Password Manager

This Python script implements a basic password manager with enhanced security features and user management capabilities. Key functionalities include:

1. User Account Creation:
    - Ensures unique usernames
    - Offers option for randomly generated or user-defined passwords
    - Implements security questions for account recovery
    - Utilizes SHA256 hashing for password and security answer storage
2. User Authentication:
    - Provides secure login functionality
    - Verifies hashed passwords for enhanced security
3. Password Management:
    - Allows users to update passwords after successful login
    - Implements a separate password update option with security question verification
    - Generates secure random passwords using a mix of letters, digits, and punctuation
4. Security Measures:
    - Employs SHA256 hashing for storing passwords and security question answers
    - Converts security answers to lowercase before hashing for consistency
    - Uses getpass for hidden password input
5. User Interface:
    - Provides a simple command-line interface
    - Offers options to create an account, log in, update password, or exit the program
6. In-Memory Storage:
    - Stores user credentials and security information in a dictionary during runtime

This implementation demonstrates fundamental principles of secure password management, including:

- Prevention of duplicate usernames
- Secure password and security answer hashing
- Multi-factor authentication through security questions
- Option for system-generated secure passwords