ToDoCo

# Documentation technique

Une image contenant texte, lettre

Description générée automatiquement

Table des matières

[La classe User: 3](#_Toc130285825)

[Le fichier security.yaml : 3](#_Toc130285826)

[Le Security Controller 4](#_Toc130285827)

[Les Voters 4](#_Toc130285828)

## La classe User:

Introduction

La classe User est un modèle qui représente un utilisateur dans notre application. Elle stocke les informations d'identification de l'utilisateur, ainsi que d'autres informations sur l'utilisateur.

Propriétés

La classe User définit les propriétés suivantes :

Username : le nom d'utilisateur

Password : le mot de passe de l'utilisateur, hashé pour la sécurité.

E-mail : l'adresse e-mail de l'utilisateur, utilisé pour l’authentification.

Rôles : les différents rôles que peut avoir l’utilisateur.

Stockage des données

Les informations sur les utilisateurs sont stockées dans une base de données relationnelle telle que MySQL. Nous utilisons Doctrine, le mappeur d'objets relationnels de Symfony, pour gérer les interactions entre la classe User et la base de données.

Utilisation

La classe User est utilisée pour vérifier les informations d'identification de l'utilisateur lors de la connexion. Elle est également utilisée pour stocker les informations sur l'utilisateur, telles que son username et son adresse e-mail, pour être utilisées dans d'autres parties de l'application.

Résumé

La classe User représente un utilisateur dans notre application et stocke les informations d'identification et les informations sur l'utilisateur. Nous utilisons Doctrine pour gérer les interactions entre la classe User et la base de données. La classe User est utilisée pour vérifier les informations d'identification de l'utilisateur lors de la connexion et pour stocker les informations sur l'utilisateur pour être utilisées dans d'autres parties de l'application.

## Le fichier security.yaml :

Le fichier security.yaml de Symfony est un fichier de configuration qui définit les stratégies de sécurité de l’ application. Il définit comment les utilisateurs sont authentifiés.

Le fichier security.yaml utilise un format de configuration YAML et peut être configuré pour utiliser diverses méthodes d'authentification telles que l'authentification basée sur des jetons, l'authentification HTTP ou l'authentification à base de formulaires.

## Le Security Controller

Introduction

Le Security Controller est un contrôleur qui gère les actions liées à la sécurité dans l’application. Il utilise le système d'authentification de Symfony pour vérifier les informations d'identification de l'utilisateur et déterminer s'il est autorisé à accéder à certaines parties de l'application.

Fonctionnalités

Le Security Controller fournit les fonctionnalités suivantes :

Connexion : la vérification des informations d'identification de l'utilisateur pour la connexion.

Déconnexion : la déconnexion de l'utilisateur.

Utilisation

Le Security Controller est utilisé pour gérer les actions liées à la sécurité de l'utilisateur dans notre application. Il est appelé lorsque l'utilisateur souhaite se connecter ou se déconnecter.

Résumé

Le Security Controller est un contrôleur qui gère les actions liées à la sécurité dans notre application, telles que la connexion et la déconnexion. Il utilise le système d'authentification de Symfony pour vérifier les informations d'identification de l'utilisateur.

## Les Voters

Afin de protéger les différentes parties de l’application, nous avons utilisé des voters. Ils sont au nombre de deux, le user Voter et le task Voter.

Le User Voter :

Il sert à vérifier que l’utilisateur est connecté et peut accéder aux différentes parties de l’application suivant son rôle.

Il est appelé lors de l’accès aux différentes pages de l’application. Il dispose de deux paramètres, View et Edit.

Le paramètre View est appelé pour chaque page nécessitant d’être connecté et permet de rediriger l’utilisateur vers la page de connexion s’ il n’est pas autorisé à accéder à la page.

Le paramètre Edit permet de vérifier le rôle de l’utilisateur. Il est appelé lorsque celui-ci essaye d’accéder à la liste des utilisateurs ou de modifier leur rôle, ce qui n’est autorisé que pour les utilisateurs disposants d’un rôle Administrateur.

Le Task Voter

Il vérifie que l’utilisateur est autorisé à interagir avec les différentes taches déjà créées. Il est appelé lorsque l’utilisateur tente de modifier ou de supprimer une tâche, ce qu’il ne peut faire que si la tâche lui appartient ou, si la tâche est anonyme et s’il a le rôle Administrateur.