|  |
| --- |
| Username hash function password |
| |  | | --- | | Experthead e10adc3949ba59abbe56e057f20f883e 123456 | | Interested 25f9e794323b453885f5181f1b624d0b 123456789 | | Ortspoon d8578edf8458ce06fbc5bb76a58c5ca4 qwerty | | Reallychel 5f4dcc3b5aa765d61d8327deb882cf99 password | | simmson56 96e79218965eb72c92a549dd5a330112 111111 | | Bookma 25d55ad283aa400af464c76d713c07ad 12345678 | | popularkiya7 e99a18c428cb38d5f260853678922e03 abc123 | | eatingcake1994 fcea920f7412b5da7be0cf42b8c93759 1234567 | | edi\_tesla89 6c569aabbf7775ef8fc570e228c16b98 password! | | Liveltekah 3f230640b78d7e71ac5514e57935eb69 qazxsw | | blikimore 917eb5e9d6d6bca820922a0c6f7cc28b pa$$word1 | | johnwick007 f6a0cb102c62879d397b12b62c092c06 bluered | | moodie 8d763385e0476ae208f21bc63956f748 moodie00 | |

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

The type of Hashing Algorithm used is MD5 (Message Direct Algorithm).

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

The level of protection provided by MD5 hashing algorithm is very poor as it generates same hash function for different output. Hacker can compute large number of passwords per second. It is neither a symmetric nor asymmetric algorithm.

Q4 - What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?

Using Hashing algorithm which is better than MD5, for example. SHA256 (which is also used in blockchain). Salts much be used as it provide extra layer of protection and different hash function is created for same password. Using Algorithm which are very slow like bcrypt which require huge computational power to be executed.

Q5 - What can you tell about the organization’s password policy?

Using weak hashing algorithm without using Salts, Common password is being used which is very easy to be cracked, no use of any special characters, number, capital letters in the password and the length of password is small (8-9 letters)

Q6- What would you change in the password policy to make breaking the passwords harder?

Increase password length from 8-9 letters to 12 letters which make cracking password more difficult, checking if password is a mix of special characters, numbers, capital letter or not, if not then ask employee to rewrite the password including special characters.