

Objectif : Crée un middleware d'authentification qui vérifie si un utilisateur est authentifié avant d'accéder à certaines routes protégées.

Instructions :

- Crée un serveur Express.
- Implémente un middleware d'authentification qui vérifie la présence d'un header "Authorization" dans la requête.

Si l'en-tête est présent, autorise l'accès à la route.

Si l'en-tête est manquant ou invalide, renvoie un message d'erreur "Accès interdit" avec le code d'état 403.

Crée une route protégée (/private) qui nécessite l'authentification pour être accessible.

Bonus (difficile)

Ajout d'une gestion des rôles (Bonus)

Voici une version enrichie de l'exercice 2 pour gérer les rôles. Vous allez créer un middleware pour vérifier les rôles avant d'autoriser l'accès à certaines routes.

Étapes

Ajoutez une simulation d'authentification.

Simulez une "authentification" simple avec un middleware. Ajoutez un utilisateur fictif (par exemple, un objet req.user) contenant des informations comme son rôle (par exemple, "user" ou "admin").

Créez un middleware de contrôle des rôles.

Ajoutez un middleware checkRole qui vérifie si l'utilisateur possède le rôle nécessaire pour accéder à une route spécifique.

Retournez une réponse 403 si l'utilisateur n'a pas les droits.

Protégez des routes en fonction des rôles.

Ajoutez des routes accessibles uniquement à certains rôles (ex. : une route "admin" accessible uniquement aux administrateurs).

Pour tester votre code plusieurs possibilités: soit via Postman, soit en ayant comme premier middleware, un middleware qui vous permet d'ajouter un user dans la requête pour "simuler" du type : req.user = {

```
  id: 1,  
  name: 'John Doe',  
  role: 'user', // Modifier en "admin" pour tester l'accès admin  
}
```