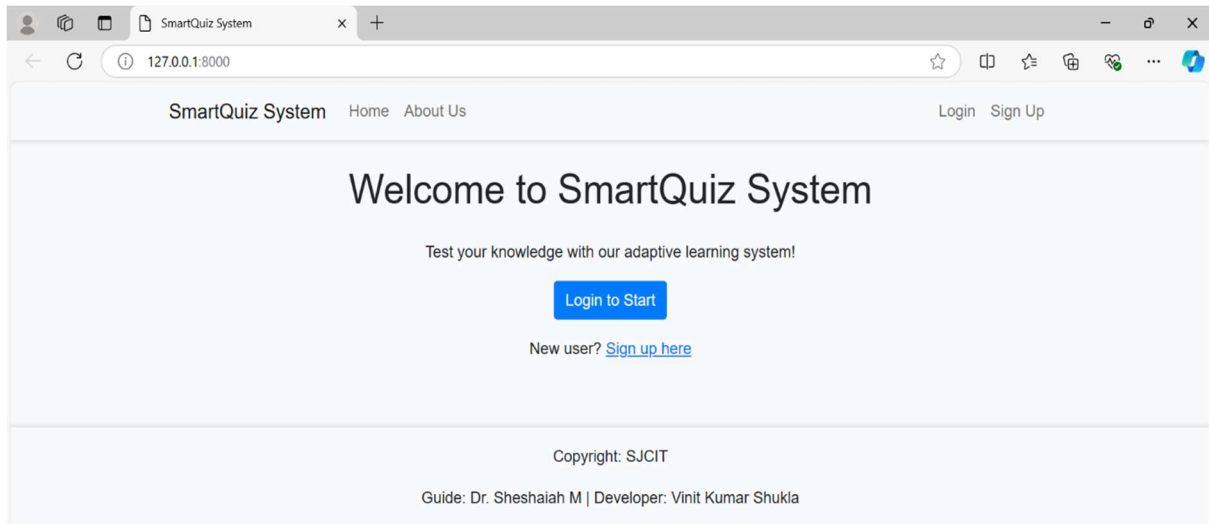
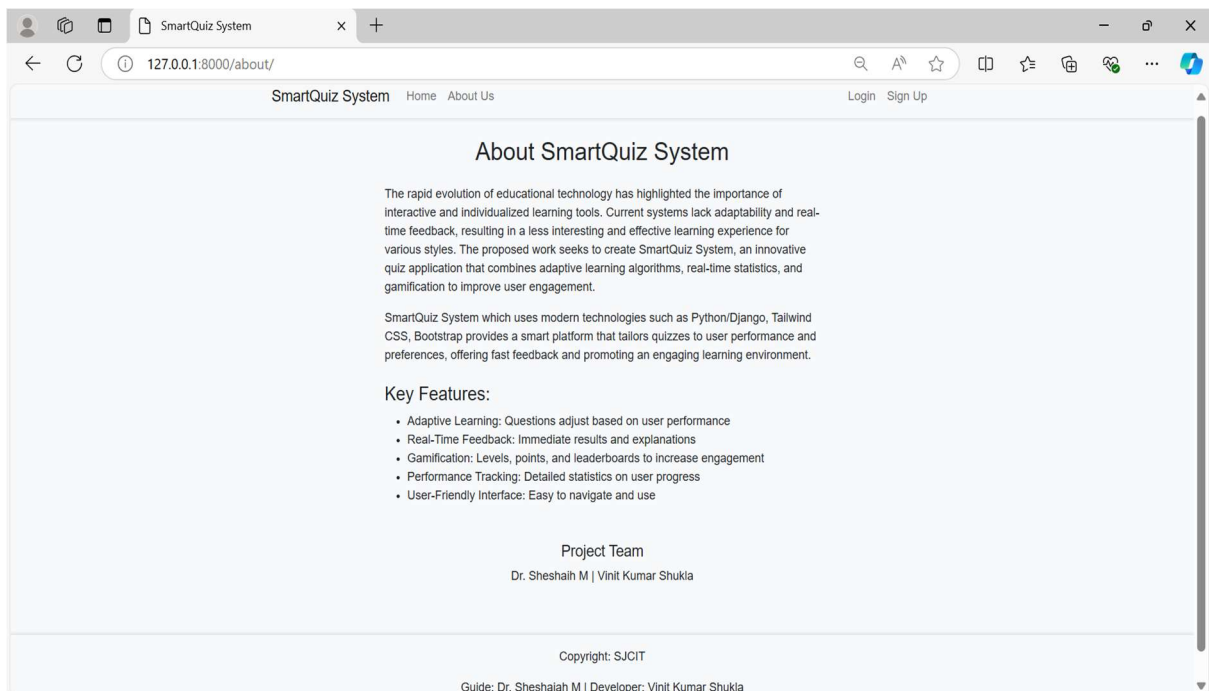


# Appendix

## Appendix A: Snapshots



**Figure A.1: Home Page**



**Figure A.2: About Us Page**

SmartQuiz System Home About Us Login Sign Up

## Sign Up

Username:  Required. 150 characters or fewer. Letters, digits and @/!+/\_ only.

Password:

- 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.
- Your password can't be entirely numeric.

Password confirmation:  Enter the same password as before, for verification.

Password-based authentication:

☒ Enabled  
☐ Disabled

Whether the user will be able to authenticate using a password or not. If disabled, they may still be able to authenticate using other backends, such as Single Sign-On or LDAP.

[Sign Up](#)

**Figure A.3: Sign Up Page**

SmartQuiz System Home About Us Login Sign Up

## Login

Username:

Password:

[Login](#)

Copyright: SJCIT

Guide: Dr. Sheshaiah M | Developer: Vinit Kumar Shukla

**Figure A.4: Login Page**

SmartQuiz System Home About Us Login Sign Up

## Login

Username:

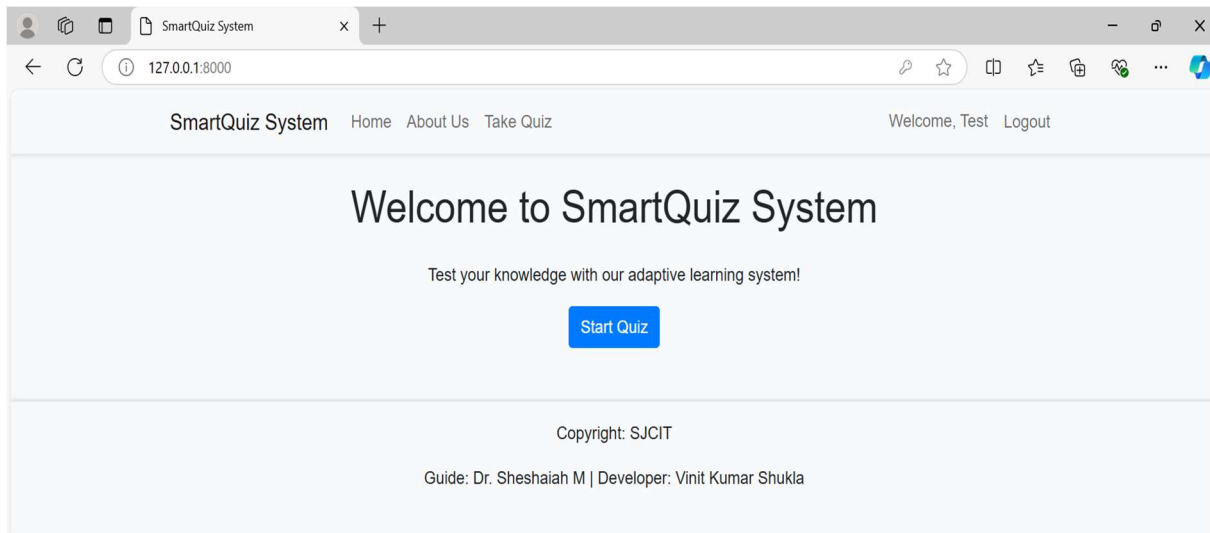
Password:

[Login](#)

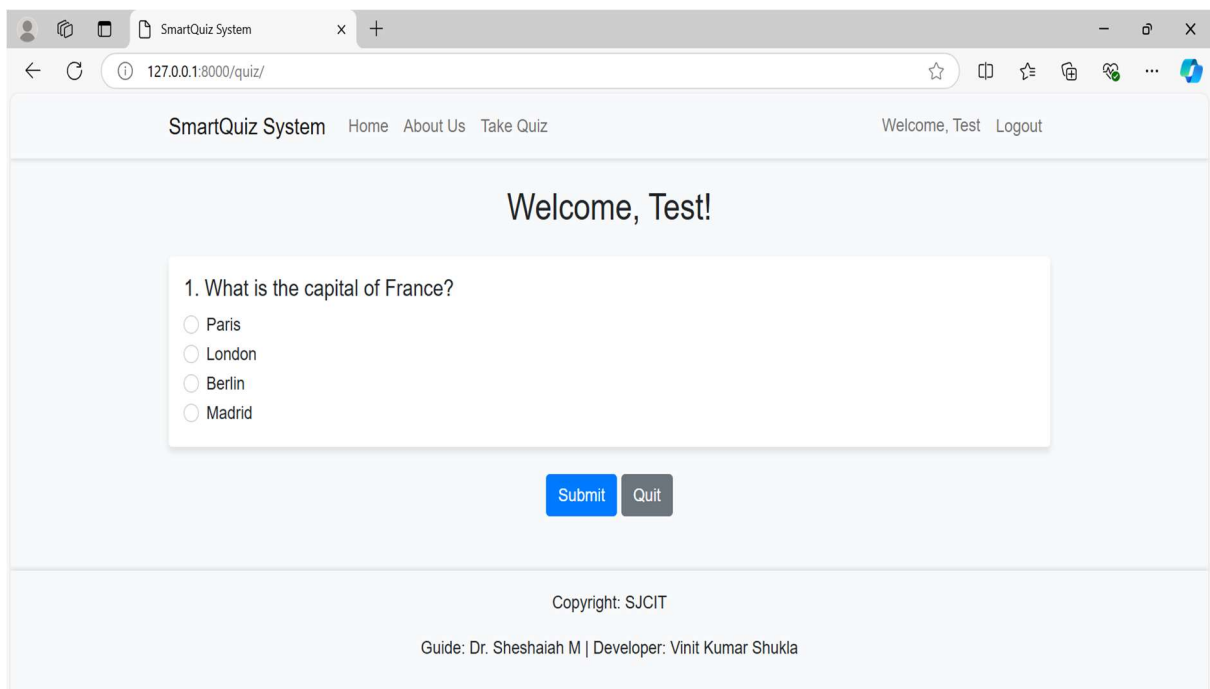
Copyright: SJCIT

Guide: Dr. Sheshaiah M | Developer: Vinit Kumar Shukla

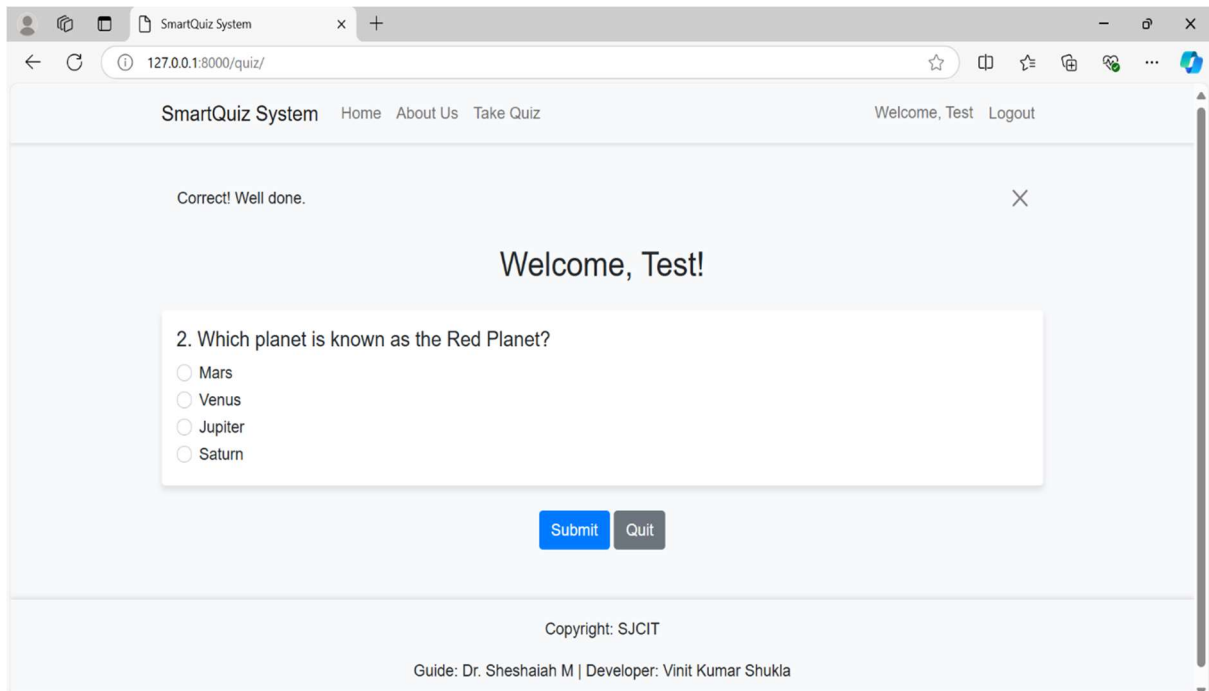
**Figure A.5: Login with credentials**



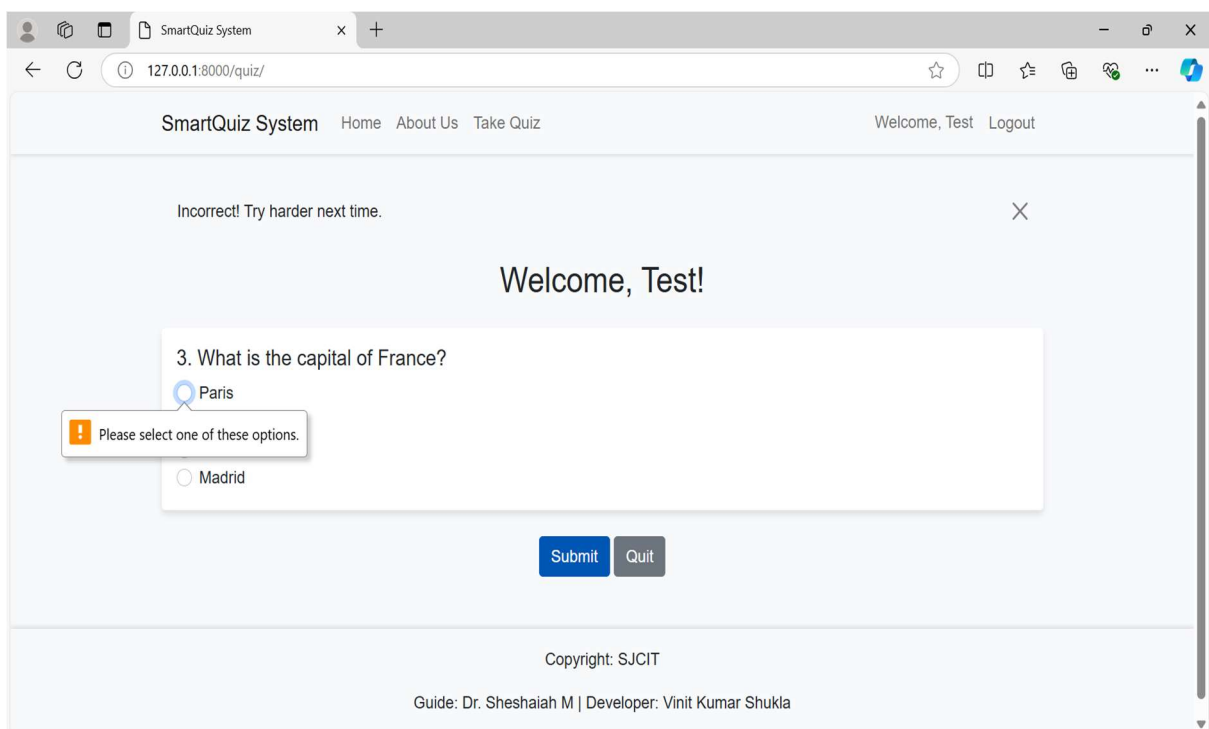
**Figure A.6: After login Welcome Page**



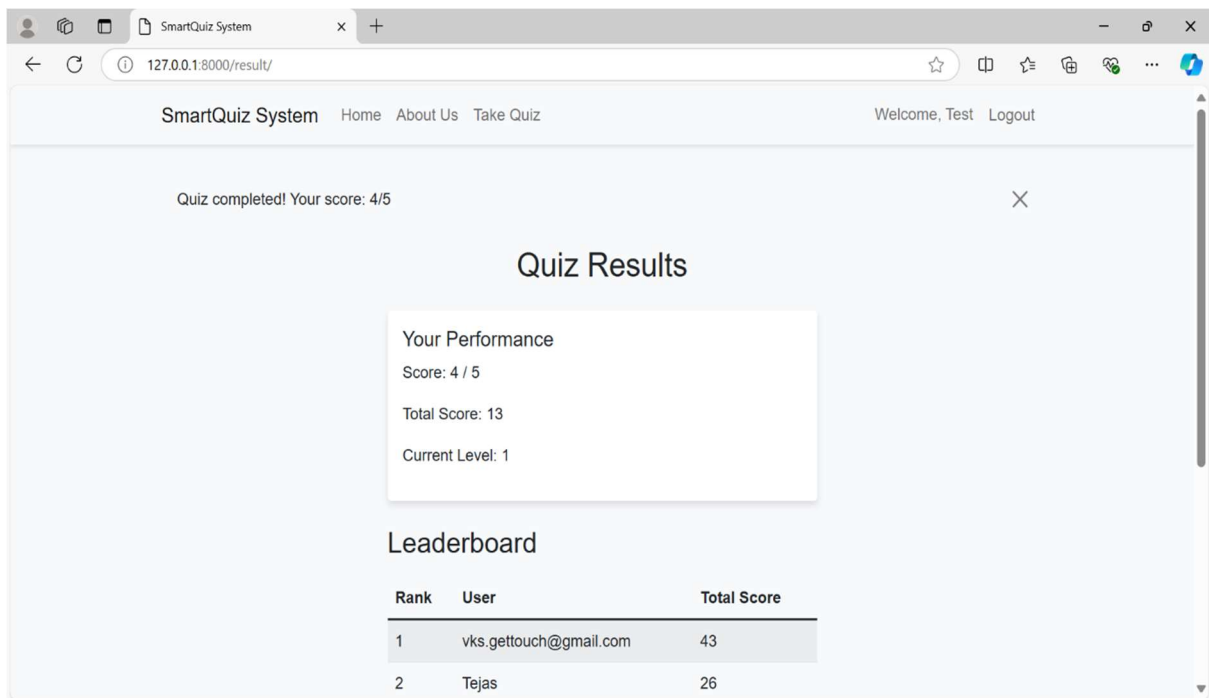
**Figure A.7: Quiz Page**



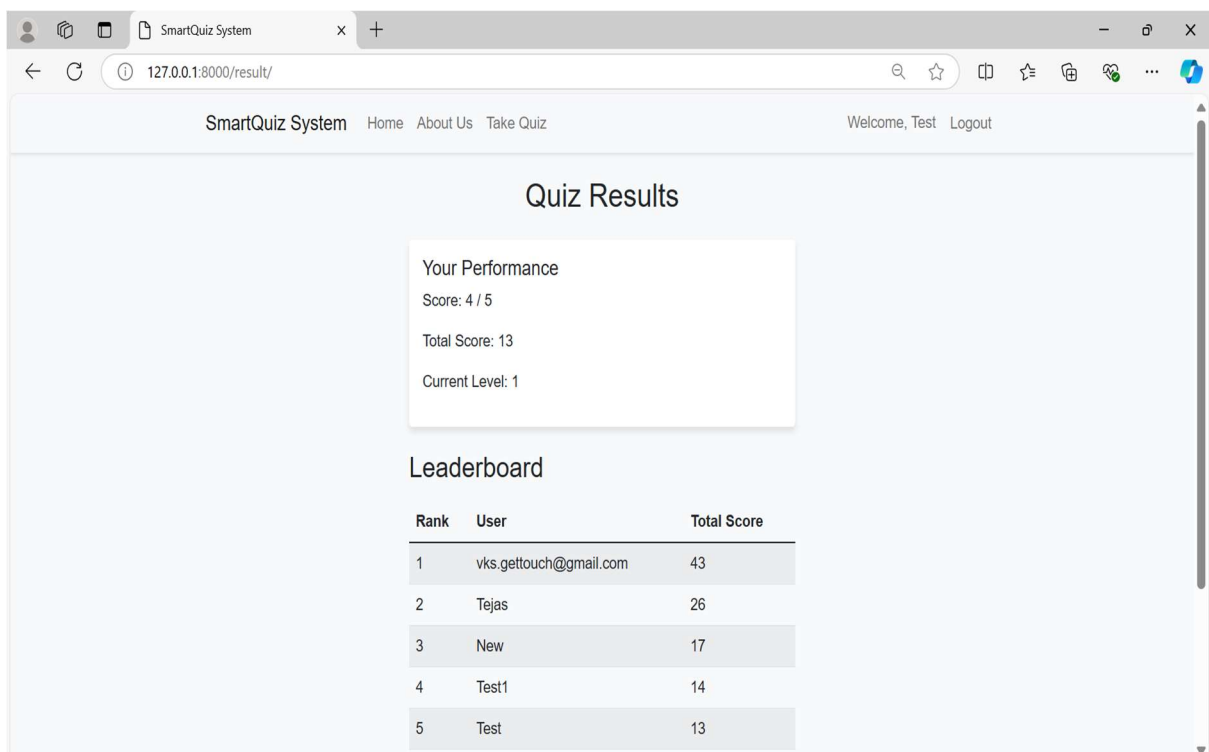
**Figure A.8: After Submit, real time feedback and adaptive learning model-based question**



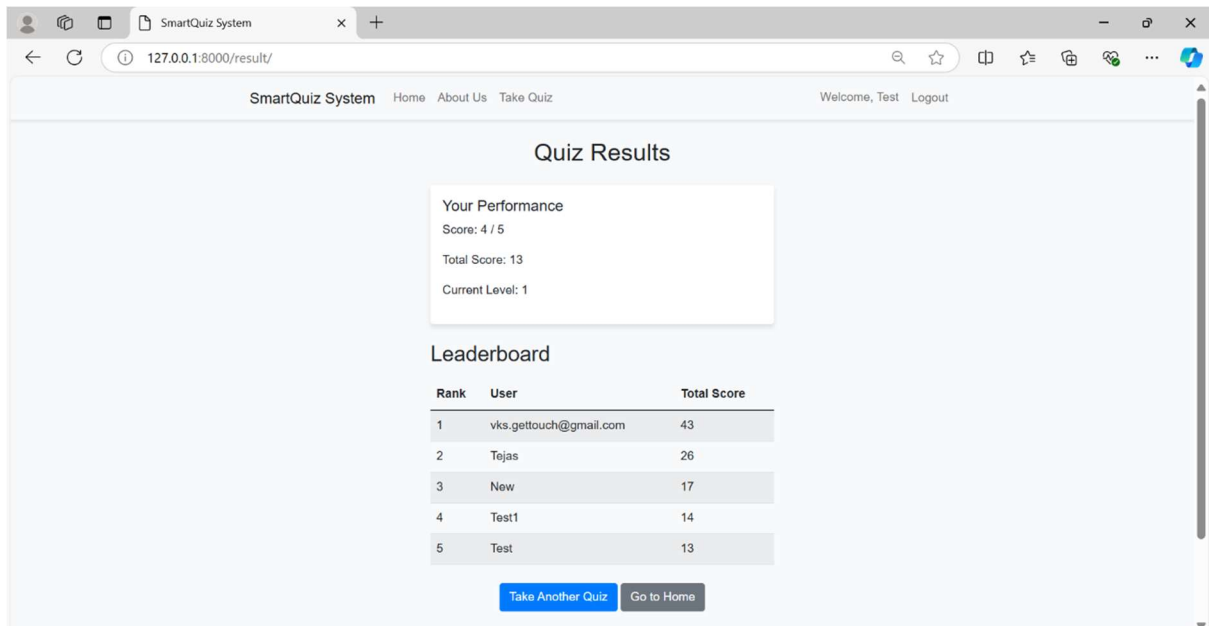
**Figure A.9: Based on attempt real time feedback as incorrect**



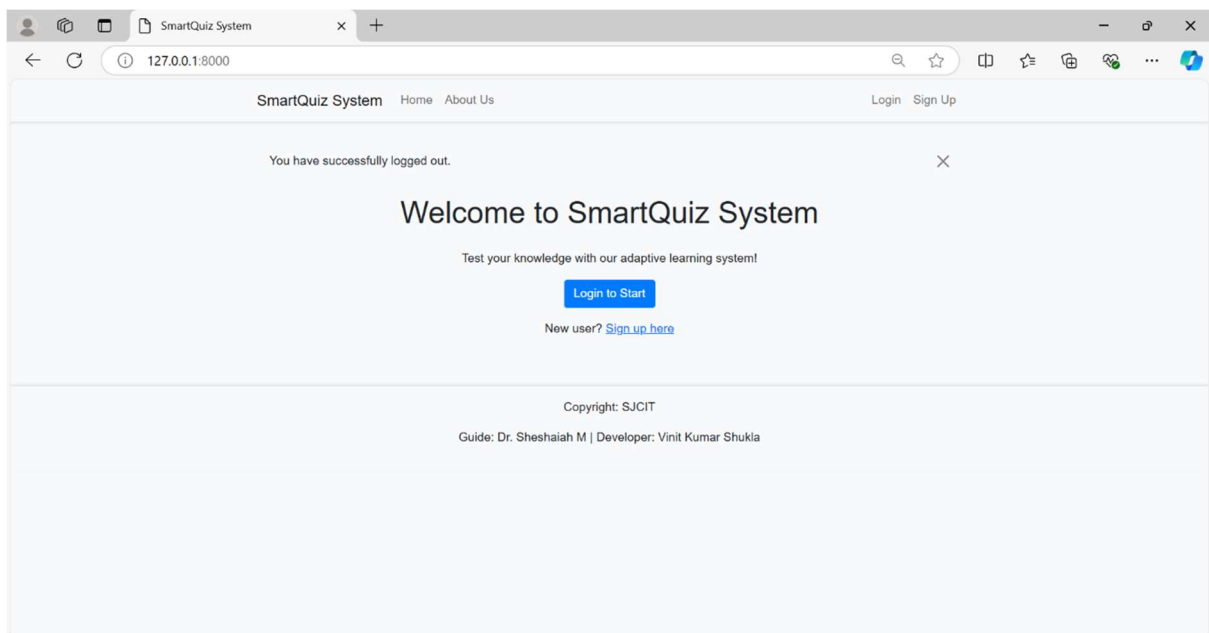
**Figure A.10: Result page which shows performance**



**Figure A.11: Gamification based leaderboard**



**Figure A.12: Option for Take another quiz or go to home**



**Figure A.13: logged out page**

## Appendix B: Glossary

- i. **Adaptive Learning:** A personalized learning approach that adjusts content and difficulty based on individual learner's needs and progress.
- ii. **AI:** Artificial Intelligence, a field of computer science that deals with creating intelligent agents capable of reasoning, learning, and problem-solving.

- iii. **Gamification:** The application of game-like elements in non-game contexts to increase engagement and motivation.
- iv. **Machine Learning:** A subset of AI that involves training algorithms on data to make predictions or decisions without being explicitly programmed.
- v. **User Interface (UI):** The visual elements of an application that allow users to interact with it.
- vi. **User Experience (UX):** The overall experience a user has when interacting with an application or system.

## Appendix C: Technology Stack

- i. **Frontend:** HTML, CSS, JavaScript, Bootstrap
- ii. **Backend:** Python, Django
- iii. **Database:** In-memory
- iv. **Machine Learning:** Scikit-learn or TensorFlow
- v. **Cloud Platform:** Heroku (or a similar platform)

## Appendix D: Deployment Guide

- i. **Create a Heroku account:** Sign up for a Heroku account if you don't have one already.
- ii. **Create a new app:** Go to the Heroku dashboard and create a new app.
- iii. **Configure the app:** Set up the necessary environment variables and dependencies.
- iv. **Deploy the code:** Push your code to Heroku using the Heroku CLI.
- v. **Access the app:** Visit the deployed app's URL to access the Adaptive Learning Model Test System.

## Appendix E: Security Best Practices

- i. **Regular updates:** Keep all software components (Python, Django, CDN, etc.) up-to-date to address security vulnerabilities.
- ii. **Strong passwords:** Use strong, unique passwords for all user accounts and administrative access.

- iii. **Data encryption:** Encrypt sensitive data (e.g., user information, quiz content) both at rest and in transit.
- iv. **Input validation:** Validate user input to prevent injection attacks and other vulnerabilities.
- v. **Regular security audits:** Conduct regular security audits to identify and address potential vulnerabilities.
- vi. **Monitor logs:** Monitor system logs for suspicious activity and anomalies.
- vii. **Implement access controls:** Restrict access to sensitive areas of the application based on user roles and permissions.