TEST SOFTWARE

Relatório de Pontos de Melhoria

1. Identificação do Caso de Teste:

- **ID do Caso de Teste**: CT001.009
- **Título do Caso de Teste**: Cadastro senha somente com números
- **Descrição do Caso de Teste**: Este caso de teste verifica se o sistema exibe mensagens de erro apropriadas quando o usuário tenta se cadastrar sem preencher campos obrigatórios.
- **Responsável pela Revisão**: Thierry Castro

2. Contexto e Objetivo:

- **Contexto**: O teste foi executado no módulo de cadastro de usuários da aplicação Kawasaki, na versão 1.0.0, em um ambiente de teste:
  Equipamento: HP Laptop - UQ05LO9A
  Plataforma: Web para Desktop
  Sistema Operacional: Windows 10 Home 22H2
  Navegador: Google Chrome - Versão 125.0.6422.176 (x64 bits)
- **Objetivo do Relatório**: Identificar e propor melhorias no caso de teste que valida a exibição de mensagens de erro para campos obrigatórios não preenchidos corretamente durante o cadastro.

3. Problemas Identificados no Caso de Teste:

- **Problema 1: Falta de Validação de Campos Obrigatórios**
  - Ao tentar cadastrar um usuário com a senha apenas com números, o sistema não exibe nenhuma mensagem de erro.
  - O problema resulta em falta de feedback ao usuário, o que pode causar confusão e frustração.

4. Análise de Impacto:

- **Segurança:** Aumenta a segurança geral do sistema, evitando que senhas fracas sejam usadas, o que poderia comprometer a proteção dos dados dos usuários.
- **Qualidade da Experiência do Usuário:** Melhora a experiência do usuário, fornecendo feedback apropriado quando entradas inválidas são fornecidas. Isso evita frustrações ao tentar se cadastrar com dados incorretos.
- **Conformidade com Normas de Segurança:** A implementação de senhas mais fortes ajuda a garantir conformidade com políticas de segurança da informação, como LGPD, GDPR ou outras regulamentações que exigem a proteção dos dados pessoais.

TEST SOFTWARE

Relatório de Pontos de Melhoria

- **Redução de Erros:** A validação adequada em campos como nome e e-mail reduz o número de erros no cadastro, minimizando a necessidade de correções manuais ou suporte técnico.
- **Responsável:** Equipe de Desenvolvimento e QA.

5. Recomendações de Melhoria:

1. **Implementação de Validações:**

- **Implementar validações de entrada** mais rigorosas que não permitam o uso de **apenas números** nos campos onde essa prática é inapropriada, como no campo de senha, nome de usuário e e-mail. Exibir mensagens de erro claras e específicas.
- No caso de senhas, exigir uma combinação de letras, números e, opcionalmente, caracteres especiais para garantir que a senha atenda aos critérios mínimos de **segurança**.
- Exibir mensagens de erro claras e específicas, como:
  "A senha deve conter ao menos 8 caracteres, incluindo letras e números."
  "O nome não pode conter apenas números."
  "Por favor, insira um e-mail válido."
- **Responsável**: Equipe de Desenvolvimento.

2. **Atualização do Caso de Teste:**

- Atualizar o caso de teste para incluir verificações detalhadas de mensagens de erro para cada campo obrigatório
- **Responsável**: Equipe de QA.

6. Métricas de Sucesso:

- Melhor feedback de usabilidade indicando clareza nas mensagens de erro.

7. Conclusão:

- Descrever a melhoria no caso de teste, especificamente a implementação de **validações adequadas para entradas de dados**, e seu impacto (positivo e negativo) é essencial para garantir um sistema mais seguro, eficiente e amigável para os usuários.

TEST SOFTWARE

Relatório de Pontos de Melhoria

1. Identificação do Caso de Teste:

- **ID do Caso de Teste**: CT001.010
- **Título do Caso de Teste**: Cadastro senha somente com Emoji
- **Descrição do Caso de Teste**: Este caso de teste verifica se o sistema exibe mensagens de erro apropriadas quando o usuário tenta se cadastrar sem preencher campos obrigatórios.
- **Responsável pela Revisão**: Thierry Castro

2. Contexto e Objetivo:

- **Contexto**: O teste foi executado no módulo de cadastro de usuários da aplicação Kawasaki, na versão 1.0.0, em um ambiente de teste:
  Equipamento: HP Laptop - UQ05LO9A
  Plataforma: Web para Desktop
  Sistema Operacional: Windows 10 Home 22H2
  Navegador: Google Chrome - Versão 125.0.6422.176 (x64 bits)
- **Objetivo do Relatório**: Identificar e propor melhorias no caso de teste que valida a exibição de mensagens de erro para campos obrigatórios não preenchidos corretamente durante o cadastro.

3. Problemas Identificados no Caso de Teste:

- **Problema 1: Falta de Validação de Campos Obrigatórios**
  - Ao tentar cadastrar um usuário com a senha apenas com emoji, o sistema não exibe nenhuma mensagem de erro.
  - O problema resulta em falta de feedback ao usuário, o que pode causar confusão e frustração.

4. Análise de Impacto:

- **Segurança**: Permitir o cadastro de uma senha composta apenas por **emojis** pode comprometer a segurança do sistema, já que emojis são caracteres não convencionais que podem não atender a critérios mínimos de complexidade, como exigência de letras e números. Emojis podem dificultar a utilização de hashing adequado e aumentar o risco de incompatibilidade entre sistemas.
- **Usabilidade**: Senhas contendo apenas emojis podem ser difíceis de digitar em alguns dispositivos e podem não ser reconhecidas por todos os sistemas de autenticação. Isso pode causar frustração ao usuário, especialmente em dispositivos onde o teclado de emojis não está disponível ou é difícil de acessar.

- **Responsável:** Equipe de Desenvolvimento e QA.

5. Recomendações de Melhoria:

Implementar Regras de Complexidade de Senha

- Validação mais rígida: Atualizar a lógica de validação para impedir que o campo de senha aceite apenas emojis. A senha deve ser composta por uma combinação de letras (maiúsculas e minúsculas), números e caracteres especiais. Emojis podem ser permitidos, mas não devem ser os únicos caracteres na senha.
- Mensagem de erro clara: Exibir uma mensagem de erro clara e específica ao usuário quando uma senha inválida for submetida. Exemplo: "A senha deve conter ao menos 8 caracteres, incluindo letras, números e símbolos. Emojis podem ser usados, mas não como única forma de senha."

Compatibilidade e Segurança de Hashing

- Garantir compatibilidade: Realizar testes de compatibilidade entre sistemas que utilizam diferentes métodos de codificação de caracteres. Alguns sistemas podem não interpretar emojis da mesma forma, o que pode gerar problemas ao processar as senhas.
- Hashing de senha seguro: Verificar se o mecanismo de hashing da senha suporta adequadamente caracteres como emojis e assegurar que isso não comprometa a segurança do armazenamento das credenciais.

6. Métricas de Sucesso:

- **Redução de Senhas Fracas**: A proporção de senhas aceitas pelo sistema que contenham apenas emojis deve ser **reduzida para 0%**, garantindo que todas as senhas atendam aos critérios de complexidade.
- **Melhora na Usabilidade**: Monitorar as taxas de sucesso no login e na criação de conta para avaliar a **usabilidade** das senhas e garantir que os usuários estejam criando senhas seguras e fáceis de lembrar, sem sacrificar a segurança.

7. Conclusão:

Permitir senhas compostas apenas por emojis apresenta riscos de segurança, compatibilidade e usabilidade. Implementar validações mais rigorosas e garantir que as senhas atendam a critérios de complexidade mínima é essencial para manter a integridade do sistema e a segurança dos usuários. Ao seguir as recomendações propostas, o sistema se tornará mais seguro e estará em conformidade com padrões de segurança, evitando vulnerabilidades e melhorando a experiência do usuário.

TEST SOFTWARE

Relatório de Pontos de Melhoria

1. Identificação do Caso de Teste:

- **ID do Caso de Teste**: CT001.011
- **Título do Caso de Teste**: Cadastro senha somente com Caracteres Especiais
- **Descrição do Caso de Teste**: Este caso de teste verifica se o sistema exibe mensagens de erro apropriadas quando o usuário tenta se cadastrar sem preencher campos obrigatórios.
- **Responsável pela Revisão**: Thierry Castro

2. Contexto e Objetivo:

- **Contexto**: O teste foi executado no módulo de cadastro de usuários da aplicação Kawasaki, na versão 1.0.0, em um ambiente de teste:
  Equipamento: HP Laptop - UQ05LO9A
  Plataforma: Web para Desktop
  Sistema Operacional: Windows 10 Home 22H2
  Navegador: Google Chrome - Versão 125.0.6422.176 (x64 bits)
- **Objetivo do Relatório**: Identificar e propor melhorias no caso de teste que valida a exibição de mensagens de erro para campos obrigatórios não preenchidos corretamente durante o cadastro.

3. Problemas Identificados no Caso de Teste:

- **Problema 1: Falta de Validação de Campos Obrigatórios**
  - Ao tentar cadastrar um usuário com a senha apenas com Caracteres Especiais, o sistema não exibe nenhuma mensagem de erro.
  - O problema resulta em falta de feedback ao usuário, o que pode causar confusão e frustração.

4. Análise de Impacto:

- **Segurança**: Permitir o cadastro de uma senha composta apenas por **Caracteres Especiais** pode comprometer a segurança do sistema, já que Caracteres Especiais são caracteres não convencionais que podem não atender a critérios mínimos de complexidade, como exigência de letras e números. Caracteres Especiais podem dificultar a utilização de hashing adequado e aumentar o risco de incompatibilidade entre sistemas.

- **Usabilidade**: Senhas contendo apenas Caracteres Especiais podem ser difíceis de digitar em alguns dispositivos e podem não ser reconhecidas por todos os sistemas de autenticação. Isso pode causar frustração ao usuário, especialmente em dispositivos onde o teclado de Caracteres Especiais não está disponível ou é difícil de acessar.

- **Responsável:** Equipe de Desenvolvimento e QA.

5. Recomendações de Melhoria:

Implementar Regras de Complexidade de Senha

- Validação mais rígida: Atualizar a lógica de validação para impedir que o campo de senha aceite apenas Caracteres Especiais. A senha deve ser composta por uma combinação de letras (maiúsculas e minúsculas), números e caracteres especiais. Caracteres Especiais podem ser permitidos, mas não devem ser os únicos caracteres na senha.

- Mensagem de erro clara: Exibir uma mensagem de erro clara e específica ao usuário quando uma senha inválida for submetida. Exemplo: "A senha deve conter ao menos 8 caracteres, incluindo letras, números e símbolos. Caracteres Especiais podem ser usados, mas não como única forma de senha."

Compatibilidade e Segurança de Hashing

- Garantir compatibilidade: Realizar testes de compatibilidade entre sistemas que utilizam diferentes métodos de codificação de caracteres. Alguns sistemas podem não interpretar Caracteres Especiais da mesma forma, o que pode gerar problemas ao processar as senhas.

- Hashing de senha seguro: Verificar se o mecanismo de hashing da senha suporta adequadamente caracteres e assegurar que isso não comprometa a segurança do armazenamento das credenciais.

6. Métricas de Sucesso:

- **Redução de Senhas Fracas**: A proporção de senhas aceitas pelo sistema que contenham apenas Caracteres Especiais deve ser **reduzida para 0%**, garantindo que todas as senhas atendam aos critérios de complexidade.

- **Melhora na Usabilidade**: Monitorar as taxas de sucesso no login e na criação de conta para avaliar a **usabilidade** das senhas e garantir que os usuários estejam criando senhas seguras e fáceis de lembrar, sem sacrificar a segurança.

TEST SOFTWARE

Relatório de Pontos de Melhoria

7. Conclusão:

Permitir senhas compostas apenas por Caracteres Especiais apresenta riscos de segurança, compatibilidade e usabilidade. Implementar validações mais rigorosas e garantir que as senhas atendam a critérios de complexidade mínima é essencial para manter a integridade do sistema e a segurança dos usuários. Ao seguir as recomendações propostas, o sistema se tornará mais seguro e estará em conformidade com padrões de segurança, evitando vulnerabilidades e melhorando a experiência do usuário.

TEST SOFTWARE

Relatório de Pontos de Melhoria

1. Identificação do Caso de Teste:

- **ID do Caso de Teste**: CT001.012
- **Título do Caso de Teste**: Cadastro senha com espaço
- **Descrição do Caso de Teste**: Este caso de teste verifica se o sistema exibe mensagens de erro apropriadas quando o usuário tenta se cadastrar sem preencher campos obrigatórios.
- **Responsável pela Revisão**:
- Thierry Castro

2. Contexto e Objetivo:

- **Contexto**: O teste foi executado no módulo de cadastro de usuários da aplicação Kawasaki, na versão 1.0.0, em um ambiente de teste:
  Equipamento: HP Laptop - UQ05LO9A
  Plataforma: Web para Desktop
  Sistema Operacional: Windows 10 Home 22H2
  Navegador: Google Chrome - Versão 125.0.6422.176 (x64 bits)
- **Objetivo do Relatório**: Identificar e propor melhorias no caso de teste que valida a exibição de mensagens de erro para campos obrigatórios não preenchidos corretamente durante o cadastro.

3. Problemas Identificados no Caso de Teste:

- **Problema 1: Falta de Validação Adequada para Espaços em Branco**
  O sistema permite o cadastro de senhas que consistem apenas de espaços ou que possuem espaços excessivos no início ou no final da senha, o que pode comprometer a segurança e gerar inconsistências no processo de autenticação.
- **Problema 2: Falta de Feedback Adequado ao Usuário**
  Quando o usuário cadastra uma senha com muitos espaços ou apenas com espaços, o sistema não fornece uma mensagem de erro clara ou, em alguns casos, aceita a senha, o que pode confundir o usuário durante o login.
- **Problema 3: Tratamento Inadequado de Espaços Durante o Login**
  O sistema pode tratar os espaços de maneira inconsistente entre o momento de cadastro e de autenticação, levando a problemas de login, como a impossibilidade de acessar a conta.

TEST SOFTWARE

Relatório de Pontos de Melhoria

4. Análise de Impacto:

Segurança:

- **Fragilidade das Senhas**: Senhas contendo apenas espaços ou com muitos espaços tornam o sistema vulnerável, já que essas senhas são fáceis de explorar e quebrar. Isso compromete a segurança do sistema e pode resultar em tentativas de login maliciosas bem-sucedidas.

Autenticação Inconsistente:

- **Erros no Processo de Login**: O tratamento inconsistente de senhas com espaçamentos pode causar falhas no login, resultando em frustração do usuário e possíveis chamadas ao suporte técnico, aumentando os custos operacionais.

Experiência do Usuário:

- **Confusão e Frustração**: Se o sistema aceita senhas inválidas sem fornecer feedback apropriado, os usuários podem enfrentar problemas ao tentar fazer login, o que impacta negativamente a usabilidade e a confiança no sistema.

- **Responsável:** Equipe de Desenvolvimento e QA.

5. Recomendações de Melhoria:

1. Implementar Validações de Espaçamento

- **Proibir Senhas Compostas Apenas por Espaços**: Atualizar a lógica de validação para impedir que o sistema aceite senhas que consistam apenas de espaços em branco.
- **Limitar Espaços no Início ou no Fim**: Adicionar regras para garantir que senhas não comecem ou terminem com espaços em branco desnecessários.

2. Melhorar o Feedback ao Usuário

- **Mensagens de Erro Claras**: Fornecer mensagens de erro descritivas quando o usuário tentar cadastrar uma senha com espaçamento inadequado, como: "A senha não pode conter apenas espaços em branco" ou "Espaços no início ou no final da senha não são permitidos."

3. Testar e Garantir Consistência no Processo de Autenticação

- **Padronização do Tratamento de Senhas**: Garantir que o tratamento de senhas no cadastro e login seja consistente, tanto no armazenamento (hashing) quanto na autenticação.

TEST SOFTWARE

Relatório de Pontos de Melhoria

6. Métricas de Sucesso:

- **Redução de Senhas Inválidas**: A taxa de tentativas de criação de senhas inválidas com espaçamento inadequado deve ser reduzida a **0%**, após a implementação das melhorias.
- **Aumento na Confiabilidade do Login**: A taxa de erros de login causados por inconsistências no tratamento de senhas com espaços deve ser reduzida drasticamente, melhorando a confiabilidade da autenticação.
- **Satisfação do Usuário**: Aumentar a satisfação do usuário, reduzindo as ocorrências de falhas de login e proporcionando uma experiência de cadastro mais clara e eficiente.

7. Conclusão:

O cadastro de senhas contendo espaçamentos, quando mal implementado, pode gerar problemas significativos de segurança, autenticação e experiência do usuário. É essencial garantir que senhas com espaços sejam tratadas de forma consistente e segura, prevenindo que senhas inválidas ou fracas sejam aceitas.