Respected Sir, Ma’am

I found several flaws in the password policy opted by your organisation. As per my findings, all the passwords were hashed using Message Digest Algorithm which is no longer reliable to use.

Below, are the cracked 19 hash-codes with their result and the type of algorithm used by them.

Hash Type Result

e10adc3949ba59abbe56e057f20f883e Md5 123456

25f9e794323b453885f5181f1b624d0b Md5 123456789

d8578edf8458ce06fbc5bb76a58c5ca4 Md5 qwerty

5f4dcc3b5aa765d61d8327deb882cf99 Md5 password

96e79218965eb72c92a549dd5a330112 Md5 111111

25d55ad283aa400af464c76d713c07ad Md5 12345678

e99a18c428cb38d5f260853678922e03 Md5 abc123

fcea920f7412b5da7be0cf42b8c93759 Md5 1234567

7c6a180b36896a0a8c02787eeafb0e4c Md5 password1

6c569aabbf7775ef8fc570e228c16b98 Md5 password!

3f230640b78d7e71ac5514e57935eb69 Md5 qazxsw

917eb5e9d6d6bca820922a0c6f7cc28b Md5 Pa$$word1

f6a0cb102c62879d397b12b62c092c06 Md5 bluered

9b3b269ad0a208090309f091b3aba9db Md5 Flamesbria2001

16ced47d3fc931483e24933665cded6d Md5 Oranolio1994

1f5c5683982d7c3814d4d9e6d749b21e Md5 Spuffyffet12

8d763385e0476ae208f21bc63956f748 Md5 moodie00

defebde7b6ab6f24d5824682a16c3ae4 Md5 nAbox!1

bdda5f03128bcbdfa78d8934529048cf Md5 Banda11s

Observations:

1. All of the hash codes given in the dump file are secured with MD5 algorithm.
2. MD5 is insecure and no longer reliable. It offers low level of protection. Higher version of Secure hash Algorithm can be used, as it can’t be decoded directly.
3. Controls to be implemented are as follows:

* Minimum password length criteria. A password should be 16 characters or more.
* A password should include a combination of letters, numbers, and characters.
* Using hashed algorithms which offer high level of security such as SHA-256, SHAW-521 & SHAW-3.
* Master password algorithm differs from traditional approaches in the manner that passwords are not stored on disk or in the cloud, but are regenerated every time from information entered by the user.

1. As per the organization’s password policy:

Minimum password length was set to be six characters and the password consists of atmost two special characters.

1. To make password policy better:

* A password should be 16 characters or more; our password-related research has found that 45 percent of Americans use passwords of eight characters or less, which are not as secure as longer passwords.
* A password should include a combination of letters, numbers, and characters.
* A password shouldn’t be shared with any other account.
* A password shouldn’t include any of the user’s personal information like their address or phone number. It’s also best not to include any information that can be accessed on social media like kids’ or pets’ names.
* A password shouldn’t contain any consecutive letters or numbers.
* A password shouldn’t be the word “password” or the same letter or number repeated.

Thanking You

*Anshika Singla*

*B.Tech in Computer Science*