CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

PL/SQL

PROJECT REPORT

On

User Authentication System:

Submitted by

Ansin Madhav SJ (24MCA20193)

***in partial fulfillment for the award of the degree of* Masters of**

Computer Applications Chandigarh University

Aug 2024 – Nov 2024

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION

1.1. Identification of Client/Need/Relevant Contemporary Issue

In an increasingly digital world, secure and user-friendly authentication systems are critical for managing user access and safeguarding sensitive data. This project is developed to address the common need for secure login and registration processes in web applications, catering primarily to web developers and businesses that need a reliable foundation for user authentication. The system combines ease of use with essential security measures, such as password hashing, to meet contemporary security standards.

1.2. Identification of Problem

Many existing online systems suffer from security vulnerabilities that expose user credentials to risks like unauthorized access and data breaches. The problem identified here is the need for a straightforward and secure user authentication system that efficiently registers and validates users without compromising their password security. This system seeks to mitigate risks by implementing best practices for password management and authentication.

1.3. Identification of Tasks

To address the problem, several key tasks were outlined:

1. Design a user interface that enables users to log in or sign up effortlessly.
2. Develop backend logic to handle registration and login requests.
3. Integrate security practices such as password hashing to protect user data.
4. Create a MySQL database to store user credentials securely.
5. Test the system thoroughly to validate functionality and security.

CHAPTER 2.
LITERATURE REVIEW/BACKGROUND STUDY

2.1. Timeline of the Reported Problem

The need for secure and efficient user authentication has grown with the expansion of internet-based services over the past two decades. Concerns about password storage and data privacy gained prominence as data breaches became more common, highlighting the necessity of secure login systems.

2.2. Existing Solutions

Current solutions include various approaches to authentication, such as session-based and token-based systems. Password hashing algorithms (e.g., bcrypt and Argon2) and multi-factor authentication methods are widely used to improve security. This project builds on these established methods by implementing secure password storage practices in a simplified authentication flow suitable for most web applications.

2.3. Bibliometric Analysis

A bibliometric analysis reveals a significant increase in research papers focused on user authentication, with trends indicating a growing emphasis on usability, security, and efficiency in authentication mechanisms. Studies emphasize that secure hashing and user-friendly interfaces are crucial for developing robust authentication systems.

2.4. Review Summary

Research suggests that combining security measures like password hashing with an intuitive interface enhances the security and usability of authentication systems. This project integrates these principles by focusing on secure data storage, validation, and responsive design.

2.5. Problem Definition

The challenge is to create a secure, efficient, and user-friendly system that meets standard security protocols and allows for straightforward user management. The system should efficiently manage login and signup processes, with robust protection against unauthorized access.

2.6. Goals/Objectives

The objectives are:

1. Provide a secure and user-friendly registration and login system.
2. Ensure data protection through password hashing.
3. Facilitate efficient database management for storing user information.
4. Build a responsive interface that accommodates both login and signup forms.

CHAPTER 3. DESIGN FLOW/PROCESS

3.1. Evaluation & Selection of Specifications/Features

The system was designed with the following specifications:

- Dual form interface for login and signup.
- Secure backend logic for processing login and signup requests.
- Database connection with MySQL for data storage.
- Password hashing to enhance security.

3.2. Design Constraints

The main constraints included:

- **Data Security**: Passwords must be hashed before storage.
- **Database Management**: User credentials must be unique and efficiently retrievable.
- **Interface Usability**: Forms must be easy to navigate and responsive on different screen sizes.

3.3. Analysis of Features and Finalization Subject to Constraints

Based on the constraints, the system incorporates hashed password storage, unique email verification, and error handling to notify users of incorrect or duplicate information. The design ensures user data is securely stored and efficiently accessed during login.

3.4. Design Flow

1. **User Input**: Users enter email and password data.
2. **Form Submission**: Data is sent to the backend via POST to submit.php.
3. **Backend Processing**:
   - For signups, passwords are hashed and stored.
   - For logins, credentials are validated using hashed passwords.
4. **Response**: Users are notified of the success or failure of their action.

3.5. Implementation Plan/Methodology

The implementation plan included:

1. **Database Setup**: Using XAMPP, MySQL tables were set up with secure structure.
2. **Frontend Development**: HTML and CSS were used for creating the UI with responsive and interactive features.
3. **Backend Development**: PHP handled form data and secure password storage.
4. **Testing**: Functionality was validated to ensure data integrity and error-free operation.

CHAPTER 4. RESULTS ANALYSIS AND VALIDATION

4.1. Implementation of Solution

The implemented solution successfully met the project requirements. The login and signup forms processed user data accurately, stored hashed passwords securely, and validated credentials on login. Testing confirmed the functionality of the following:

- **Registration Process**: Unique email validation, password hashing, and storage.
- **Login Process**: Verification of stored hashed passwords and user feedback.
- **Database Security**: Passwords were securely stored with hash algorithms, reducing vulnerability to unauthorized access.

CHAPTER 5. CONCLUSION AND FUTURE WORK

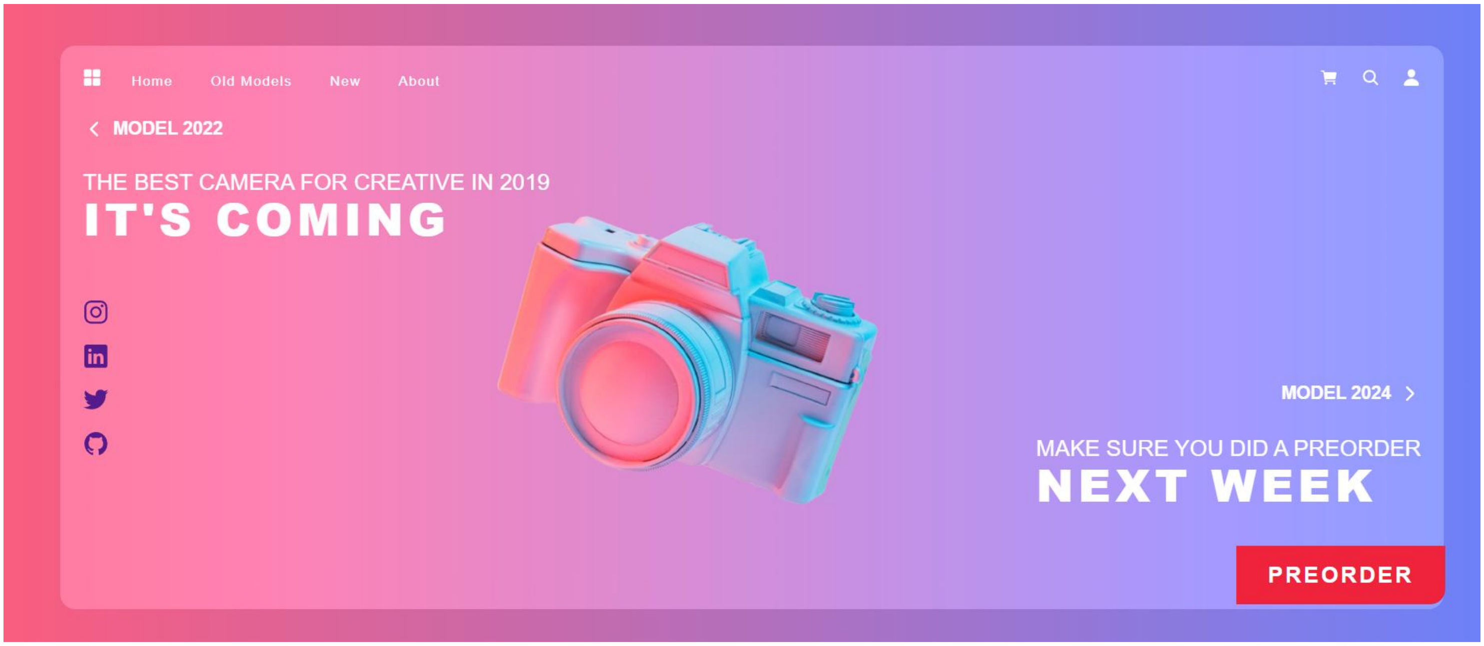
5.1. Conclusion

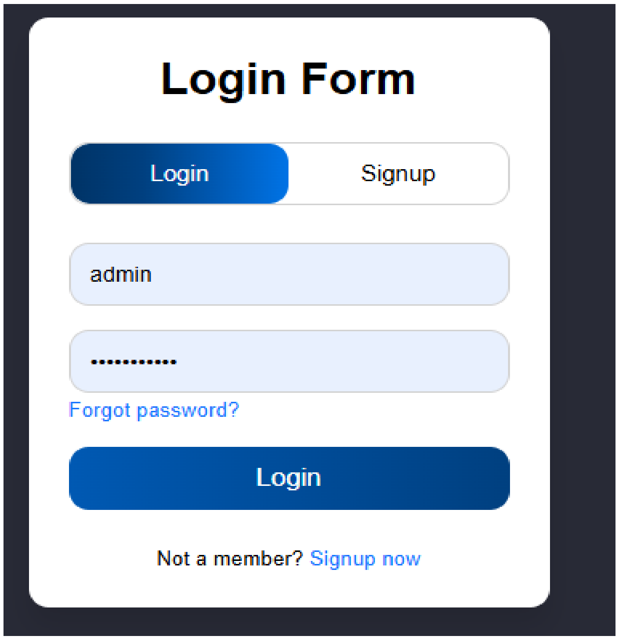
This project achieved the goal of creating a secure and user-friendly authentication system with password hashing, effective data storage, and smooth functionality. The application meets essential security standards, efficiently manages user credentials, and provides a responsive, intuitive user interface. These features make the system a strong foundation for future web applications requiring user authentication.

5.2. Future Work

To further enhance the project, future iterations could include:

1. **Email Verification**: To verify user accounts before granting access.
2. **Password Recovery**: Allow users to reset their passwords securely.
3. **Session Management**: Track and manage user sessions for secure, extended access.
4. **Multi-Factor Authentication**: Add extra layers of security to increase protection against unauthorized access.





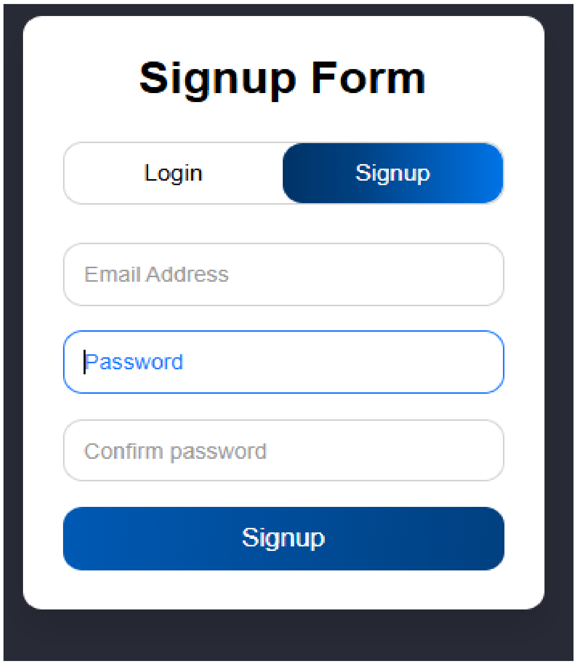
Login Form

admin

•••••••••••

Forgot password?

Not a member? Signup now



Signup Form

Email Address

Password

Confirm password