Dear Sir/Ma’am,

After successfully trying to crack all the leaked hashes, I have found several vulnerabilities in Goldman Sachs’ password policy. This report includes all of my observations and suggestions which would help improve your password policy.

My very first finding was that all of the compromised hashes were hashed using MD5 hashing algorithm.

Unfortunately, MD5 has been cryptographically broken and considered insecure. For this reason, it should not be used for anything. Instead, developers should switch to the Secure Hash Algorithm or a Symmetric Cryptographic Algorithm. With current GPUs and hash cracking tools, using MD5 is barely better than using nothing at all. It is always recommended to store user passwords using a hashing algorithm and you should find that it is equally easy to use SHA-2 in place of MD5 in any modern programming framework.

Secure Hash Algorithm (SHA) and Message Digest (MD5) are the standard cryptographic hash functions to provide data security for authentication

I was able to crack all the compromised hashes in a very small time using hashcat [<https://hashcat.net/hashcat/>] and several wordlists I downloaded from <https://hashcat.net/forum/thread-1236.html>.

I would suggest implementing the following controls to make cracking much harder for the hacker in the event of a password database leaking again:

* Stop the usage of MD5 algorithm to hash passwords.
* Use stronger hashing algorithms such as SHA-256 or SHA-3.
* One way of making the password hard to crack is by maintaining credentials from multitude of services in a manager like dashlane because they tend to use varied hashing algorithms & even hashing over hashed passwords to store and keep the strength high, meeting to the rigidity of a strong case for an algorithm to process.
* Use alphanumeric character with special characters.
* Reducing occurrence of an adjective on noun or verb which is an obvious prey to brute force attacks.
* Reduce redundancy across services such that in case of a leak out of one service doesn’t make the other passwords vulnerable.

I have also observed that the company’s password policy is not up to the mark because of the following reasons:

* The average password length is 11.
* Minimum length for password is set to 6.
* Most of the passwords do not include an upper-case character. Lack of upper-case characters splits the password strength by half.
* There is no prescribed pattern for password creation. Users can use any combination of characters and numbers to create a password.
* Lack of usage of special characters.

Here is a list of changes I would make in the password policy to make cracking the passwords harder:

* Minimum password length should be set to 12 characters.
* Mandating minimum 3 special characters and minimum one capital letter.
* Applying a hashing algorithm over another, recursively to have a strong hashing function.
* Don’t let users include their username, actual name, date of birth and other personal information while creating a password.
* Caution over use of verbs are nouns or adjectives.
* Training users to follow these policies to keep their passwords safe.

**Shashank N**

[**shashanknraj456@gmail.com**](mailto:shashanknraj456@gmail.com)

**Hashing 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:**

96e79218965eb72c92a549dd5a330112: **111111**

fcea920f7412b5da7be0cf42b8c93759: **1234567**

5f4dcc3b5aa765d61d8327deb882cf99: **password**

25d55ad283aa400af464c76d713c07ad: **12345678**

d8578edf8458ce06fbc5bb76a58c5ca4: **qwerty**

e99a18c428cb38d5f260853678922e03: **abc123**

7c6a180b36896a0a8c02787eeafb0e4c: **password1**

3f230640b78d7e71ac5514e57935eb69: **qazxsw**

6c569aabbf7775ef8fc570e228c16b98: **password**!

25f9e794323b453885f5181f1b624d0b: **123456789**

917eb5e9d6d6bca820922a0c6f7cc28b: **Pa$$word1**

f6a0cb102c62879d397b12b62c092c06: **bluered**

e10adc3949ba59abbe56e057f20f883e: **123456**