GOLDMAN SACHS ENGINEERING VIRTUAL PROGRAM

Memo

To: The Forage

from: Riya Tanwar

CC: Goldman Sachs

Major findings in relation to controls used by an organization and my proposed uplifts regarding the same

The password dump file which I was provided with contains hashes which uses MD5(Message Digest) hashing algorithm which is not actually secure. I suggest the organization to use stronger algorithm such as SHA-256 and SHA-3. Although MD-5 is a widely used hash function but it has been found to have well-documented weaknesses and deprecation by security professionals. One of the major requirements of a cryptographically hashed function is that it should be infeasible to find two distinct message that hash to the same value. MD-5 fails to fulfill this requirement because it is able to generate two different message that have the same hash which puts the customer's security at risk as hackers can easily access the passwords.

Therefore, Hashing alone is not the right way to store passwords in the server's database. Adding Salt to Hash passwords (means adding random data to the hash passwords) should be implemented to make cracking much harder for hackers in the event of a password database leak again.

The organization's password policy is not up to the mark because almost all of the passwords which I cracked contains: only numbers (111111, 123456, 123456789, 12345678, 1234567), properly spelled words (qwerty, password, password1, bluered, password!) and combination of lowercase letters and numbers(abc123) which is not a good password policy. The good password policy must be at least 8 characters long, should contain uppercase, lowercase, special characters and numbers. It should not contain properly spelled words and should be unique. Therefore, I would like to suggest the organization to follow the same password policy so that attackers find it harder to break the passwords.

New Delhi, India, 110028