re_S16_A2_SL6_backend

Entrega no AVA

Nome: _____ Turma: _____

Título da atividade: Segurança em autenticação e autorização

1. **Pontos principais do conteúdo**

Em sistemas modernos, a segurança nos processos de autenticação e autorização é essencial para proteger dados sensíveis e garantir acesso controlado às funcionalidades do sistema. Ferramentas como OAuth 2.0 e JWT (JSON Web Token) são amplamente utilizadas para implementar essas práticas de maneira eficiente e segura.

2. **Explicação detalhada**

2.1 Auth 2.0:

- **Definição:** um protocolo de autorização que permite que aplicativos acessem recursos em nome de um usuário sem expor as credenciais deste.
- **Fluxos de autorização:** authorization code, implicit, password credentials e client credentials.
- **Pontos-chave:**
  - Delegação de acesso sem compartilhar senhas;
  - Uso em APIs para autenticação de terceiros.

2.2. JWT (JSON web token)

- **Definição:** um padrão aberto para criar tokens que representam dados com segurança.
- **Componentes do JWT:**

  - **header:** informações sobre o algoritmo de assinatura e tipo de token;
  - **payload:** dados ou declarações (claims);
  - **signature:** validação do token.

- **Vantagens:**
  - formato compacto e independente;
  - autossuficiência: contém todas as informações necessárias;
  - amplamente utilizado para autenticação baseada em token.

2.3. Exemplos práticos

Imagine uma aplicação em que:

- um usuário se autentica para acessar o painel de administração;
- a autenticação é realizada utilizando OAuth 2.0 (Authorization code flow) para validar as credenciais;
- após a autenticação, o usuário recebe um JWT, que é usado para autorizar as requisições subsequentes.

---

3. Roteiro da atividade

Situação-problema:

Vocês foram contratados para desenvolver uma API que gerencia o acesso a um sistema bancário. Para proteger as informações dos usuários, você deve implementar práticas seguras de autenticação e autorização, utilizando OAuth 2.0 e JWT. O sistema precisa:

- garantir que somente usuários autenticados possam acessar seus dados;
- expirar tokens automaticamente após um período ou quando o usuário fizer logout;
- proteger endpoints sensíveis, como o de transações financeiras.

Situação fictícia produzida pela SEDUC-SP.

4. **Perguntas dissertativas**

1. Expliquem como o protocolo OAuth 2.0 pode ser implementado para autenticar os usuários no sistema bancário. Considere os diferentes fluxos de autorização e a escolha do mais adequado para esta situação.

2. Quais informações são geralmente armazenadas no payload de um JWT e como elas podem ser utilizadas para autorização em APIs? Explique como garantir que o JWT não seja manipulado por terceiros.

3. Citem um exemplo prático de como a API poderia proteger um endpoint sensível (como um de transações financeiras) usando JWT. Descreva o fluxo completo de autenticação e autorização.

4. Quais medidas adicionais de segurança poderiam ser adotadas no sistema para complementar o uso de OAuth 2.0 e JWT? Inclua práticas como uso de HTTPS, políticas de CORS e outros métodos de mitigação de vulnerabilidades.