memo

Goldman Sachs Engineering Virtual Program

To : Goldman Sachs
From: Ankit Tanwar
CC : Forage

Major findings used by the organisation to prevent successful cracking of passwords and suggestions to change the policies of the organisation.

After a detailed analysis of the passwords which I cracked, it was found that the organisation uses MD-5 algorithm which is outdated nowadays and least secure in password database leaking. Also, the organisation did not follow the current password policy used by the industry as it allows the user to have 6 characters short passwords and reuse username as the part of their passwords.

Major uplifts proposed to prevent successful cracking of password and increase the security level of user:

- Strong hashing algorithms such as bcrypt, PBKDF2, scrypt, SHA-256 should be used.
- Adding salt to the hash algorithms will give an extra layer of security to the passwords.
- The length of password should be 8-10 characters long having a combination of uppercase letters, lowercase letters, numbers and special characters as it will give hackers extra time to crack them.
- The password should have to be unique and the user should be educated regarding creation of strong passwords.
- The appropriate way to create a user-friendly password is by the usage of passphrase.

(+91)9999883439 • ankitt0204@gmail.com • New Delhi, India