To whom it may concern,

I have reviewed the attached file and compiled the usernames with corresponding passwords that I was able to crack in the table attached below. The usernames without corresponding passwords were ones with stronger passwords, and are more difficult to crack.

Username	Password
experthead	123456
interestec	123456789
ortspoon	qwerty
reallychel	password
simmson56	111111
bookma	12345678
popularkiya7	abc123
eatingcake1994	1234567
heroanhart	password1
edi_tesla89	password!
liveltekah	qazxsw
blikimore	Pa$$word1
johnwick007	bluered
flamesbria2001	
oranolio	
spuffyffet	
moodie	moodie00
nabox	
bandalls	

The hashing algorithm that was used to protect the passwords was MD5, which is not the best option to use for passwords, as it is easily breakable. Out of 19 passwords, 14 were cracked with minimal effort. There is very little protection, as the MD5 hashing algorithm fails the very basic property of any cryptographic hash function, which is to make it infeasible to find two different messages that hash to the same function. The only benefit that this algorithm provides is fast hashing, which is the exact reason why this algorithm offers minimal password protection. With fast hashing comes less protection. Thus, brute force attacks are more likely to crack passwords using this algorithm over others.

To make cracking more difficult, the company should consider implementing a two factor authentication policy, which often deters hackers. Even if a hacker has the ability to crack the password, they may not have access to the client's cell phone or email address, making the probability of a successful breach minimal. Changing the hashing algorithm from MD5 to bcrypt seems to be a better option as well.

The password policy seems to be very lenient, with a minimum character length of 6. There is no combination of letters, numbers, or symbols necessary for the client to input, making many passwords very weak. Capitalization can occur at any point, but is not required. My recommendation would be to require clients to have passwords with a length of 10-12 characters, and require a combination of letters, numbers, and a minimum of 3 symbols, which would make the time to crack passwords increase.

Thank you,

Vandana Thannir