# Authentication Tests

## 1. User Login:

- Verify login with valid credentials.

- Verify login with invalid credentials.

- Test login with empty username/password fields.

- Ensure account lockout after a certain number of failed login attempts.

- Check case sensitivity of username and password.

## ~~2. Multi-Factor Authentication (MFA):~~

~~- Verify login with MFA enabled.~~

~~- Ensure that MFA can be set up and disabled by the user.~~

~~- Test MFA with different methods (e.g., SMS, email, authenticator app).~~

~~- Check behavior when the second factor is incorrect or not provided.~~

## 3. Password Management:

- Test password strength requirements during registration and change.

- Verify password change functionality.

- Ensure password reset functionality works and is secure.

- Check if the old password is required when changing to a new password.

- Ensure that passwords are encrypted in the database.

## 4. Session Management:

- Verify that a session is created upon successful login.

- Ensure session timeout after inactivity.

- Test session termination upon user logout.

- Validate that sessions are invalidated after password change.

- Test concurrent session management (e.g., one user cannot have multiple active sessions if not allowed).

## 5. Single Sign-On (SSO):

- Verify SSO integration with third-party identity providers (e.g., Google, Azure AD).

- Ensure correct handling of SSO login and logout.

- Test SSO token expiration and refresh.

# Authorization Tests

## 1. Role-Based Access Control (RBAC):

- Verify that users are assigned appropriate roles.

- Ensure that users can only access features and data permitted by their roles.

- Test role assignment and revocation processes.

- Verify that role changes are applied immediately (or as expected).

2. Permission Management:

- Validate that permissions can be assigned and revoked accurately.

- Ensure that permissions are granular enough to cover different access levels.

- Test for proper enforcement of permissions in various parts of the application.

## 3. Access Control:

- Verify access control rules for different user types (e.g., admin, regular user).

- Ensure unauthorized users cannot access restricted pages or data.

- Test for proper error messages when access is denied.

- Validate access control for APIs and backend services.

## 4. Data Access:

- Verify that users can only access their own data.

- Test for data leakage between different user accounts.

- Ensure that sensitive data is properly masked or hidden where necessary.

- Validate that export functionalities respect data access rules.

## 5. Audit and Logging:

- Ensure that all authentication and authorization events are logged.

- Verify that logs capture necessary details (e.g., timestamp, user ID, action).

- Test access to audit logs (restricted to authorized users).

- Validate that log integrity is maintained.

# Security Tests

## 1. Brute Force Protection:

- Verify rate limiting on login attempts.

- Test CAPTCHA implementation after multiple failed login attempts.

- Ensure alerts are triggered for suspicious login activities.

## 2. Token Management:

- Verify secure storage and transmission of authentication tokens.

- Test token expiration and renewal mechanisms.

- Ensure that tokens are invalidated on logout.

## 3. Data Encryption:

- Verify that data is encrypted in transit (using HTTPS).

- Ensure sensitive data is encrypted at rest.

## 4. Vulnerability Scanning:

- Perform regular security scans for vulnerabilities in authentication and authorization mechanisms.

- Ensure proper handling of discovered vulnerabilities.

# Usability Tests

## 1. User Experience:

- Verify that error messages are user-friendly and do not reveal sensitive information.

- Ensure that the authentication and authorization flows are intuitive.

- Test the responsiveness and performance of authentication and authorization features.

## 2. Accessibility:

- Ensure that login, password management, and other relevant pages are accessible to users with disabilities.

- Test compatibility with screen readers and other assistive technologies.

## 3. Localization:

- Verify that authentication and authorization features support multiple languages if the application is internationalized.

# Recovery Tests

## 1. Account Recovery:

- Test account recovery process for lost usernames.

- Verify that users can securely reset their passwords.

- Ensure proper validation of user identity during account recovery.