To: Goldman Sachs

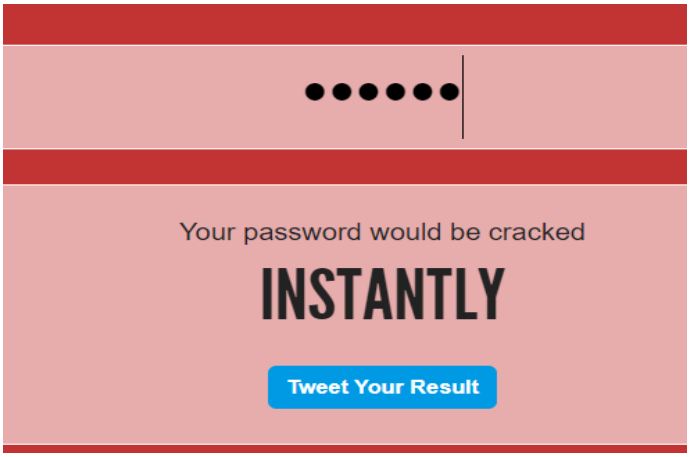
From: Tejas Adhikari(tejas.adhikari@somaiya.edu)

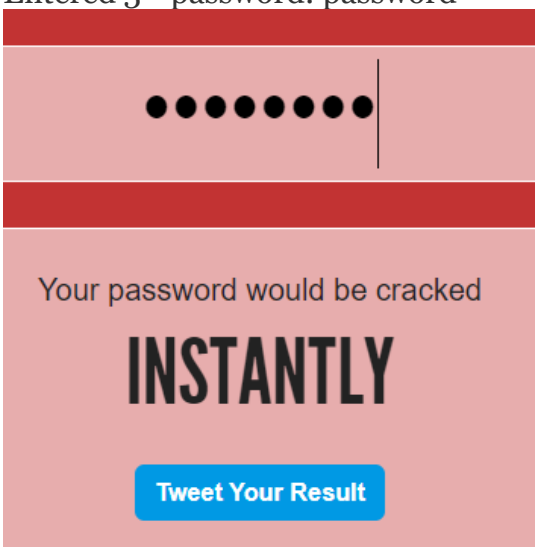
Subject: Crack leaked password database

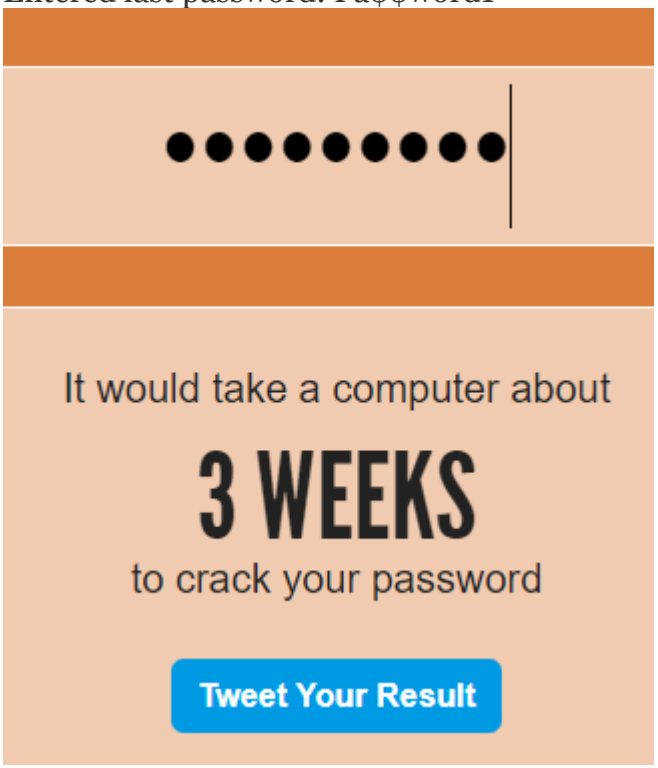
Date: 01/05/2021(dd/mm/yyyy)

Questions:

- **What type of hashing algorithm was used to protect passwords?**
  - MD5
- **What level of protection does the mechanism offer for passwords?**
  - I guess level 2 protection this mechanism offers as hashing and encrypting comes under level 2 protection for passwords
- **What controls could be implemented to make cracking much harder for the hacker in the event of a password database leaking again?**
  - Multiple tries like brute force should be eliminated, I have an idea but not so sure that it might work: Like Google sends an email if someone is trying to enter the password more than 3-4 times, so that the user gets alerted about someone trying to enter your account.
- **What can you tell about the organization's password policy (e.g. password length, key space, etc.)?**
  - From the resources provided, I checked one of the website which displays the password length, so at first lets check the passwords that are extracted from hashcat.
  - Following are the passwords:
    - e10adc3949ba59abbe56e057f20f883e:123456
    - 25f9e794323b453885f5181f1b624d0b:123456789
    - 5f4dcc3b5aa765d61d8327deb882cf99:password
    - fcea920f7412b5da7be0cf42b8c93759:1234567
    - 25d55ad283aa400af464c76d713c07ad:12345678
    - e99a18c428cb38d5f260853678922e03:abc123
    - d8578edf8458ce06fbc5bb76a58c5ca4:qwerty
    - 96e79218965eb72c92a549dd5a330112:111111
    - 7c6a180b36896a0a8c02787eeafb0e4c:password1
    - 6c569aabbf7775ef8fc570e228c16b98:password!
    - 3f230640b78d7e71ac5514e57935eb69:qazxsw
    - f6a0cb102c62879d397b12b62c092c06:bluered
    - 917eb5e9d6d6bca820922a0c6f7cc28b:Pa$$word1
  - Entering some of the passwords in the website(https://howsecureismypassword.net/)
  - Entered 1st password: 123456

- 

- Entered 3rd password: password
- 

- Entered last password: Pa$$word1
- 

    - I think mandating 1 uppercase, 1 special character, 1 lowercase character in the password, also the password length should be at least 8 characters.
- **What would you change in the password policy to make breaking the passwords harder?**
    - I would change the level of protection at first and after that adding validation rules such as password length, characters specification in the password. Also, if someone is trying the password more than 4-5 times, the user should be alerted via an email.

I would like to thank Goldman Sachs and Forage for this opportunity, It was fun learning as well exploring new fields. This opportunity helped me expand my knowledge. So, A big Thankyou.