# Memorandum

To: Joanna

From: Divya Hari Kumar

Date: 11 March, 2023

The following table is the list of usernames, encrypted passwords and the passwords which I cracked using the hashcat tool:

| **Username** | **Encrypted Password** | **Password** |
| --- | --- | --- |
| experthead | e10adc3949ba59abbe56e057f20f883e | 123456 |
| interestec | 25f9e794323b453885f5181f1b624d0b23b453885f5181f1b624d0b | 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 |
| flamesbria2001 | 9b3b269ad0a208090309f091b3aba9db | Flamesbria2001 |
| oranolio | 16ced47d3fc931483e24933665cded6d | Oranolio1994 |
| spuffyffet | 1f5c5683982d7c3814d4d9e6d749b21e | Spuffyffet12 |
| moodie | 8d763385e0476ae208f21bc63956f748 | moodie00 |
| nabox | defebde7b6ab6f24d5824682a16c3ae4 | nAbox!1 |
| bandalls | bdda5f03128bcbdfa78d8934529048cf | Banda11s |

**What type of hashing algorithm was used to protect passwords?**

The MD5 hashing algorithm was used to protect the passwords. MD5 (message-digest algorithm) is a cryptographic protocol used to authenticate messages, verify content, and create digital signatures. It is a widely used algorithm in the field of cryptography and data security. It produces a 128-bit hash value from any given piece of data, allowing users to compare two pieces of data for authenticity. This makes it an important tool for ensuring the integrity and authenticity of digital information. MD5 has been used for various applications including authentication of digital documents, software updates, and secure communications.

**What level of protection does the mechanism offer for passwords?**

The Internet Engineering Task Force (IETF) has recently declared that MD5 hashes are no longer considered cryptographically secure methods and should not be used for cryptographic authentication. This decision was made due to the fact that MD5 hashes have been found to be vulnerable to collision attacks, which can allow malicious actors to generate two different messages with the same hash. As a result, it is now recommended that organizations use other more secure hashing algorithms, such as SHA-256 or SHA-512, for their cryptographic authentication needs. It yields hexadecimal from 0-15 or 0-F, which indicates that each of the digits are of four bits each.

**What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?**

There are many different controls which could be implemented to make cracking much harder for the hacker in the event of a password database leaking again. A few of them could be as follows:

* Alphanumeric Constraints:

Considering the latest trend in password setting, most domains and websites require the user to include:

Contain at least one lowercase letter, an uppercase letter, a digit and a special character

Have a password length of at least 8 characters

* Multi-Factor Authentication:

MFA could be used in order to reduce the chances of hacking/leaking passwords as it would ensure that the user provides multiple pieces (factors) of evidence (authentication). A few of those factors include OTPs, unique question’s answer and password. It will contribute to being a layer of security.

* Occurrence of Username/Email ID in Password:

Restriction in the use of a user's unique username, a substring of their Email ID or simply even their own name could help in reducing the risk in the breach of security. It is very common that people use it, therefore, this control would not only help in increasing the difficulty of cracking the password but also make it unique from the user’s set of passwords, in case any of them have been leaked.

**What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?**

Considering the given set of passwords, the following are my observations on the organization’s password policy:

* The password length is varying but the minimum seems to be about 6 characters. For example, if we consider the password “qwerty”- it can be easily guessed, cracked or even found using any brute force attacks.
* There is no restriction on using uppercase letters, digits or special characters. It reduces the password strength drastically.
* The users have used their own names or usernames as their password like in the password “moodie00” which is very easy to crack. This restriction would have reduced the risk of leaking the password as well.

Overall, the organization’s password policy could be improved by implementing any of the controls that I mentioned earlier and could add a better hashing method on top of it for stronger encryption.

**What would you change in the password policy to make breaking the passwords harder?**

The following are a few of the changes I would change in the password policy to make breaking the passwords harder:

* Restricting the use of username/name of the user
* Password must contain at least:
  + One uppercase letter
  + One lowercase letter
  + One digit
  + One special character
* Restrict using a continuous sequence of letters or numbers such as abc…, zyx…, 123…, 987…, etc.