DEAR Sir/Mam,

It was very easy to crack with ***crack station*** wordlist or ***rockyou.txt*** ,I would suggest that you use very strong password mechanism to create hashes for the password based on Secure Hash Algorithm.

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 is an ***iterative*** hash function

* MD5 is generally a ***considerable mechanism*** for storing passwords in production.
* MD5 produces a ***128-bit hash.***
* MD5 is born out of ***RSA’s algorithm*** .
* MD5 is a utility that can ***generate a digital signature of a file (SHA)****.*it belongs to a family of one-way hash functions called***message digest algorithms***. The MD5 system is ***defined in* *RFC 1321***.
* The algorithm takes as input a message of ***arbitrary length*** and produces as output a ***128-bit "fingerprint"*** of the input called ***Secure Hash Algorithm.*** It is conjectured that it is ***computationally infeasible*** to produce two messages having the same message digest, or to produce any message having a given prespecified target message digest. The MD5 algorithm is ***intended for* *digital signature applications***, where a large file must be ***"compressed"*** in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as ***RSA.***

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

Answer:

One way of making the password hard to crack is by ***maintaining credentials from multitude of* *services in a manager*** like dash lane because they tend to use ***varied hashing*** algorithms & even hashing over hashed passwords to store and keep the ***strength high***, meeting to the rigidity of a strong case for an algorithm to process.

* ***Reduce redundancy*** across services such that in case of a leak out of one service doesn’t make the ***other passwords vulnerable.***
* ***Use alphanumeric and special character character*** with ***special characters***  Reducing occurrence of an ***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.)?

A: It can be very well determined that the organization's ***password policy is not up to the* *mark*** as:

* A strong password must be at ***least 8 characters*** long.
* It should not contain any of your ***personal information***—specifically your real name, user name, or even your company name.
* It must be very ***unique from your previously*** used passwords.
* It should not contain any word spelled completely.
* It should contain characters from the four ***primary categories, including***: uppercase letters, lowercase letters, numbers, and characters.

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

* Your password should be ***easy*** for you to remember but ***difficult*** for others to guess.
* Your password should be different than the passwords you use to log into other accounts, like your email or bank account.
* Longer passwords are usually more secure.
* Your password should not be your email, phone number or birthday.

AKSHAY ANANDRAO KOKADWAR