

## JWT AUTHORIZATION AND CORS

### PREREQUISITES:

The task is a continuation of **Homework 5** and should be done in the same repo.

### TASK 6.1

Add authorization to the already existing **REST** service.

- Add `login(username, password)` method which should return **JWT** token.
- Add a middleware which will proxy all the requests (except **login**) and check that **HTTP Authorization** header has the correct value of **JWT** token.
- In case of the **HTTP Authorization** header is absent in the request, the **middleware** should stop further controller method execution and return **HTTP 401** code (**Unauthorized Error**) and standard error message.
- In case of **HTTP Authorization** header has invalid **JWT** token in the request, the middleware should return **HTTP** code **403** (**Forbidden Error**) and standard error message.

### TASK 6.2

Add **CORS** middleware to access service methods from WEB applications hosted on another domains (<https://github.com/expressjs/cors>).

## EVALUATION CRITERIA

2. Task 6.1 is implemented partially; `login` method is added and **JWT** token is generated.
3. Task 6.1 is implemented partially; **JWT** token checking method is implemented.
4. Task 6.1 is fulfilled to the full extent; authorization working using middleware.
5. Task 6.2 is fulfilled to the full extent.