josif 2024
16ª JORNADA CIENTÍFICA E TECNOLÓGICA
13º SIMPÓSIO DE PÓS-GRADUAÇÃO
DO IFSULDEMINAS
ISSN: 2319-0124
REALIZAÇÃO INSTITUTO FEDERAL Sul de Minas Gerais
APOIO CNPq FAPEMIG

SOFTWARE VERIFICADOR E GERADOR DE SENHAS: Software web para verificar senhas do usuário e gerar senhas.

Vinicius H. LIMA[1] Paulo C. SANTOS[2]

RESUMO

Este projeto aborda o desenvolvimento de um software para verificar e gerar senhas, o objetivo é demonstrar ao usuário a força de segurança da senha. Os problemas mais comuns referente a segurança da informação são a segurança das contas online, esses problemas ocorrem no momento da criação de senhas para as contas. Dessa forma, foi desenvolvido um software que possibilita a conscientização da comunidade para manter as senhas das suas contas mais seguras usando métodos de proteção apresentadas no web site e mostrar de forma instantânea a força da senha. Para este fim, foi utilizado um computador pessoal com o processador AMD Ryzen 5 2600, 16gb de memória RAM, um HD de 500gb, teclado e mouse, e também foi utilizado o computador do Instituto Federal do Sul de Minas - Campus Muzambinho com o processador Intel Core i5-13500 2.50 GHz, 8gb de memória RAM, um HD de 250gb e teclado e mouse.

Palavras-chave: Segurança da Informação; Verificação de Senhas; Geração de Senhas Fortes; Desenvolvimento de Software; Proteção de Contas Online.

1. INTRODUÇÃO

A segurança da informação, em nosso mundo cada vez mais digital, é um pilar fundamental para proteger dados sensíveis e garantir a integridade das comunicações online. Conforme o estudo de Tan et al. (2020), a criação de políticas de senha que equilibram segurança e usabilidade é essencial, pois, embora políticas tradicionais como requisitos de classe de caracteres sejam amplamente adotadas, elas podem ter limitações contra atacantes experientes. Diante de ameaças cibernéticas cada vez mais sofisticadas, a implementação de medidas de segurança robustas se torna imprescindível. Entre essas medidas, a proteção de credenciais de acesso, como as senhas, emerge como uma das linhas de defesa mais importantes e exige um gerenciamento cuidadoso.

A segurança de senhas é um desafio crescente no cenário digital atual, especialmente com o aumento exponencial dos ataques cibernéticos. Senhas fracas expõem tanto usuários quanto organizações a riscos, como roubo de identidade, vazamento de dados confidenciais e acesso não autorizado a sistemas. De acordo com Alroomi e Li (2023), uma análise abrangente das políticas de criação de senhas em websites revelou que muitas políticas ainda são inadequadas, com uma grande proporção de sites não aplicando critérios de complexidade robustos e permitindo a reutilização de senhas simples.

[1]Bolsista PIBIC/CNPq, IFSULDEMINAS – *Campus* Muzambinho. E-mail: endereco.eletronico@gmail.com.
[2]Discente do Técnico em Agropecuária Integrado, IFSULDEMINAS – *Campus* Muzambinho. E-mail: endereco.eletronico2@ifsuldeminas.edu.br.

Para enfrentar esses desafios, utilizamos o zxcvbn, um estimador de força de senha desenvolvido por Amador e colaboradores (2023), para avaliar a robustez das senhas escolhidas pelos participantes. O zxcvbn fornece *feedback* em tempo real para auxiliar os usuários na criação de senhas mais seguras. No entanto, como observado por Amador e colaboradores (2023), o zxcvbn possui limitações, como a dificuldade em avaliar senhas com combinações não convencionais ou geradas aleatoriamente.

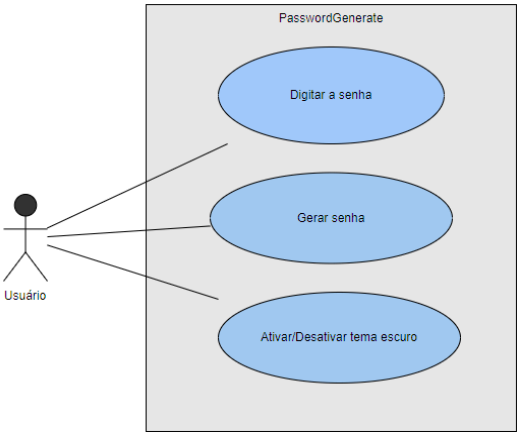
Com isso, o objetivo do projeto é desenvolver uma aplicação que verifica a força das senhas do usuário Além disso, o *software* poderá sugerir senhas seguras geradas aleatoriamente, difíceis de serem descobertas por *hackers* mal-intencionados. Essas sugestões devem incentivar os usuários a adotar senhas únicas para cada conta, minimizando o risco de comprometimento múltiplo caso uma senha seja vazada.

2. MATERIAL E MÉTODOS

Para a execução deste trabalho, foram colocados em funcionamento dois computadores com configurações distintas. Um deles, disponibilizado pelo Instituto Federal de Ciência e Tecnologia do Sul de Minas Gerais - Campus Muzambinho, possuía um processador AMD Ryzen 5 2600 com frequência de 3,40 GHz, 16 GB de memória RAM, HD de 500 GB, teclado e mouse. O segundo computador estava equipado com um processador Intel(R) Core(TM) i5-13500 de 2,50 GHz, 8 GB de memória RAM e um HD de 250 GB, também com teclado e mouse.

Para o desenvolvimento do software foram utilizadas as seguintes tecnologias: o framework back-end Electron, linguagem de programação JavaScript, HTML e CSS. O processo de desenvolvimento seguiu o método Kanban utilizando a plataforma Notion, e os diagramas de classes de uso foram criados usando as ferramentas online Visual Paradigm e LucidChart.

Figura 1. Diagrama de Caso de Uso



Fonte: do autor(2024).

3. RESULTADOS E DISCUSSÃO

Ao concluir o desenvolvimento do *software*, os resultados mostraram que ele realiza a verificação precisa da força das senhas. As senhas fracas são destacadas com uma descrição em vermelho, indicando perigo ao utilizar esta senha. Senhas com força média são identificadas por uma indicação amarela e uma descrição que serve como um alerta. Senhas fortes são marcadas com uma indicação verde e uma descrição correspondente. Esses resultados confirmam que o programa opera conforme o esperado, permitindo a verificação segura de senhas pessoais sem armazená-las.

Figura 2. Página da aplicação demonstrando o verificador de senha.

Fonte: do autor(2024).

Além disso, a funcionalidade de geração de senhas pode criar senhas com mais de 12 caracteres, proporcionando maior segurança. O gerador está funcionando corretamente e gera senhas com base na quantidade de caracteres especificada pelo usuário.

4. CONCLUSÃO

Conforme os resultados obtidos do projeto e a análise da verificação de senha e do gerador, pode-se concluir que o programa é uma ferramenta eficaz para auxiliar os usuários na avaliação da segurança de suas senhas e na demonstração de sua força. Através de uma interface simples com dicas para auxiliar na criação das senhas. O software destaca pontos fracos e sugere melhorias.

Além disso, o gerador de senhas proporciona opções de criação de senhas robustas, que atendem aos critérios de segurança. O uso deste programa contribui significativamente para a prática de boas políticas de segurança digital, ajudando a proteger informações pessoais e reduzir o risco de comprometimento de dados. Em suma, o programa pode facilitar na criação de senhas, e

também promove uma maior conscientização sobre a importância da segurança cibernética para os usuários.

REFERÊNCIAS

AMADOR, J.; MA, Y.; HASAMA, S.; LUMBA, E.; LEE, G.; BIRRELL, E. Prospects for improving password selection. In: KELLEY, P. G.; KAPADIA, A. (Eds.). Proceedings of the Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023). USENIX Association, 2023. p. 263-282.

Alroomi, S., & Li, F. (2023). Measuring Website Password Creation Policies At Scale. Georgia Institute of Technology and Kuwait University.

TAN, Joshua; BAUER, Lujo; CHRISTIN, Nicolas; CRANOR, Lorrie Faith. Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements. In: ACM SIGSAC Conference on Computer and Communications Security (CCS '20), 2020, Virtual Event, USA. Proceedings […]. New York: ACM, 2020. p. 1407-1427.