Dear Sir/ Madam,

After cracking the hashing algorithms, I identified many vulnerabilities in your password policy and will suggest some improvements to make breaking the passwords more difficult.

All the compromised passwords used the MD5 cryptographic hash function which has many weaknesses, the main issue being MD5 is vulnerable to collision attacks in which the hashing algorithm takes two different inputs and produces the same hash. This property means the MD5 hash function is considered “broken” and very high-risk.

Judging from the cracked passwords listed below, the password policy allows employees to use any combination of numbers and characters. The space character is not a valid input, and the minimum password length may be six and the maximum twelve, although the size of the sample passwords is too small for this conclusion to be definitive.

To make breaking the passwords harder, a lower-risk hash function should be implemented such as SHA-2 which is resistant to collision attacks and mostly resistant to length extension attacks, or Bcrypt which is the standard password hash algorithm used in most systems. Bcrypt includes a salt and is designed to withstand brute-force attacks by intentionally being slower to operate. The unsalted passwords listed below could be cracked using online websites such as CrackStation, which is very insecure.

The password policy should be changed so that passwords include at least one of the following: number, letter, special character, capital letter, and a minimum length of 8. Employees should also avoid easy to guess passwords such as pet names and birthdates as well as avoid repeating their passwords for multiple accounts.

Yours faithfully,

Jonida Kolgjini

Cracked passwords of non-salted hashes:

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**

Cracked passwords of salted hashes:

flamesbria2001:9b3b269ad0a208090309f091b3aba9db : **Flamesbria2001**

oranolio:16ced47d3fc931483e24933665cded6d : **Oranolio1994**

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e : **Spuffyffet12**

moodie:8d763385e0476ae208f21bc63956f748 :**moodie00**

nabox:defebde7b6ab6f24d5824682a16c3ae4 : **nAbox!1**

bandalls:bdda5f03128bcbdfa78d8934529048cf : **Banda11s**