

تحليل كلمات المرور المشفرة

طريقة التحليل

تم استخدام قاعدة بيانات الهاش المتاحة وأدوات فك التشفير عبر الإنترنت لتحديد كلمات المرور من خلال قيم MD5 المقدمة.

نتائج فك التشفير

1. 5f4dcc3b5aa765d61d8327deb882cf99: تم فك تشفير هذه القيمة إلى كلمة "password".
2. 6cb75f652a9b52798ee0e17941b2c76b: تم فك تشفير هذه القيمة إلى كلمة "123456".
3. d8578edf8458ce06fbc5bb76a58c5ca4: تم فك تشفير هذه القيمة إلى كلمة "qwerty".

نقاط الضعف

1. الطول: كلمات المرور المستخدمة قصيرة.
2. التعقيد: لا تحتوي على تنوع في الأحرف (كبيرة، صغيرة) أو إضافة أرقام ورموز.
3. الشبوع: الاعتماد على كلمات مرور شائعة يجعلها سهلة التخمين والكسر.

اقتراحات لتحسين قوة كلمات المرور

1. زيادة الطول: ينصح بأن تكون كلمات المرور أطول من 12 حرفاً.
2. إضافة التنوع: استخدام مزيج من الأحرف الكبيرة، الصغيرة، الأرقام والرموز يزيد من صعوبة التخمين.
3. تجنب الشبوع: يجب تجنب استخدام كلمات المرور الشائعة والأنماط المتوقعة كـ "123456" أو "password".
4. استخدام عبارات المرور: تشجع على استخدام عبارات مرور أطول تتكون من عدة كلمات تجعل عملية الاختراق أكثر صعوبة.