Respected Sir/Madam,

I was able to crack 13 passwords from the given 19 hashcodes in the password dump file very easily using <https://crackstation.net/>



Q1) What type of hashing algorithm was used to protect passwords?

Ans1) MD5 type was used.

Q2) What level of protection does the mechanism offer for passwords?

Ans2) MD5 has been cryptographically broken and considered insecure. For this reason, it is not reliable and shouldn’t be used for application.

Q3) What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

Ans3)

* Stop the usage of MD5 algorithm to hash passwords.
* Use stronger hashing algorithms such as SHA-256 or SHA-3.
* Use alphanumeric character with special characters.
* Reducing occurrence of an adjective on noun or verb which is an obvious prey to brute force attacks.
* Reduce redundancy across services such that in case of a leak out of one service doesn’t make the other passwords vulnerable.

Q4) What can you tell about the organization’s password policy (e.g. password length, key space, etc.)?

Ans 4) I observed that the company’s password policy is not up to the mark because of the following reasons:

* The average password length is 11.
* Minimum length for password is set to 6.
* Most of the passwords do not include an upper-case character. Lack of upper-case characters splits the password strength by half.
* There is no prescribed pattern for password creation. Users can use any combination of characters and numbers to create a password.
* Lack of usage of special characters.

Q5) What would you change in the password policy to make breaking the passwords harder?

Ans 5) I would make the following changes in the password policy to make cracking the passwords harder:

* Minimum password length should be set to 12 characters.
* Mandating minimum 3 special characters and minimum one capital letter.
* Applying a hashing algorithm over another, recursively to have a strong hashing function.
* Don’t let users include their username, actual name, date of birth and other personal information while creating a password.
* Caution over use of verbs are nouns or adjectives.
* Training users to follow these policies to keep their passwords safe.

**- Khushboo Nijhawan**

**(**[**khushboo.nijhawan2020@vitstudent.ac.in**](mailto:khushboo.nijhawan2020@vitstudent.ac.in)**)**