**Cracked leaked password database at Goldman Sachs by Forage**

Respected Sir/Ma’am,

I am Anushka N Mishra, participated in the Virtual Engineering Program and engaged in all the resources available.

After considering all the given hash protected password list, I found that there are certain improvements requirements in order to make the password stronger. Thus, this email concludes the suggestions to improve the password policy.

It is concluded from the password dump file that:

* All the password which are compromised were using MD5 (Message Digest algorithm 5) which is a weaker hash algorithm and is prone to collisions.
* The minimum password length is 6.
* No special character, capital letter or numbers is mandatory.

Thus, the passwords in the dump file are too weak to be cracked. MD5 algorithm makes the storage of passwords even worse, and were easily cracked using cracking tools in kali-Linux like hash-cat or online hash decrypt tools. From the “Anatomy of a hack” as provided in resource, it is very clear that a weak password is a piece of cake for hackers and crackers and if MD5 is used is a boon. It describes how various techniques like brute-force attack can be used to hack such passwords using premade combinations of passwords.

Hence it is recommended to use the latest hashing techniques such as SHA (Secure hash Algorithm) to minimise the risk. Also ‘Salt’ which is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase can be used to make the passwords stronger.

Following measures can be taken to make strong passwords:

* The password should be more than 8 characters.
* The passwords should contain numbers i.e., alphanumeric in nature.
* The password should contain the special characters such as(@,&,#,$, etc).
* The password must be a combination of capital and small letters.
* Do not use actual name, date of birth, username or any other personal information in the passwords.
* Use latest hashing algorithms to store passwords, which uses latest and updated security measures.

Thank You!