Política de Acesso ao Conteúdo

Propósito

Essa política de acesso deve te ajudar a entender como pessoas (referindo tanto a pessoas quanto a programas e scripts) podem acessar o conteúdo do blog, incluindo como gerenciar seu login e tokens de autenticação e validação.

Todas as regras e definições quanto às validações, são diretamente relacionadas aos usuários e posts gerenciados pela API.

Autenticação de acesso

Para acessar a aplicação, é necessário que você possua uma conta de usuário

É possível criar uma conta de usuário usando a requisição “Cadastrar usuário” na coleção do Postman

Ao cadastrar sua conta, acesse o link enviado no seu e-mail, através desse link sua conta será validade. Se você não acessar esse link, não conseguirá prosseguir com a autenticação da API

Com uma conta verificada, você também terá seu próprio cargo, que será usado nas requisições relacionadas ao acesso de conteúdo.

Com sua conta, use-a na requisição de Login no Postman. Você receberá o corpo da requisição, com um token de renovação, e no cabeçalho Authorization, seu JSON Web Token. Use esse token nas próximas requisições, enviando-o dentro do cabeçalho Authorization na requisição, como um token Bearer

Acesso ao conteúdo

Ao tentar acessar o conteúdo da aplicação, deve-se levar em conta que há requisições abertas, ou seja, que não necessitam de autenticação - justamente, não falaremos dessas requisições aqui, como a criação de um usuário, porque não possuem controle de acesso, uma vez que todas são liberadas.

Dito isso, apenas trataremos sobre requisições que necessitam de autenticação, ou seja, confirmação de quem está acessando a API pode acessar a API.

Caso esteja trabalhando com acesso de conteúdo fora da API, é necessário também um usuário representando quem está acessando os dados, para então usar o controle de acesso adequadamente, seguindo as diretivas abaixo

Além da autenticação, se é necessário controlar quais pessoas dentro da API podem acessar quais entidades (como usuários ou posts), e o que fazer sob cada entidade. Isso é relacionado com seu usuário através do seu cargo, todas as implementações do controle de acesso ao conteúdo da aplicação devem seguir estritamente os cargos definidos a seguir:

Os cargos disponíveis são:

Admin

Administrador, podem realizar todos os tipos de operações possíveis em qualquer usuário, seja a si mesmo, ou a outro usuário, como criar, atualizar, ler ou apagar. O mesmo é possível com posts, sejam escritos pelo próprio admin, ou por outras pessoas

Editor

Pessoas que podem criar, editar, atualizar e remover apenas posts criados por si, além também de poder ver todos os posts, tanto feitos por si quanto por outra pessoa. Não possuem nenhuma permissão em relação a usuários.

Leitor

Pessoas que podem apenas ler os posts feitos por qualquer pessoa. Não possuem nenhuma permissão em relação a usuários, ou outras ações com posts, como cadastrar ou apagar

Além das permissões relacionadas aos cargos, também há uma dupla confirmação ao tentar remover um post ou usuário, independente do cargo, será necessário fornecer um JSON Web Token válido, juntamente com as credenciais de acesso, para confirmar a ação, que se torna nociva e problemática se usada sem cautela

Acesso de conteúdo e Redes

Para acessar a API, é possível usar de qualquer lugar do mundo, isto é, com acesso a internet e credenciais corretas, usando qualquer IP ou rede

Distribuição de conteúdo

Todos os dados gerados e trafegados pela API, são de exclusivo acesso e direito da API, ou seja, não podem ser copiados ou divulgados de qualquer forma que não seja pela própria API em si.