ContraSegur es una herramienta avanzada para la creación, análisis y gestión segura de contraseñas. A continuación, se describe paso a paso su funcionamiento y principales características:

La interfaz intuitiva de ContraSegur permite generar contraseñas aleatorias de alta entropía. Estas contraseñas combinan letras mayúsculas, minúsculas, números y símbolos especiales, lo que garantiza que cada clave sea única y extremadamente difícil de descifrar.

Además, se incluye un teclado virtual y una tabla ASCII integrada que facilitan la inserción de caracteres complejos sin complicaciones para el usuario.

Mientras el usuario escribe su contraseña, el sistema realiza una validación dinámica. Una barra de progreso muestra el nivel de fortaleza de la clave, y diversos indicadores (checkboxes) se activan conforme se cumplen los requisitos de seguridad.

Para mejorar la retroalimentación, ContraSegur emplea un Set para detectar contraseñas comunes y un Array de patrones predefinidos que identifican secuencias predecibles. De este modo, el usuario recibe sugerencias inmediatas para fortalecer su contraseña.



Al clicar "Iniciar sesión", ContraSegur realiza un análisis exhaustivo mediante expresiones regulares (RegEx), detectando posibles patrones vulnerables.

Simultáneamente, calcula el tiempo estimado que tomaría descifrar la contraseña mediante fuerza bruta.

Luego, se presenta un informe detallado con la siguiente información:

- Nivel de seguridad general y vulnerabilidades encontradas.
- Tiempo aproximado para romper la contraseña (en años y días).
- Puntuación técnica basada en longitud y diversidad de caracteres.
- Evaluación semántica adicional utilizando el algoritmo **zxcvbn**.

Una vez validada la contraseña, el sistema pregunta si el usuario desea guardarla. En caso afirmativo, los datos se

almacenan de forma segura en **LocalStorage** y **Cookies**, utilizando estructuras de tipo clave-valor y Arrays para una gestión eficiente.

Si el nombre de usuario ya existe en el sistema, ContraSegur ofrece dos opciones: mantener la contraseña anterior o actualizarla, evitando así duplicidades o conflictos.

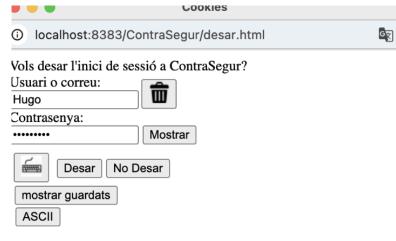
La función "Mostrar inicios de sesión guardados" permite visualizar una tabla dinámica generada mediante manipulación del DOM. En esta tabla, el usuario puede consultar, editar o eliminar credenciales con total facilidad.

También es posible cargar archivos externos que contengan listas de contraseñas comunes, lo

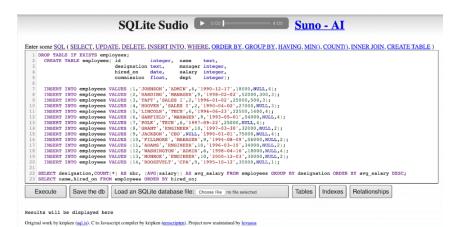
que amplía la capacidad de detección de amenazas del sistema.

ContraSegur es completamente personalizable y multilingüe. Utiliza Objetos para gestionar diferentes idiomas, los cuales pueden ampliarse mediante una base de datos SQLite.

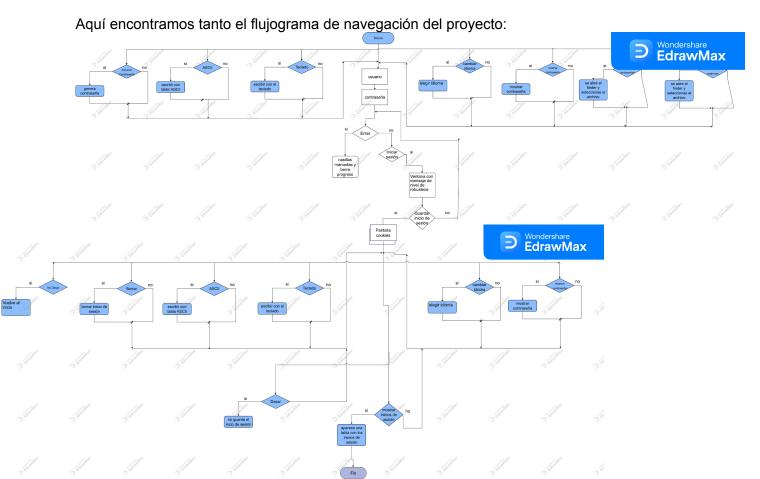
Gracias a esta integración, las traducciones se cargan de forma dinámica, haciendo que la plataforma sea accesible para usuarios de distintas regiones. Si se utiliza junto



con **SQLite Studio**, es posible añadir nuevos idiomas, integrar contraseñas cifradas (usando MD5, SHA1, AES) y definir nuevos patrones de seguridad personalizados.



ContraSegur combina usabilidad, robustez y adaptabilidad para ofrecer una experiencia segura y eficiente en la gestión de contraseñas. Ideal tanto para usuarios individuales como para entornos empresariales o educativos.



Seguido de las variables y estructuras principales del programa junto a las funciones principales y las tecnologías utilizadas para realizar este trabajo

Variables y Estructuras

- diccionari: Set con contraseñas comunes prohibidas.
- patrons: Array de RegExp para detectar patrones inseguros (ej. "123").
- Idiomes: Array de objetos con textos multidioma (es, ca, en).
- **CostComputacional**: Calcula tiempo para romper la contraseña.

Funciones Principales

- 1. Validación
 - Comprovar(): Verifica longitud, mayúsculas, números, etc.
 - o resumen(): Devuelve mensajes de error ("Contraseña común", "Falta símbolo").

2. Seguridad

- o Iniciar(): Usa zxcvbn para puntuar fortaleza (0-4) y estima tiempo de hackeo.
- CheckPasswordPatron(): Detecta secuencias predecibles.

3. Utilidades

- o random(): Genera contraseñas aleatorias.
- o mostrar_contrasenya(): Alterna entre mostrar/ocultar contraseña.

4. Base de Datos

- o SQL Diccionari(): Carga contraseñas desde SQLite.
- o updatedatabase(): Genera gueries SQL para actualizar hashes (MD5/SHA1).

Tecnologías Usadas

- Frontend: HTML, CSS, JavaScript.
- Seguridad: zxcvbn, hashes (MD5/SHA1).
- Persistencia: localStorage, SQLite.

Notas:

ContraSegur es una herramienta en constante evolución. Su desarrollo está orientado a la mejora continua, incorporando nuevas funcionalidades, tecnologías de seguridad actualizadas y opciones de personalización según las necesidades de los usuarios. Con cada versión, se optimiza tanto la experiencia como la protección, garantizando que el programa se mantenga a la vanguardia en materia de seguridad digital. Las futuras actualizaciones buscarán ampliar aún más sus capacidades, integrando inteligencia adaptativa, cifrados más robustos y compatibilidad con otros sistemas de autenticación avanzada.

Créditos:

- Contrasenyes Segures: Versió Pre-alfa o Prototip HTML/JavaScript
 - Mossos d'Esquadra: Contrasenyes segures
 - YouTube: Condicions de servei
 - W3Schools: <u>How TO Password Validation</u>
 - **GitHub**: https://github.com/prosselloe/ContraSegur/
- **Dropbox.Tech**: **zxcvbn** | realistic password strength estimation
 - John the Ripper (Cracker)

- JavaScript Secure Hash Algorithm (SHA1) & MD5 functions
 - MD5 (Message-Digest Algorithm 5)
 - CryptoJS: JavaScript standard and secure cryptographic algorithms
- Read Text Files Using the JavaScript FileReader | HTML Goodies
- Estructuras de datos con JavaScript Parte 3: Map y Set
- AlaSQL.is JavaScript SQL database for browser API
- Netlify: https://dreamy-kleicha-d4c27a.netlify.app/
- https://github.com/z125709