Dear Sir/Madam,

I’ve tried to crack/decrypt all of the leaked passwords. And I’ve come to a conclusion that there are some issues with your existing password policy and improvements are stated in this email.

All the passwords which were leaked were in the Message Direct 5(MD5) format. And we know that this is the most basic technique to hash the passwords.

It was very easy to crack the password using technologies like Hashcat, terminal and webapps. I would suggest you to make improvements in the existing password policy based on Secured hash Algorithm.

After going through the decrypted results, we can conclude that:

* There are no certain rubrics for password creation like: minimum length, alphanumeric combination of letters, any kind of special characters.

I would recommend you to make the following improvements to the existing policy:

* Do not allow any user to include username or date of birth in the password.
* Do not allow user to include series of alphabets or numbers.
* Make the use of alphanumeric characters mandatory.
* Make the use of Upper and lowercase alphabets for better security.
* Increase the minimum characters to 8 and above.

You can access the decrypted password through the file attached below.

Thanking you,

Ch.Sethu Gouri Shankar,

Computer Science and Engineering,

BVRIT-N.

Table

Description automatically generated