Sistema de Autenticação e Autorização
Valor: 20,0 pts

Sistema de Autenticação e Autorização: Crie um sistema de login seguro usando JWT para autenticar usuários. Depois disso, implemente diferentes níveis de acesso para os usuários (por exemplo, administrador, moderador e usuário comum) e restrinja o acesso a certas partes do aplicativo com base nos tokens JWT gerados.

Exercício 1: Implementação de Autenticação com JWT (10 pontos)

Você foi contratado para desenvolver um sistema de autenticação seguro para uma plataforma online. O objetivo principal é garantir que apenas usuários autenticados tenham acesso aos recursos da plataforma. Requisitos específicos que você deve atender:

- 1) Cadastro de Usuário: Os usuários devem poder se cadastrar na plataforma fornecendo informações como nome de usuário, senha e tipo de conta (por exemplo, administrador, moderador ou usuário comum).
- 2) Login Seguro: Implemente um sistema de login seguro onde os usuários possam entrar na plataforma fornecendo suas credenciais (nome de usuário e senha). As credenciais devem ser verificadas em relação às informações armazenadas no banco de dados.
- 3) Geração de Token JWT: Após um login bem-sucedido, gere um token JWT (JSON Web Token) para o usuário autenticado. Este token deve conter informações sobre o usuário, como seu ID e tipo de conta.

Exercício 2: Implementação de Autorização com JWT (10 pontos)

Agora que a autenticação está funcionando corretamente, é hora de implementar diferentes níveis de acesso para os usuários e restringir o acesso a certas partes da plataforma com base nos tokens JWT gerados. Detalhes sobre como você deve prosseguir:

- 1) Níveis de Acesso: Defina três níveis de acesso para os usuários: administrador, moderador e usuário comum. Cada tipo de conta terá permissões diferentes dentro da plataforma.

- 2) Restrição de Acesso: Com base no tipo de conta e nas permissões associadas, restrinja o acesso a certas partes da plataforma. Por exemplo, apenas administradores devem ter permissão para criar ou excluir conteúdo, enquanto usuários comuns só podem visualizar conteúdo.
- 3) Validação do Token JWT: Antes de permitir o acesso a um recurso protegido, valide o token JWT enviado pelo cliente para garantir sua autenticidade e verificar se o usuário tem permissão para acessar o recurso solicitado.

Ao concluir esses dois exercícios, você terá implementado com sucesso um sistema de autenticação e autorização seguro usando JWT. Certifique-se de testar exaustivamente o sistema para garantir sua eficácia e segurança.

COMO ENTREGAR

- **1)** Crie uma conta no GitHub, caso ainda não tenha uma.
- **2)** Crie um repositório chamado Arquitetura de Aplicações Web ou um repositório para essa entrega, se preferir. Você pode entregar ambos os projetos de uma única vez, em um mesmo repositório.
- **3)** Crie um arquivo readme.md e insira prints do funcionamento do seu sistema, de forma que seja possível visualizar o login, a geração do token JWT e o esquema de autorização (níveis de acesso) na página principal do seu repositório (readme.md).
- **4)** O link para o seu repositório deverá ser entregue no canvas: **https://newtonpaiva.instructure.com/**, na área da disciplina de Arquitetura de Aplicações Web.

- **Exemplo:**
  - **Link da sua entrega**: https://github.com/joaosilva/aaw
  - Exemplo para inserir os prints no arquivo readme.md:

  - Lembrando que as imagens dos seus prints também deverão estar no repositório (exemplo: aaw/img/print1.png).
  - Arquivos do repositório: Projeto SisAutenticaAutoriza README.md.