

تحدي الأول

، تقييم قوتها، ونقاط الضعف المحتملة، واقتراحات لتحسينها MD5 بالتأكيد! إليك تحليل لكلمات المرور المستخرجة من

1. كلمة المرور: "password" (hash: 5f4dcc3b5aa765d61d8327deb882cf99)

قوة كلمة المرور: ضعيفة جدًا

نقاط الضعف:

قصيرة (8 أحرف).

هي واحدة من أكثر كلمات المرور شيوعًا واستخدامًا في العالم "password" شائعة جدًا؛

سهولة التنبؤ، ما يجعلها هدفًا سهلاً لهجمات القواميس

اقتراحات للتحسين:

إضافة أحرف كبيرة وصغيرة، رموز، وأرقام

جعلها أطول (12 حرفًا أو أكثر)

"MySecurePa\$\$w0rd2024!". تكون فريدة وصعبة التخمين مثل (passphrases) استخدام جمل مرور

2. كلمة المرور: "secret" (hash: 6cb75f652a9b52798ee0e17941b2c76b)

قوة كلمة المرور: ضعيفة

نقاط الضعف:

قصيرة (6 أحرف).

أيضًا سهولة التنبؤ "secret" شائعة جدًا؛ كلمة

لا تحتوي على تنوع في الأحرف (كلها أحرف صغيرة)

اقتراحات للتحسين:

إضافة تعقيد باستخدام أحرف كبيرة، أرقام، ورموز

جعلها أطول؛ على الأقل 12 حرفاً.

تجنب الكلمات الشائعة التي يمكن أن تكون ضمن القواميس التي تستخدم في الهجمات.

3. كلمة المرور: "qwerty" (hash: d8578edf8458ce06fbc5bb76a58c5ca4)

قوة كلمة المرور: ضعيفة جداً

نقاط الضعف:

قصيرة جداً (6 أحرف)

شائعة جداً لأنها متواجدة على لوحة المفاتيح كترتيب أحرف "qwerty" متوقعة وسهلة التخمين؛

لا تحتوي على أي رموز أو أرقام أو أحرف كبيرة.

اقتراحات للتحسين:

"أو "qwerty" 123456" تجنب الأنماط الواضحة مثل

استخدام كلمات مرور تتكون من مجموعة متنوعة من الأحرف والرموز.

إنشاء جملة مرور معقدة تحتوي على أكثر من 12 حرفاً.

طرق لتحسين قوة كلمات المرور

1. استخدام توليد كلمات مرور عشوائية: استخدم أدوات توليد كلمات مرور عشوائية (مثل مدير كلمات المرور) لإنشاء 1. كلمات مرور معقدة وغير متوقعة.

2. زيادة الطول: كلما زاد طول كلمة المرور، أصبحت أكثر صعوبة في الكسر. كلمات المرور التي تحتوي على 12. حرفاً أو أكثر تكون أكثر أماناً.

3. التنوع في الأحرف: يجب أن تحتوي كلمة المرور على مزيج من الأحرف الكبيرة والصغيرة، الأرقام، والرموز. الخاصة.

إضافة طبقة ثانية من الأمان باستخدام المصادقة الثنائية يزيد بشكل كبير من حماية (2FA) استخدام المصادقة الثنائية. 4. الحساب حتى لو تم كشف كلمة المرور.

عدم إعادة استخدام كلمات المرور: لا تستخدم نفس كلمة المرور لأكثر من حساب، حتى لا تعرض جميع حساباتك 5. للخطر إذا تم اختراق أحدها.

باتباع هذه الأساليب، يمكنك تعزيز قوة كلمات المرور وتقليل فرص اختراقها.