# Misuser stories Acceptance Criteria

(The 2 Key Security Aspects being Covered)

**Misuser Story:** As a disgruntled employee, I want to change account balances to disrupt operations and manipulate the transactions.

**Acceptance Criteria:**

- Employees have role-based access controls that restrict direct manipulation of account balances i.e., we restrict the user to have access to the other users account and cannot act upon it.
- All changes to account balances must be traceable to a specific, auditable transaction and are recorded time to time on the Django admin portal.
- Alerts are in place for any modifications that don't correlate with a legitimate transaction and also the alerts are notified to the admin in the admin-side management.

**Misuser Story:** As a hacker, I want to intercept data transmitted between the database SQL2 and the user and also between 2 users and that can be seen using the postman service or the other Post methodologies used in the lab.

**Acceptance Criteria:**

- All data in transit must be encrypted and have restricted to access to each user.
- The application will implement certificate pinning to prevent man-in-the-middle attacks.
- Regular security audits and penetration tests can be conducted.
- And also we can use the View-sets and class to properly align the pages and control the traffic flow from one class to the other and also to the database.