T7 - MSc Pool

Authentication

Project

Authentication

- The totality of your source files, except all useless files (binary, temp files, obj files,...), must be included in your delivery.

You're about to handle authentication and rights in your Time Manager application.

First and foremost, take the time to complete the bootstrap and make sure you practised all the concepts. In particular, insist on :

- Authentication management
- JSON Web Token
- Hashing passwords
- The XSRF Token
- Routing with view-router and its *hook* `'beforeEach()'`

API AND ROUTES

First of all, you need to adapt your API to add **Roles** and update your **user** schema to manage passwords.

Employees can be in multiple teams.

You also need to instantiate your database and tables by creating admin users with an **administrator** role, with the ability to do anything they want on the application.

Authentication must be accomplished using *JSON Web Tokens*, via the *Joken* library.
Create a c-xsrf-token, and then forge a JWT integrating it.

As you know, you must send the JWT in HTTP Only, and return the xsrf-token when connecting.
Each time you use a route, check the match of the request's xsrf-token with the one from the JWT.
This way, you will also retrieve the user's id and role.

Update your routes to handle passwords.

There is no CRUD for roles. Roles are predefined. The only possible action is to read these. The associations of the technologies used make it possible not to create routes, and through associations, retrieve the name of the role directly on the user.

DISPLAY

You know need to add new features of the application: connection, disconnection, role promotion/demotion.

> You may want to start from you existing application code; if so, comment all your routes to recreate new ones.
> Or restart your project from scratch…

For simplicity and maintability reasons, you may want to break apart the functionnalities of the **User** component into three components: authentication, registration and profile management. Bind them with the proper routes.

> Don't forget to add buttons and dropdowns in your template, and to trigger new methods.

PERMISSIONS MANAGEMENT

Finally, restrict access to certain pages of your site, regarding the role of the user.

> By the way, did you handle teams management?

{ EPITECH. }