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

Answer: MD5

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

Answer:

MD5 Message Digest Algorithm

* MD5, is a cryptographic hashing function.
* MD5 is **insecure.**
* Hash function producing a ***128-bit hash value***.
* MD5 is generally a ***considerable mechanism*** for storing passwords in production.
* MD5 is born out of ***RSA’s algorithm***.
* MD5 is a utility that can **generate a digital signature of a file**.
* The algorithm takes as input a message of **arbitrary length** and produces as output a **128-bit "fingerprint" or "message digest"** of the input.

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

Answer:

* *Maintaining credentials from multitude of services in a manager.*
* *Using a combination of Alpha-Numeric & special Symbolic value.*
* *Avoid using the same password for the different platform*
* *Reducing occurrence of an adjective on noun or verb which is an obvious prey to brute force attacks.*

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

Answer:

* Creating a strong password using a set of ***Alpha-Numeric & special Symbolic value.***
* Minimum length should at least of standards.
* Use of different letter case should be implemented.
* Not avoiding the occurrence of verbs.

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

Answer:

* Periodic Change should be required.
* Minimum Password character length should be at least 11.
* Avoid creating a password which is familiar like Birth Year, dates.
* Use of random Characters while creating password.
* Avoid passwords which are easy to guess.