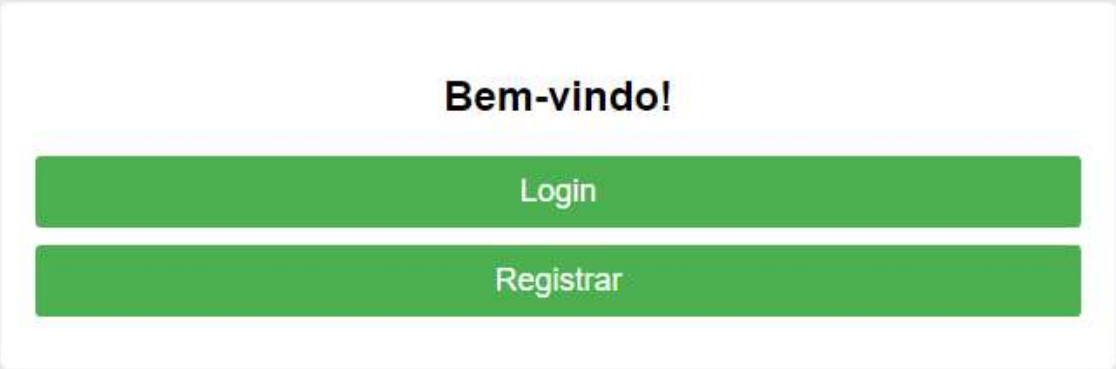


Manual de Funcionamento

Começaremos o nosso manual apresentando as telas de acesso a nosso programa.

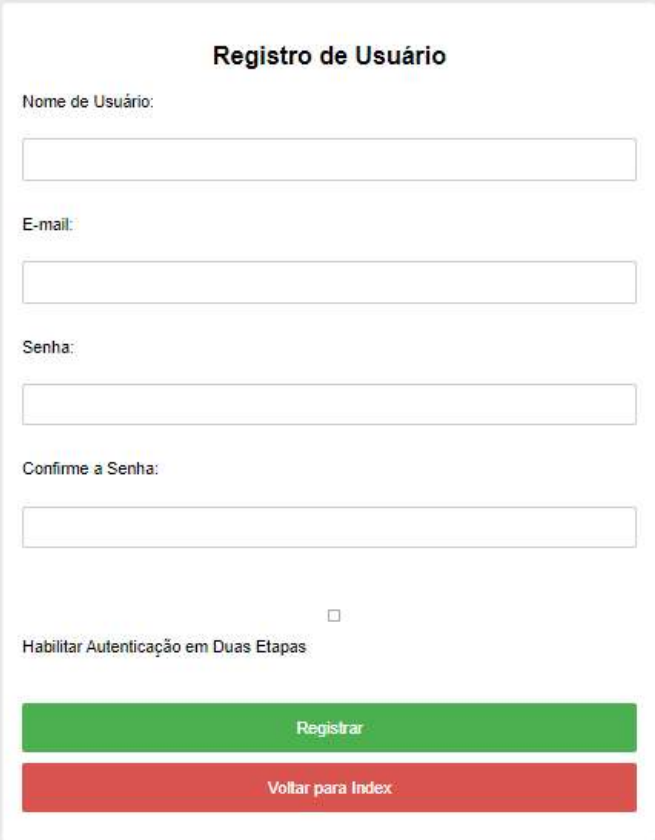
Index



A tela de boas-vindas apresenta o título "Bem-vindo!" no topo. Abaixo dele, há dois botões de ação: "Login" e "Registrar", ambos em um fundo verde com texto branco.

Essa é a tela inicial do nosso programa, a partir dela podemos ir em 2 direções, mas partiremos do ponto que é seu primeiro acesso.

Registrar

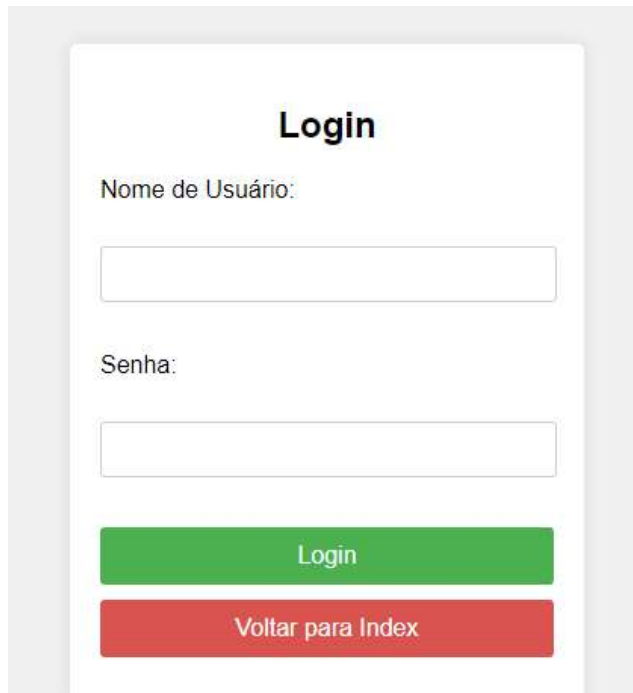


O formulário de registro, intitulado "Registro de Usuário", contém os seguintes campos e elementos:

- Nome de Usuário: Campo de texto.
- E-mail: Campo de texto.
- Senha: Campo de texto.
- Confirme a Senha: Campo de texto.
- Uma caixa de seleção desativada para "Habilitar Autenticação em Duas Etapas".
- Botão "Registrar" em verde.
- Botão "Voltar para Index" em vermelho.

Esta é a página na qual faremos o registro do usuário, no qual pegaremos alguns dados pessoais para utilizar o nosso programa. Você criará seu user e, após isso, precisará informar seu Email, criar uma senha forte, sendo obrigado a usar letras maiúsculas e minúsculas, caracteres especiais e números. Ao final, você irá escolher se seu usuário usará autenticação de duas etapas ou não. Lembrando que assim que for registrado ele logará automaticamente, indo para a verificação de duas etapas ou não a partir de sua decisão.

Login

A login form interface with a white background and a light gray border. At the top, the word "Login" is centered in bold black text. Below it, the label "Nome de Usuário:" is followed by a white text input field with a thin gray border. Underneath, the label "Senha:" is followed by another white text input field with a thin gray border. At the bottom, there are two buttons: a green button with the text "Login" in white, and a red button with the text "Voltar para Index" in white.

Caso você já tenha registro, você virá para esta tela, onde irá informar o seu usuário e sua senha.

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

Logo após fazer o login, caso você tenha escolhido a opção de duas etapas, você será redirecionado para a tela de autenticação, onde você terá que colocar o código que será enviado ao seu Email. Caso você erre o código essa tela será exibida.

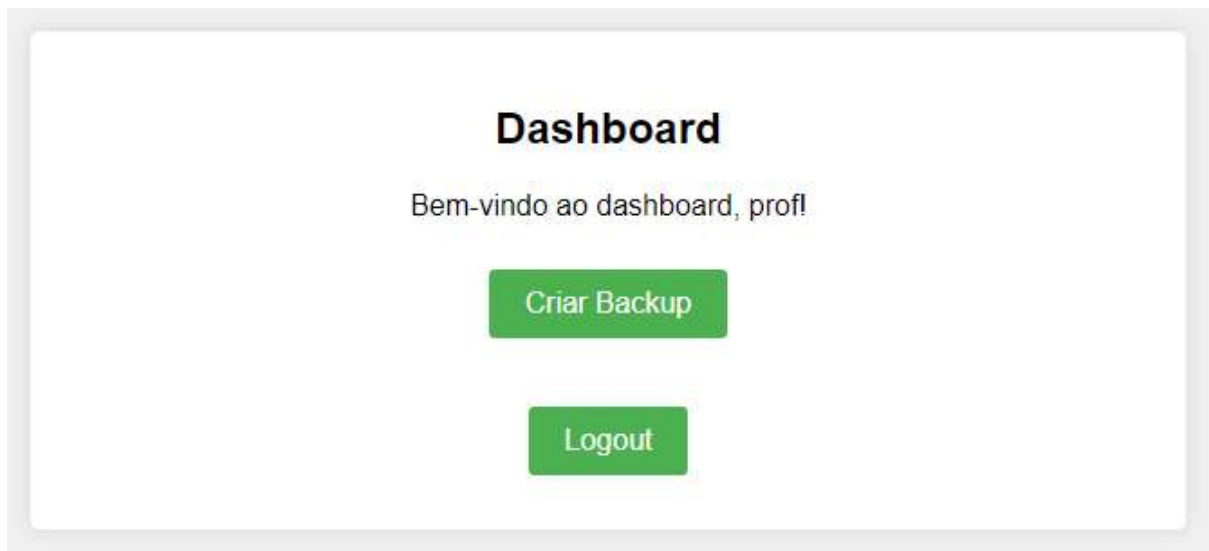
Verificar Código de Autenticação

Código de autenticação incorreto!

Abortar

Tentar Novamente

Dashboard



Essa é a tela principal do programa, onde você pode se deslogar ou criar um backup do banco de dados do servidor.

Criar Backup



Essa é a tela onde você criará o backup, contendo as informações de todos os usuários do programa, depois voltará ao Dashboard.

Metodologia STRIDE

A metodologia STRIDE é uma abordagem usada para identificar e mitigar potenciais ameaças à segurança em sistemas de software. Cada letra em "STRIDE" representa uma categoria de ameaça específica, a partir dela pontuamos alguns problemas na aplicação:

1.Spoofing (Falsificação)

Refere-se à capacidade de um invasor se passar por outro usuário ou sistema. Isso pode incluir falsificação de identidade, autenticação ou dados.

A autenticação de duas etapas previne que possíveis invasores se passem por outros usuários no sistema.

2. Tampering (Alteração) Envolve a modificação não autorizada de dados ou informações transmitidas. Isso pode comprometer a integridade dos dados, levando a decisões errôneas ou ações não autorizadas.

//Não é possível alterar nenhum dado a partir da aplicação.

3. Repudiation (Repúdio): Refere-se à capacidade de um usuário negar que realizou uma ação específica. Isso pode ser um problema em sistemas que precisam de registros de auditoria para rastrear atividades.

//O usuário não pode negar o acesso pelo registro de login. Mas pode negar o backup pois ele não informa o usuário que fez o backup.

4. Information Disclosure (Divulgação de Informações): Envolve a exposição não autorizada de informações sensíveis. Isso pode ocorrer através de vazamentos de dados, acesso indevido a informações confidenciais, entre outros.

// O invasor pode fazer o download do banco de dados.

5. Denial of Service (Negação de Serviço): Refere-se a ataques que visam tornar um sistema indisponível para seus usuários legítimos. Isso pode ser feito sobrecarregando recursos, explorando vulnerabilidades de softwares, entre outras técnicas.

// Se o usuário não fizer logout ele pode navegar entre as páginas livremente.

6. Elevation of Privilege (Elevação de Privilégio): Envolve ganhar acesso não autorizado a recursos ou funcionalidades que normalmente não seriam permitidos ao invasor. Isso pode permitir que o invasor execute ações maliciosas com privilégios elevados.

// Qualquer usuário registrado poderá ter acesso a todas as informações dos usuários do banco de dados.

Conclusão

O desenvolvimento de aplicações seguras é essencial para proteger dados sensíveis, garantir a privacidade dos usuários e manter a integridade dos sistemas. Segurança robusta previne danos financeiros e reputacionais, fortalece a confiança dos usuários, reduz custos a longo prazo e promove inovação ética. É uma obrigação moral e prática para todas as partes envolvidas no desenvolvimento e uso de tecnologias digitais.