Dear Sir/Mam,

While trying to crack all the hashes. I found that your password policy is very vulnerable and in this email comprises of all the findings and suggestions to improve your policy.

Message Digest and Secure Hash Algorithm are the standard cryptographic hash functions to provide data security for authentication.

All the passwords were made using MD5 which provides less security and is also cryptographically broken. I cracked passwords using crackstation and it was very easy to crack most of the passwords.

After analysing all the cracked passwords, I found following things about your password policy.

1. Minimum length of passwords was upto 6 words.
2. There were no guidelines or criteria for making passwords, so the passwords can be created using any combination of words and letters , which makes user to set a password which may be easier to crack.

My recommendation for a better password policy is :

1. Password should be a combination of special characters, uppercase and lowercase letters.
2. Do not repeat passwords similar to old passwords or avoid common passwords . For eg:- password,12345 etc.
3. Password length should be increased to 8 words minimum.
4. Passwords should not contain username, email address, phone numbers or any personal information while creating password
5. Use a secure password hashing algorithm.
6. Advice users to use passphrases

Thanking you,

Name : Saurabh Khare

**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