Framework – CSID

Séance du vendredi 14 janvier 2022

Quentin LEULY

Objectifs de la séance :

- Implémenter la connexion d'un utilisateur
- Protéger certains endpoints et/ou méthodes en fonciton du rôle de l'utilisateur

Travail à faire

1. Récupérer les classes présentes dans le gist à l'adresse https://gist.github.com/Kaway/8a83b80e4ea5c5da94515d98a6e3527f et les ajouter à votre projet (adaptez le package de ces classes à votre projet)
2. Créer un *UserController (**/users**)*, permettant de :
   - **POST /** : créer un utilisateur (accessible à tous)
   - **PUT /me/password** : changer le mot de passe d'un utilisateur (uniquement possible de changer son propre mot de passe)
   - **PUT /users/{id}/authority** : changer l'*Authority* d'un utilisateur (uniquement les utilisateur ayant l'*Authority* ADMIN)
   - **GET /** : lister tous les utilisateurs en base (STAFF & ADMIN)
   - **GET /me** :renvoyer les informations de l'utilisateur courant (**GET /me**)
3. Protéger les endpoints suivants :
   - **GET /owners** : uniquement les utilisateurs avec l'Authority ADMIN
   - **PATCH /owners/{uuid}** : uniquement les utilisateurs ayant l'Authority STAFF
   - **POST /owners/{uuid}/bonsais/{bonsaiId}/transfer** : uniquement les utilisateurs avec l'Authority USER & le bonsai transféré doit appartenir à l'utilisateur connecté ou l'utilisateur connecté est ADMIN

- **DELETE /owners/{uuid}** : uniquement les utilisateurs avec l'Authority ADMIN
- **DELETE /owners/{uuid}/bonsais/{bonsaiId}** : uniquement les utilisateurs avec l'Authority USER & le bonsai transféré doit appartenir à l'utilisateur connecté ou l'utilisateur connecté est ADMIN
- **POST /owners/{uuid}/bonsais** : uniquement les utilisateurs avec l'Authority USER & le bonsai transféré doit appartenir à l'utilisateur connecté ou l'utilisateur connecté est ADMIN

- **DELETE /bonsais/{uuid}** : uniquement les utilisateurs avec l'Authority USER & le bonsai transféré doit appartenir à l'utilisateur connecté ou l'utilisateur connecté est ADMIN
- **PATCH /bonsais/{uuid}** : uniquement les utilisateurs avec l'Authority USER & le bonsai transféré doit appartenir à l'utilisateur connecté ou l'utilisateur connecté est STAFF
- **PUT /bonsais/{uuid}** : uniquement les utilisateurs avec l'Authority USER & le bonsai transféré doit appartenir à l'utilisateur connecté ou l'utilisateur connecté est STAFF

Quelques informations utiles

- Récupérer l'utilisateur connecté

```
AppUser credentials = (AppUser) SecurityContextHolder.getContext().getAuthentication().getCredentials();
```

Vous aurez accès à l'id de l'utilisateur et donc du owner

- Restreindre l'accès à une méthode ou une classe (controller ou service généralement) selon l'Authority de l'utilisateur

```
@PreAuthorize("hasRole('ADMIN')")
```

- Resteindre l'accès à des endpoints sans passer par l'annotation précendente (à mettre dans le fichier « *WebSecurityConfig.java* ») :

```
http.authorizeRequests()
        .antMatchers("/votre-url").hasAuthority("ADMIN")
        .antMatchers("/votre-url-2").hasAuthority("STAFF")
```

- Les *Authorities* définies dans le projet sont hiérarchiques : ADMIN > STAFF > USER ; une méthode avec l'accès restreint aux USER sera accessible par les utilisateurs STAFF et ADMIN.