Funcionalidade escolhida: Login

S (Spoofing - Falsificação de Identidade)

- **Existe algum risco? Se sim, qual?**
    - Existe. Por exemplo, caso seja vazada uma lista de emails, um atacante pode tentar testar logar com todos os emails e uma senha genérica. Caso ele acerte a senha de algum usuário, ele pode se passar por ele.
- **Que tipo de atacante se beneficiaria?**
    - Criminosos comuns ou oportunistas: Buscam acesso a qualquer conta para cometer fraudes.
    - Atacantes direcionados: Pessoas com uma motivação pessoal contra um usuário específico.
    - Fraudadores: Atacantes que buscam acesso a contas com informações financeiras ou cartões de crédito.

T (Tampering - Adulteração)

- **Existe algum risco? Se sim, qual?**
    - Existe. Com base no caso anterior, um atacante que faz login na conta de outro usuário, pode alterar a senha dele, realizando uma alteração indevida nos dados.
- **Que tipo de atacante se beneficiaria?**
    - Atacantes direcionados: Pessoas com uma motivação pessoal contra um usuário específico.
    - Chantagistas (Ransomware): Atacantes que "sequestram" a conta e exigem um pagamento (resgate) para devolver o acesso ao usuário legítimo.
    - Atacantes que buscam persistência: Ao alterar a senha e o e-mail de recuperação, o atacante garante que apenas ele terá acesso à conta por um longo período para extrair informações ou usá-la para outros fins ilícitos.

R (Repudiation - Repúdio/Negação)

- **Existe algum risco? Se sim, qual?**
    - Existe. O atacante pode realizar ações indevidas através de um login de outro usuário, e o sistema pode não ter logs suficientes para provar que não foi o usuário legítimo.
- **Que tipo de atacante se beneficiaria?**

- Golpistas: Utilizam a conta da vítima para realizar ações ilegítimas, fazendo com que a culpa recaia sobre o proprietário da conta.
- Difamadores: Usam a identidade de outra pessoa para postar conteúdo controverso, ilegal ou difamatório, protegendo sua própria identidade e prejudicando a reputação da vítima.
- Criminosos: Realizam atividades ilegais (como assédio, ameaças ou compartilhamento de material ilícito) a partir da conta comprometida para dificultar o rastreamento por parte das autoridades.

I (Information Disclosure - Divulgação de Informação)

- **Existe algum risco? Se sim, qual?**
  - Existe. O atacante pode vazar os dados do usuário no qual ele logou, ou se conseguir logar como administrador, vazar informações sigilosas.
- **Que tipo de atacante se beneficiaria?**
  - Ladrões de identidade: Buscam dados pessoais (nome completo, CPF, endereço, etc.) para abrir contas, solicitar crédito ou realizar outras atividades fraudulentas em nome da vítima.
  - Concorrentes: Se o acesso for a uma conta de administrador ou de um funcionário, o objetivo pode ser roubar segredos comerciais.
  - Hacktivistas: Podem vazar informações em massa para expor práticas de uma empresa, causar dano à sua reputação ou como forma de protesto.

D (Denial of Service - Negação de Serviço)

- **Existe algum risco? Se sim, qual?**
  - Existe. Caso vaze uma lista de emails e o sistema bloqueie o login por determinado tempo caso o usuário erre n vezes a senha, um atacante pode propositalmente bloquear todos os logins.
- **Que tipo de atacante se beneficiaria?**
  - Concorrentes: Podem lançar este ataque para frustrar os usuários da plataforma rival, prejudicando a experiência do cliente e a reputação da empresa alvo.
  - Hacktivistas: Utilizam o ataque como uma forma de protesto visível e disruptivo contra uma organização ou plataforma.
  - Vândalos digitais: Atacantes cuja única motivação é causar o caos, testar os limites do sistema ou simplesmente provar que são capazes de fazê-lo, sem um objetivo financeiro ou ideológico claro.

E (Elevation of Privilege - Elevação de Privilégio)

- **Existe algum risco? Se sim, qual?**

    - Existe. Se o atacante conseguir logar como administrador, ele pode dar permissões indevidas para outros usuários.
- **Que tipo de atacante se beneficiaria?**
    - Atacantes persistentes: Grupos sofisticados que buscam controle total e de longo prazo sobre o sistema. Eles podem elevar privilégios para criar backdoors, desativar logs e se mover lateralmente pela rede da organização.
    - Criminosos com fins lucrativos: Buscam acesso de administrador para manipular o sistema em seu favor, como desviar pagamentos, criar contas falsas com privilégios ou roubar e vender a base de dados completa.
    - Insiders: Um funcionário que já possui acesso limitado pode tentar explorar uma vulnerabilidade para escalar seus próprios privilégios, obtendo acesso a informações ou funcionalidades que estão fora de sua alçada.