

سلسلة تحديات الأمن السيبراني الأسبوعية للطلاب المتوسطين والمحترفين.

التحدي الأسبوعي رقم 1: تحليل كلمة المرور

الوصف:

لديك مجموعة من كلمات المرور المخزنة بتنسيق مشفر. مهمتك هي فك تشفير كلمات المرور وتحليل قوتها. مجموعة كلمات المرور (بشكل مشفر):

5f4dcc3b5aa765d61d8327deb882cf99

6cb75f652a9b52798ee0e17941b2c76b

d8578edf8458ce06fbc5bb76a58c5ca4

المهام:

قم بفك تشفير كلمات المرور المشفرة.

حلل كلمات المرور المستخرجة من حيث قوتها. ما هي نقاط الضعف المحتملة؟

اقترح أساليب لتحسين قوة كلمات المرور.

الهدف:

فهم كيفية تشفير كلمات المرور، وكيفية تحليل قوة كلمات المرور وتحديد نقاط الضعف فيها.

فك تشفير كلمات المرور:

الهاشات مشفرة باستخدام خوارزمية MD5.

فك تشفير الهاشات:

1. "5f4dcc3b5aa765d61d8327deb882cf99" = "password"

2. "6cb75f652a9b52798ee0e17941b2c76b" = "123456"

3. "d8578edf8458ce06fbc5bb76a58c5ca4" = "qwerty"

تحليل قوة كلمات المرور:

1. password:
 - كلمة شائعة جدًا.
 - ضعيفة للغاية ويمكن تخمينها بسهولة باستخدام أدوات التخمين أو هجمات القاموس.
2. 123456:
 - من بين أسوأ كلمات المرور التي يمكن استخدامها.
 - بسيطة ومتكررة وشائعة جدًا.
3. qwerty:
 - بناء على ترتيب الحروف في لوحة المفاتيح.
 - رغم أنها ليست كلمة، إلا أنها أيضًا شائعة وسهلة التخمين.

نقاط الضعف المحتملة:

- البساطة: كلمات المرور الشائعة مثل "password" و"123456" هي أهداف سهلة جدًا لهجمات القاموس وهجمات القوة الغاشمة (Brute Force).
- الطول: كلمات المرور المستخرجة قصيرة جدًا، مما يسهل كسرها.
- عدم التعقيد: كلمات المرور لا تحتوي على أحرف خاصة أو أحرف كبيرة أو مزيج من الأرقام والأحرف.

تحسين قوة كلمات المرور:

1. استخدام كلمات مرور أطول: يفضل أن تكون كلمات المرور 12 حرفًا أو أكثر.
2. تعقيد أكبر: دمج الأحرف الكبيرة والصغيرة والأرقام والأحرف الخاصة يجعل من الصعب تخمين كلمة المرور.
3. استخدام عبارات مرور: استخدام جملة أو عبارة أطول يزيد من القوة دون الحاجة إلى تعقيد إضافي.
4. استخدام مديري كلمات المرور: يمكن لمديري كلمات المرور إنشاء كلمات مرور قوية عشوائية وتخزينها بشكل آمن.
5. تفعيل المصادقة الثنائية (2FA): استخدام طبقة إضافية من الأمان بجانب كلمة المرور.

اسم الطالبة / شهد عادل علي.

تخصص تقنية المعلومات