

# SECURE PASSWORD MANAGEMENT SYSTEM

## INDEX:

1)ABSTRACT.....	2
2)INTRODUCTION.....	3
3)PURPOSE.....	5
4)FEATURES.....	7
5)CONTRIBUTIONS.....	9
6)TECHNOLOGIES USED.....	11
7)FUTURE WORK.....	13
8)SCREENSHOTS.....	14
9)CONCLUSION.....	25

## **1)ABSTRACT**

This project aims to design and develop a secure password management system that enables users to store, manage, and retrieve their passwords safely. The system provides a user-friendly interface for users to register, store, and manage their passwords for various accounts. It features password generation, retrieval, update, and deletion capabilities, ensuring that users' passwords are protected using encryption and secure password hashing algorithms. The system also includes a to display stored passwords, a search function to find passwords by account name or username, and a password strength indicator to evaluate password security. Additionally, the system implements two-factor authentication to provide an extra layer of security. Built using a Python framework (Flask) and a database (MySQL), this system ensures the confidentiality, integrity, and availability of users' sensitive password information.

## 2)INTRODUCTION

In the modern digital landscape, handling passwords is both vital and challenging because of the expanding range of online services and the rising threat of security breaches. While passwords are a common method for verifying identities, they are frequently targeted by cybercriminals, underscoring the importance of safeguarding sensitive information effectively.

In today's digital age, individuals juggle multiple online accounts, each with its own unique login credentials. As the number of accounts grows, so does the complexity of managing them. To maintain security, each password must meet specific complexity requirements and be unique to each account. However, remembering numerous complex passwords can be overwhelming, leading many to reuse passwords across multiple sites for convenience. This practice significantly increases the risk of a broad security breach if one of these sites is compromised, as cybercriminals can exploit stolen credentials to infiltrate other accounts that share the same password.

Users often opt for passwords that are easy to remember, but this convenience comes at a cost. Simple passwords like "123456" or "password" are highly susceptible to brute-force attacks and password guessing techniques, making them a security risk. On the other hand, strong passwords that combine uppercase and lowercase letters, numbers, and special characters offer better protection. However, creating and recalling unique, complex passwords for each account can be a daunting task without a systematic approach or tool to manage them.

The Secure Password Management System (SPMS) is an all-inclusive solution crafted to overcome these difficulties by offering a secure and intuitive platform for managing passwords.

A Secure Password Management System is designed to securely handle passwords for multiple online accounts. It focuses on protecting sensitive information by maintaining the confidentiality, integrity, and availability of user data. The system incorporates a strong security framework that includes advanced encryption, secure password hashing, and two-factor authentication to ensure that user passwords are well-protected against unauthorized access..

The system features an easy-to-use interface that simplifies password management. Users can quickly register, store, and manage passwords for multiple accounts all in one place. It also allows users to create strong, unique passwords for each account, enhancing security. Additionally, the system offers straightforward options for retrieving, updating, and deleting passwords, which helps users maintain excellent password practices. By streamlining the management process, the system aids users in staying organized and secure, minimizing the risk of password-related security breaches.

A notable feature of the Secure Password Management System is its capacity to generate strong, unique passwords for users. Utilizing a sophisticated algorithm, the system creates complex passwords that are difficult to guess or crack, providing a strong defense against unauthorized access and significantly lowering the risk of security breaches. By automatically producing robust passwords, the system removes the need for users to create their own, which are often weak and susceptible to attacks. With this system, users can be confident that their online credentials are safeguarded by nearly unbreakable passwords.

### **3)PURPOSE**

This Secure Password Management System is an all-encompassing platform designed to offer a secure and dependable space for users to store, manage, and access their passwords. Featuring an easy-to-use interface, it allows users to effortlessly register, save, and manage passwords for different accounts. Its key feature is the ability to create strong, unique passwords, which are hard for hackers to guess or break, thereby improving security and shielding users from potential breaches.

This System provides several useful features such as password retrieval, updates, and deletion. Users can effortlessly access, adjust, and remove passwords as required. The system's dashboard offers a comprehensive view of all saved passwords, usernames, and URLs, simplifying the management and tracking of credentials. This efficient setup helps users easily access their online accounts and maintain organization.

It emphasizes security by using strong encryption to protect stored passwords, so unauthorized access to the database does not compromise the encrypted data. It also incorporates two-factor authentication through tools like pyotp or Google Authenticator, adding a second verification step for users. This dual-layered approach significantly enhances security and makes it much more difficult for attackers to gain unauthorized access to user accounts, ensuring better protection for sensitive information.

The system features a search function that helps users quickly locate passwords by account name or username. It also includes a password strength indicator that assesses the security of passwords and offers suggestions for improvement, helping users enhance their password protection.

This System is developed with the Flask framework in Python and uses MySQL for its database, ensuring it is scalable, reliable, and high-performing. Its modular architecture facilitates easy integration with other security tools and technologies. The user interface is created using HTML, CSS, and jQuery, offering a user-friendly and intuitive experience for interacting with the system.

## **4)FEATURES**

### **1. User Registration**

- To get started, users create an account by choosing a unique username and password. During registration, the system collects essential details, such as email addresses and other identifying information, to ensure secure authentication during future logins. These details are stored securely to prevent unauthorized access.

### **2. Password Storage**

- To get started, users create an account by choosing a unique username and password. During registration, the system collects essential details, such as email addresses and other identifying information, to ensure secure authentication during future logins. These details are stored securely to prevent unauthorized access.

### **3. Password Generation**

- The system offers a password generation feature, which creates strong, unique passwords based on user-defined criteria, such as length and complexity. This ensures that passwords meet security best practices, making it harder for hackers to guess or crack them.

### **4. Password Retrieval**

- When users need to access their stored passwords, they can do so securely through the system. This feature is designed to provide secure access to credentials without compromising security.

## **5. Password Update**

- If users need to update their passwords, they can modify them through the system. Updated passwords are securely stored and encrypted, ensuring that they remain protected from unauthorized access.

## **6. Password Deletion**

- Users can remove passwords that are no longer needed or linked to inactive accounts. The system ensures that these credentials are securely deleted from storage, preventing unauthorized access to sensitive information.

## **7. Dashboard**

- The dashboard provides a central view of all stored passwords, displaying essential details like usernames, passwords, and URLs. It also includes a search function, making it easy to locate specific passwords quickly.

## **8. Security**

- The system prioritizes security, using the advanced encryption algorithm and hashing algorithms, including libraries like python-cryptography/pyAesCrypt and bcrypt, to securely store passwords. This ensures that passwords are protected from unauthorized access and data breaches.

## **9. Two-Factor Authentication (2FA)**

- To add an extra layer of security, the system supports two-factor authentication with libraries like pyotp or Google Authenticator. Users must provide an additional verification code, typically sent to their mobile device, along with their master password, to access their account. This ensures that even if a user's master password is compromised, their account remains secure.

## 5)CONTRIBUTIONS

### 1)Name: Nagendra Neelima Korrapati

**Blazer Id: nkorrapa**

- Implemented two-factor authentication using OTP.
- Developed password generation functionality.
- Fixed various defects in the system.

### 2)Name: Praveen Vaddi

**Blazer Id: pvaddi**

- Set up the codebase, repository, and virtual environment.
- Handled user registration and form validations.
- Implemented password strength verification.

### 3)Name: Sandeep Vaddi

**Blazer Id: vaddis**

- Worked on thank you, login, and logout functionalities.
- Conducted regression testing.
- Created documentation for the project.

### 4)Name: Leela Siva Rama Krishna Neelapala

**Blazer Id: lneelapa**

- Designed the dashboard user interface.
- Implemented search functionality.
- Performed functional and regression testing.



**5)Name: Duggimpudi Bala Delphy Supreetha**

**Blazer Id: dduggimp**

- Developed functionality to view and delete accounts.
- Implemented QR code display feature.

**6)Name: Akhila Reddy Palwai**

**Blazer Id: apalwai**

- Fixed various defects in the system.
- Created new account setup and edit account functionality.

## **6)TECHNOLOGIES USED**

### **1. Programming Language: Python**

- Python is a high-level, interpreted language known for its ease of reading and writing. It supports various programming styles, including procedural, object-oriented, and functional programming. This language was selected for this project due to its simplicity, versatility, and extensive library support, which make it well-suited for web development, data analysis, and machine learning.

### **2. Framework: Flask**

- Flask is a lightweight and adaptable web framework for Python. It is designed for simplicity and ease of extension, making it ideal for creating web applications. Flask is particularly effective for small to medium-sized projects, offering a flexible approach to organizing and managing code.

### **3. Database: MySQL**

- MySQL is an open-source relational database management system that uses SQL for data access and management. It is a popular choice for web applications due to its reliability and the large developer community that supports it, making it easy to find tools and libraries to meet various needs.

### **4. Libraries:**

- **python-cryptography/pyAesCrypt\*\*:**
  - o These libraries handle encryption and decryption processes. pyAesCrypt provides a user-friendly interface for AES encryption, ensuring secure data management.

- **bcrypt:**
  - o This library is used for hashing passwords securely. Its robust hashing algorithm is known for being resistant to brute-force attacks due to its computational intensity.

## **5. UI Technologies: HTML, CSS, jQuery**

- HTML (Hypertext Markup Language): The standard language for creating and organizing content on web pages and applications.
- CSS (Cascading Style Sheets): Used to define the visual presentation and layout of web pages, enhancing the user interface and experience.

## **6. jQuery:**

- A fast, lightweight JavaScript library that simplifies HTML manipulation, event handling, and animations, providing an easy-to-use API for interacting with HTML and CSS.

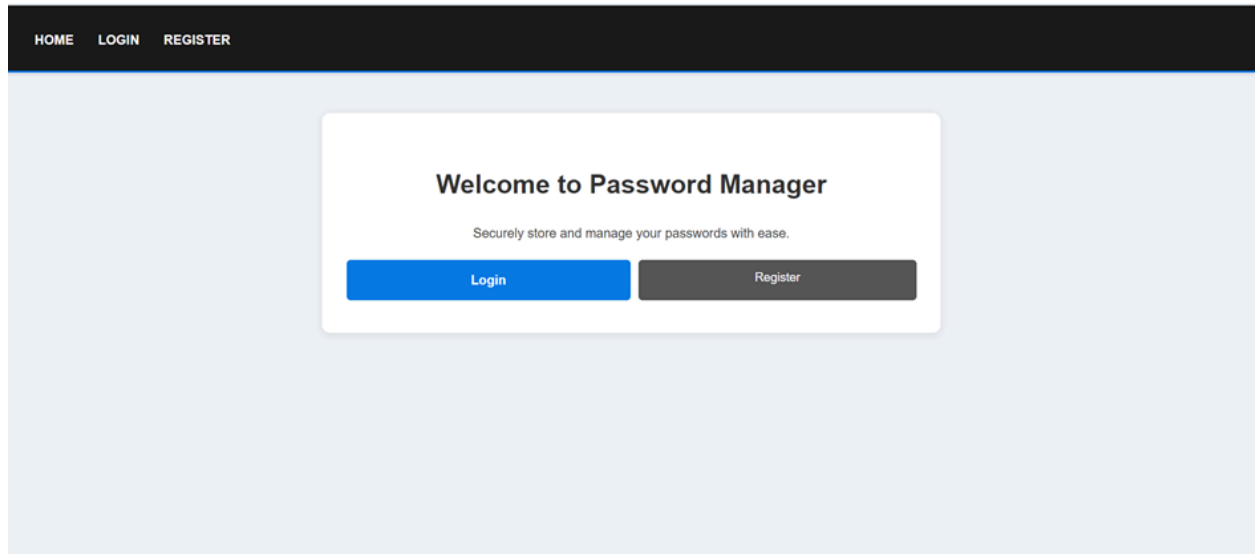
## 7)FUTURE WORK

1. **Password Breach Monitoring:** By integrating with breach monitoring services the system can inform users if their credentials have been compromised in a data breach. This integration uses APIs to check and report compromised accounts, allowing the system to notify users when their passwords appear in breach databases. This helps users quickly take action to protect their accounts.
  
2. **Advanced Password Analysis:** Develop advanced tools that simulate password cracking to help users detect and strengthen weak passwords. These tools evaluate password security by replicating various attack techniques, enabling users to understand the potential vulnerabilities in their passwords and motivating them to enhance their security measures.

## 8)SCREENSHOTS

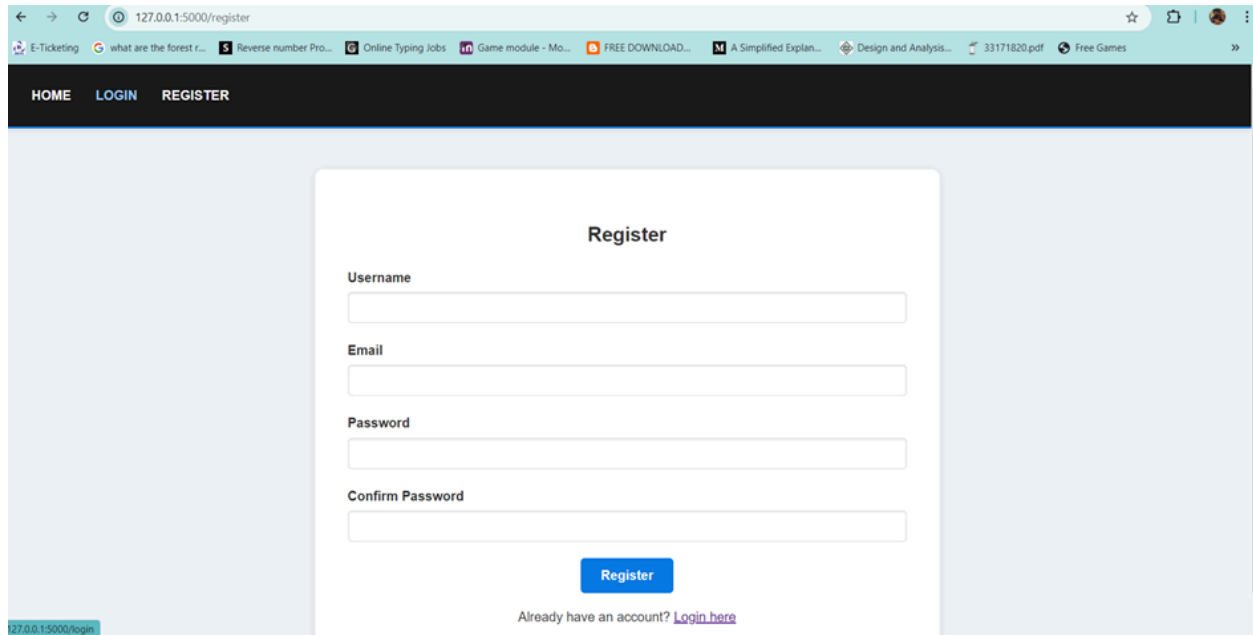
### Home :

This is the home page that welcomes users with options to log in or register, emphasizing secure password storage and management.



## Register :

On clicking the register button,new users can signup by creating a username and password.



The screenshot shows a web browser window with the address bar displaying "127.0.0.1:5000/register". The browser's tab bar contains several open tabs, including "E-Ticketing", "what are the forest r...", "Reverse number Pro...", "Online Typing Jobs", "Game module - Mo...", "FREE DOWNLOAD...", "A Simplified Explan...", "Design and Analysis...", "33171820.pdf", and "Free Games". The website's navigation bar is dark with links for "HOME", "LOGIN", and "REGISTER". The main content area features a white "Register" form with the following fields: "Username", "Email", "Password", and "Confirm Password". Each field is represented by a text input box. Below the form is a blue "Register" button. At the bottom of the form, there is a link that says "Already have an account? [Login here](#)".

When you click the "Register" button, if the username or password already exists an error message pops up and password strength is also indicated

## Register

Username or email already exists!

Username

nkorrapa\_K

Email

nkorrapa55@uab.edu

Password

.....

✓

Strong

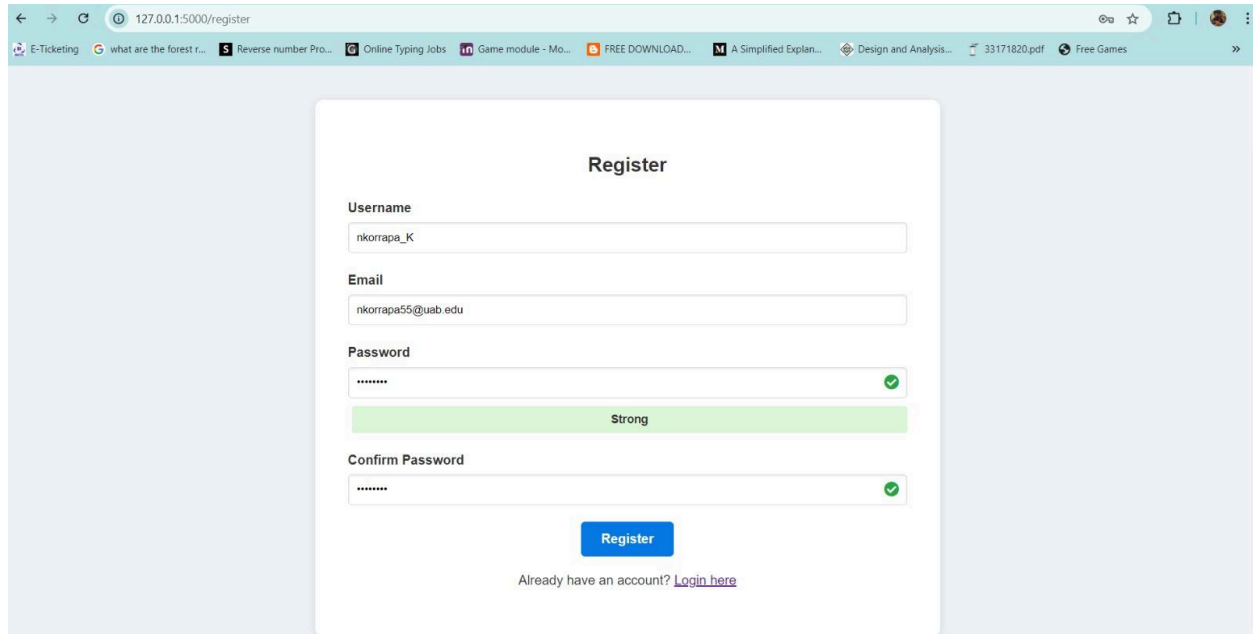
Confirm Password

.....

✓

Register

Already have an account? [Login here](#)

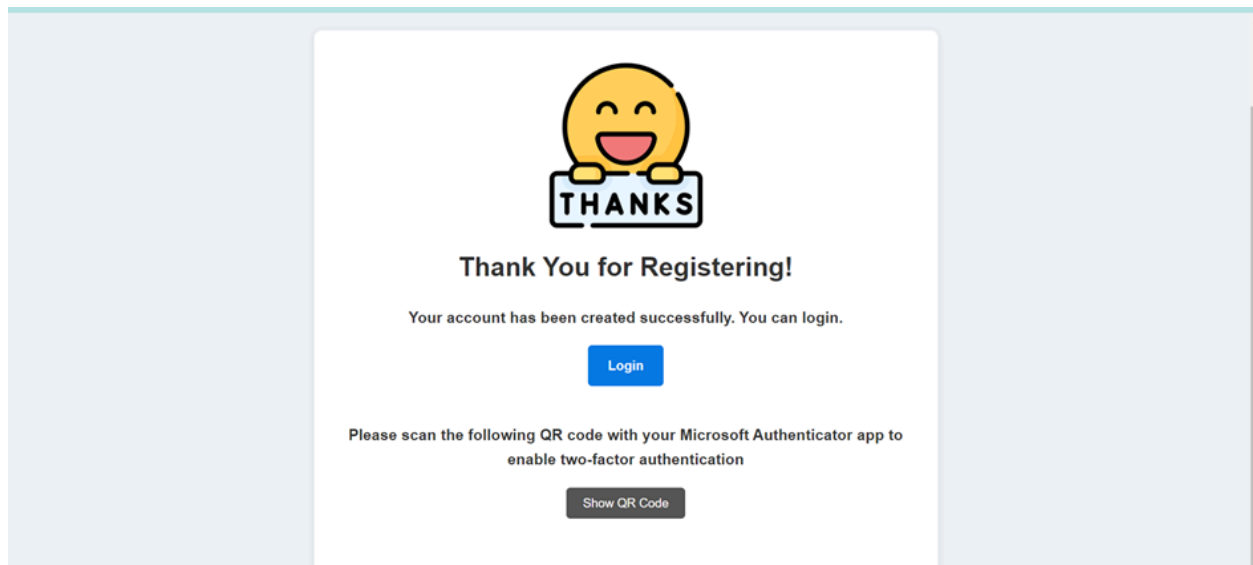


The screenshot shows a web browser window with the address bar displaying "127.0.0.1:5000/register". The browser's tab bar includes several open tabs: "E-Ticketing", "what are the forest r...", "Reverse number Pro...", "Online Typing Jobs", "Game module - Mo...", "FREE DOWNLOAD...", "A Simplified Expl...", "Design and Analysis...", "33171820.pdf", and "Free Games". The main content area displays a registration form with the following fields and elements:

- Username:** A text input field containing "nkorrapa\_K".
- Email:** A text input field containing "nkorrapa55@uab.edu".
- Password:** A text input field with masked characters "\*\*\*\*\*". To the right of the field is a green checkmark icon. Below the field is a green progress bar labeled "Strong".
- Confirm Password:** A text input field with masked characters "\*\*\*\*\*". To the right of the field is a green checkmark icon.
- Register Button:** A blue button labeled "Register".
- Footer:** A link that says "Already have an account? [Login here](#)".

**Thank you:**

If all of the information given is correct after clicking the register button, a thankyou page will appear.



The screenshot shows a web browser window displaying a thank you page. The page features a large yellow smiley face emoji with its arms raised, holding a sign that says "THANKS". Below the emoji, the text reads:

- Thank You for Registering!**
- Your account has been created successfully. You can login.

Below this text is a blue button labeled "Login". Further down, the text says:

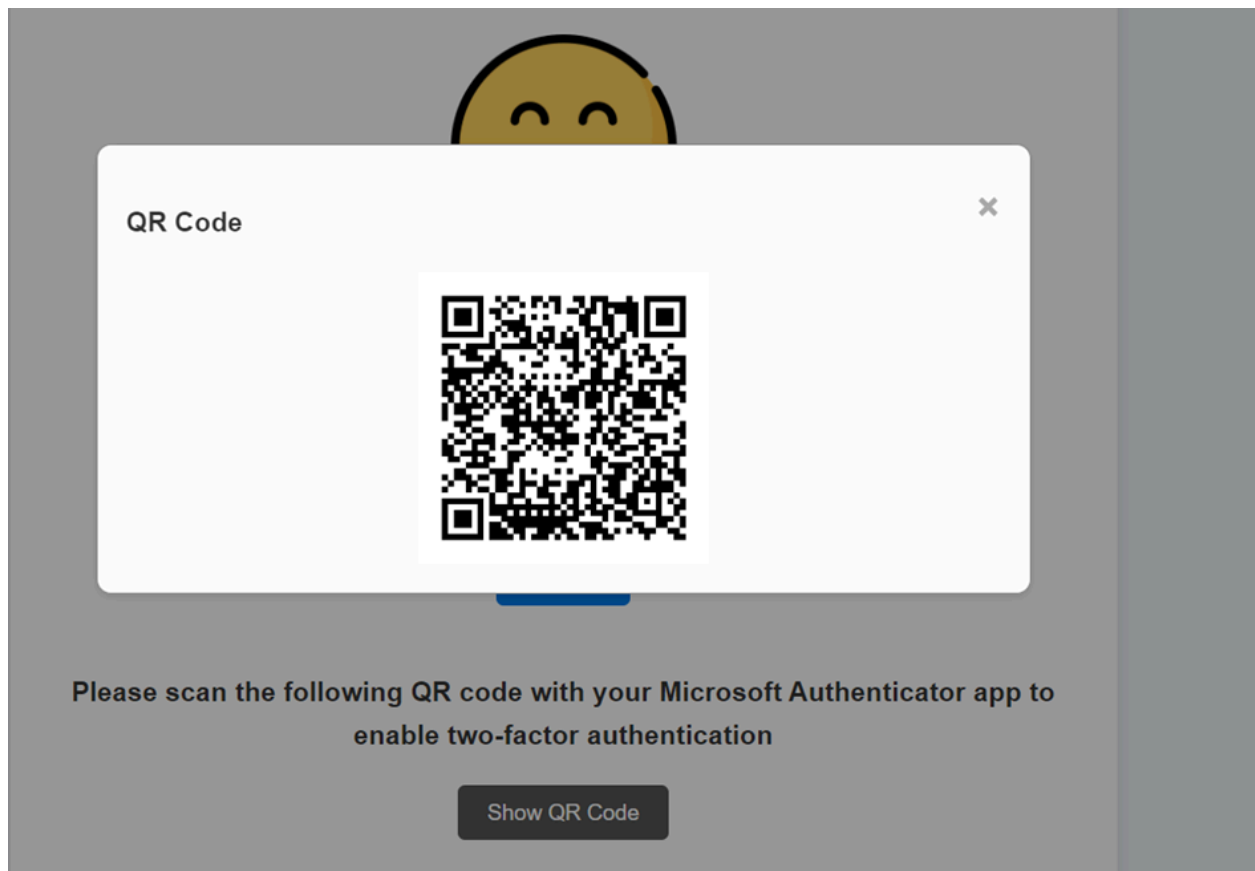
- Please scan the following QR code with your Microsoft Authenticator app to enable two-factor authentication

At the bottom of the page is a dark gray button labeled "Show QR Code".



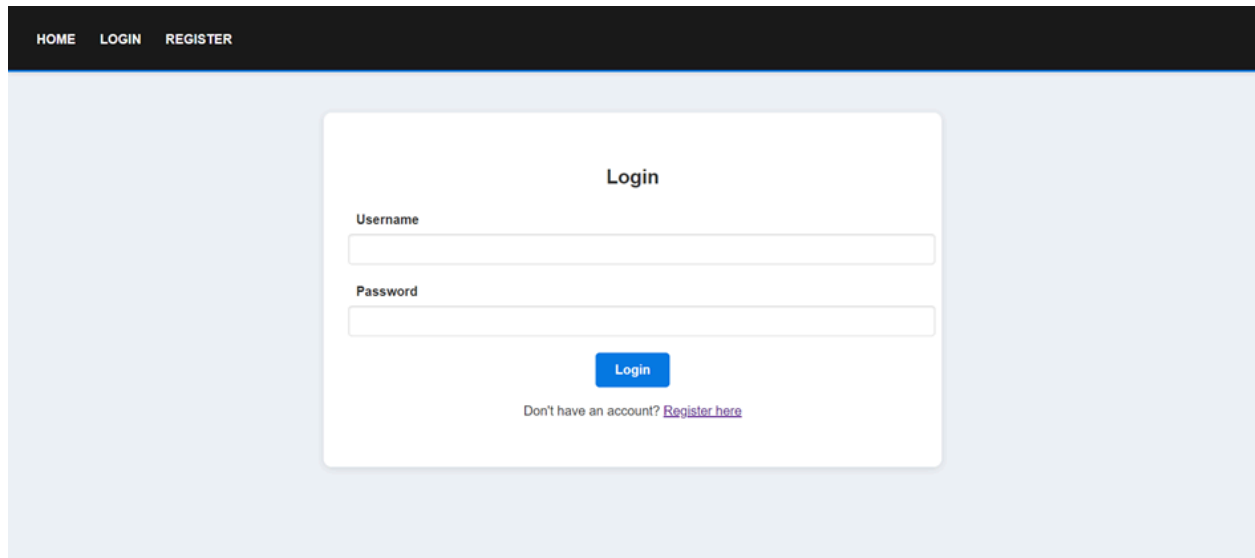
## Show QR:

A QR code shows when we click the Show QR code on the Thank You page used for logging in other device. To establish two factor authentication, we must utilize the Microsoft Authenticator app.

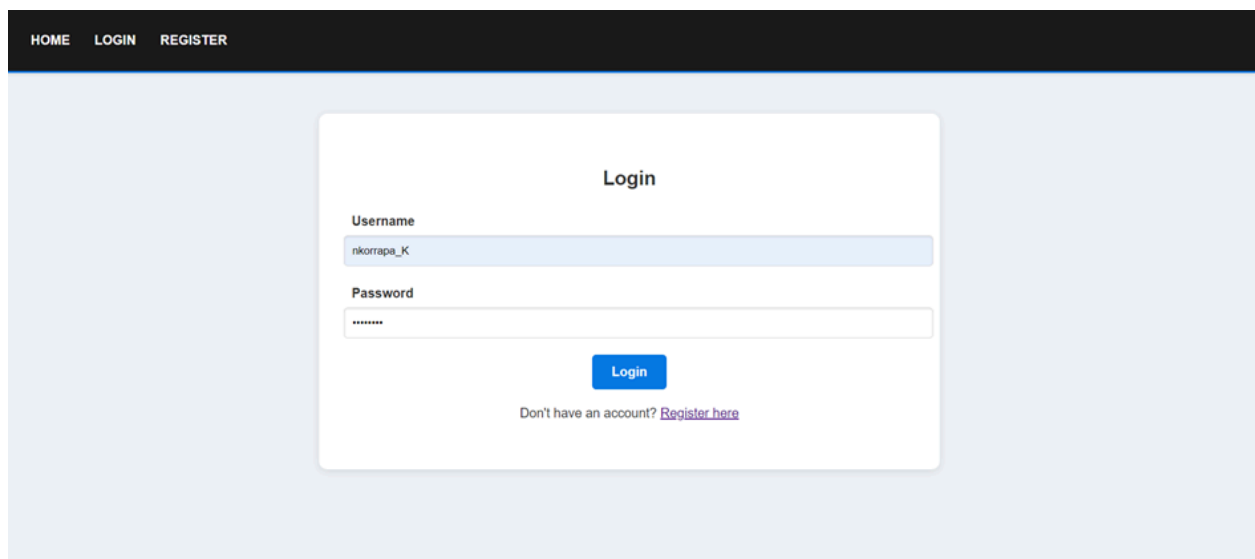


## Login

For logging in you can provide us your current username and password by clicking the login button to access their accounts.



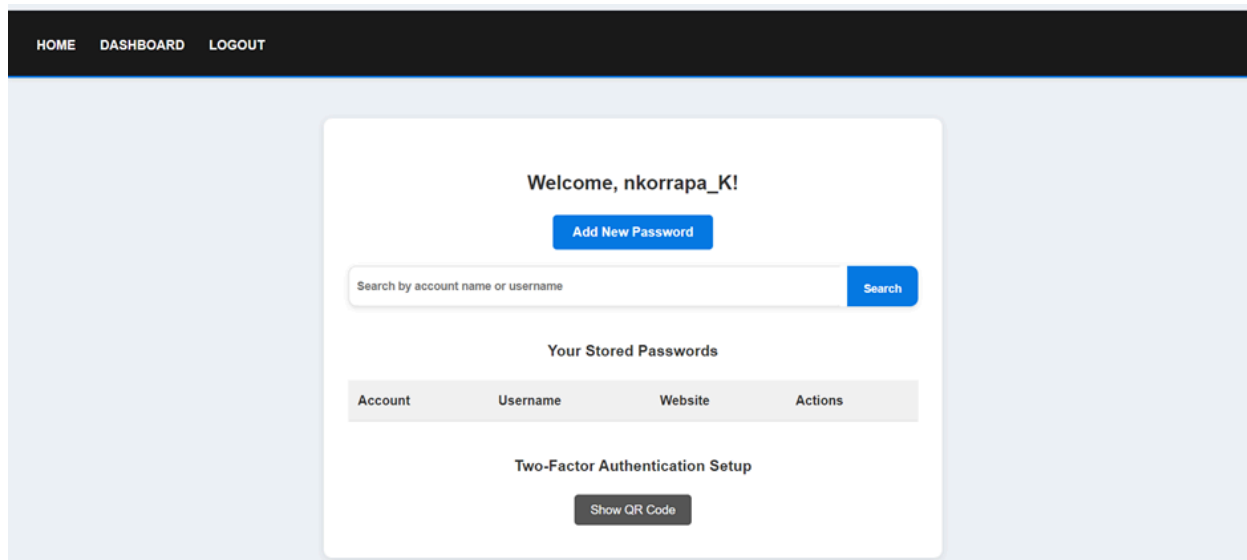
A screenshot of a web application's login page. At the top, a dark navigation bar contains the links 'HOME', 'LOGIN', and 'REGISTER'. The main content area has a light blue background. In the center, a white rounded rectangle contains the title 'Login'. Below the title are two input fields: 'Username' and 'Password'. A blue 'Login' button is positioned below the password field. At the bottom of the white box, there is a link that says 'Don't have an account? [Register here](#)'.



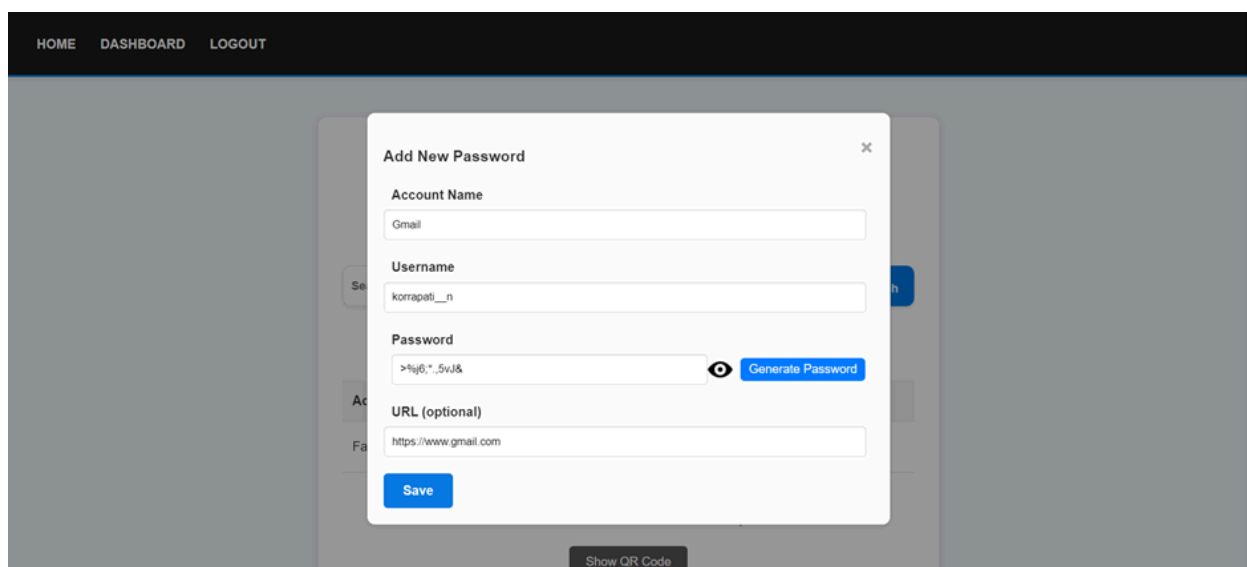
A second screenshot of the same login page, but with data entered. The 'Username' field now contains the text 'nkorrapa\_K' and the 'Password' field contains a series of dots representing a masked password. The 'Login' button and the 'Register here' link remain visible at the bottom of the form.

## Dashboard

After successfully logging in, this dashboard will appear, where you may click the "add new password" option to store your credentials.



User is asked to enter account name, username, password(generates the strong password) and URL for the account



It shows all the accounts we added and allows user to view, delete, edit the information.




## Welcome, nkorrapa\_K!

Add New Password

Search by account name or username

Search

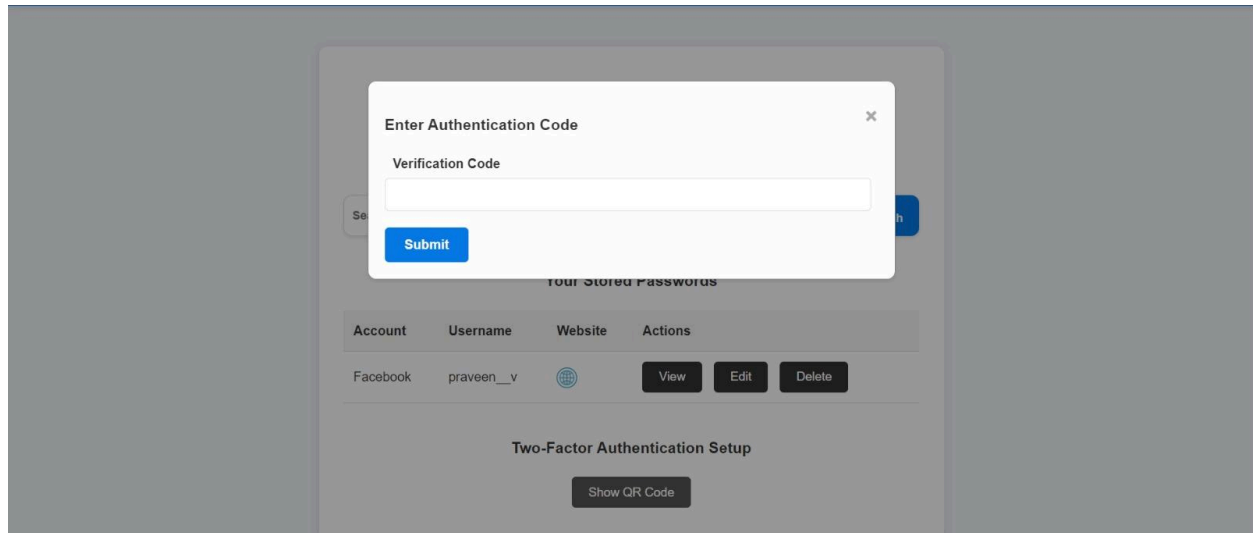
### Your Stored Passwords

Account	Username	Website	Actions
Facebook	nkorrapa__k		<div>View</div> <div>Edit</div> <div>Delete</div>
Gmail	korrapati__n		<div>View</div> <div>Edit</div> <div>Delete</div>
linkedin	Neelima__K		<div>View</div> <div>Edit</div> <div>Delete</div>

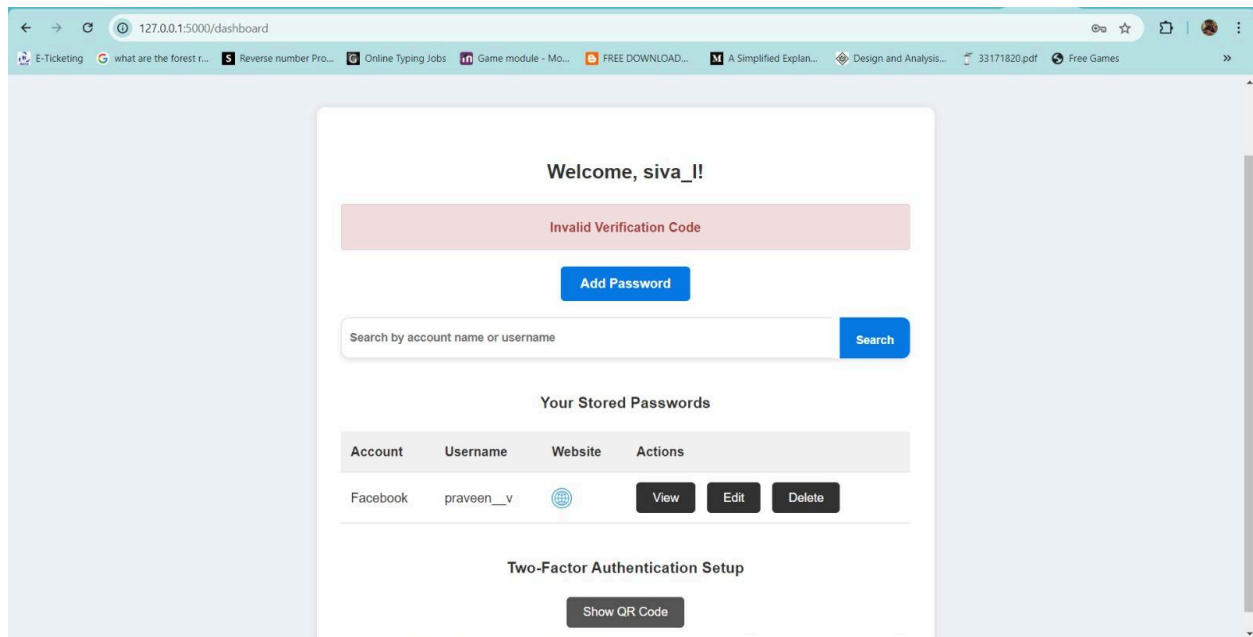
### Two-Factor Authentication Setup

Show QR Code

User needs to enter verification code if user need to view, Edit or delete the information.

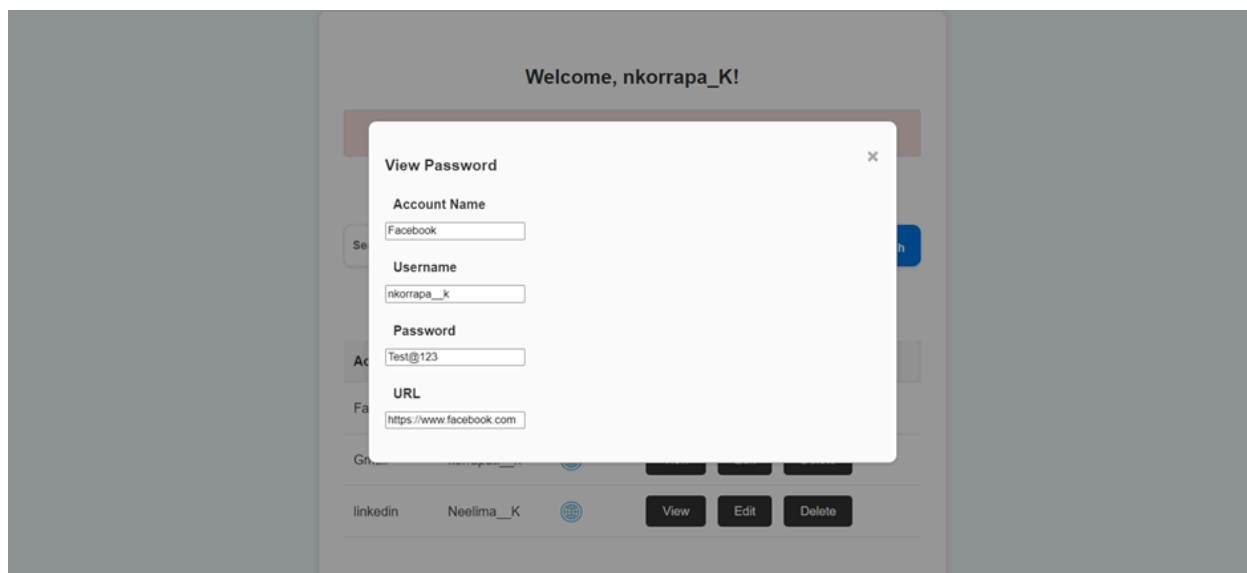


Shows warning when user enters incorrect verification code.



View:

This image allows users to view details of accounts, like account name, username, password, url related to the account.



Edit:

This screenshot depicts the interface for editing, adding user information or generating new password.

Add/Edit Password

Account Name


Facebook

Username

nkorrapa\_\_k

Password

b-@cCjD:3F:.



Generate Password

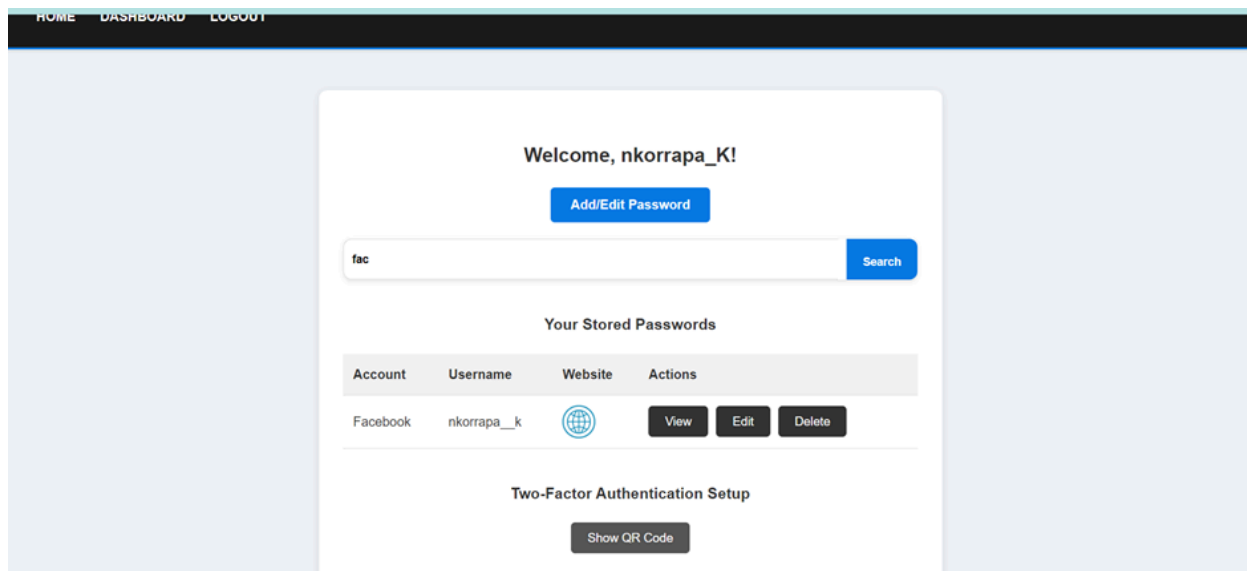
URL (optional)

https://www.facebook.com

Save

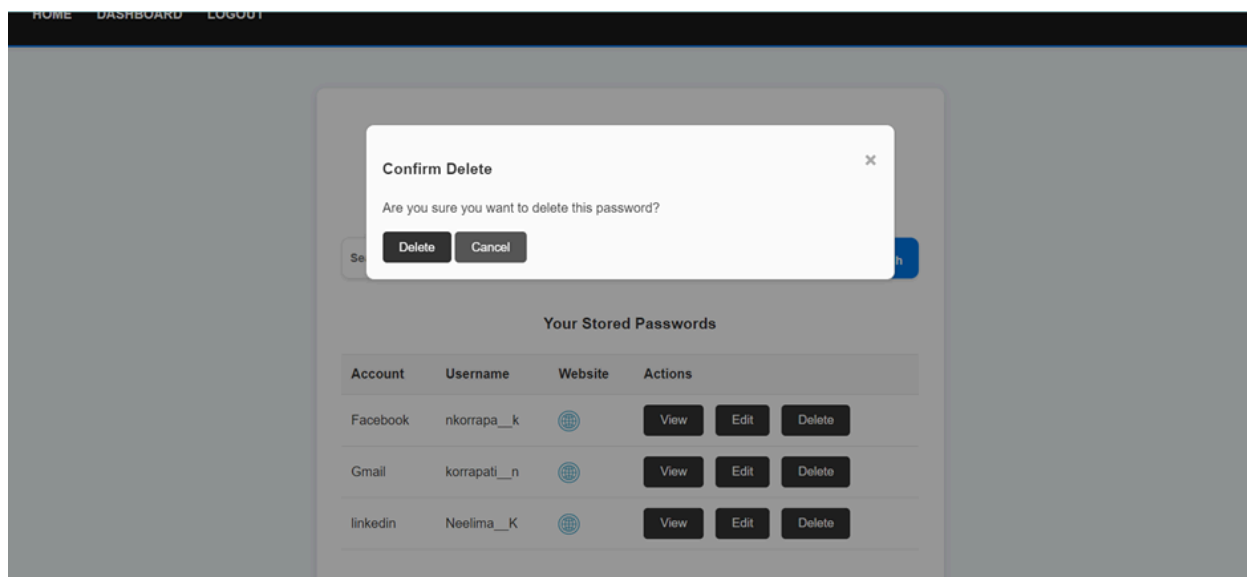
Search:

This image showcases the search functionality, enabling users to search for specific data or account within the application.

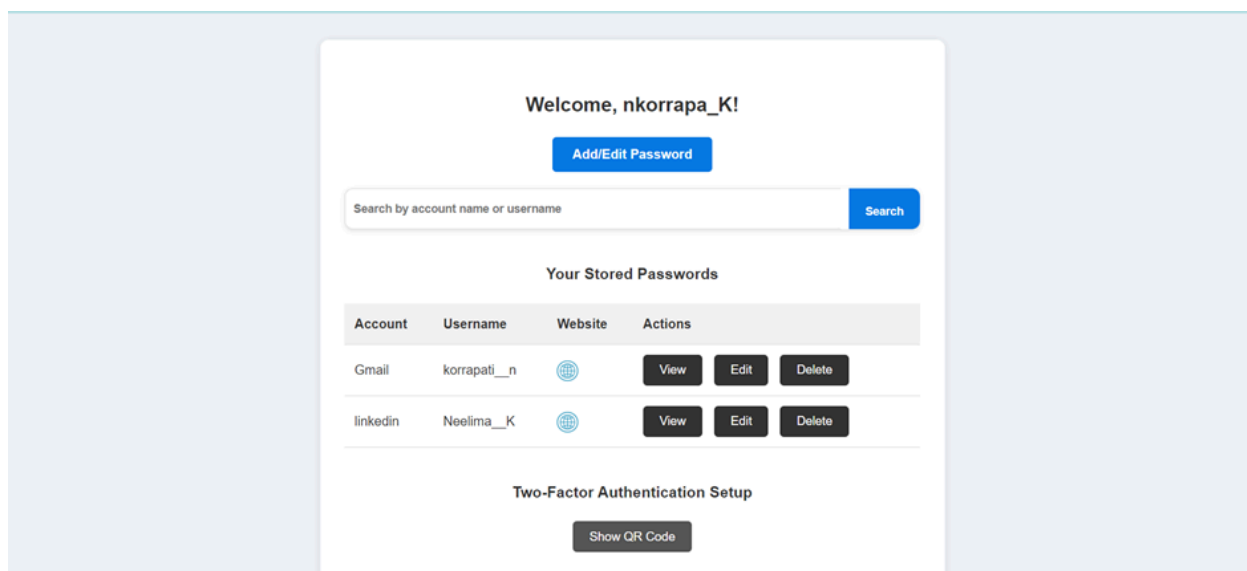


Delete:

This screenshot shows the option for users to delete information or accounts, including a confirmation prompt to prevent accidental deletions.

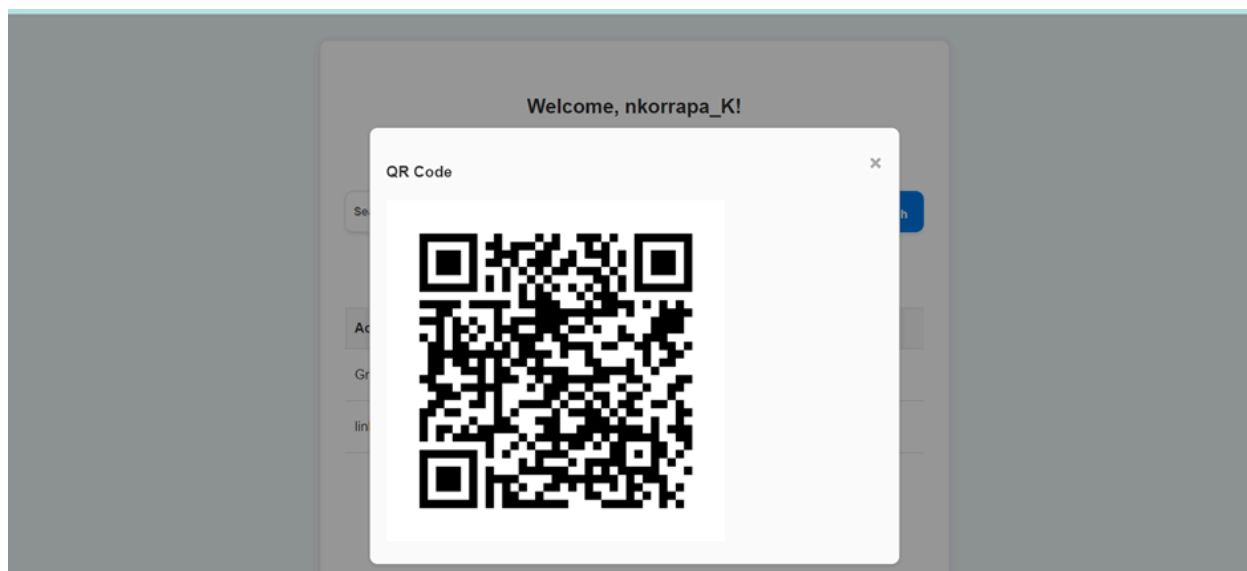






Show QR:

This is another instance of the QR code display if they don't scan the QR at beginning which is used for logging in, accessing specific information.



Logout:

This screenshot represents the logout functionality, allowing users to sign out of their accounts securely.

The screenshot shows a web browser window with the address bar displaying "127.0.0.1:5000/login". The browser's tab bar contains several open tabs, including "E-Ticketing", "what are the forest r...", "Reverse number Pro...", "Online Typing Jobs", "Game module - Mo...", "FREE DOWNLOAD...", "A Simplified Explan...", "Design and Analysis...", "33171820.pdf", and "Free Games". The website's navigation bar is black with white text links for "HOME", "LOGIN", and "REGISTER". A green banner message states "You have been logged out." Below this, a white login form is centered on a light blue background. The form is titled "Login" and contains two input fields: "Username" and "Password". A blue "Login" button is positioned below the password field. At the bottom of the form, a link reads "Don't have an account? [Register here](#)".

## **9)CONCLUSION**

The Secure Password Management System (SPMS) is a platform designed to tackle the challenges of password management in the modern digital landscape. It offers a secure and user-friendly interface for storing, managing, and retrieving passwords. The system employs advanced encryption, secure password hashing, and two-factor authentication to protect user credentials. Two-factor authentication is done after registering and viewing, editing or deleting your stored passwords. Key features include password addition, retrieval, updating, and deletion, all aimed at maintaining strong password practices. By integrating these security measures, SPMS ensures the confidentiality, integrity, and availability of user data, providing a robust solution for effective password management.