GOLDMAN SACHS – VIRTUAL ENGINEERING PROGRAM

Dear Sir/Madam,

After a thorough research, I was found that organizations use a defunct password hashing algorithm named MD5 (Message Digest). This algorithm provides very little protection and has multiple vulnerabilities.

Using <https://www.md5online.org/md5-decrypt.html> and <https://crackstation.net> I was able to crack all the passwords.

After cracking the passwords, I noted the following faults:

1. Minimum password length is set to 6
2. There are no set of rules to set the password – users are free to use any combination of letters & numbers.

I recommend the following changes to the organization’s password policy:

1. Set the minimum password length to 8 characters.
2. Don’t let users include their username, actual name or any other personal information as their password.
3. Make use of uppercase, lowercase and special characters mandatory.
4. Install a software that checks the password strength

Thank you

Regards,

Satviki Shukla

(B.Tech Electronics & Telecommunications)

CRACKED PASSWORDS:

|  |  |  |  |
| --- | --- | --- | --- |
| HASH | TYPE | | RESULT |
| experthead:  e10adc3949ba59abbe56e057f20f883e | MD5 | 123456 | |
| interestec:  25f9e794323b453885f5181f1b624d0b | MD5 | 23456789 | |
| ortspoon:  d8578edf8458ce06fbc5bb76a58c5ca4 | MD5 | qwerty | |
| reallychel:5f4dcc3b5aa765d61d8327deb882cf99 | MD5 | password | |
| simmson56:96e79218965eb72c92a549dd5a330112 | MD5 | 111111 | |
| bookma:25d55ad283aa400af464c76d713c07ad | MD5 | 12345678 | |
| popularkiya7:e99a18c428cb38d5f260853678922e03 | MD5 | abc123 | |
| eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 | MD5 | 1234567 | |
| heroanhart:7c6a180b36896a0a8c02787eeafb0e4c | MD5 | password1 | |
| edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 | MD5 | password! | |
| liveltekah:3f230640b78d7e71ac5514e57935eb69 | MD5 | qazxsw | |
| blikimore:917eb5e9d6d6bca820922a0c6f7cc28b | MD5 | Pa$$word1 | |
| johnwick007:f6a0cb102c62879d397b12b62c092c06 | MD5 | bluered | |
| flamesbria2001:9b3b269ad0a208090309f091b3aba9db | MD5 | Flamesbria2001 | |
| oranolio:16ced47d3fc931483e24933665cded6d | MD5 | Oranolio1994 | |
| spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e | MD5 | Spuffyffet12 | |
| moodie:8d763385e0476ae208f21bc63956f748 | MD5 | moodie00 | |
| nabox:defebde7b6ab6f24d5824682a16c3ae4 | MD5 | nAbox!1 | |
| bandalls:bdda5f03128bcbdfa78d8934529048cf | MD5 | Banda11s | |