

## Lab 15: Authorization with JWT Token

In this lab you will add the possibility access non-public information from a second API server that requires a token as authorization method. The info will be about the amount of revenues for all the shown films, as well as the total audience for a subset of “premium” users.

### 1. Access another server by means of a JWT token

Add the possibility that authenticated users see the total amount of revenues (in millions of dollars) of the films in their film list. Such information should be reloaded every time the view with the list of films is refreshed, e.g., when the filter is changed.

Some users are registered in the system as “premium users”. Thus, the database must be changed accordingly. For premium users, also the total audience of each film will be shown.

Follow the programming pattern shown during the lectures:

- Create an authenticated API endpoint on the authentication server that allows to retrieve the token.
- Use the token to query a second API server, named “server2”, that will return the information.

To simplify the computation of the total amount of revenues, in “server2” just compute a random number in the range 0 to  $10 \cdot N$  for each film (where  $N$  is the number of characters of the film title, spaces excluded), sum all the numbers, and return such a value. In this way “server2” will not have to use any database to store information.

For the audience, just take the revenue number, multiply it by 1 million, divide it by a random value between 8 and 12 and round it to the nearest integer.

Finally, if you want, just for practice, push your solution of this lab on the private repository used to practice submission for the exam.

#### **Hints:**

1. For the JWT, decide a secret (change it from the lecture examples!), and use the same value that will be hardcoded in both servers (for simplicity and convenience, as a constant JS variable).
2. You can use the following website to check the JWT content: <https://jwt.io/>  
Note that you cannot use it to check or generate signatures for your application.