1.3 B-02 : Create session tokens

Introduction :

La création de tokens de session est un élément clé dans la gestion de l'authentification et de la sécurité dans les applications Web. Dans ce projet, j'ai mis en œuvre la création de tokens de session en utilisant des technologies telles que JSON Web Tokens (JWT) et les cookies sécurisés. Cette compétence est essentielle pour garantir la sécurité des sessions utilisateur et pour permettre des interactions sécurisées entre l'application frontend et l'API backend.

1. **Utilisation de JSON Web Tokens (JWT) :**

- Création et signature: J'ai généré des tokens JWT contenant des informations utilisateur spécifiques, comme l'ID de l'utilisateur et d'autres données nécessaires. Ces tokens sont signés à l'aide d'une clé secrète qui est stockée dans un fichier .env pour garantir leur authenticité.

- Expérience et validité : Les tokens JWT peuvent avoir une durée de validité spécifiée, après laquelle ils expirent automatiquement, içi dans l'api j'ai fait en sorte que le token expire en 1 heure. Cela renforce la sécurité et garantit que les sessions restent valides uniquement pendant une certaine période.
  PS : le code est disponible dans la fonction signin du lien.

  Lien :

  https://github.com/Lucas-Moreno/code-epitech/blob/main/back/src/controllers/auth.controller.ts

2. **Utilisation de Cookies Sécurisés :**

- Option de Sécurité : L'utilisation de cookies sécurisés permet également de définir des options telles que le domaine, le chemin et la durée de validité du cookie.

Lien :

https://github.com/Lucas-Moreno/code-epitech/blob/main/back/src/controllers/auth.controller.ts

3. **Gestion de sessions utilisateur :**

- Connexion et déconnexion : Les tokens de session ont été utilisés pour gérer les sessions utilisateur, permettant aux utilisateurs de se connecter et de se déconnecter de manière sécurisée.
- Protection des routes : Les tokens de session ont également été utilisés pour protéger les routes nécessitant une connexion. Si un utilisateur n'est pas authentifié, il est redirigé vers la page de connexion.

4. **Sécurité Renforcée :**

- Confidentialité des Données : L'utilisation de tokens de session sécurisés contribue à garantir la confidentialité des données des utilisateurs en empêchant leur accès non autorisé, de plus bcrypt, une librairie javascript à été mis en place pour crypter les mots de passes de la base de données .
- Eviter les attaques : En stockant les tokens de manière sécurisée et en les signant, je réduis le risque d'attaques telles que la falsification de token et l'usurpation d'identité.

5. **Conclusion :**

La création de tokens de session est un élément crucial dans la mise en œuvre d'une authentification sécurisée dans les applications Web. En utilisant des technologies telles que JWT et les cookies sécurisés, nous avons réussi à créer des sessions utilisateur fiables et sécurisées. Cette compétence joue un rôle fondamental dans la construction d'applications Web modernes, garantissant l'expérience utilisateur tout en maintenant la sécurité des données.