Security report

User registration:

- A salt is randomly created with “SHA1PRNG” algorithm.
- Plain password provided by a user combined with a salt.
- Plain password with salt are hashed with “SHA-256” function and stored in the database
- If a user is already in the database, 409 error is returned.

User authentication:

- Hashed password and salt retrieved from a database for provided username.
- Plain password with salt are hashed with “SHA-256” and compared with hashed.
- If there is no such user in the db, or password does not match authentication failed and 401 error returned, otherwise a token is provided to a user.

Token system:

- Every request requires a token in the authentication header.
- In case of invalid token 401 error returned.

Design choices:

- “SHA-256” algorithm was chosen because every implementation of the Java platform is required to support it.
- Salt hashed together with a plain password to increase uniqueness of a password.
- Pepper is not used, to achieve more portability of the REST API. Pepper has to be stored in a server memory, so it’s harder to launch a server on another environment.
- All SQL quires are parametrized to prevent SQL injection.