

التحدي الأسبوعي رقم ١ : تحليل كلمة المرور

الحل

فك تشفير كلمات المرور المشفرة :

- 5f4dcc3b5aa765d61d8327deb882cf99 : هذه التجزئة تمثل كلمة المرور "password"
- 6cb75f652a9b52798ee0e17941b2c76b : هذه التجزئة تمثل كلمة المرور "123456"
- d8578edf8458ce06fbc5bb76a58c5ca4 : هذه التجزئة تمثل كلمة المرور "qwerty"

تحليل كلمات المرور المستخرجة من حيث قوتها :

• password:

ضعيفة : كلمة مرور بسيطة وشائعة جدًا ، ويسهل تخمينها باستخدام الهجمات المعروفة أو القاموس.

• 123456:

ضعيفة : سلسلة أرقام متتالية هي من أشهر وأسهل كلمات المرور ، وغالبًا ما تُخترق بسهولة.

• qwerty:

ضعيفة : سلسلة أحرف مرتبة بشكل متسلسل على لوحة المفاتيح ، مما يجعلها ضعيفة وسهلة التخمين.

نقاط الضعف المحتملة :

- جميع كلمات المرور قصيرة وسهلة التخمين.
- تعتمد على أنماط شائعة ومعروفة ، مما يجعلها هدفًا سهلاً لهجمات التخمين العشوائي أو هجمات القاموس.
- لا تحتوي على تنوع في الأحرف ، مثل استخدام الأحرف الكبيرة والصغيرة ، الرموز الخاصة ، أو الأرقام غير المتسلسلة.

اقتراحات لتحسين قوة كلمات المرور :

- **استخدام كلمات مرور أطول :** يجب أن تكون كلمات المرور بطول لا يقل عن ١٢ حرفًا.
- **زيادة التعقيد :** من خلال استخدام مزيج من الأحرف الكبيرة والصغيرة ، الأرقام ، والرموز الخاصة.
- **تجنب الأنماط الشائعة :** مثل الكلمات الشائعة أو الأنماط المتسلسلة على لوحة المفاتيح.
- **استخدام كلمات مرور عشوائية :** يمكن استخدام مولدات كلمات مرور عشوائية لإنشاء كلمات مرور قوية.
- **التحقق الثنائي (2FA) :** استخدام المصادقة الثنائية لتعزيز الأمان.
- **استخدام مدير كلمات مرور :** لتوليد وتخزين كلمات مرور معقدة وفريدة لكل حساب.