Goldman Sachs

MEMORANDUM

To: Goldman Sachs Virtual Software Engineering Internship Team
From: Mate Narh
Date: 25th October, 2021
Re: Goldman Sachs Goldman Sachs Virtual Software Engineering Internship Deliverable

Q	Prompt	Answer
1	*What type of hashing algorithm was used to protect passwords?*	• **MD5**
2	*What level of protection does the mechanism offer for passwords?*	• MD5 is significantly weak in the password protection it offers – acquired 68% success rate on the 19 dump file hashes within fractional time • Unsalted MD5 hashes are also easily susceptible to dictionary & brute-force attacks and output collisions
3	*What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?*	• Employing effective password salting that avoids salt reuse and short salts • Diversifying passwords to include long assortments of alphanumeric & special characters and devoid of obvious dictionary keywords and their "*leet speak*" equivalents – for instance, *Password/Pa$$word*
4	*What can you tell about the organization's password policy (e.g. password length, key space, etc.)?*	• Minimum password length: 6 • Maximum password length: 10 • Password capitalization: Minimum
5	*What would you change in the password policy to make breaking the passwords harder?*	• Banning common passwords and 'leet speak' equivalents like *Password* & *Pa$$word* • Enforcing multifactor authentication • Regulate 8-character minimum password length • Requiring 1 minimum letter capitalization