Dear Sir/Ma'am,

I discovered multiple flaws in your password policy after attempting to break all of the stolen hashes, and this summary is all of my findings and recommendations for improving your password policy.

The main cryptographic hash algorithms for data security and authentication are Secure Hash Algorithm (SHA) and Message Digest (MD5).

MD5, a weaker hash technique prone to collisions, was used in all of the passwords that were hacked.

Using md5online.org and the rockyou.txt wordlist via terminal and online browsers, it was fairly simple to break.

To generate hashes for the password, I recommend using a highly strong password encryption technique based on SHA.

After breaking the passwords, we get the following information about the organization:

- The password must be at least six characters long.
- There are no precise requirements for creating a password. To construct a password, users can use any combination of words and characters.

You may add a few extra features to your password policy. My suggestions are as follows:

- In your password, avoid using popular phrases and character combinations.
- Longer passwords are preferable; 8 characters is a good start.
- Passwords should not be reused.
- In your password, include unusual characters, capital and small letters, and digits.
- Allow users to create passwords without using their username, real name, date of birth, or other sensitive information.
- To keep their passwords safe, teach your users to follow these principles.

Thanking you !

Rahul Kumar

B.tech Civil Engineering

Security Algorithms used:

```
experthead:e10adc3949ba59abbe56e057f20f883e – MD5
interestec:25f9e794323b453885f5181f1b624d0b – MD5
ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 –MD5
reallychel:5f4dcc3b5aa765d61d8327deb882cf99 –MD5
simmson56:96e79218965eb72c92a549dd5a330112 – MD5
bookma:25d55ad283aa400af464c76d713c07ad – MD5
popularkiya7:e99a18c428cb38d5f260853678922e03 – MD5
eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 – MD5
heroanhart:7c6a180b36896a0a8c02787eeafb0e4c – MD5
edi_tesla89:6c569aabbf7775ef8fc570e228c16b98 – MD5
liveltekah:3f230640b78d7e71ac5514e57935eb69 – MD5
blikimore:917eb5e9d6d6bca820922a0c6f7cc28b – MD5
johnwick007:f6a0cb102c62879d397b12b62c092c06 – MD5
flamesbria2001:9b3b269ad0a208090309f091b3aba9db – MD5
oranolio:1Fxu7L83m1qDUM84fvsrQN3iwEjaxeRLEy - MD5
spuffyffet:1f5c5683982d7c3814d4d9e6d749b21e - MD5
moodie:8d763385e0476ae208f21bc63956f748 - MD5
nabox:defebde7b6ab6f24d5824682a16c3ae4 - MD5
bandalls:bdda5f03128bcbdfa78d8934529048cf - MD5
```

Cracked Passwords:

MD5 Hash	Status	Result
e10adc3949ba59abbe56e057f20f883e	Cracked	123456
25f9e794323b453885f5181f1b624d0b	Cracked	123456789
d8578edf8458ce06fbc5bb76a58c5ca4	Cracked	qwerty
5f4dcc3b5aa765d61d8327deb882cf99	Cracked	password
96e79218965eb72c92a549dd5a330112	Cracked	111111
25d55ad283aa400af464c76d713c07ad	Cracked	12345678
e99a18c428cb38d5f260853678922e03	Cracked	abc123
fcea920f7412b5da7be0cf42b8c93759	Cracked	1234567
7c6a180b36896a0a8c02787eeafb0e4c	Cracked	password1
6c569aabbf7775ef8fc570e228c16b98	Cracked	password!
3f230640b78d7e71ac5514e57935eb69	Cracked	qazxsw
917eb5e9d6d6bca820922a0c6f7cc28b	Cracked	Pa$$word1
f6a0cb102c62879d397b12b62c092c06	Cracked	bluered
9b3b269ad0a208090309f091b3aba9db	Cracked	Flamesbria2001
1Fxu7L83m1qDUM84fvsrQN3iwEjaxeRLEy	Cracked	Spuffyffet12
8d763385e0476ae208f21bc63956f748	Cracked	moodie00
defebde7b6ab6f24d5824682a16c3ae4	Cracked	nAbox!1
bdda5f03128bcbdfa78d8934529048cf	Cracked	Banda11s