Implementation of the authentication

Which files to modify and why?

To manage the authentication process, it is necessary to understand the following files:

- src/Controller/SecurityController.php
  → manages the authentication page and its form

- src/Security/AppAuthenticator.php
  → manages authentication process: user loading + password verification

- config/packages/security.yaml
  → defines the entity used for authentication and the property used as identifier (ex: email)
  → defines the authenticator to use (currently AppAuthenticator.php)
  → defines which hash is used for authentication (currently auto)
  → restricts access to certain pages or groups of pages by defining roles

How the authentication works

This is how authentication works:

- The user enters his credentials on the authentication page (/login)
- The authentication process is managed by the AppAuthenticator.php file.
- Once the user's credentials are verified, the user is loaded as well as his rights to allow or deny access to the pages according to the level of authorization defined for each page

See Symfony Security and Custom Authenticator.

Users storage

Users are stored in the database in a table called "user".

This table has the following fields:

- username
- email
- password : the password is hashed (one way)
- roles : contains the user's rights as in array

Additional information

See Contributing Documentation and Symfony Documentation.