Crack leaked password database at Goldman Sachs by Forage

Respected Sir/Ma’am,

I am Tanmay Shukla, I have participated in the “Crack Leaked Password Database” internship and have engaged in all available resources.

I found the following:

1. MD5 (Message Digest algorithm 5) is weak and insecure. It can be easily broken by hackers; therefore, it is recommended to use the latest hashing techniques such as SHA (Secure Hash Algorithm) to minimize the risk.
2. A hash function is used to generate a unique hash code for each combination of characters in alphanumeric form. It serves to secure any data and information, for example, in the blockchain.
3. Password cracking tools are used to recover the password of an encrypted file or system.
4. From the "Anatomy of a Hack" as given in the source, it is very clear that a weak password is a plaything for hackers and crackers and if MD5 is used, it is a benefit. It describes how various techniques such as brute force attack can be used to hack such passwords using pre-made password combinations.
5. A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or a passphrase Salts are used to protect passwords in storage. Used in SHA-256.
6. Password strength checker can be used to check the password strength, how strong or weak the password is.

After attempting to crack and recover passwords from the provided password dump file, the following conclusions are drawn:

1. The password policy used does not comply. The passwords used are too weak.
2. The MD5 algorithm makes password storage even worse and they were easily cracked using kali-linux cracking tools like hashcat or online hash decryption tools.

The following measures can be taken to create and store strong passwords:

1. Password reuse should be avoided.
2. Do not use any personal information such as name, parent's name, date of birth, etc. in passwords.
3. Use the latest hashing algorithms to store passwords that use the latest and updated security measures.
4. The length of the password should be at least 6 to 8 characters.
5. Passwords should be alphanumeric in nature, i.e. at least one combination of alphabet and number.
6. Password should contain at least one special character like $, @, # etc.

Thank you!

Security Algorithms used:

experthead:e10adc3949ba59abbe56e057f20f883e – MD5
interestec:25f9e794323b453885f5181f1b624d0b – MD5
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5
simmson56:96e79218965eb72c92a549dd5a330112 – MD5
bookma:25d55ad283aa400af464c76d713c07ad – MD5
popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5
liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5
johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5
flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5
oranolio:16ced47d3fc931483e24933665cded6d - MD5
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5
moodie:8d763385e0476ae208f21bc63956f748 - MD5
nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5
bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5

Cracked Passwords:

experthead:e10adc3949ba59abbe56e057f20f883e - 123456
interestec:25f9e794323b453885f5181f1b624d0b - 123456789
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 - qwerty
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 - password
simmson56:96e79218965eb72c92a549dd5a330112 - 111111
bookma:25d55ad283aa400af464c76d713c07ad - 12345678
popularkiya7:e99a18c428cb38d5f260853678922e03 - abc123
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 - 1234567
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c - password1
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 - password!
liveltekah:3f230640b78d7e71ac5514e57935eb69 - qazxsw
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b - Pa$$word1
johnwick007:f6a0cb102c62879d397b12b62c092c06 - bluered