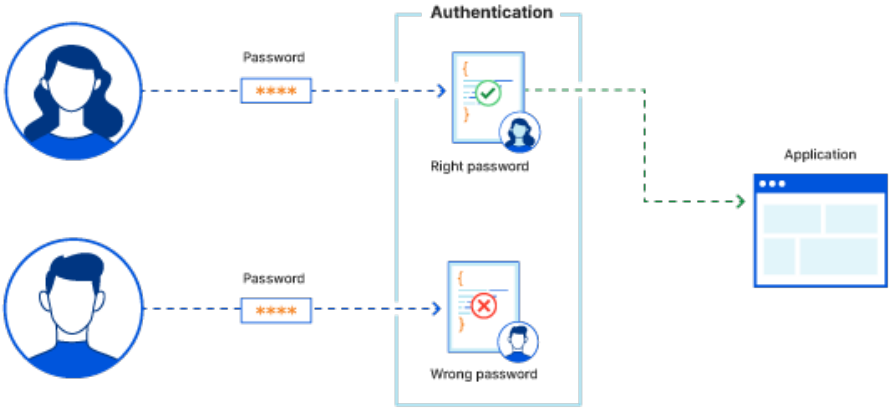
Security Features

User Authentication

→Implementation: The authentication mechanism is implemented in the authentication.py file. It uses SHA-256 hashing for storing passwords securely.
→How it Works: When a user attempts to log in, the system hashes the entered password and compares it with the stored hash. This ensures that even if the database is compromised, the attacker cannot retrieve the original password.
→The system checks if the entered password matches the stored password for that username.
→Testing: The test_authentication.py file contains unit tests that verify the correct functionality of the authentication mechanism, including password hashing and user verification.



Basic Access Control Mechanism

• Implementation: Access control is managed in the access_control.py file. It uses SQLite to store user-group mappings.
• How it Works: The system differentiates between two groups of users: 'H' and 'R'. Users in group 'H' can access all fields, while users in group 'R' have restricted access. This ensures that sensitive information is only accessible to authorized users.
• Testing: The test_access_control.py file contains tests that verify if the access control mechanism correctly restricts or allows access based on user groups.