Authorization & JWT - Bases Fundamentais

1. O que é Authorization numa API?

Authorization é o mecanismo que permite ao servidor decidir se um utilizador tem permissão para aceder a um determinado recurso. Depois do login, o utilizador deve provar a sua identidade em cada pedido protegido.

2. O que é Stateless?

Uma API stateless não guarda sessões no servidor. Cada pedido deve conter toda a informação necessária para ser validado. No teu projeto, essa informação é o token JWT enviado no header Authorization.

3. O que é o Header Authorization?

Os headers são metadados do pedido HTTP. O header Authorization é usado para enviar credenciais. No padrão moderno usamos: Authorization: Bearer

4. O que é um JWT?

JWT (JSON Web Token) é uma credencial digital assinada. Contém três partes: Header, Payload e Signature. O payload contém dados como o email (sub) e a data de expiração (exp). A assinatura garante que o token não foi alterado.

5. Porque o token é seguro?

O token é seguro porque está assinado com uma SECRET_KEY. Se alguém alterar o payload, a assinatura deixa de ser válida. Sem a SECRET_KEY ninguém consegue gerar tokens válidos.

6. Fluxo completo no teu projeto

- Utilizador faz login com email e password.
- Password é validada com bcrypt.
- Servidor gera JWT com expiração.
- Cliente envia token no header Authorization.

- Servidor valida token com jwt.decode().
- Se válido → acesso permitido. Se inválido → 401.

Este modelo demonstra que compreendes autenticação moderna baseada em tokens, segurança com hashing, separação de responsabilidades e arquitetura stateless.