DESCRIPCIÓN INICIAL PARA EL PROYECTO "ENCRIPTACIÓN DE CONTRASEÑA SEGURA"

La seguridad de las contraseñas es un tema crucial en el ámbito digital actual. Las contraseñas son la primera línea de defensa contra el acceso no autorizado a cuentas, sistemas y datos personales. Sin embargo, a menudo los usuarios eligen contraseñas débiles o reutilizan las mismas en múltiples servicios, lo que las convierte en objetivos fáciles para los atacantes. Este proyecto tiene como objetivo crear una herramienta que no solo evalúe la seguridad de una contraseña, sino que también ofrezca recomendaciones para mejorarla, garantizando un nivel adecuado de protección frente a amenazas comunes.

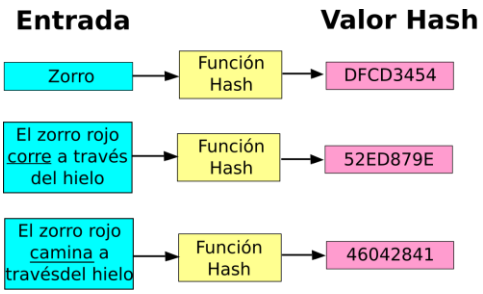
IMPORTANCIA DE LAS CONTRASEÑAS SEGURAS

Una contraseña segura es fundamental para proteger la privacidad y la integridad de los datos personales y corporativos. Contraseñas débiles o predecibles son vulnerables a técnicas como:

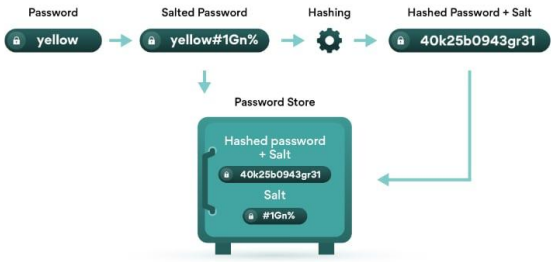
- **Ataques de fuerza bruta:** Consisten en probar todas las combinaciones posibles hasta encontrar la contraseña correcta.
- **Ataques de diccionario:** Los atacantes utilizan listas de contraseñas comunes para intentar acceder a una cuenta.
- **Ataques de relleno de credenciales (credential stuffing):** Los atacantes prueban combinaciones de contraseñas previamente filtradas en diferentes servicios.

Definiciones clave

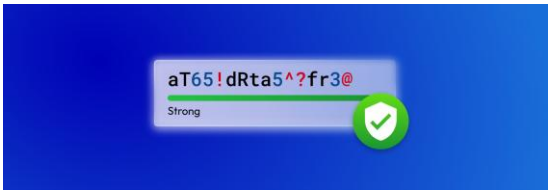
1. **Contraseña débil:** Contraseñas fáciles de adivinar, como "david456", "password" o el nombre del usuario.
2. **Contraseña segura:** Aquella que es difícil de adivinar por su longitud, complejidad y aleatoriedad. Suele incluir mayúsculas, minúsculas, números y caracteres especiales.
3. **Algoritmo de hash:** Método criptográfico que transforma datos (como una contraseña) en una cadena fija de caracteres, siendo irreversible. Ejemplos: bcrypt, SHA-256, Argon2.



4. **Salting:** Técnica para añadir una cadena aleatoria a una contraseña antes de aplicar el hash, dificultando los ataques por diccionario.



5. **Entropía:** Medida de imprevisibilidad en una contraseña. Una mayor entropía implica mayor seguridad.



Objetivo del proyecto

Desarrollar una herramienta que:

1. **Evalue la seguridad de una contraseña** en función de criterios como longitud, entropía y presencia de caracteres variados.
2. **Identifique contraseñas comunes o filtradas**, comparándolas con bases de datos de contraseñas comprometidas.
3. **Sugiera contraseñas alternativas** que cumplan con estándares de seguridad reconocidos.
4. Eduque al usuario sobre cómo crear contraseñas seguras y gestionar sus credenciales.

Motivación

El proyecto surge de la creciente necesidad de herramientas que ayuden a los usuarios a fortalecer su seguridad digital. Con el incremento de brechas de datos y ataques cibernéticos, una contraseña débil puede ser el punto de entrada para un atacante, con consecuencias graves como robo de identidad, pérdida de información confidencial y daños financieros.

Tecnologías y principios involucrados

- **Lenguajes de programación:** Se pueden usar Python, JavaScript u otros lenguajes para implementar la lógica de validación y generación de contraseñas.
- **Bases de datos:** Para almacenar listas de contraseñas comunes o comprometidas (por ejemplo, la base de datos de Have I Been Pwned).
- **Criptografía:** Implementar algoritmos de hash y salting para simular prácticas seguras de manejo de contraseñas.
- **Principios de UX/UI:** Diseñar una interfaz amigable que permita a los usuarios interactuar fácilmente con la herramienta.

Amenazas iniciales

1. **Uso indebido del proyecto:** Personas malintencionadas podrían intentar usar la herramienta para generar contraseñas predecibles para atacar a otros usuarios.
2. **Fallos en la evaluación de contraseñas:** Si los criterios de evaluación son deficientes, podría etiquetarse como segura una contraseña que no lo es.
3. **Falta de educación del usuario:** Incluso con una herramienta poderosa, los usuarios podrían no entender cómo utilizar contraseñas seguras de forma correcta.

Soluciones iniciales

- Implementar límites en el uso de la herramienta para prevenir abusos.
- Diseñar un algoritmo robusto para evaluar la seguridad de las contraseñas.
- Incluir secciones educativas o mensajes que expliquen la importancia de contraseñas seguras y cómo gestionar credenciales de manera efectiva.

Resultados esperados

1. Reducir el uso de contraseñas débiles entre los usuarios que utilicen la herramienta.
2. Contribuir a la prevención de ataques relacionados con credenciales débiles.
3. Incrementar la concienciación sobre prácticas de seguridad digital.