From:goldmansachsIT@gmail.com

To: seniormanagement@email.com

Subject: Information Security

Body:

Goldman Sachs

Dear Sir/Madam,

Using my python code, I was able to implement a brute force method using a password database from 'https://raw.githubusercontent.com/berzerk0/Probable-Wordlists/master/Real-Passwords/Top12Thousand-probable-v2.txt' by using a hashing library to convert the passwords from this list into a MD5 hash type and checking to see if there are any matches. I would then scrape the password that the hash belonged to from the database. This meant, all 19 hashes were decrypted.

The MD5 hashing algorithm was used to protect the passwords and it was clear from the 128 bits and 32 characters each hash had. MD5 should not be used as it provides minimal protection, is very insecure and is fat to decrypt. Typically, it should only be used to authenticate files. To make cracking harder, passwords should be more complex. Examples include using a minimum of 12 characters for a password, include at least two special characters, a mixture of upper case and lower-case letters, password salt the passwords and for the system to use a hashing algorithm that provides a high level of protection such as SHA. The password policy is outdated as the minimum length for a password was 6 and there was no criterion for a password to be created. Other than the examples listed above, password cracking could also be made more difficult if passwords were not reused and had no strings of characters in them relating to any personal information.

Kind Regards,

Michael Ishak