

FACULTY OF COMPUTING AND TELECOMMUNICATION
Institute of Computing Science



WliT - Cybersecurity

“Web application project”

APPLICATION SECURITY

Supervisor dr inż. Michał...

By Hicham Kernaf

POZNAŃ 2024

Table of Contents

1. Introduction	3
1.1. Goals	3
2. Application description	4
2.1. Requirements	4
2.1.1. Functional	4
2.1.2. Non-Functional	4
3. Architecture	5
3.1. Tech stack	5
3.2. Database structure	6
4. UML diagrams	8
4.1. Register account	8
4.2. Login account	10
4.3. Password reset	12
5. Web application features	14
6. Graphical interface design.	16

1. Introduction

For the Application Security subject, we have created a safe web application with a possibility to create accounts with distinct usernames and safely secured information about those accounts like password and email.

1.1. Goals

- Design, development and maintenance of web applications.
- Design and implementation of a secure web application.
- Development of system design documentation containing:
 - functional and non-functional requirements of the application,
 - UML diagrams,
 - database schema,
- Application should have a public side and a management side which is accessible only for trusted users.

2. Application description

We have created a web application that allows users to download books and give feedback . The app has an implemented registration and login features with username and strong password checks. There is also a forgot password feature which sends out a token to an email provided by the user.

2.1. Requirements

2.1.1. Functional

- registration, login and forgot password implementation,
- password strength check,
- unique email and username check,
- email verification,
- safe database for user information,
- session management
- book publication and feedback features.
- Comment control.

2.1.2. Non-Functional

- Clear and simple UI,
- Securing the webApp in terms of Owasp Top10.

3. Architecture

3.1. Tech stack

The application is built using the python web framework Django plus the integration of the cookiecutter Package. The database used is PostgreSQL.

Dependency	Version
Python	3.11.4
Django	3.1.1
Cookiecutter	2.5
django-allauth	0.42
django-crispy-forms	1.9.2
django-anymail	8.0
psycopg2	2.8.6

Table 1: Project dependencies

Python is a high-level, general-purpose programming language. Its design philosophy emphasizes code readability with the use of significant indentation.

Django is a free and open-source, Python-based web framework that runs on a web server. It follows the model–template–views architectural pattern.

Cookiecutter is a Python open source library for building coding project templates.

Django-allauth is a Django package that provides a set of views, templates, and helper functions to handle user authentication, registration, and account management.

Django-crispy-forms is an application that helps to manage Django forms. It allows adjusting forms' properties (such as method, send button or CSS classes) on the backend without having to re-write them in the template

django-anymail lets you send and receive email in Django using your choice of transactional email service providers (ESPs)

Psycopg2 is the most popular PostgreSQL database adapter for the Python programming language. Its main features are the complete implementation of the Python DB API 2.0 specification and the thread safety (several threads can share the same connection).

3.2. Database structure

the database consist of the following relational tables:

<input type="checkbox"/>	Name	Data type	Not NULL?	Primary key?
<input type="checkbox"/>	id	bigint	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	password	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	last_login	timestamp with time zo...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	is_superuser	boolean	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	username	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	first_name	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	last_name	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	email	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	is_staff	boolean	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	is_active	boolean	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	date_joined	timestamp with time zo...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	name	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Table 2: Users database table

<input type="checkbox"/>	Name	Data type	Not NULL?	Primary key?
<input type="checkbox"/>	id	integer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	email	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	verified	boolean	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	primary	boolean	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	user_id	bigint	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Table 3: Account email address database table

<input type="checkbox"/>	Name	Data type	Not NULL?	Primary key?
<input type="checkbox"/>	id	integer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	created	timestamp with time zo...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	sent	timestamp with time zo...	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	key	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	email_address_id	integer	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Table 4: Account email confirmation database table

<input type="checkbox"/>	Name	Data type	Not NULL?	Primary key?
<input type="checkbox"/>	id	bigint	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	title	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	author	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	pdf	character varying	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	cover	character varying	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	description	text	<input type="checkbox"/>	<input type="checkbox"/>

Table 5: Books database table

<input type="checkbox"/>	Name	Data type	Not NULL?	Primary key?
<input type="checkbox"/>	id	bigint	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	text	text	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	created_date	timestamp with time zo...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	book_id	bigint	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	user_id	bigint	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Table 6: Books comments database table

4. UML diagrams

4.1. Register account

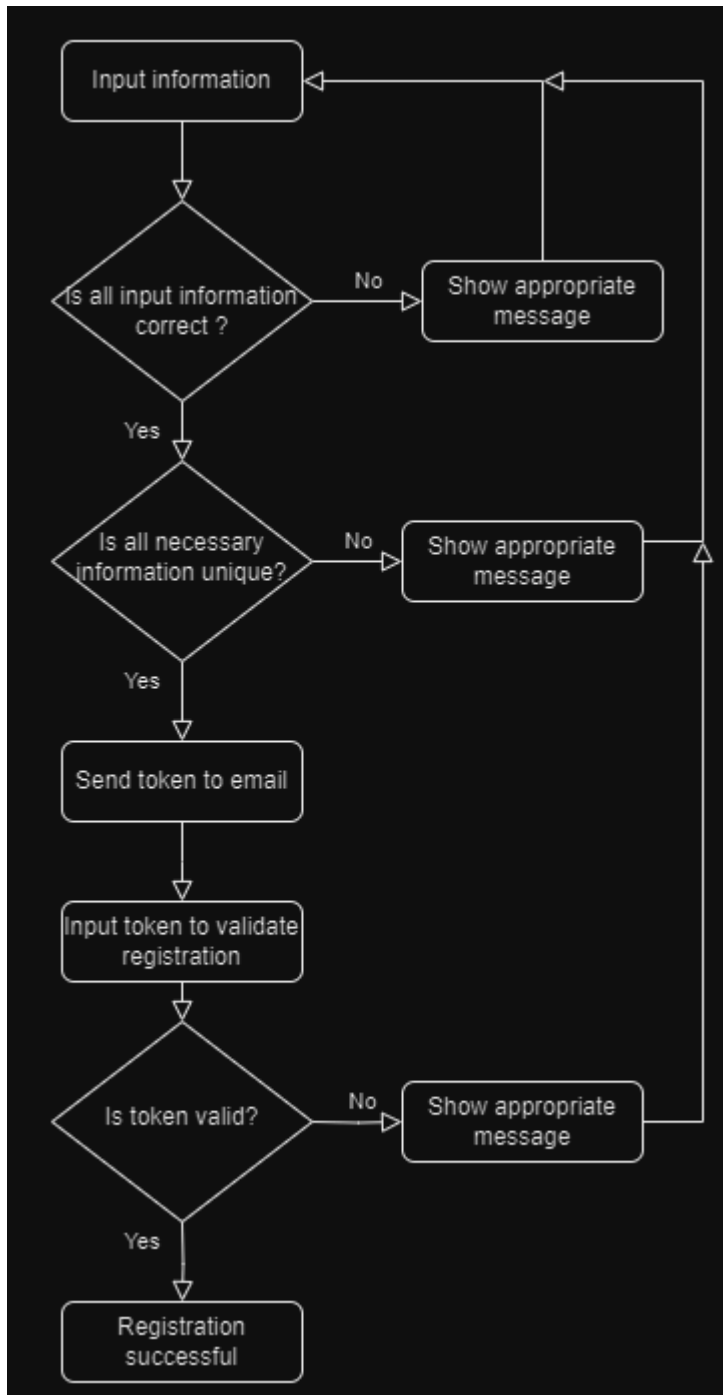


Figure 1: Account registration UML diagram

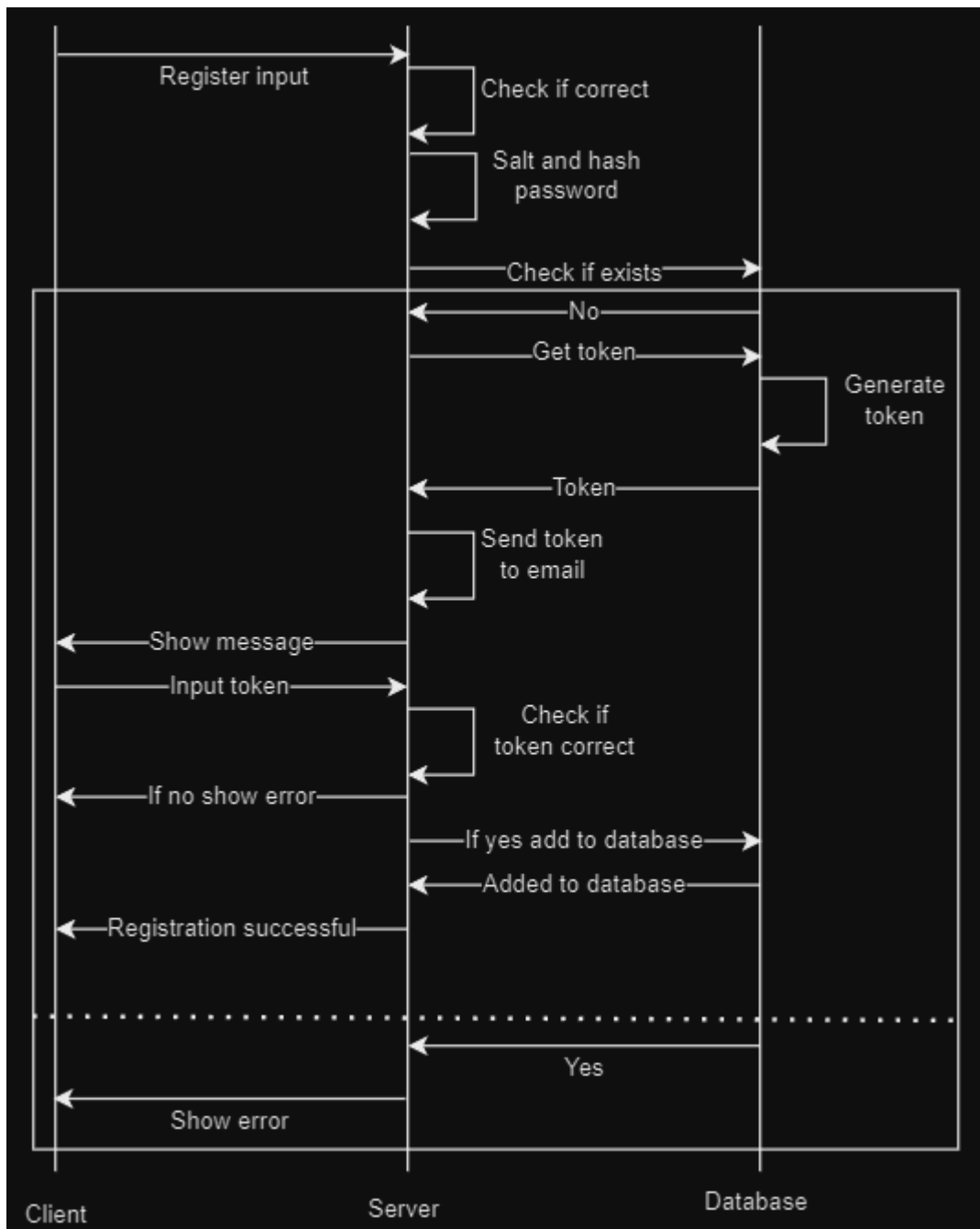


Figure 2: Account registration sequence diagram

4.2. Login account

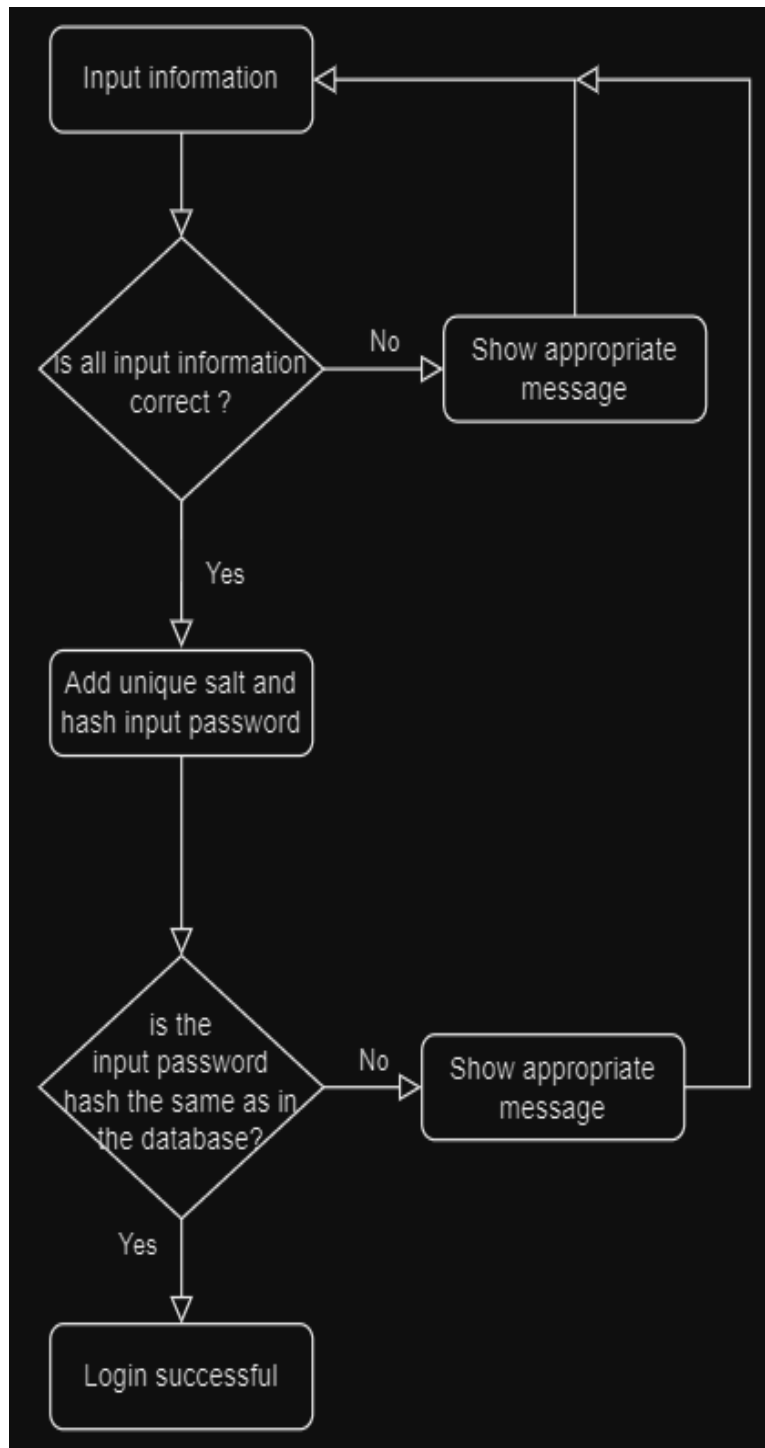


Figure 3: Account login UML diagram

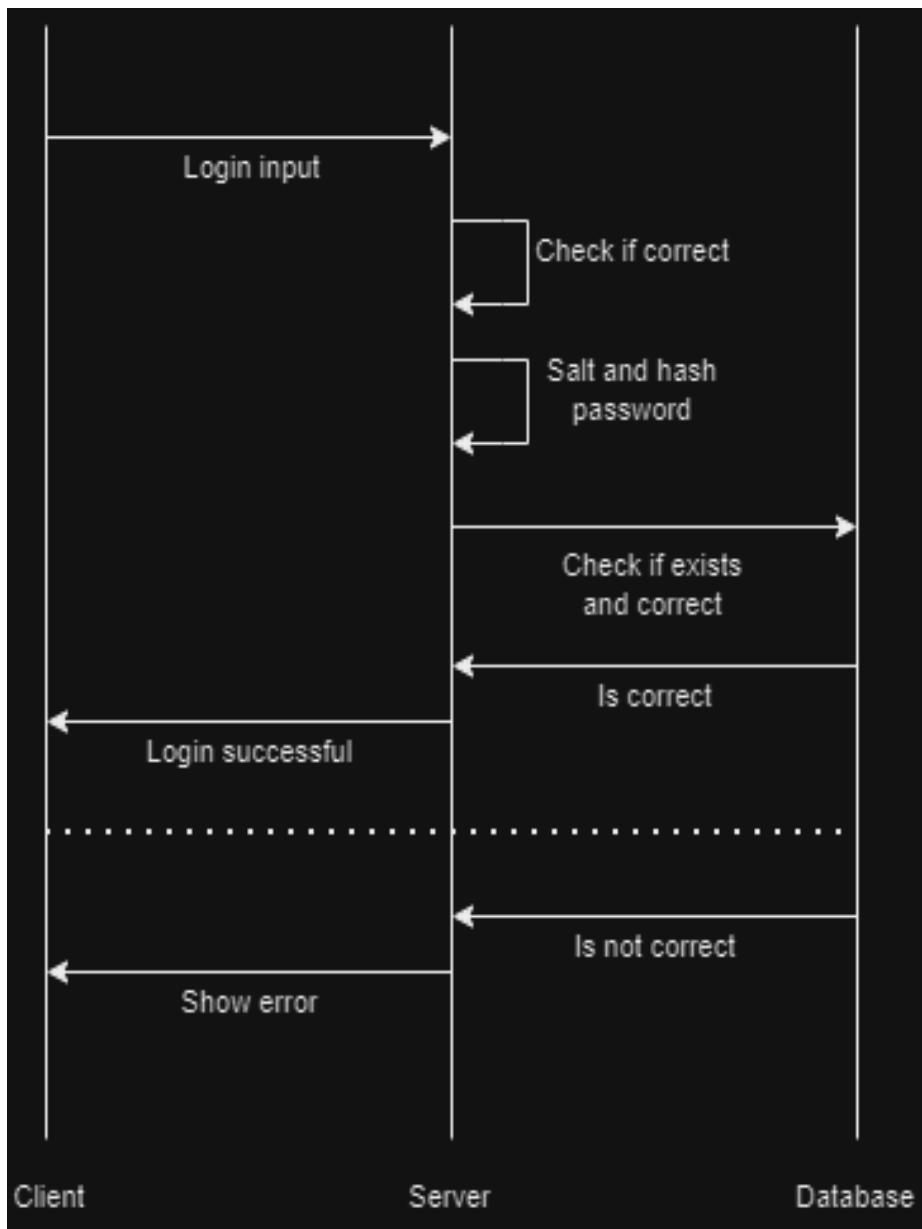


Figure 4: Account login sequence diagram

4.3. Password reset

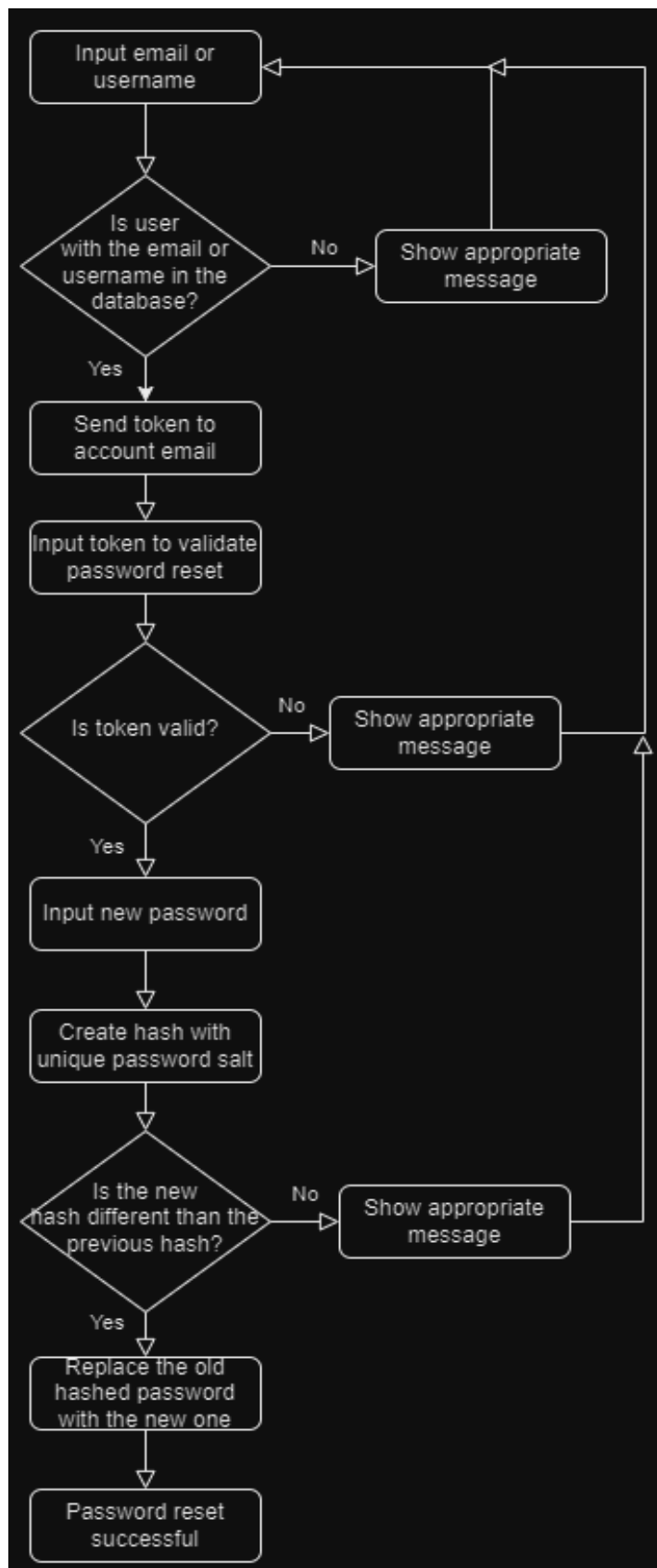


Figure 5: Forgot password UML diagram

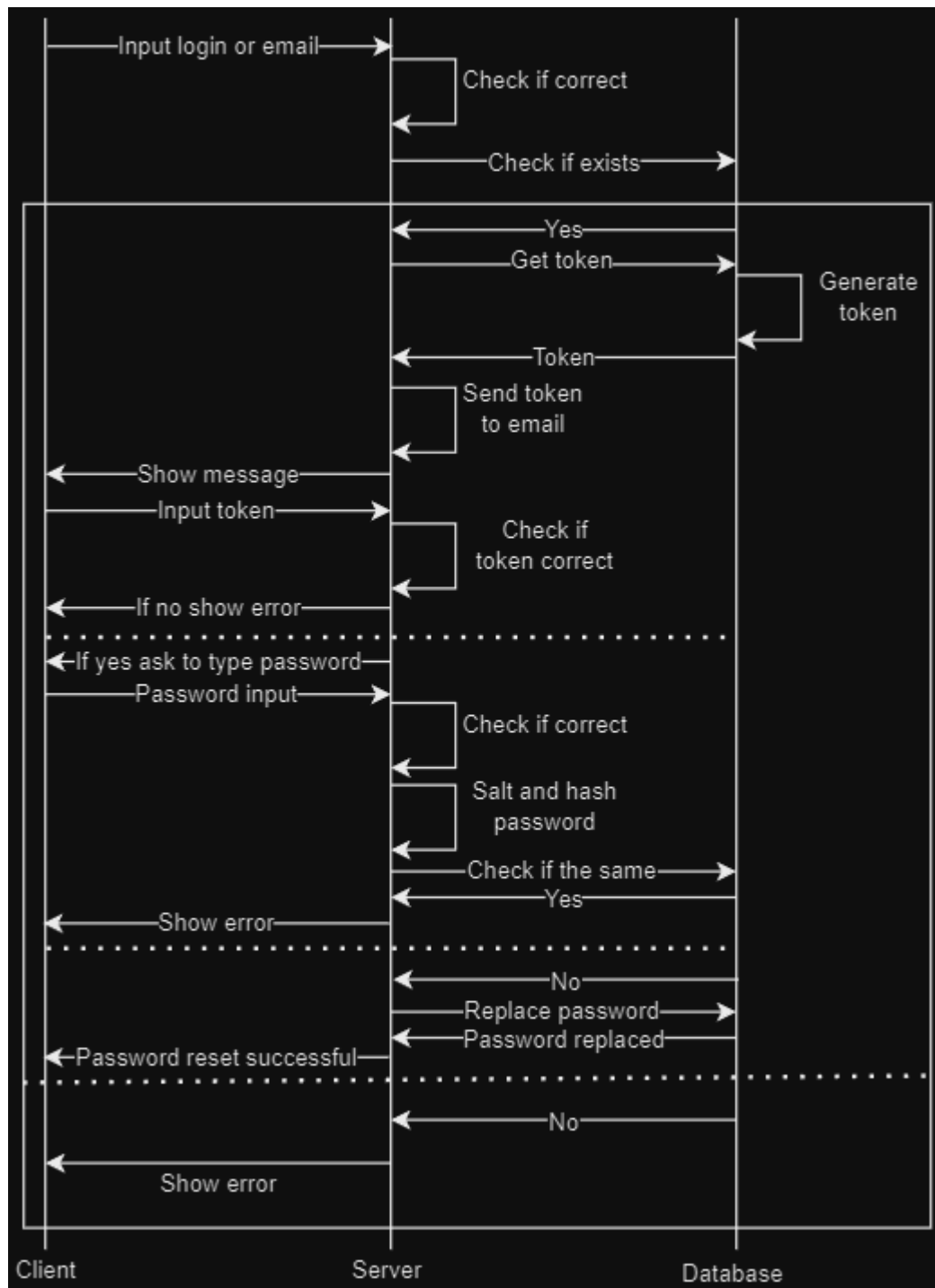


Figure 6: Forgot password sequence diagram

5. Web application features

The web app is built on the Ability of the Admin to edit ,delete and publish pdf books with title, an author name, a cover and a description of the book.

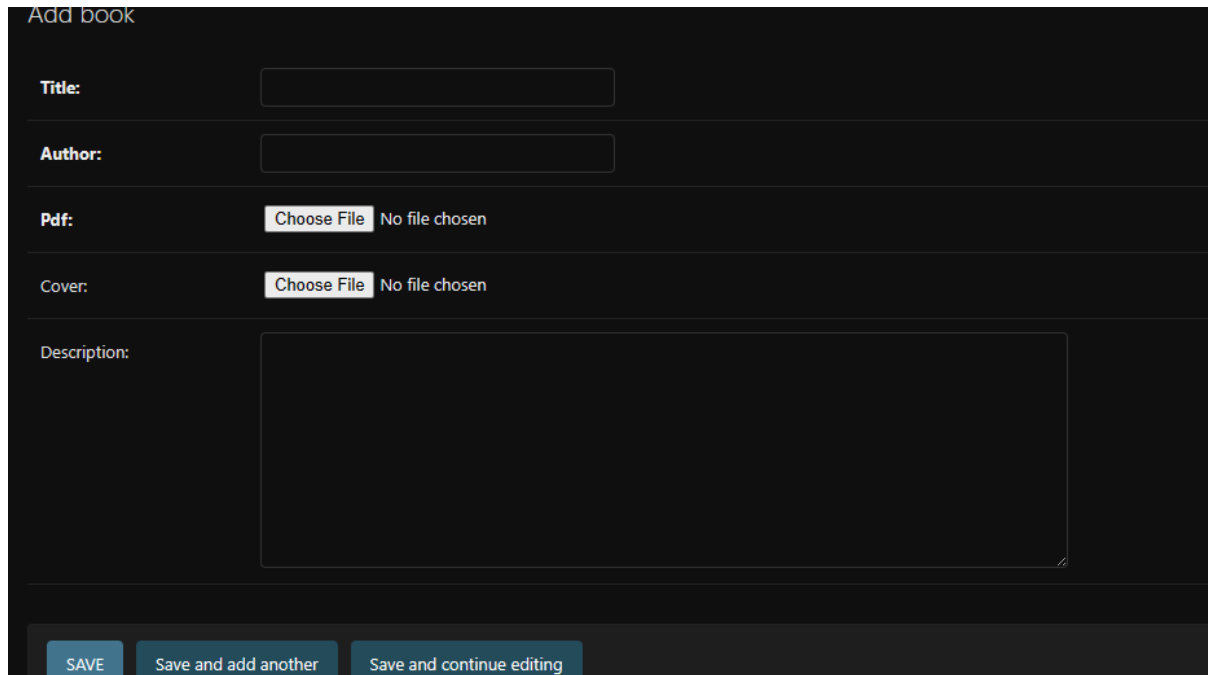


Figure 7: Page with adding book functionality

in case the user was not signed in, he can only download the books without commenting.

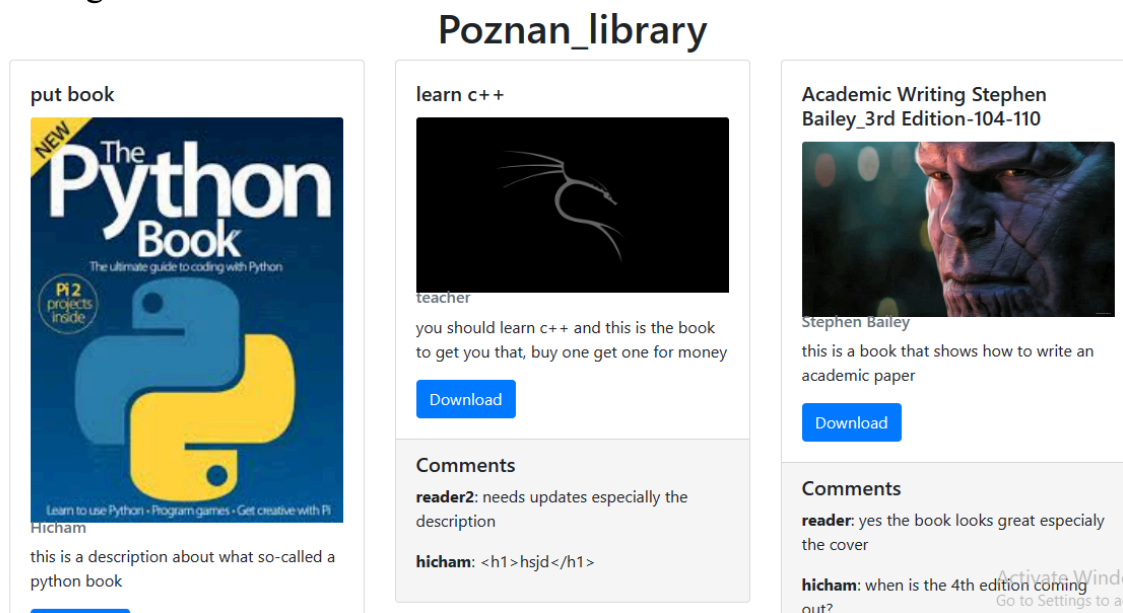


Figure 8: Non signed in user view.

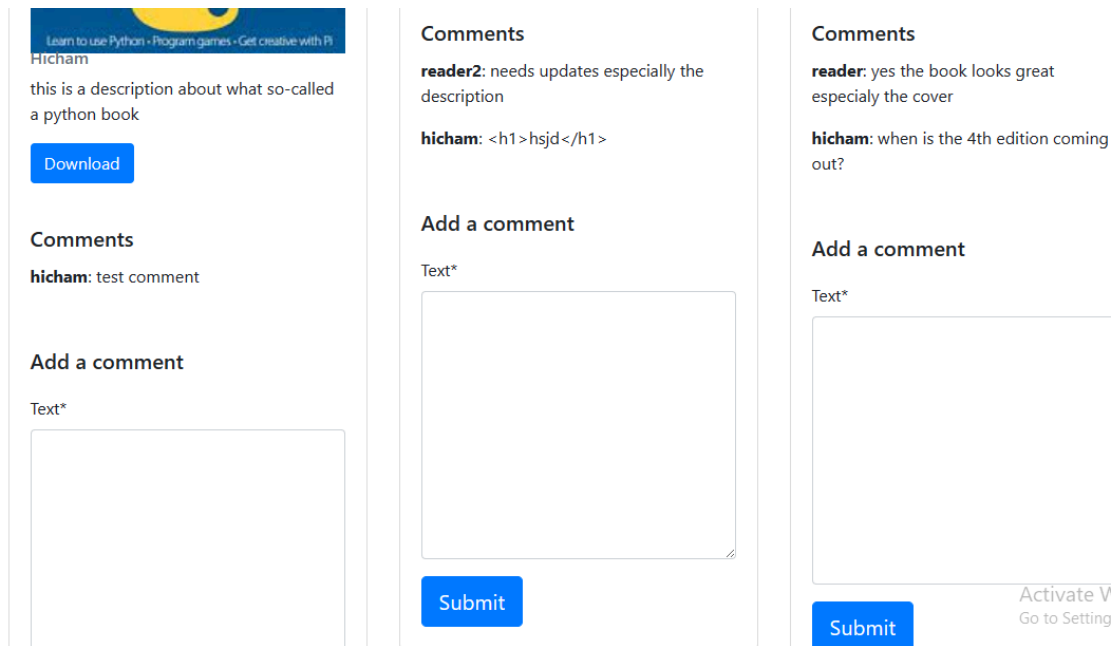


Figure 8: Signed in user view.

The admin can edit user's comment or delete them:

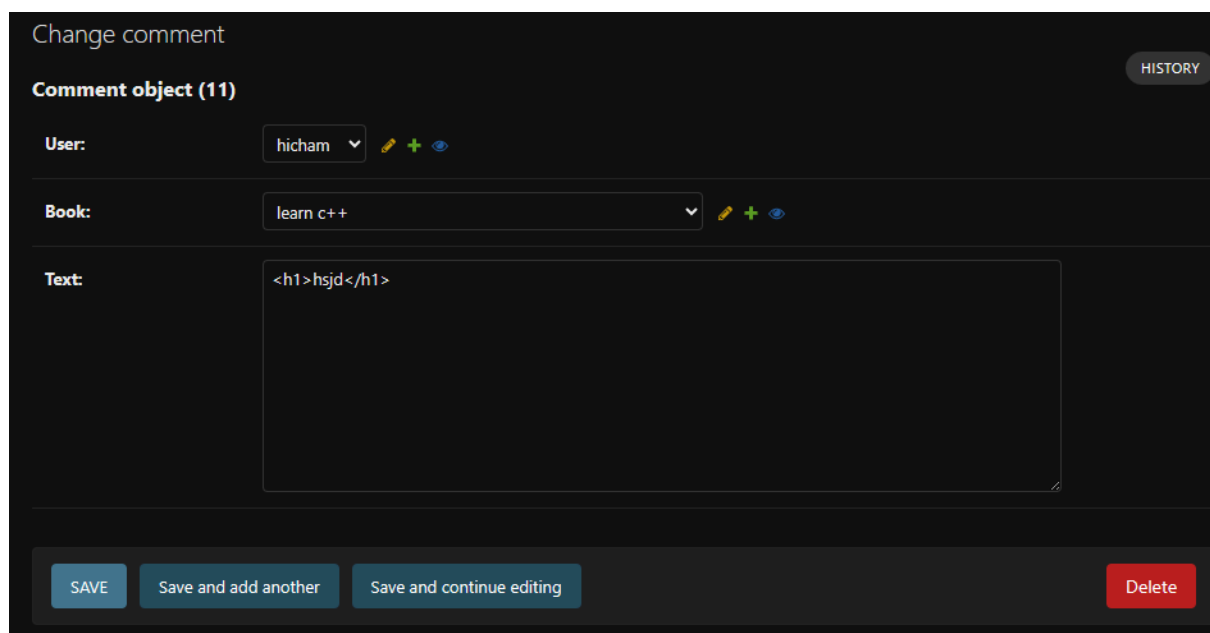
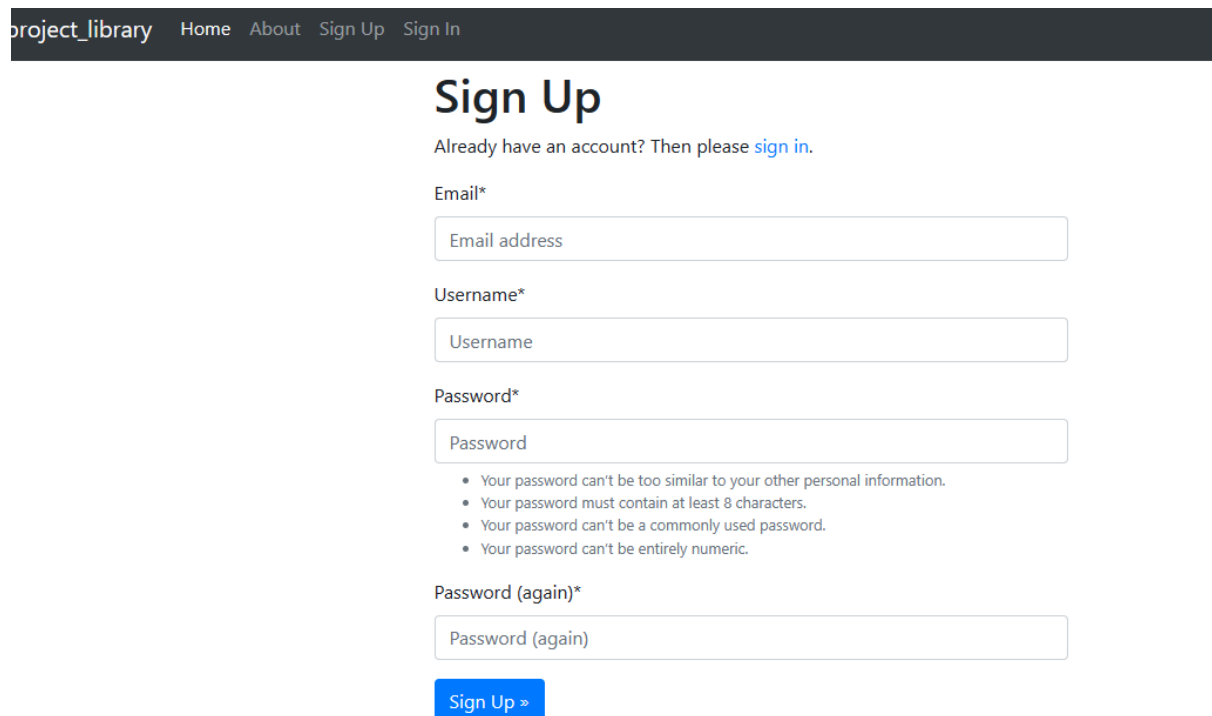


Figure 8: Admin comment control page.

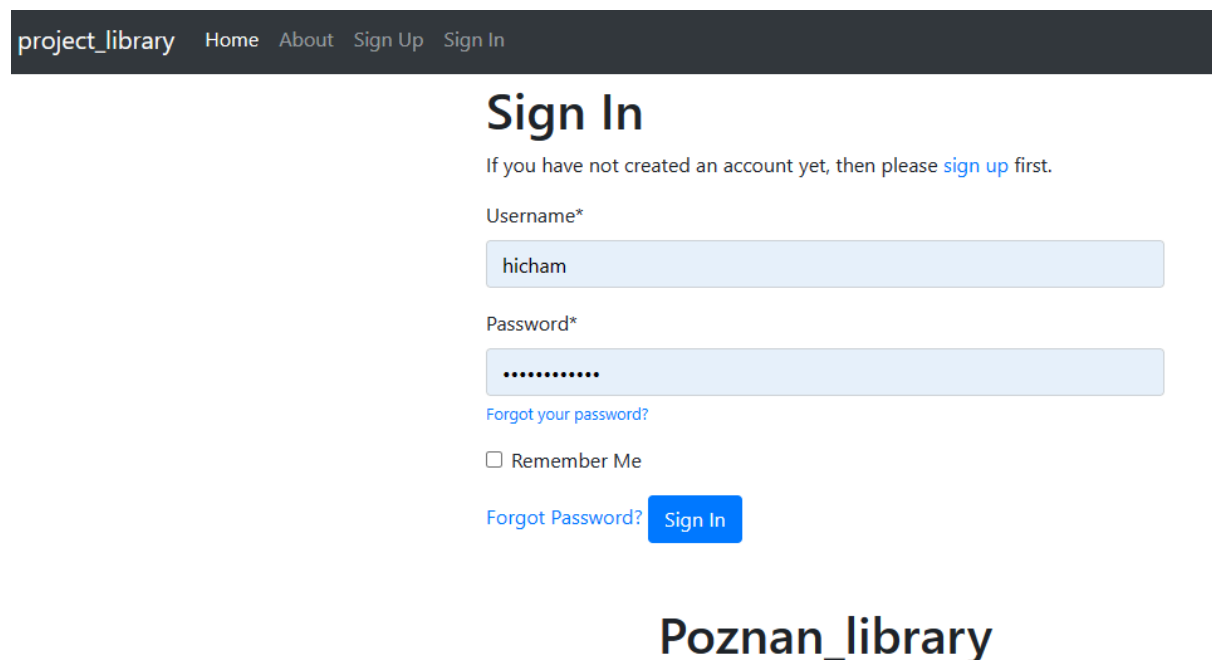
6. Graphical interface design.

The interface was created with simplicity and intuitiveness in mind.



The screenshot shows the 'Sign Up' page of the 'project_library' application. The page has a dark header with navigation links: 'project_library', 'Home', 'About', 'Sign Up', and 'Sign In'. The main heading is 'Sign Up'. Below it, a message says 'Already have an account? Then please [sign in](#).' The form consists of four input fields: 'Email*' (placeholder 'Email address'), 'Username*' (placeholder 'Username'), 'Password*' (placeholder 'Password'), and 'Password (again)*' (placeholder 'Password (again)'). Below the password fields, there are four bullet points providing password requirements: 'Your password can't be too similar to your other personal information.', 'Your password must contain at least 8 characters.', 'Your password can't be a commonly used password.', and 'Your password can't be entirely numeric.' At the bottom of the form is a blue button labeled 'Sign Up »'.

Figure 7: Sign up page



The screenshot shows the 'Sign In' page of the 'Poznan_library' application. The page has a dark header with navigation links: 'project_library', 'Home', 'About', 'Sign Up', and 'Sign In'. The main heading is 'Sign In'. Below it, a message says 'If you have not created an account yet, then please [sign up](#) first.' The form consists of two input fields: 'Username*' (containing the text 'hicham') and 'Password*' (containing masked characters '.....'). Below the password field, there is a link 'Forgot your password?'. Below that is a checkbox labeled 'Remember Me'. At the bottom of the form is a blue button labeled 'Sign In'.

Figure 8: Sign in page

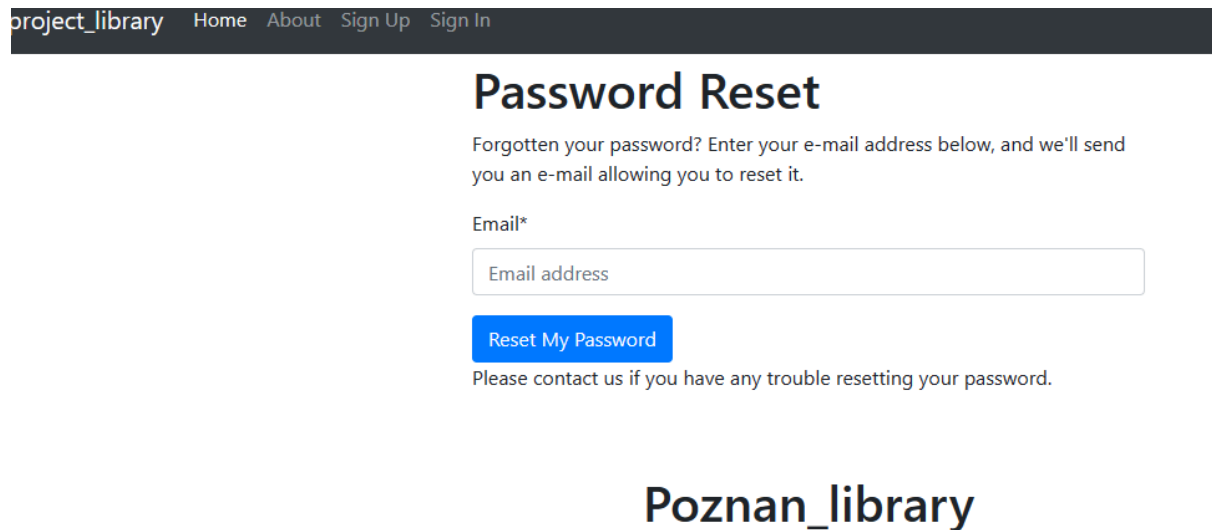


Figure 9: Password reset page

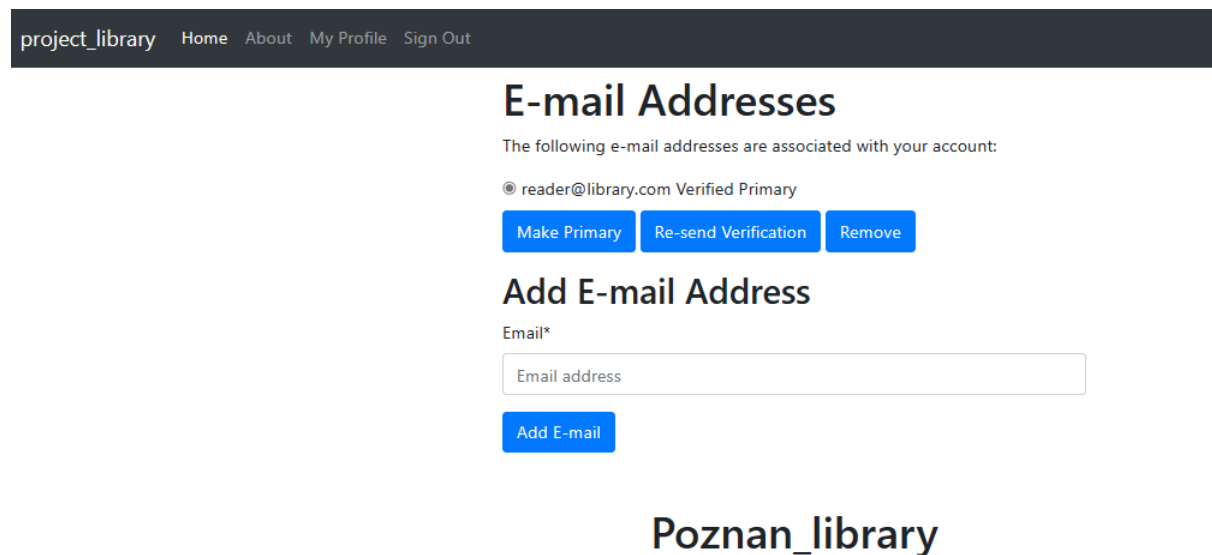


Figure 10: User profile page

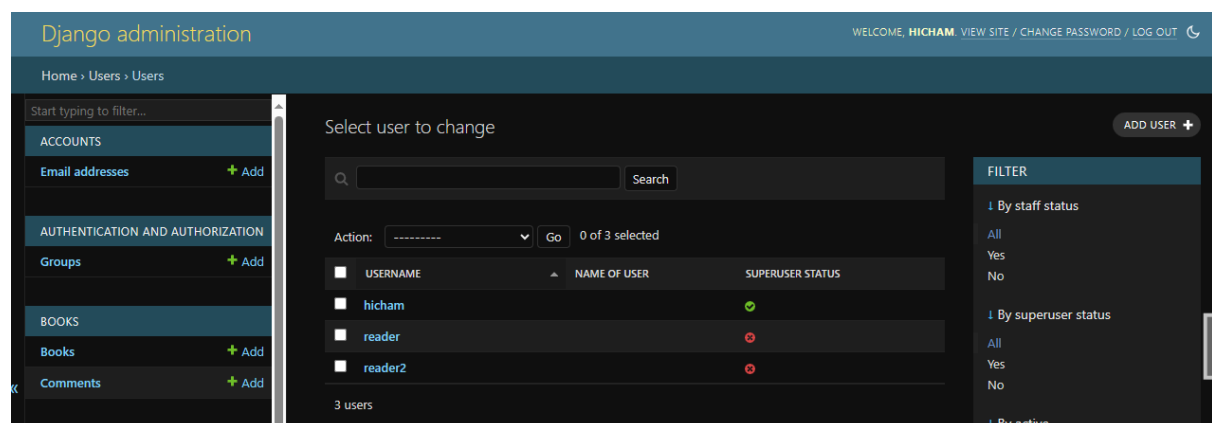


Figure 11: Admin panel page