

Security

Based on the codebase created during the previous module, implement follow functionality:

1. Add Spring Security module to your project and configurate it for Authentication access for all endpoints (except Create Trainer/Trainee profile). Use Username/Password combination.
2. Use salt and hashing to store user passwords in DB.
3. Configure Spring Security to use Login functionality.
4. Add Brute Force protector. Block user for 5 minutes on 3 unsuccessful logins
5. Implement Logout functionality and configure it in Spring Security.
6. Implement Authorization – Bearer token for Create Profile and Login functionality Use JWT token implementation.
7. Configure CORS policy in Spring Security.

Notes:

1. During Create Trainer/Trainee profile username and password should be generated as described in previous module.
2. All functions except Create Trainer/Trainee profile. Should be executed only after Trainee/Trainer authentication.