

حل التحدي

فك تشفير كلمات المرور المجموعة المعطاة من كلمات المرور مخزنة بتنسيق MD5، وهو نوع من التجزئة (hashing) أحادي الاتجاه. بمعنى أنه لا يمكن "فك" التجزئة إلى النص الأصلي بنفس الطريقة التي تُستخدم لفك التشفير. بدلاً من ذلك، يمكن استخدام جداول قوس قزح أو قواميس الكلمات لفك تشفير كلمات المرور، ولكن النتائج ليست مضمونة دائماً.

كلمات المرور المشفرة وفك تشفيرها

1. 5f4dcc3b5aa765d61d8327deb882cf99 → password

2. 6cb75f652a9b52798ee0e17941b2c76b → 123456

3. d8578edf8458ce06fbc5bb76a58c5ca4 → qwerty

تحليل قوة كلمات المرور

- كلمة المرور: password: قوتها: ضعيفة جداً، لأنها واحدة من أكثر كلمات المرور شيوعاً.

نقاط الضعف: سهولة التخمين أو تجريب كلمات المرور.

- كلمة المرور 123456:

قوتها: ضعيفة، فهي أيضاً تعتبر من كلمات المرور الأكثر استخداماً.

نقاط الضعف: لا تحتوي على أحرف خاصة أو أرقام غير متتابة مما يجعلها سهلة التخمين.

- كلمة المرور: qwerty

قوة: ضعيفة، حيث تعتمد على ترتيب أحرف لوحة المفاتيح.

نقاط الضعف: معروفة كأحد كلمات المرور الضعيفة ومتكررة الاستخدام.

أساليب لتحسين قوة كلمات المرور

1. زيادة الطول: استخدم كلمات مرور لا تقل عن 12-16 حرفاً.

2. استخدام مزيج من الأحرف: تضمين أحرف كبيرة وصغيرة، أرقام، وأحرف خاصة.

3. تجنب الكلمات الشائعة: الابتعاد عن الكلمات الشائعة أو العبارات السهلة.

4. استخدام عبارات مرور: يمكن استخدام جمل أو عبارات طويلة يسهل تذكرها.

5. تفعيل المصادقة الثنائية: إضافة طبقة أمان إضافية للمصادقة على الدخول.

الهدف: يهدف هذا التمرين إلى تعزيز الفهم حول كيفية تشفير كلمات المرور وتحليل قوتها، وتحديد نقاط الضعف والتحديات التي تواجه مستخدمي كلمات المرور.