**Goldman Sachs Virtual Internship**

**Task 1**

**By *Suhana,*** [***b21229@students.iitmandi.ac.in***](mailto:b21229@students.iitmandi.ac.in)

After conducting the analysis, it was determined that the organization uses MD5 password hashing algorithm which offers very little protection if the password database is leaked and can be cracked easily. Also, the current password policy is not aligned with industry best practices allowing users to have short passwords (generally 6 characters) and reuse usernames as passwords.

Thus, to increase the strength of passwords, the following points should be kept in mind:

* Use a strong password hashing algorithm like bcrypt or scrypt which will increase the time taken to crack individual passwords.
* Implement Salting to prevent usage of rainbow tables to speed up cracking.
* Prevent reusing usernames as passwords.
* Increase the minimum password length to about 15 characters or more so that the computational effort is increased and we get time to change the leaked passwords.
* Users should be educated to create safe and easy to remember passwords. The best way to create a user-friendly password is by using passphrases. Also, Upper case characters, Lower case characters, some special characters and numbers should be used. For ex. Cats2Love4@Ice-Creams6