### **Workflow d'authentification à l'arrivée sur le site**

1. **Vérifier la présence d'un token dans localStorage** :
   * Lorsqu'un utilisateur arrive sur le site, le code vérifie si un token d'accès (access\_token) est présent dans localStorage.
2. **Vérifier l'expiration du token d'accès** :
   * Si un token d'accès est trouvé, il est décodé pour vérifier son expiration. Si le token n'est pas expiré, l'utilisateur est considéré comme authentifié.
   * Si le token est expiré, le code tente de rafraîchir le token en utilisant le token de rafraîchissement (refresh\_token).
3. **Rafraîchir le token d'accès** :
   * Une requête est envoyée au serveur pour obtenir un nouveau token d'accès en utilisant le token de rafraîchissement.
   * Si la requête de rafraîchissement est réussie, les nouveaux tokens sont stockés dans localStorage, et l'utilisateur est considéré comme authentifié.
   * Si la requête de rafraîchissement échoue (par exemple, si le token de rafraîchissement est également expiré), l'utilisateur est redirigé vers la page de connexion.
4. **Utiliser les tokens pour les requêtes HTTP** :
   * Toutes les requêtes HTTP envoyées à l'API incluent automatiquement le token d'accès dans l'en-tête Authorization.
   * Si une requête reçoit une réponse 401 (Unauthorized), cela signifie que le token d'accès est invalide ou expiré, et le code tente de rafraîchir le token d'accès.
   * Si le rafraîchissement échoue après une réponse 401, l'utilisateur est déconnecté et redirigé vers la page de connexion.