

Parte 1

Casos de Teste Manuais

Caso de Teste 1: Validação de Email Inválido

- **Cenário:** O usuário insere um e-mail inválido no campo "Email".
- **Passos para Execução:**
 1. Acesse o formulário de login na aplicação web.
 2. Digite um valor inválido no campo "Email" (ex.: usuario@dominio, usuario@.com).
 3. Insira uma senha válida com no mínimo 8 caracteres no campo "Senha".
 4. Observe o comportamento do botão "Entrar".
- **Resultado Esperado:**
 - A mensagem "Formato de e-mail inválido." é exibida abaixo do campo "Email".
 - O botão "Entrar" permanece desabilitado.

Caso de Teste 2: Validação de Senha Inválida

- **Cenário:** O usuário insere uma senha com menos de 8 caracteres.
- **Passos para Execução:**
 1. Acesse o formulário de login na aplicação web.
 2. Digite um endereço de e-mail válido no campo "Email" (ex.: usuario@dominio.com).
 3. Insira uma senha com menos de 8 caracteres (ex.: 12345) no campo "Senha".
 4. Observe o comportamento do botão "Entrar".
- **Resultado Esperado:**
 - A mensagem "A senha deve ter pelo menos 8 caracteres." é exibida abaixo do campo "Senha".
 - O botão "Entrar" permanece desabilitado.

Caso de Teste 3: Validação de Login Bem-Sucedido

- **Cenário:** O usuário insere e-mail e senha válidos e tenta fazer login.
- **Passos para Execução:**
 1. Acesse o formulário de login na aplicação web.
 2. Digite um endereço de e-mail válido no campo "Email" (ex.: usuario@dominio.com).
 3. Digite uma senha válida com no mínimo 8 caracteres (ex.: senha1234) no campo "Senha".
 4. Clique no botão "Entrar".
- **Resultado Esperado:**
 - O login é efetuado com sucesso.
 - O usuário é redirecionado para a página inicial ou painel.

Cenários Exploratórios

1. **Teste de Segurança com Scripts Maliciosos:**
 - Insira um script malicioso (ex.: <script>alert('teste')</script>) no campo "Email" e/ou "Senha".
 - **Objetivo:** Verificar se o sistema está vulnerável a ataques de injeção de código.
2. **Teste de Limites de Caracteres:**
 - Insira uma quantidade extrema de caracteres nos campos "Email" e "Senha" (ex.: 255 caracteres).
 - **Objetivo:** Verificar se o sistema lida corretamente com entradas fora do padrão esperado.

Parte 2

Link do repositório do github:

https://github.com/ErictonFelicidade86/Teste_QA

Parte 3

Relatório de Defeitos

Data: 14/01/2025

Relatório por: Ericton Brito

Sistema Testado: Formulário de Login

Ambiente: Navegador Chrome | Versão [131.0.6778.265]

Problema 1: O formulário aceita senhas com menos de 8 caracteres

- **Descrição:**
O formulário permite que o usuário envie senhas com menos de 8 caracteres sem exibir a mensagem de erro "A senha deve ter pelo menos 8 caracteres."
- **Passos para Reproduzir:**
 1. Acesse o formulário de login na aplicação.
 2. Insira um e-mail válido no campo "Email" (ex.: usuario@dominio.com).
 3. Insira uma senha com menos de 8 caracteres no campo "Senha" (ex.: 12345).
 4. Clique no botão "Entrar".
- **Resultado Esperado:**
O sistema deve exibir a mensagem "A senha deve ter pelo menos 8 caracteres." e não permitir o envio do formulário.
- **Resultado Observado:**
O formulário é enviado sem exibir a mensagem de erro.
- **Impacto:**
Usuários podem criar senhas fracas, comprometendo a segurança do sistema.

Problema 2: O botão Entrar não está desabilitado quando o campo Email está vazio

- **Descrição:**
O botão "Entrar" permanece habilitado, mesmo quando o campo "Email" está vazio, permitindo o envio do formulário.
- **Passos para Reproduzir:**
 1. Acesse o formulário de login na aplicação.

2. Deixe o campo "Email" vazio.
3. Insira uma senha válida com no mínimo 8 caracteres no campo "Senha" (ex.: senha1234).
4. Observe o estado do botão "Entrar".

- **Resultado Esperado:**

O botão "Entrar" deve estar desabilitado até que todos os campos estejam preenchidos corretamente.

- **Resultado Observado:**

O botão "Entrar" está habilitado, mesmo com o campo "Email" vazio.

- **Impacto:**

Usuários podem tentar enviar o formulário sem preencher todos os campos, resultando em falhas no fluxo de login e potenciais erros de back-end.

Recomendações:

- Atualizar a validação do campo "Senha" para verificar o comprimento mínimo de 8 caracteres antes de permitir o envio.
- Implementar validação para desabilitar o botão "Entrar" até que todos os campos estejam preenchidos corretamente.

Prioridade: Alta

Severidade: Crítica