

# JWT: Refactorización del controlador

Implementa la seguridad de tu API Rest con Spring Boot

# AuthenticationController

- Petición de login
  - Logueamos al usuario vía *AuthenticationManager*
  - Almacenamos el *Authentication* en el contexto de seguridad
  - Devolvemos el usuario y token al cliente.
- Petición me
  - Igual de sencilla que en la autenticación básica

# Reto

- Pedido
  - Basándonos en el código del ejemplo 12, en el que *refactorizamos* la funcionalidad de Pedido (controlador, servicio y repositorio), implementar dicha funcionalidad aquí, con JWT.
- Puedes implementarlo también para el resto de controladores.

# Reto

- ¿No os dan rabia las aplicaciones en las que os tenéis que registrar e, inmediatamente, os piden las credenciales para *loguearos*?
- ¿No os gustan más aquellas en las que al registraros, os loguea automáticamente?
- Combinar el mecanismo de registro y login, para que el registro devuelva también el token.
- Es posible que merezca la pena que desaparezca *UserController* y pasar todo el código a *AuthenticationController*, pasando a llamarse este último *UserAuthenticationController*.