Dear Sir/Ma'am

I tried to crack the all leaked password and I successfully cracked all those passwords/hashes and found lots of vulnerability in your password policy. In this report, I conclude all the findings and suggestions to improve the password policy.

To crack the passwords I use the Hashcat tool. MD5 and SHA are the standard cryptographic hash algorithms to provide data security for multimedia authentication. All the hashes which are compromised were using MD5 which is a weaker hash algorithm and is subject to collisions.

By using a tool like Hashcat it is easy to crack the passwords. I would advise that you use a very strong password encryption mechanism to create hashes for the password based on SHA.

After performing the task, we find the following entities in the organization's password policy:

- Users can use any combination of letters and words to create a password. No specific requirement was used in the password creation.
- No use of special character.
- The minimum length for a password is set to 6.

You can take specific steps/changes in your password policy to make breaking the password harder. My suggestion is:

- **Make it long:** This is the most critical factor. Choose nothing shorter than a minimum of 8 characters, more if possible.
- **Doesn’t Rely on Obvious Substitutions:** Avoid common words and character combinations.
- **Use a mix of characters:** The more you mix up letters, numbers, and symbols, the more potent your password.
- **Don’t use memorable keyboard paths:** Do not use sequential keyboard paths either (like *qwerty*).
- **Don't use personal information**: Do not let users include their username, actual name, date of birth, and other personal information.
- **Don’t reuse your passwords:** Do not use the same password across websites/social media.

Thanking You,

Name: Aniket B Sanap

Email: aniketsanap43@gmail.com