Projet Dev-Auth

contact@ls-a.fr
https://www.ls-a.fr

Table des matières

Contexte

Vous devez réaliser une application de création de blog. Chaque personne peut créer son espace, dès le moment où celle-ci a créé son compte. Le blog de chaque personne peut être disponible en public (chaque visiteur peut lire les contenus sans pour autant être identifié) ou en privé (le visiteur doit disposer d'un compte et être identifié pour visualiser le contenu).
Des privilèges doivent être plus élevés pour créer du contenu : dans ce cas, une authentification à deux facteurs est nécessaire.

Fonctionnalités

Le site doit proposer pour toutes et tous :

- Sur la page d'accueil, une sélection de quelques blogs mis en avant
- Sur la page d'un blog public, la liste des contenus

Le site doit proposer pour les personnes identifiées :

- La possibilité d'accéder aux blogs privés

Le site doit proposer pour les personnes ayant activé l'authentification à deux facteurs :

- La possibilité de créer son espace personnel
- La possibilité d'ajouter, de modifier ou supprimer des contenus de son espace personnel

Inscription et connexion

Le système pour créer un compte et se connecter doit proposer les éléments suivants :

- Inscription par identifiant (adresse mail) et mot de passe
- Inscription par différents fournisseurs d'identité (au choix : Auth0, Google, Facebook, Discord, Steam, Twitter, GitHub, ...)

La connexion doit pouvoir se dérouler par le même biais que l'inscription.
Après la connexion, le site doit suggérer la possibilité d'utiliser l'authentification à deux facteurs (présentée plus bas dans ce document).

Note : plusieurs équipements doivent pouvoir être connectés en simultané au même compte. Exemple, le même compte peut être connecté sur un téléphone et un ordinateur.

Maintien de la connexion

La connexion, une fois réalisée, doit fournir à la personne se connectant un JWT (JSON Web Token), preuve de la connexion valide. Ce JWT doit contenir à minima les éléments suivants :

- L'identifiant de l'utilisateur
- Si l'utilisateur utilise l'authentification à deux facteurs ou non.

A chaque requête, le JWT doit être envoyé par le client, vérifié par le serveur pour déterminer les autorisations associées à l'utilisateur.

Déconnexion

L'application doit permettre de se déconnecter de l'équipement en cours, mais également de tous les équipements connectés sur le compte d'un seul coup. Pour cela, il faudra considérer tous les JWT concernés comme inopérants. Dans le cas d'une déconnexion de tous les équipements, il faudra demander un code via l'authentification à deux facteurs.

Authentification à deux facteurs

L'application doit être connectable à l'application Google Authenticator disponible sur l'App Store et le Play Store. Par le biais d'un qrCode, il doit être possible d'ajouter l'application de blog dans Google Authenticator.
Note : il n'est pas nécessaire de disposer d'un nom de domaine pour cette étape.

Bonus : Serveur OAuth2 pour les images

L'application devrait permettre d'ajouter des images à chacune des publications. Dans ce cas, les images seront transférées de l'application vers un second serveur implémentant OAuth2 avec le type de grant "client credentials".

Ce protocole permettra de s'assurer que seule l'application peut envoyer de nouvelles images, et non des utilisateurs non autorisés.

Modalités de réalisation

Le projet doit être réalisé par groupe de 2 à 4 personnes. La note sera portée sur les éléments suivants :

- Les fonctionnalités sont présentes
- Une documentation est présente pour l'installation du projet

- Les bonnes pratiques de développement sont respectées (qualité du code, commentaires)
- Des malus pourront être appliqués en cas de non-respect du nombre de personnes par groupe, de plagiat ou de rendu en retard.