**15 JULY, 2022**

1]

Hashing Algorithm used:

MD5 Level of protection: MD5 (message digest algorithm) is a bad password hashing algorithm because it is too fast and memory conserving. Attacker can compute the hash of large number of passwords per second.

2]

Recommendations to implement password:

- Try using better algorithm in place of MD5. Eg.SHA256

- Always use salts with hashes where feasible.

- For better security use slow algorithm like bcrypt. Which make harder for attacker because it requires more CPU cycles to authenticate user.

3]

Observations on organization password policy:

- weak hash functions used with no salting

- common passwords are used which can be easily guessed and cracked

- No use of capital letters, numbers and special symbols together.

4]

Changes to be made in password policy:

- we can increase the password length to 12 because less characters length it becomes easy for hacker to crack the password using brute force attack.

- Don’t use common phrase as password. Use of mix characters.

- check your password security with password strength checker tools and websites.

Thank you

Aditya Sharma