How to secure a password manager using the hash?

Problem-based learning (PBL) for students of the Advanced Algorithmics 1 course

Contextual information:

A password manager is a centralized tool for securely managing and organizing passwords associated with user accounts. To enhance security, the password manager uses encryption and hashing technologies to guarantee confidentiality and protect unauthorized access to information. The password manager offers the possibility of automatically generating complex, unique passwords to prevent the reuse of passwords and overcome their weakness against attacks.

Required work:

As a team of engineers, you want to create a secure password manager. This tool must allow you to import a file containing user data, and then perform the following tasks:

1. Generate a random, complex and unique password for each existing user. The password must contain :

- At least 12 characters
- At least one special character (@, !, #, %, $)
- At least one capital letter
- At least one number

2. Store the hashed password information in a new file. Only the administrator has access to this file.
3. Create new users via the graphical interface using Tkinter, specifying their full name, e-

mail address and a complex password according to the criteria required in 1.

4. Through the graphical user interface, a user can reset his password if the following authentication strategy is validated:

- Send a reset request by e-mail to the administrator from the GUI, specifying the user's full name.
- The administrator verifies the user's existence by e-mailing back the first five characters of the hashed password. For existing users, use a personal e-mail address.
- The user confirms his/her identity to the administrator by entering a code consisting of the five characters received, followed by the first letter of the surname, the last letter of the surname and the first letter of the first name.
- Once the code has been validated, the password reset page appears and the new password is added to the database.

Note :

1. You are authorized to use the smtplib, ssl and EmailMessage packages to send information by e-mail.
2. For security reasons, create a new e-mail address for the administrator.

Resources for dealing with the problem situation

1. The dataset
2. Course 4 and TD4
3. Files course
4. Tkinter graphical interfaces course

APP learning objectives:

1. Understand and master hashing algorithms.
2. Handle csv files.
3. Learn and master new libraries.