**Documentation de l'Implémentation de l'Authentification avec Symfony**

**Introduction**

Cette documentation a pour objectif d'aider les débutants à comprendre comment mettre en place l'authentification dans une application Symfony. Vous apprendrez quel(s) fichier(s) modifier, comment fonctionne le processus d'authentification et où sont stockés les utilisateurs.

**Fichiers à Modifier**

Pour implémenter l'authentification dans Symfony, vous devrez généralement travailler sur les fichiers suivants :

**1. SecurityController.php**

Le fichier **SecurityController.php** contient les actions liées à l'authentification, telles que l'affichage du formulaire de connexion et la gestion des erreurs d'authentification. Vous pouvez personnaliser ce fichier pour modifier le comportement de l'authentification, mais il est généralement géré par Symfony en fonction de votre configuration.

**2. security.yaml**

Le fichier **security.yaml** est le cœur de la configuration de sécurité de votre application. C'est ici que vous définissez les hacheurs de mots de passe, les fournisseurs d'utilisateurs, les pare-feu et les autorisations. C'est l'endroit où vous spécifiez comment l'authentification et l'autorisation sont gérées.

**Processus d'Authentification**

Le processus d'authentification dans Symfony suit généralement ces étapes :

**1. L'Utilisateur Accède à la Page de Connexion**

L'utilisateur accède à la page de connexion de votre application, qui est généralement accessible via une route définie dans **security.yaml**, comme **/login**.

**2. Le Formulaire de Connexion est Affiché**

Le code dans la méthode **loginAction** du **SecurityController.php** est responsable de l'affichage du formulaire de connexion. Les erreurs d'authentification précédentes et le dernier nom d'utilisateur entré sont récupérés et renvoyés à la vue.

**3. Soumission du Formulaire**

L'utilisateur soumet le formulaire de connexion en entrant ses informations d'identification (nom d'utilisateur et mot de passe).

**4. Vérification des Informations d'Identification**

Symfony vérifie les informations d'identification soumises en interne en utilisant la configuration définie dans **security.yaml**. Si les informations sont correctes, l'utilisateur est authentifié.

**5. Gestion des Erreurs**

Si les informations d'identification sont incorrectes, Symfony gère l'affichage des erreurs en utilisant la vue de connexion. Les erreurs sont récupérées depuis le service **AuthenticationUtils**.

**6. Accès Restreint**

Une fois authentifié, l'utilisateur peut accéder aux pages restreintes de l'application en fonction des autorisations définies dans **security.yaml**.

**Stockage des Utilisateurs**

Les utilisateurs sont stockés dans la base de données de l'application. La configuration du stockage des utilisateurs est définie dans **security.yaml** sous la section **providers**. Dans cet exemple, les utilisateurs sont stockés dans la table **User** de la base de données.

Pour personnaliser davantage l'authentification, vous pouvez explorer la configuration de sécurité dans **security.yaml** et adapter le **SecurityController.php** en fonction de vos besoins spécifiques.