

1- فك تشفير كلمات المرور:

كلمات المرور مشفرة باستخدام خوارزمية MD5 ، يمكن فك تشفيرها عن طريق هجمات "القاموس" أو "قواعد البيانات العكسية".

• 5f4dcc3b5aa765d61d8327deb882cf99:

○ باستخدام قاعدة بيانات عكسية، الإجابة password .

• 6cb75f652a9b52798ee0e17941b2c76b:

○ فك كلمة المرور 123456.

• d8578edf8458ce06fbc5bb76a58c5ca4:

○ فك كلمة المرور qwerty.

2- تحليل قوة كلمات المرور:

1. password

○ هي كلمة مرور شائعة جداً وتعتبر ضعيفة.

2. 123456

○ هذه الكلمة عبارة عن ارقام المتتالية وهي سهلة التخمين.

3. qwerty

○ هي كلمة مرور بسيطة تعتمد على ترتيب لوحة المفاتيح وهي سهلة التخمين.

نقاط الضعف:

• جميع كلمات المرور قصيرة وسهلة التخمين.

• جميع كلمات المرور موجودة في قواعد البيانات الخاصة بكلمات المرور المتداولة بشكل عام.

3- اقتراحات لتحسين قوة كلمات المرور:

1. زيادة الطول كلمة المرور على الأقل 12 حرفاً .

2. استخدام مزيج من الأحرف الكبيرة والصغيرة أو الرموز أو الأرقام.

3. استخدام كلمات مرور عشوائية وغير معروفة وغير متوقعة .

4. التجزئة باستخدام خوارزميات أقوى MD5 قديمة وغير آمنة.

5. من الأفضل استخدام خوارزميات حديثة مثل Argon2 .

مثال على تشفير كلمة مرور باستخدام Argon2 :

كلمة المرور SW23@DRIF&85

تشفيرها 5f95894186c29dbeecf528f290bb88d4