Java Technologies - Lab 6

[valid 2025-2026]

Security
We continue our project.

Compulsory (1p)

- Integrate Spring Security and verify that all your endpoints are now protected.
- Create a mock `/login` endpoint.
- Configure the security chain such as to permit unauthenticated requests only to the `/login` endpoint.

Homework (2p)

- Refactor your domain such as students and instructors are also *users* of the application. Other users may exist, such as an administrator.
- Configure Spring Boot to read the users and their roles (ADMIN, INSTRUCTOR, STUDENT) from the database.
- Implement JWT-based authentication and a login endpoint issuing tokens.
- Protect POST/PUT/DELETE endpoints with role-based access and keep GET endpoints public where reasonable.
- Implement password storage with BCrypt and a user registration flow.
- Add method-level security with `@PreAuthorize` and test it.
- Secure Actuator endpoints: expose only health and info publicly; require auth for metrics.

Advanced (2p)

- Integrate with Keycloak (or another IdP) for OIDC flows and map roles.
- Implement two-factor authentication via email or TOTP for ADMIN users.