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

MD5 was the hashing algorithm used to protect passwords.

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

**The MD5 algorithm is a one-way hash function, it’s not reversible. So, there is no direct method to decrypt a hash and get back the original password. But in 2005, Bruce Schneier, an American cryptographer, declared that the MD5 algorithm was broken. The main reason was that collisions has been detected in the hash function.**

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

Following can be the controls—

1. **use long passwords with character variety**

2. **don't user real words**

3. **Use a different password on each website**

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

Character length of password is 32 and use of hexadecimal characters.

Bit length is 128 with no key space

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

 I highly recommend using salt to store passwords, whatever your choice for the hashing algorithm, it will highly decrease the chance of your passwords to be cracked. With a good salt, databases attack won’t be as efficient, and brute-force attacks will take much more time.