Dear Sir/Ma’am

I discovered several weaknesses in your password policy while trying to decipher all the leaked hashes, and this email summarizes my findings and offers recommendations for how to strengthen your password policy.

**Findings**

All the passwords were encrypted using weaker hash algorithm – **MD5**. MD5 is insecure and provides a **very low level of protection** and should not be used in any application. With the help of crackstation.net, it was very simple to crack.

**Organization’s password policy**

1. Minimum length for password: 6
2. No specific rules/ conditions for password creation (i.e., users are free to use any combination of word and letters to create a password)

**Possible controls to be implemented to make cracking much harder for the hacker in the event of a password database leaking again**

1. Passwords should have a minimum length that is neither too short nor too long.
2. Inclusion of special character, Capital and Small letters, numbers in password.
3. Using high-level protection algorithm (example: SHA-256 or SHA-3) instead of MD5.
4. Use salting to avoid the usage of rainbow tables which accelerates cracking.

**Possible changes in Password policy to make breaking the passwords harder**

1. Minimum length for password: 8.
2. Minimum one special character, one numerical and one character to be used in password.
3. Users shouldn't be permitted to create passwords using their username, real name, date of birth, or other personal information.
4. Passwords must not contain common words and character combinations.
5. The strength of the password should be displayed to the user as they type it in using an external API-based.
6. A software that makes recommendations for enhancing the strength of password.

Thanking you,

Name: Chebrolu Tejaswi

M.Tech (Integrated) CSE with Spl in Data Science

Vellore Institute of Technology