|  |  |  |  |
| --- | --- | --- | --- |
| AMEAÇAS | PROBABILIDADE | IMPACTO | ESTRATEGIAS |
| Um atacante tenta todas as combinações possíveis de senhas até encontrar a correta. | Alta, especialmente se o sistema permitir múltiplas tentativas de login sem mecanismos eficazes de proteção. | : Pode comprometer a conta de um usuário e levar à obtenção de acesso não autorizado, causando danos financeiros, vazamento de dados e perda de confiança. |  imitar o número de tentativas de login com bloqueio temporário após várias tentativas incorretas (como você já implementou com o contador de tentativas).   Utilizar autenticação multifatorial (2FA) como a que você mencionou. |
| Senhas são armazenadas em texto simples (como no seu código) sem qualquer tipo de hash ou criptografia. | Alta, especialmente se os atacantes tiverem acesso ao armazenamento local do navegador (localStorage). | Vazamento de senhas de usuários, comprometedores de suas contas. |  **ashing**: Nunca armazene senhas em texto claro. Utilize funções de hash seguras como bcrypt ou Argon2 para armazenar apenas o hash da senha.   **Armazenamento Seguro**: Nunca armazene dados sensíveis no localStorage. Considere usar cookies seguros e protegidos por HttpOnly e Secure, ou um backend seguro para o armazenamento de senhas. |