

التحدي الأسبوعي رقم ١: 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):

م	الكلمات المشفرة
١	f4dcc3b5aa765d61d8327deb882cf99°
٢	cb75f652a9b52798ee0e17941b2c76b٦
٣	d8578edf8458ce06fbc5bb76a58c5ca4

❖ المهام:

♦ قى بفك تشفير كلمات المرور المشفرة.

م	الكلمات المشفرة	الكلمات بعد فك التشفير
١	f4dcc3b5aa765d61d8327deb882cf99°	password
٢	cb75f652a9b52798ee0e17941b2c76b٦	123456
٣	d8578edf8458ce06fbc5bb76a58c5ca4	qwerty

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

م	كلمات المرور	التحليل
١	password	🚩 قوة كلمة المرور: ○ ضعيفة للغاية. 🚩 نقاط الضعف: ○ تعتبر كلمة شائعة جداً. ○ لا تحتوي على أحرف كبيرة، أرقام أو رموز. ○ من السهل اختراقها باستخدام هجمات القوة الغاشمة أو القواميس
٢	123456	🚩 قوة كلمة المرور: ○ ضعيفة جداً. 🚩 نقاط الضعف: ○ تتكون من أرقام متسلسلة وبسيطة. ○ من أكثر كلمات المرور الشائعة على الإنترنت. ○ يمكن اختراقها بسهولة باستخدام أي تقنيات تحليل كلمات المرور.
٣	qwerty	🚩 قوة كلمة المرور: ○ ضعيفة. 🚩 نقاط الضعف: ○ تتبع تسلسل أحرف شائع على لوحة المفاتيح. ○ سهولة التخمين من قبل البرامج التي تعتمد على تخمين الأنماط.

♦ اقترح أساليب لتحسين قوة كلمات المرور.

- ✓ استخدام كلمات مرور طويلة: كلما كانت كلمة المرور أطول، كلما كانت أصعب في الاختراق. يفضل أن تتكون من ١٢ حرفاً على الأقل.
- ✓ تنوع الأحرف: استخدام مزيج من الأحرف الكبيرة والصغيرة، الأرقام، والرموز الخاصة
- ✓ عدم استخدام الكلمات الشائعة
- ✓ استخدام كلمات مرور عشوائية:
- ✓ يمكن استخدام مولدات كلمات المرور العشوائية لإنشاء كلمات مرور قوية وغير متوقعة.
- ✓ من الأفضل استخدام برنامج لإدارة كلمات المرور لتخزين وإنشاء كلمات مرور معقدة لكل حساب بدلاً من تذكرها يدوياً.

الاسم: صخر حامد عرب

طالب الدراسات العليا تخصص الامن السيبراني