

Manual de Funcionamento - Metodologia STRIDE

Este manual descreve o funcionamento de uma aplicação, para sistema de gerenciamento de backups desenvolvida para objetivo é fornecer orientações claras sobre como utilizar a aplicação de maneira eficiente e segura.

Uso da Aplicação

- **Insira Nome de Usuário e Senha(forte):** Nome(user), Senha(user@123).
- **Para Registrar crie:** Nome de Usuário, E-mail e Senha
- **Caso necessário, utilize a autenticação de dois fatores para maior segurança.**

Requisitos de Sistema

Para utilizar a aplicação é necessário:

- Dispositivo compatível (Computador, Notebook ou tablet).
- Editor de código-fonte (Visual studio code).
- Servidores com código aberto(banco de dados MySQL).
- Navegador web atualizado (Firefox, Chrome, Safari).

Funcionalidades Principais

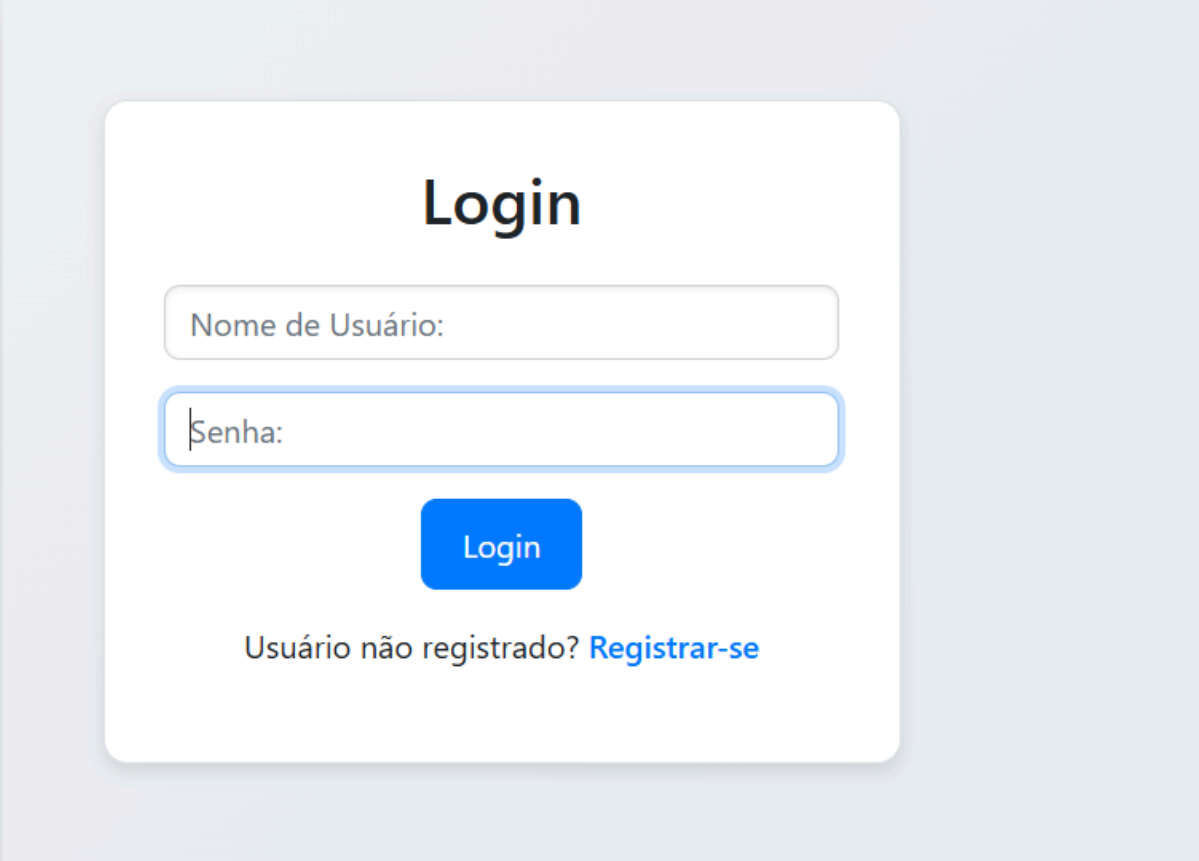
A aplicação possui as seguintes telas:

- Login
- Registrar
- Autenticação em duas etapas onde o usuário irá receber um código

- Dashboard onde será possível criar Backup ou fazer Logout

OBS: Para melhor entendimento siga as instruções abaixo.

1. Faça seu login:

A login form interface with a light gray background. In the center is a white rounded rectangle containing the title "Login" in bold black font. Below the title are two input fields: the first is labeled "Nome de Usuário:" and the second is labeled "Senha:". Below the password field is a blue button with the text "Login" in white. At the bottom of the white box, the text "Usuário não registrado?" is followed by a blue link "Registrar-se".

Login

Nome de Usuário:

Senha:

Login

Usuário não registrado? [Registrar-se](#)

2. Faça seu registro:

Registro de Usuário

Nome de Usuário:

Email:

Senha:

Confirme a Senha:

☐ Habilitar Autenticação em Duas Etapas

☐ Eu concordo com os termos da LGPD

Eu compreendo que o e-mail fornecido será utilizado exclusivamente para comunicação relacionada a esta aplicação. Ao marcar esta caixa, você confirma que leu e concorda com os termos e condições de uso e políticas de privacidade.

Registrar

Usuário já registrado? [Login Aqui](#)

3. Faça sua autenticação:

Autenticação em Duas Etapas

Um código de autenticação foi enviado para você. Por favor, insira o código abaixo:

Código de Autenticação:

Verificar Código

Mostrar Código de Autenticação

4. Crie seu Backup:

Criar Backup

Backup criado com sucesso: [backup_2024-08-18_06-40-58.csv](#)

Criar Backup

Voltar ao Dashboard

Identificação dos Pontos de Atenção Utilizando a Metodologia STRIDE

Spoofing: O código utiliza sessões para garantir que o usuário esteja autenticado antes de acessar a página (`if (!isset($_SESSION['userid']))`). Isso ajuda a proteger contra o spoofing, garantindo que a autenticação do usuário seja verificada.

Tampering (Violação): O código garante que todas as entradas do usuário sejam validadas e sanitizadas para evitar injeção de SQL e outros ataques de adulteração. O código da autenticação e da atualização (`$stmt->bind_param("i", $userid);`) faz uso dessa técnica para garantir que os dados fornecidos pelo usuário não sejam manipulados.

Repudiation (Repúdio): O código não parece ter medidas explícitas contra repudiation. Contudo, a autenticação em duas etapas e o armazenamento de mensagens de erro e sucesso em sessões podem ajudar a rastrear ações dos usuários, mas isso não é uma proteção direta contra repudiation. Para uma proteção mais robusta, seria necessário implementar logs detalhados e uma forma de validar ações realizadas pelos usuários.

Information Disclosure (Divulgação de Informação): O código tenta evitar a divulgação de informações sensíveis, mas não faz isso de forma completa. Mensagens de erro são apresentadas ao usuário (`$_SESSION['error']`), mas não incluem detalhes técnicos que poderiam revelar informações sensíveis sobre o sistema ou a falha (`$_SESSION['error'] = "Erro ao concluir autenticação em duas etapas: " . $mysqli->error;`). A mensagem de erro não é diretamente exibida ao usuário final, ajudando a proteger informações internas.

Denial of Service (Negação de Serviço): O código não inclui proteção específica contra DoS. No entanto, limitar o número de tentativas de autenticação e adicionar mecanismos de proteção como CAPTCHA em formulários de login poderia ajudar a mitigar ataques DoS.

Elevation of Privilege (Elevação de Privilégio): O código não aborda explicitamente a elevação de privilégios. A proteção contra essa ameaça geralmente envolve a verificação de permissões e autenticação apropriada antes de permitir o acesso a recursos ou funcionalidades sensíveis. Aqui, o código garante que apenas

usuários autenticados (com uma sessão válida) possam acessar a página, mas não faz verificações adicionais de privilégios específicos.

Conclusão

O sistema realiza o processo de login com segurança, incluindo medidas contra CSRF e SQL Injection, além de implementar a autenticação em duas etapas se necessário. O design da página é modernizado com CSS e Bootstrap, além disso também permite que novos usuários se cadastrem no sistema. Ele lida com a criação de novos registros de usuário e validação de dados.