**Subject:** Crack leaked password database

Dear Sir/Ma’am,

While cracking and reviewing the leaked hashes, I have found multiple loopholes and vulnerabilities in the shared password list. Please find the below suggestions and ideas to further improve the password selection process and make breaking the passwords more difficult.

All the compromised passwords are using the **MD5** cryptographic hash function which has many weaknesses, the main issue being MD5 is vulnerable to collision attacks in which the hashing algorithm takes two different inputs and produces the same hash. This property means the MD5 hash function is considered “broken” and very high-risk. This provides very poor level of protection as multiple tools such as Hashcat and free-to-use web apps can be used to crack the hashes.

I used **Hashcat** along with [**CrackStation’s** Human only dictionary](https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm) and [**MD5 Online**](https://www.md5online.org/md5-list-decrypter.html) to crack these.

To make breaking the passwords harder, a lower-risk hash function should be implemented such as **SHA512crypt** which is resistant to collision attacks and mostly resistant to length extension attacks, or **Bcrypt** which is the standard password hash algorithm used in most systems. SHA512crypt passes the password through 5,000 hashing iterations to make decrypting harder and near impossible. Bcrypt includes a salt and is designed to withstand brute-force attacks by intentionally being slower to operate. The unsalted passwords listed below could be cracked using online websites such as CrackStation, which is very insecure.

Judging from the cracked passwords listed below, the password policy allows employees to use any combination of numbers and characters. The space character is not a valid input, and the minimum password length may be six and the maximum fourteen, although the size of the sample passwords is too small for this conclusion to be definitive. The organisation’s **average password length is almost eight characters** but has multiple passwords shorter than eight and easy to guess which pose a high security risk. Their key space is smaller than modern standards.

The password policy should be changed so that passwords include the following:

* Use of number, letter, special character, capital letter
* Keeping a **threshold on length**. Set minimum length of 8.
* Employees should also avoid easy to guess passwords such as pet names and birthdates as well as avoid repeating their passwords for multiple accounts.
* **Reduce redundancy** across services such that in case of a leak out of one service doesn’t make the **other passwords vulnerable**.
* **Not allowing sibling credentials** **to assist** the password naming, like name / user name / email / date of birth / sex.
* **Avoiding the occurrence of English verbs** like book, popular, eating, hero, life, John Wick, crack me, expert that makes the password vulnerable to brute force attacks.

Fond regards,

Pratyush Kumar