



## Assessment Lab Node-05

### Objetivos

- Explorar a implementação de JSON Web Tokens (JWT) para autenticação e autorização.
- Integrar JWT com middleware para proteger rotas.

### Instruções

#### Fase 1 – Instalação e configuração

1. abra o projeto do Lab Node-02.
2. instale o pacote **jsonwebtoken** utilizando o comando **npm install jsonwebtoken**

#### Fase 2 - Configuração do Middleware para JWT

3. crie um middleware para verificar a autenticidade dos **tokens** JWT.
4. no middleware, utilize a função **jsonwebtoken.verify()** para verificar o token e extrair as informações do utilizador.
5. se o token for inválido/expirado, deverá devolver um erro **401 (unauthorized)**.
6. se o token for válido, adicione as informações do utilizador ao objeto **req** para utilização posterior.

#### Fase 3 – Proteção de rotas

3. importe o middleware de verificação de JWT no início do ficheiro do controlador.
4. aplique o middleware às rotas que necessitam de proteção.
5. verifique se as rotas protegidas estão acessíveis apenas com um token JWT válido.

#### Fase 4 - Criação de Tokens JWT

6. crie um endpoint para o login do utilizador.
7. no endpoint anterior, utilize a função **jsonwebtoken.sign()** para gerar um token JWT contendo as informações do utilizador (ex: ID, nome, e-mail).
8. defina uma **secret key** para assinar o token JWT.
9. retorne o token JWT no corpo da resposta do endpoint de login.

#### Fase 6 - Pesquisa

- Como armazenar tokens JWT de forma segura no lado do client(ex: **cookies** com a flag **HttpOnly**)?
- Como renovar tokens JWT automaticamente antes de expirarem?