

# Memo

**To:** Goldman Sachs

**From:** Nilakshi Nagrale

**CC**: Other recipients

After successfully cracking all the leaked hashes, several vulnerabilities in the password policy were found. Following are all the details of the findings along with a few suggestions to improve the password policy.

The standard cryptographic functions that provide data security for authentication include Message Digest (MD5) & Secure Hash Algorithm (SHA). But all the compromised passwords were secured using MD5, which is weak and more prone to hash collisions.

Designed by Ronald Rivest in 1991, MD5 is an iterative hash function that takes a message of arbitrary length as its input and produces a 128-bit message digest as its output. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest.

Regardless, passwords encrypted using MD5 could be cracked easily by using tools such as Hashcat in Linux/windows environment. After careful examination, following observations regarding password policy were made:

* Minimum password length limit was set to 6, which is indeed a basis for poor password creation.
* No specific requirements (e.g., Special characters, numbers, etc) mentioned while creating a password.

Following suggestions can be implemented in strengthening the password policy:

* Mandate the use of use alphanumeric characters with special characters (at least 1 Capital letter & 1 special character)
* Increase the base limit of password length to 8 characters.
* Refrain your users from including their personal information (e.g., Name, birth date, birth place, etc) in their passwords.
* System Admins can initialize the use of 2FA and install an Intrusion Detection System to detect brute force attacks.
* Initialize the use of SHA for encrypting the passwords as it is more secure and not vulnerable to hash collisions.

Thankyou.

