Fundación Educativa Jesuitas Noroeste ANPA Colexio Apóstol Santiago

¿Es segura tu contraseña? Mi web analiza si te pueden hackear

1. DATOS PERSONALES

- **Autores:** Natalie Cleaver Rodas - Laura Romero Hermoso
- **Centro Educativo:** Colexio Apóstol Santiago (Vigo).

2. RESUMEN DEL PROYECTO

Hemos creado una **página web para comprobar si tus contraseñas son seguras** o si un hacker podría adivinarlas fácilmente. Nuestro objetivo es que todos nos demos cuenta de que usar claves simples es un peligro hoy en día. Para ello, **programamos un evaluador que analiza lo que escribes al momento** y te dice qué tan fuerte es tu clave. Nuestro código sabe distinguir si usas palabras normales de un diccionario o si has mezclado letras, números y símbolos raros. Al final, los resultados demuestran que nuestro sistema funciona muy bien: **reconoce que las contraseñas mezcladas son mucho mejores** y que al usar símbolos es clave para que nadie nos robe nuestra identidad en internet

3. INTRODUCCIÓN

Hoy en día, casi toda nuestra vida está en internet, por eso la **ciberseguridad es superimportante** para proteger nuestra privacidad. El problema es que mucha gente usa contraseñas muy flojas y por eso les roban las cuentas. Para ayudar a solucionar esto, hemos creado una **herramienta que enseña a la gente si sus claves son fuertes de verdad**.. Nuestra idea es que, al usar la pagina web, recibes un aviso al momento con colores y gráficos para que entiendas por qué tu clave es segura o no. Así, todos aprenderemos a protegernos mejor y será mucho más difícil que alguien entre en nuestras cuentas sin permiso

4. PROPÓSITO DEL TRABAJO

Hemos hecho este trabajo para crear una **página web que ayude a mis compañeros y profes del Colexio Apóstol Santiago** a entender cómo se crear contraseñas que nadie

pueda adivinar. El gran problema hoy en día es que casi todos usamos claves muy típicas y fáciles, y así los hackers pueden robarnos las cuentas muy rápido usando programas automáticos. Con nuestro evaluador, queremos que cualquiera pueda **ver con claridad si su contraseña es fuerte de verdad**. Nuestro propósito es que en el cole dejemos de usar claves solo porque son fáciles de recordar y aprendamos que lo más importante es **mezclar letras, números y símbolos**. Queremos demostrar con pruebas reales que cuanto más variada sea la clave, más protegida estará nuestra identidad en internet.

5. ESTUDIO DEL ESTADO DE LA ARTE

Para investigar este tema, hemos visto cómo ha cambiado la forma de proteger nuestras cuentas. Antes solo se comprobaba si la contraseña estaba en una lista de palabras comunes, pero ahora se usan matemáticas para medir su 'entropía', que es lo difícil que resulta de adivinar. Hemos aprendido que existen guías oficiales (como las del NIST) que explican que la fuerza de una clave depende de cuántas combinaciones puedes hacer: cuantas más letras, números y símbolos uses, más combinaciones posibles hay. Los hackers usan programas de 'fuerza bruta' para probar miles de claves por segundo, pero si mezclas tipos de caracteres diferentes, el tiempo que tardarían en entrar en tu cuenta crece muchísimo. Nuestro proyecto usa estas mismas ideas para demostrar que las claves variadas son las más seguras.

6. HIPÓTESIS

Nuestra hipótesis es que **si escribo contraseñas que mezclan letras, números y símbolos en mi web, el sistema las marcará como seguras con mucha más precisión** que si solo uso palabras normales de un diccionario. Esto se basa en que es mucho más difícil adivinar una clave cuanto más variada sea, porque hay muchas más combinaciones posibles. Un buen programa debe dar una puntuación más alta a estas claves mezcladas que a las palabras comunes. Con esto, queremos demostrar que nuestro **código funciona bien y que sabe distinguir perfectamente entre una contraseña floja y una que es difícil de hackear** porque es más compleja y variada.

7. MATERIAL Y MÉTODOS

Para hacer nuestra página web, usamos los lenguajes básicos de internet: **HTML** para crear la estructura, **CSS** para que el diseño quedara bien y **JavaScript** para que la página funcione y piense. Lo más importante es que programé unas reglas especiales (llamadas **Expresiones Regulares**) que permiten a nuestro código revisar lo que escribes mientras lo vas tecleando. El sistema analiza al momento si estás mezclando a la vez letras mayúsculas, minúsculas, números y símbolos especiales. También dediquamos tiempo a diseñar una pantalla que fuera fácil de usar y a hacer muchas pruebas para corregir fallos. Así nos aseguramos de que el programa diera más puntos a los símbolos, porque son los que hacen que una contraseña sea casi imposible de adivinar para un hacker.

8. RESULTADOS

Después de hacer varias pruebas con la pagina web, hemos visto que cuanto más variada es la contraseña, mejor nota de seguridad le da el programa. Por ejemplo, si ponía una palabra fácil como 'password', el sistema nos decía que su nivel era 'Bajo' porque es muy previsible. En cambio, al probar con algo más difícil como 'C0ntr@seña.2026', el evaluador marcaba una fortaleza alta al momento. Esto demuestra que nuestro código funciona bien y que no solo mira si la clave es larga, sino que valora mucho que mezcles letras, números y símbolos. Los resultados confirman que al usar una clave variada hace que sea muchísimo más segura y difícil de adivinar para un hacker en todos los casos que he analizado.

9. CONCLUSIONES

Al final, los resultados demuestran que **nuestra hipótesis era totalmente cierta**: el programa sabe ver si una contraseña es segura analizando lo compleja que es. Hemos comprobado que usar reglas de programación para revisar si mezclas letras, números y símbolos es una forma muy buena de **protegernos contra los hackers**. Esto coincide con lo que dicen los expertos en ciberseguridad: que cuanto más variada y 'al azar' sea una clave, más difícil es que la adivinen con ataques automáticos. Nuestro proyecto demuestra que **podemos crear nuestras propias herramientas para aprender a cuidar nuestras cuentas de internet**. Al final, nuestra pagina web no solo sirve para poner nota a una contraseña, sino para que todos entendamos mejor la seguridad de una forma visual y fácil.

10. BIBLIOGRAFÍA

- **INCIBE. (2023).** *Guía de contraseñas seguras para ciudadanos* . Instituto Nacional de Ciberseguridad.
- **Mozilla Developer Network. (2024).** *Regular Expressions in JavaScript* . MDN Web Docs.
- **NIST. (2020).** *Special Publication 800-63B: Digital Identity Guidelines* . National Institute of Standards and Technology.
- **OWASP Foundation. (2023).** *Authentication Cheat Sheet: Password Strength Requirements* .
- **Stallings, W. (2021).** *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson.
- **Kaspersky Lab. (2024).** *Research on Password Entropy and Brute Force Vulnerabilities* . Documentación técnica de referencia.