**Respected Sir/ Ma’am,**

This email is regarding the findings, vulnerabilities and suggestions which I had after a thorough and deep check on the password hashes and their security state.

The popular hashing algorithms which are used for hashing passwords these days are (Secure Hash Algorithm) SHA-246, SHA-512, MD6, etc.

Nearly 13 passwords were cracked using **hashcat** and **crackstation** wordlist. All these passwords were hashed using the MD5 algorithm. These passwords were not something new but the old and very commonly used phrases and words.

A suggestion is there to use strong passwords and more complex algorithms such as SHA-256, etc.

After cracking the passwords, the following findings for the organizations password policy were found: -

* The minimum length of passwords was 6 and the maximum length of passwords (cracked) was 9.
* The hashing algorithm used was MD5 (Message Digest), has been cryptographically broken and is considered insecure, providing a 128-bit hash to secure passwords.
* Most of the passwords were just commonly used words and phrases, which were already exploited in some old password breaches.

The above findings suggest that the passwords used were not only short in length but also weak in nature (use of common words). Hence, the following changes could be applied to the organization’s password policy, for making the passwords stronger and hack proof: -

* The minimum length specified of passwords, should be of at least 8 – Digits.
* Use of upper-case letters, special characters as well as digits should be encouraged.
* Instead of using passwords, use of passphrases should be encouraged.
* Password managers and password generators should be used for randomized and complex passwords.
* Instead of using MD5, other newer and more complex algorithms (such as – SHA-256, etc.), should be used.
* Salts and Hashes should be used, in order to safeguard passwords, thereby making it harder for attackers to crack the passwords.

These were my findings on the organization’s password policy and the cracked passwords obtained.

**Thank You,**

**Harsh Pathak**