

experthead:e10adc3949ba59abbe56e057f20f883e MD5  
Result: 12345

interestec:25f9e794323b453885f5181f1b624d0b MD5  
Result:123456789

ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 MD5  
Result:qwerty

reallychel:5f4dcc3b5aa765d61d8327deb882cf99 MD5  
Result:password

simmson56:96e79218965eb72c92a549dd5a330112 MD5  
Result:111111

bookma:25d55ad283aa400af464c76d713c07ad MD5  
Result:12345678

popularkiya7:e99a18c428cb38d5f260853678922e03 MD5  
Result:abc123

eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 MD5  
Result:1234567

heroanhart:7c6a180b36896a0a8c02787eeafb0e4c MD5  
Result:password1

edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 MD5  
Result:password!

liveltekah:3f230640b78d7e71ac5514e57935eb69 MD5  
Result:qazxsw

blikimore:917eb5e9d6d6bca820922a0c6f7cc28b MD5  
Result:pa\$\$word1

johnwick007:f6a0cb102c62879d397b12b62c092c06 MD5  
Result:bluered

flamesbria2001:9b3b269ad0a208090309f091b3aba9db MD5  
Result:

oranolio:16ced47d3fc931483e24933665cded6d MD5  
Result:

spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e MD5

moodie:8d763385e0476ae208f21bc63956f748 MD5  
Result:

nabox:defebde7b6ab6f24d5824682a16c3ae4 MD5

Result:

bandalls:bdda5f03128bcbdfa78d8934529048cf MD5

Result:

- Some of the hashes are (MD5)message Digest hashing algorithm and some of them are not found.
- It is very easy to use the aircrack-ng cracking tool and with the wordtxt possible passwords.txt file.
- The hashes are given are in the MD5 hashing algorithm.It can crack instantly, by using the aircrack-ng and password are very weak it seems.that the user did not used any other upper case letters,numbers and symbols.
- The reference website (<https://www.security.org/how-secure-is-my-password/>)to now know the password strength that I have used.
- We should give the strong password suggestions,like using symbols and numbers,when user is creating.
- We should give the conditions to the user while creating the password.That password should contain lower case,upper case, numbers and symbols.
- The minimum length of the password should more than 6 to 10 letters.
- And we should use the hashing algorithms like SHA-512,Whirlpool and RIPEMD-320 etc.
- By this things that we can minimize the successful breach.
- Avoid common words and character combinations in your password.
- Longer passwords are better, 8 characters is a starting point.
- Don't reuse your passwords.
- Include special character, Capital and Small letters, numbers in your password.
- Don't let users include their username, actual name, date of birth and other personal information while creating a password.
- Train your users to follow these policies to keep their passwords safe.

