Security Testing

Plans

Objective:
Ensure that the timetable system is secure, restricts unauthorized access, and protects sensitive data.

Scope:

- Validate that only authenticated and authorized users can access specific backend resources.
- Ensure data access is restricted based on user roles.
- Test backend endpoints for security vulnerabilities such as unauthorized access, missing authentication, or misconfigured permissions.

Test Cases:

- **Authentication and Authorization:** Ensure that users must authenticate to access the system.
- **Data Integrity and Consistency:** Ensure that no unauthorized modifications can occur.

Tools:

- **Testing Framework:**
    - **From backend**: Quarkus with RestAssured (for automated testing of API endpoints).
    - **From frontend**: Vitest
- **Manual Security Testing:** For specific scenarios such as access validation and response consistency.

Acceptance Criteria: Refer to Jira.

Progress + Results

Link to Tests:

- Frontend: jetedge/frontend/src/tests/security.test.ts at develop · hotungkhanh/jetedge
- Backend: jetedge/backend/src/test/java/org/acme/security/jpa/JpaSecurityRealmTest.java at main · hotungkhanh/jetedge

Test Cases

- **Unauthorized Access Tests:**
    - **Purpose:** Ensure that unauthenticated users are restricted from accessing secure endpoints.
    - **Tested Endpoints:** `/login`, `/rooms`, `/units`
    - **Expected Results:**
        - When accessed anonymously, these endpoints return an **HTTP 401 Unauthorized** status.
        - This verifies that the endpoints are protected by the basic authentication mechanism.
    - **Frontend Test Implementation:**
        - fetch GET request to `/login` endpoint returns HTTP 401 given incorrect combination of username and password
    - **Backend Test Implementations:**
        - `shouldNotAccessLoginWhenAnonymous`: Tests that the `/login` endpoint is inaccessible without authentication.
        - `shouldNotAccessRoomsWhenAnonymous`: Tests that the `/rooms` endpoint returns a 401 status for anonymous users.

        - `shouldNotAccessUnitsWhenAnonymous`: Tests that the `/units` endpoint returns a 401 status for unauthenticated access.

- **Authenticated Access Tests:**
    - **Purpose:** Verify that users with valid credentials can access the secured endpoints.
    - **Tested Endpoints:** `/login`, `/rooms`, `/units`
    - **Expected Results:**
        - Authenticated requests should return an **HTTP 200 OK** status.
        - This confirms the backend properly authenticates users with Basic Authentication.
    - **Frontend Test Implementation:**
        - fetch GET request to `/login` endpoint returns HTTP 200 and with the payload string “jetedge“ give correct combination of username and password
    - **Backend Test Implementations:**
        - `shouldAccessLoginWhenUserAuthenticated`: Verifies that authenticated users can access the `/login` endpoint and receive their username in the response body.
        - `shouldAccessRoomsWhenUserAuthenticated`: Tests that users with valid credentials can successfully access the `/rooms` endpoint.
        - `shouldAccessUnitsWhenUserAuthenticated`: Tests that authenticated users can access the `/units` endpoint and receive an appropriate response.