.**explanation of the main concepts**

what is password ?

A password is a word, phrase, or group of characters used to distinguish between an authorized user or process and an unauthorized user (in order to grant access). To put it another way, a password is used to establish identification or grant access to a resource.

Password strength :

Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it estimates how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly.

OWAPS :

The Open Worldwide Application Security Project® (OWASP) is a nonprofit foundation that works to improve the security of software.

As a part of their general advice on web application security, OWASP offers password standards. Developers and organizations can make more secure password policies and contribute to user account protection by adhering to OWASP's password standards.

The following password requirements are recommended by OWASP: passwords should be at least 12 characters long, contain a combination of uppercase and lowercase letters, numbers, and special characters, not contain common words, phrases, or patterns, be stored securely and encrypted, expire periodically, and users should be required to change them. Web applications should also implement password policies to encourage users to create strong passwords, restrict failed login attempts, and provide other security features.

**main components:**

* User Input: The password that the user enters is collected by this component.
* Password Strength Checker: This feature assesses the password's strength using OWASP recommendations.
* Output: The user obtains the result of the password strength measurement by this component.

**functionnal flow**

The functional flow of a password security project would involve the following steps:

* A user creates a password and submits it for testing.
* The password strength tester evaluates the password based on OWASP standards, such as length, complexity, and uniqueness.
* If the password meets the recommended standards, it is accepted and stored securely. If not, the user is prompted to create a stronger password that meets the requirements.
* The password policy enforcer ensures that all passwords created by users adhere to the recommended standards.
* The password storage module encrypts and securely stores passwords to prevent unauthorized access.
* The password expiration and change module prompts users to change their passwords periodically to reduce the risk of compromise.