Goldman Sachs Task 1: Crack leaked password database

Dear Sir/Madam,

Hope you are doing well!

After trying to crack the passwords you provided, I found there're potential risks existing in the password policy of the organization, and I would like to be explain all my findings, conclusions as well as my suggestions to improve the password policy.

All passwords you provided are coded using Message-Digest (MD5) cryptographic hash function, which is a standard algorithm but comparatively weak and insecure, and could be attacked in a short time using Brute Force.

Because of that, some controls could be implemented to avoid the password database leaking again:

1. Using a hashing algorithm which provides a high level of protection, such as SHA - 256 or SHA - 3.
2. Introduce password salting to safeguard passwords in storage.

Also, there're something else that are damaging the security of passwords in your password policy:

1. The minimum password length is set to be 6, which is supposed to be longer.
2. Passwords are allowed to be any combination of letters, numbers and symbols, even pure letters/numbers are allowed.

Here're my suggestions:

1. Set the minimum password length to be at least 8 characters.
2. Avoid containing common words like 'password', or simple string of numbers like '11111' '123456' in passwords, nor users' names and dates of birth.
3. Recommend users to include capital letters, small letters, numbers, and special characters in their passwords.

Hope you find them useful!

Thanks,
Xiaokun Du