SECUREPASS+ (SP+)

Autores: Christian Yamith Salazar Botina

Bootcamp Ciberseguridad

Simulador de Evaluación, Cifrado y Simulación de Seguridad de Contraseñas

Objetivo General

Diseñar e implementar una aplicación de escritorio capaz de evaluar la fortaleza de contraseñas, generar tokens personalizados cifrados, presentar versiones mnemotécnicas y simular ataques de fuerza bruta para concientizar sobre los riesgos de contraseñas débiles

Objetivos Especificos

1. Desarrollar un algoritmo de evaluación que determine el nivel de seguridad de una contraseña usando criterios técnicos (longitud, caracteres, palabras comunes).
2. Implementar mecanismos de cifrado combinando los algoritmos César y Vigenère para fortalecer los tokens generados.
3. Crear un generador de tokens personalizados que mezcle la contraseña con entradas adicionales del usuario, aumentando la entropía.
4. Transformar contraseñas cifradas en frases mnemotécnicas legibles para mejorar la recordación sin comprometer la seguridad.
5. Simular ataques de fuerza bruta sobre contraseñas cifradas y mostrar al usuario la facilidad o dificultad de vulnerarlas, fomentando el uso de contraseñas robustas.

Tesis

“La concientización sobre la seguridad de contraseñas puede mejorarse significativamente mediante herramientas interactivas que evalúen, refuercen y simulen la vulnerabilidad de claves, integrando cifrado, análisis léxico y técnicas mnemotécnicas en una sola interfaz educativa.”

Descripción

SecurePass+ es una aplicación desarrollada en Python que permite al usuario **registrar una contraseña**, evaluarla, **cifrarla con técnicas clásicas**, **visualizar su versión mnemotécnica** y, finalmente, **comprobar su seguridad simulando ataques de fuerza bruta**.
Incluye tanto una interfaz gráfica amigable (GUI en Tkinter) como una versión CLI (por consola), brindando al usuario diversas formas de interactuar con el sistema.

Este enfoque integral está diseñado no solo como una herramienta técnica, sino también como una **herramienta educativa en ciberseguridad**, útil en entornos académicos y personales.

Lenguajes y Tecnologías Usadas

Tecnología	Descripción
Python 3	Lenguaje principal
Tkinter	Interfaz gráfica (GUI)
NLTK	Procesamiento del lenguaje natural (detección de palabras y nombres comunes)
JSON	Almacenamiento estructurado de contraseñas cifradas
Algoritmos clásicos de cifrado	César y Vigenère
Simulación de ataques	Fuerza bruta en ambas técnicas de cifrado
Git & GitHub	Control de versiones y publicación del proyecto

Justificación

La necesidad de una aplicación educativa para concientizar sobre seguridad informática y prácticas adecuadas de protección de datos está ampliamente respaldada por estudios actuales. Cobweb (2024) informa que el 81 % de los usuarios reutiliza contraseñas y no emplea prácticas seguras, lo que incrementa significativamente la probabilidad de brechas de seguridad [1]. Eccentrix (2023) refuerza esta idea al señalar que “usuarios informados son la primera línea de defensa” frente al phishing, malware y accesos no autorizados, destacando que los entrenamientos en ciberseguridad reducen los incidentes de forma notable [2].

Asimismo, HelpDesk Heroes (2025) señala que el error humano es uno de los factores más vulnerables en los sistemas actuales, y que la educación continua mejora la postura de seguridad digital de los usuarios [3].

Por su parte, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA) recomienda el uso de contraseñas únicas, aleatorias, de al menos 16 caracteres y acompañadas de gestores de contraseñas, como uno de los métodos más efectivos para proteger cuentas e identidades [4].

Walden University destaca la necesidad de contraseñas complejas (que incluyan letras mayúsculas, minúsculas, números y símbolos) y del uso de autenticación de dos factores (2FA) como barrera esencial contra accesos no autorizados [4][5].

Desde una perspectiva técnica, Han (2022) revisa métodos de recorte, cifrado y validación de contraseñas, destacando la importancia de la educación del usuario y el uso de hash para reforzar la autenticación [8]. Finalmente, Barnett (2023) destaca el uso de la tokenización como método irreversible que garantiza la integridad de los datos y permite cumplir con normativas internacionales como PCI DSS, HIPAA y GDPR [9].

El presente proyecto responde a estas problemáticas, integrando módulos de evaluación de contraseñas, generación de tokens, encriptación doble, mnemotecnia y simulación de ataques de fuerza bruta, para educar al usuario en seguridad de la información de forma práctica e interactiva.

Bibliografia

[1] Cobweb (13 agosto 2024). *The Importance of Strong Password Practices*.

[2] Eccentrix (8 agosto 2023). *The Importance of Cybersecurity Awareness: Educating Users to Mitigate Risks*.

[3] HelpDesk Heroes (24 febrero 2025). *Cybersecurity Awareness Training: Educating Users*.

[4] Cybersecurity & Infrastructure Security Agency (CISA). *Secure Our World Passwords Tip Sheet*. (2023).

[5] Walden University. *Cybersecurity 101: Why Choosing a Secure Password Is So Important*.

[6] OWASP. *Authentication – OWASP Cheat Sheet Series*.

[7] Academia.edu. M. P. Vaishnnave et al. (2020). *A Study on Cyber Security for Password Generation*.

[8] Han, L. (2014). *Password Cracking and Countermeasures in Computer Security: A Survey*. ArXiv.

[9] Patrick Barnett (Secureworks). *Tokenization and Encryption: Not Just for Credit Cards* (5 septiembre 2017).