Plano de Segurança de Acesso para Sistema Web

1. Lista de Usuários e Permissões

Neste sistema, os usuários são divididos em quatro grupos principais, cada um com um conjunto específico de permissões. As permissões seguem o princípio do menor privilégio, garantindo que o acesso seja restrito ao necessário.

Grupos de Usuários

* Administrador (Ex: admin\_user)
  + Função: Gerenciamento completo do sistema.
  + Permissões:
    - Criar, ler, atualizar e deletar usuários e posts.
    - Gerenciar configurações do sistema.
    - Visualizar logs de acesso.
* Editor (Ex: editor\_user)
  + Função: Gerenciamento de conteúdo.
  + Permissões:
    - Criar posts.
    - Ler todos os posts.
    - Atualizar e deletar posts de sua autoria e de outros autores.
* Autor (Ex: author\_user)
  + Função: Criação de conteúdo.
  + Permissões:
    - Criar posts.
    - Ler todos os posts.
    - Atualizar e deletar apenas os seus próprios posts.
* Leitor (Ex: reader\_user)
  + Função: Consumo de conteúdo.
  + Permissões:
    - Ler apenas posts publicados.
    - Criar, atualizar e deletar seus próprios comentários.

### 2. Lógica de Controle de Acesso

A segurança do sistema é baseada em dois pilares: **autenticação** (verificação de identidade) e **autorização** (verificação de permissão).

1. **Autenticação**:
   * Quando um usuário tenta fazer login, o sistema verifica as credenciais.
   * As senhas são armazenadas de forma segura com criptografia (hashing).
   * Após a validação, um token de acesso é gerado para a sessão do usuário.
2. **Autorização**:
   * A cada solicitação do usuário, o sistema verifica seu token de acesso.
   * O sistema consulta a permissão do usuário com base em seu papel (ex: Administrador, Autor).
   * Se a permissão for válida, a ação é executada. Caso contrário, a solicitação é bloqueada e um erro **403 Forbidden** é retornado.

### 3. Simulação de Tentativas de Acesso Inválido

A seguir, uma demonstração de como a lógica de segurança se comportaria em cenários de acesso não autorizado.

#### Cenário 1: Login Inválido

* **Tentativa**: Um usuário não registrado tenta fazer login.
* **Resultado**: O sistema rejeita o login e exibe a mensagem "Credenciais inválidas". Várias tentativas seguidas podem resultar em um bloqueio temporário (rate limiting) para evitar ataques de força bruta.

#### Cenário 2: Acesso a Funcionalidade Restrita

* **Usuário**: author\_user (um Autor).
* **Ação**: Tenta deletar um post que não foi criado por ele.
* **Resultado**: O sistema verifica que a permissão de **Autor** permite deletar apenas seus próprios posts. A requisição é bloqueada e um erro **403 Forbidden** é retornado.

### 4. Print das Permissões do Usuário

