Date: Sept 3rd, 2020

To: Evaluator, Goldman Sachs

From: Rupali Shekhawat

Subject: Analysis of the Leaked Password Database

Dear Evaluator,

I hope all is well. I am writing to inform you about my developments regarding the Password Database. After thoroughly checking the provided hashes, I have concluded that the "MD5" hashing algorithm was used to protect passwords. The security of the MD5 hash function is severely compromised and it is vulnerable to collision attacks. The organization’s password policy is very weak and should be updated to make cracking much harder for the hackers in the event of a password database leaking again. On analysing the passwords used by the users, I have concluded that the minimum character length allowed is 6 and the usage of letters, characters, numbers is allowed with no constraints. The password policy needs to change to make breaking the passwords harder. Following changes can be made for better password protection:

1. The use of both upper-case and lower-case letters
2. Inclusion of one or more numeric digits
3. Inclusion of special characters, such as @, #, $
4. Prohibition of words found in a password blacklist
5. Prohibition of words found in the user's personal information
6. Prohibition of passwords that match the format of calendar dates, license plate numbers, telephone numbers, or other common names
7. Prohibition of use of company name or an abbreviation

These are the results that have been predicted from the Leaked Password Database.

Regards,

Rupali Shekhawat