Januray 06th, 2026

**MFA Project Details**

University of Engineering and Technology, Mardan

Komail Ahmad Khalil | 22MDBCS259

Information Security

Dr. Raza Ullah

The Project Combines both the subjects of **Data Science** and **Information Security**, it is a small **Web-Based** application where some of it’s security features are discussed below:  
  
This project incorporates robust security measures to ensure safe user authentication and account verification. The primary focus is on maintaining data integrity and preventing unauthorized access through secure methods.

1. **Email Verification**:
   * During account registration, the system generates a unique verification code using Python's random module. This code is securely sent to the user's provided email address using the smtplib library, ensuring only valid email addresses are used for account creation.
   * The user is required to enter the received verification code on a dedicated verification page before completing the registration process. This step guarantees the authenticity of the email address and prevents the creation of fake or invalid accounts. By integrating this verification mechanism, the project ensures that only legitimate users gain access to the system.
2. **Password Management**:
   * User passwords are never stored in plain text. Instead, they are securely hashed using the werkzeug.security library, which applies a one-way hashing algorithm. This technique ensures that even if the database is compromised, the actual passwords remain protected and cannot be easily decrypted.
   * During the login process, the entered password is hashed on the server side and compared to the hashed version stored in the database. This ensures that the system validates users without ever exposing or transmitting raw password data. This method prevents vulnerabilities such as password leaks or brute-force attacks.
3. **Interactive Features for Enhanced Usability**:
   * To improve user experience during login, the project includes a "show password" toggle functionality. This feature allows users to view their entered password by clicking an eye icon, ensuring they can verify their input before submitting. Importantly, this feature does not compromise security, as the password is still hashed before being validated.

By combining these mechanisms, the project creates a secure environment for user authentication and account management. The email verification process ensures that only valid users are registered, while hashed passwords provide strong protection against data breaches. Interactive elements like the "show password" toggle enhance usability without undermining security, striking a balance between functionality and safety. These measures collectively safeguard user accounts and maintain the integrity of the system.

**NOTE:** To run the project, navigate to project folder and open terminal, type **python** **app.py** and hit enter, you’ll be provided with a link in a terminal, click on it to see the work in action. You may also be needed to provide your google account credentials for sending email.

You can also visit the below link to know more:   
 <https://support.google.com/accounts/answer/185833?hl=en>