# 

# Starter discussion questions?

**What are the 10 most commonly used passwords?**

**What is a hashing algorithm?**

# Scenario:

A network administrator has access to a database of user details for their own website. Passwords are not stored in plaintext but a hash of each users’ password is stored.

The admin suspects some of the users have weak passwords that are compromising the security of the network.

Your job is to discover which users have weak passwords so that the admin can force them to reset their passwords before their accounts are hacked.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **firstname** | **surname** | **username** | **hash** |
| 1 | Anthony | Johnson | ajohnson0 | F075E48000CE019587C1953BB925DCCD |
| 2 | Karen | Fisher | kfisher1 | E10ADC3949BA59ABBE56E057F20F883E |
| 3 | Carlos | Williamson | cwilliamson2 | B0F1296F3E4457FB6EBA127F3B5CCA73 |
| 4 | Jeffrey | Howell | jhowell3 | 715368C1933E8DD6B8DCB7C6B3D2DBD7 |
| 5 | Mildred | Torres | mtorres4 | 5F4DCC3B5AA765D61D8327DEB882CF99 |
| 6 | Marilyn | Butler | mbutler5 | 5AD65DDD958F193CC576D8CA6A017BBC |
| 7 | Samuel | Lawrence | slawrence6 | 841981280AF265485B929571466D82F9 |
| 8 | Keith | Wells | kwells7 | 35C62F282F9E85AB3E6D7382B3FC72D3 |
| 9 | Gregory | Nguyen | gnguyen8 | E75029090B49A3712BFFBC49A623713E |
| 10 | Diana | Gardner | dgardner9 | D8578EDF8458CE06FBC5BB76A58C5CA4 |

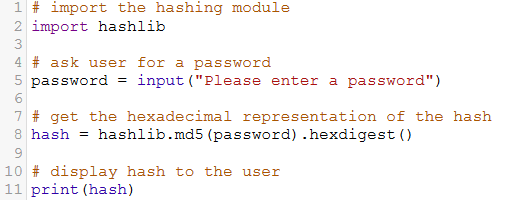
# Research and discussion Question Which users have weak passwords?

Can you tell from the hash alone? Hint – 3 hashes below are the result of using the MD5 hash function on one of the top 5 passwords used in 2017

# Notes:

# Create a MD5 generator tool in python:

You can generate hashes in python with the hashlib module



You can find and run a copy of this code here: <https://create.withcode.uk/python/Qj>

# Extension ideas:

1. Ask the user to input a salt as well as a password to your MD5 hash for additional security  
   *(HINT – a salt is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase)*

***Hint****: If your salt is “1234” and your password is “password”, you’d generate the MD5 hash of “1234password”*

1. Generate a SHA256 hash as well as a MD5

***Hint****: Use hashlib.****sha256*** *instead of hashlib.md5*

1. Generate a SHA512 hash as well as MD5

***Hint****: Use hashlib.****sha512*** *instead of hashlib.md5*

1. Write a program that will load a file and generate a MD5 digest of its contents

***Hint****:* [*http://stackoverflow.com/questions/3431825/generating-an-md5-checksum-of-a-file*](http://stackoverflow.com/questions/3431825/generating-an-md5-checksum-of-a-file) *discusses some different ways to do this*

1. Each of the following hashes are generated from a password that is a 4 digit numerical pin code. Write a program that will discover the password for any of the hashes below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ID** | **firstname** | **surname** | **username** | **hash** |
| 1 | Ernest | Reed | ereedk | B8002139CDDE66B87638F7F91D169D96 |
| 2 | Peter | Wells | pwellsl | 7EA25C95B0792CA4CE01EA18BBDA2D44 |
| 3 | Edward | Martin | emartinm | D39934CE111A864ABF40391F3DA9CDF5 |
| 4 | Martin | Weaver | mweavern | 024D2D699E6C1A82C9BA986386F4D824 |
| 5 | Jean | Hunter | jhuntero | D77C703536718B95308130FF2E5CF9EE |
| 6 | Catherine | Garza | cgarzap | 67606D48E361CE176CA71FD54FCF4286 |
| 7 | Jacqueline | Welch | jwelchq | B29EED44276144E4E8103A661F9A78B7 |
| 8 | Joseph | Ramos | jramosr | 109D2DD3608F669CA17920C511C2A41E |
| 9 | Judy | Perry | jperrys | 64D52E08CC03E6090BC1EF30B73CCB85 |
| 10 | Antonio | Sanchez | asanchezt | E643B33B3019892367371B27BC0E63C2 |

***Hint****: Use a for loop to generate a MD5 hash for each of the 9999 possible pin codes. Check if it matches one of the hashes above.*

**Note**: all user details in this example are randomly generated.