What type of hashing algorithm was used to protect passwords?

ANS:  Message Digest Algorithm  is used for the protection of passwords and MD5 hashing function is used for the protection of the passwords.

What level of protection does the mechanism offer for passwords?

ANS: Low level of protection is provided by this mechanism. This mechanism is extremely insecure for the protection of password. Message digest algorithm (MD5) are used for the storage of passwords but due to the inefficiency of the mechanism causes lot of multiple attacks on the password storage data base. This MD5 hash values can be decode easily within seconds.

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

ANS: By preventing the user from not to use the same username as password and by not allowing any duplication of username and password of the users and by accessing the user to use long password by which the cracking of the password becomes much harder and by accessing the user to use any special characters.

There are some guidelines for the developers who write the code for storing or retrieving data.

1. Uses statements in the back end script for avoiding attacks on database.

2. Allow the password of the user only if the password length is greater than 8 and make sure that the password of the user must contain some special character as well

These are the controls could be implemented to make the cracking much harder.

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

Password length is less than 8 for every password which is a loop hole for the organization’s password policy and the key space is 128 bits as compared to key space of sha512 -256 bits which is not good for organization’s password policy. From this we can conclude that our organization police is not good.

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

By preventing the user from not to use the same username as password and by not allowing any duplication of username and password of the users and by accessing the user to use long password by which the cracking of the password becomes much harder and encourage the user to use any special characters in password.

Allowing the user’s password only if the password length is greater than 8 with some special characters.

1. Changing the hashing algorithm MD to SHA.

2. Using SHA 512 hashing function to hash the password which provides key space with 256 bits.

By these changes in the password policy makes cracking the password much harder.

OUTPUT:









