servidor de recursos.

Servidor de recursos

- Será nuestra API, el servidor que aloja el recurso protegido al que queremos acceder.
- Puede formar parte de la misma aplicación que el servidor de autenticación.

Luces, cámara, acción

- Ahora, nos toca ver a estos 4 actores en acción.
- Lo hacemos en la siguiente lección.