GOLDMAN SACHS VIRTUAL SOFTWARE ENGINEERING INTERNSHIP

Dear Goldman Sachs Associate,

Date: August 1, 2022
Subject: Cracking the Passwords

Q: What type of hashing is used to protect the passwords

A: The type of hashing that was used to protect the passwords was MD5, which is iterative and produces a 128bit hash.
Example: experthead:e10adc3949ba59abbe56e057f20f883e, the password we are cracking is after the ":"

Q: What level of protection does the mechanism offer?

A: Since our passwords are only 32 characters the MD5 is considered weak because it is too fast so hackers can use this and crack many passwords in a short time. The MD5 is very direct as opposed to other hashing methods which require a lot of time and memory to crack.

Q: What controls can be implemented to make cracking much harder for the hacker in the event of a database leak?

A: Instead of using MD5, the user can implement passwords using a better algorithm such as RSA or SHA, these both take a lot longer and are harder to crack. The slower the algorithm the better because it will take a lot longer and is more draining for the CPU. Using salts wherever applicable and maybe even the addition of a two-factor authentication.

Q: What can you tell about the organization's password policy?

A: They don't have many requirements for the password, the hashing algorithm is very weak (MD5) and they are using very common passwords, the first one being "123456".

Q: What would you change in the password policy to make breaking the passwords harder?

A: We can up the requirements for our passwords to have a longer password, include at least 1 number, symbol, and capital letter. These will all increase the amount of password combinations exponentially.

Best Regards,
Jerry Su