ToDo CO

Documentation technique

Guide d’authentification

Contexte

L'application ToDo&Co est développée sur le framework symfony qui propose un composant performant permettant de gérer l'authentification des utilisateurs

Authentification

Le système d'authentification

La section Firwalls de config/packages/security.yaml est la section la plus importante. Un " Firwalls " est votre système d'authentification : le pare-feu définit quelles parties de votre application sont sécurisées et comment vos utilisateurs pourront s'authentifier (par ex. formulaire de connexion, jeton API, etc.)

```
firewalls:
    dev:
        pattern: ^/(_(profiler|wdt)|css|images|js)/
        security: false

    main:
        anonymous: true
        lazy: true
        pattern: ^/
        form_login:
            login_path: login
            check_path: login
            csrf_token_generator: security.csrf.token_manager
            always_use_default_target_path:  true
            default_target_path:  /
        logout:
            path: logout
        switch_user: true
```

Autorisations

Les utilisateurs peuvent maintenant se connecter à l'application en utilisant le formulaire de connexion. Génial! Maintenant, vous devez apprendre comment refuser l'accès et travailler avec l'objet Utilisateur. C'est ce qu'on appelle l'autorisation, et sa tâche est de décider si un utilisateur peut accéder à une ressource (une URL, un objet modèle, L'utilisateur reçoit un rôle précis lorsqu'il ouvre une session (p. ex., ROLE_ADMIN). Vous ajoutez du code pour qu'une ressource (par ex. URL, controller) ait besoin d'un "attribut" spécifique (par ex. un rôle comme ROLE_ADMIN) pour être accessible. Rôles

Lorsqu'un utilisateur se connecte, Symfony appelle la méthode getRoles() sur votre objet User pour déterminer les rôles de cet utilisateur. Dans la classe User qui a été générée précédemment, les rôles sont un tableau stocké dans la base et chaque utilisateur reçoit toujours au moins un rôle : ROLE_USER

Access control

Les règles de restriction d'accès sont définies dans le fichier **security.yaml** sous le paramètre **access_control**. Les règles décrites ci-dessous définissent les comportements suivants:

- L'url "/login" est accessibles aux utilisateurs non authentifiés
- Toutes les urls commençant par"/users" ne sont accessibles qu'aux utilisateurs ayant le rôle administrateur.
- L'ensemble des autres urls est accessible aux utilisateurs authentifiés ayant le rôle ROLE_USER.

```
access_control:
    - { path: ^/login, roles: IS_AUTHENTICATED_ANONYMOUSLY }
    - { path: ^/users, roles: ROLE_ADMIN }
    - { path: ^/, roles: ROLE_USER }
```

Par Maria lalij