

Dear sir/ma'am,

Good day. On the test of trying to crack the leaked hashes from your database, several vulnerabilities were found in your password policies. Please find the list of suggestions to change your password strategy.

Your passwords followed the MD5 Hash functions. Some of the common Hash Functions are SHA and MD5. I'd suggest that you use SHA as it's more secure. I used CrackStation and Hashcat (rockyou.txt) to crack your passwords. I strongly recommend you to enhance your encryption policy.

Unfortunately, 13 out of 19 your passwords were compromised as MD5 is prone more to vulnerabilities. Some of the common vulnerabilities I could find was,

- Passwords were of minimal length.
- The nature of your passwords were very common.
- Special character usage was a bit less.

Suggestions to improve security:

- Avoid common passwords and short length of passwords.
- Use a mixture of special characters, numbers, uppercase letters and lowercase letters.
- Don't incorporate personal information in the passwords. ie. Name, Date of birth, Place of birth etc.
- Passwords could be of length > 8 characters.
- Make sure that these standards are practiced by your staff.

Thank you.

Regards,
Krithika Nithyanandam