

Dyma

Accueil

FORMATION

Formation initiale

COMMUNAUTÉ

Général

Algorithmes

Flutter

HTML&CSS

Java

JavaScript

PHP

React

Symfony

Bugs et corrections

ACTIVITÉ

Formations

Vidéo

Valider le cours

Quiz

Leçon suivante

PHP > 24. Authentification avec les sessions > 143. Comment fonctionne l'authentification ?

4 minutes

Comment fonctionne l'authentification ?

Il existe aujourd'hui deux principales approches pour l'authentification : l'utilisation de sessions et l'utilisation de tokens `JWT`.

Nous allons commencer par l'authentification basée sur les sessions en utilisant tout ce que nous avons appris dans le cours sur les `cookies` et sur les sessions.

Nous allons donc apprendre l'authentification par mot de passe utilisant les sessions.

Il s'agit de l'authentification de base d'une application Web et il est essentiel de la maîtriser.

Authentification par mot de passe en utilisant les sessions

L'authentification par mot de passe est toujours fondée sur deux étapes : l'inscription et la connexion.

Nous allons commencer par l'inscription.

L'inscription d'un utilisateur

Pour inscrire un utilisateur, vous envoyez un formulaire à votre serveur, en `HTTP` avec la méthode `POST` qui contient obligatoirement a minima un identifiant (pseudo, email etc) et un mot de passe.

Ensuite, le serveur va enregistrer, après plusieurs étapes (validation, hachage comme nous le verrons), l'utilisateur dans la base de données.

La connexion d'un utilisateur

Pour la connexion, la première étape est l'envoi en `POST` des identifiants de l'utilisateur au serveur.

La deuxième étape, est la récupération de l'utilisateur dans la base de données qui correspond à l'identifiant unique.

La troisième étape est la vérification du mot de passe, qui n'est bien sûr pas en clair comme nous le verrons.

La quatrième étape est la création de la session, et sa sauvegarde dans la base de données. La session contiendra a minima son `id` et un identifiant unique de l'utilisateur.

Enfin, dernière étape, nous créons un `cookie` contenant l'`id` de la session venant d'être créée pour permettre le maintien de la connexion pendant plusieurs requêtes.

La persistance de la connexion d'un utilisateur

A chaque requête le navigateur va envoyer les `cookies` associés à votre domaine en respectant les options définies.

Il enverra donc le `cookie` contenant l'`id` de la session à chaque requête au serveur.

Le serveur va utiliser l'`id` de la session pour authentifier chaque requête de la manière suivante :

Premièrement, il va récupérer l'`id` de la session sur le `cookie`.

Deuxièmement, il va récupérer les données de la session dans la base de données en utilisant l'`id`. La session contient les informations permettant de récupérer l'utilisateur, la plupart du temps son `id` comme nous l'avons vu.

Troisièmement, l'utilisateur est récupéré grâce son `id` contenu dans la session.

La déconnexion d'un utilisateur

Pour déconnecter un utilisateur, il suffit de supprimer le `cookie` ainsi que la session dans la base de données.

Authentification par mot de passe en utilisant les sessions

L'inscription d'un utilisateur

La connexion d'un utilisateur

La persistance de la connexion d'un utilisateur

La déconnexion d'un utilisateur