

# Lab 9: Authentication and Authorization

---

## Objective

The objective of this lab is to implement an authentication mechanism for the social network developed during the course, using the [Flask-Login](#) module.

## Activity Description

1. On the main screen of the user interface, you must add a login form. This form should include two fields: one for the username and one for the password. In addition, a button is required to submit the login request. At the same time, create a dedicated route on the server that checks the data entered by the user and, if appropriate, authenticates them in the social network using **Flask-Login**.
2. Under the login form, include a link that redirects users who are not yet registered to a dedicated registration page. This page will contain a complete form for entering all the data needed to register a new user on the platform, with client-side validations.  
At the same time, create a dedicated route on the server that handles the collection of the data entered in the registration form and adds the new user to the database. It is recommended to use [werkzeug.security](#) to hash the password before saving it in the database.
3. Make changes to restrict the actions of unauthenticated users: prevent the creation of new posts and comments. For authenticated users, the navbar will display a welcome message and a logout link/button. In addition, the user's posts will be highlighted with a colored background, and it will be possible to add new posts and comments.  
Make sure these changes are applied both in the user interface, where the components for creating posts and comments will be hidden from unauthenticated users, and on the server. On the server, you will need to add the `@login_required` decorators to the relevant functions to prevent access by unauthenticated users.
4. When the logout button is clicked, log the user out of the platform by using an appropriate route on the server.

**NOTE:** from now on, created posts and comments will automatically be associated with the user currently authenticated in the application.