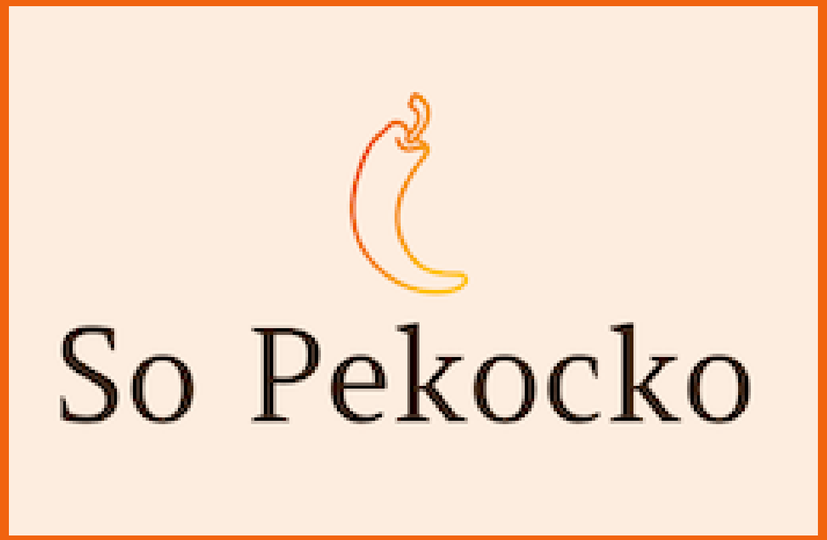


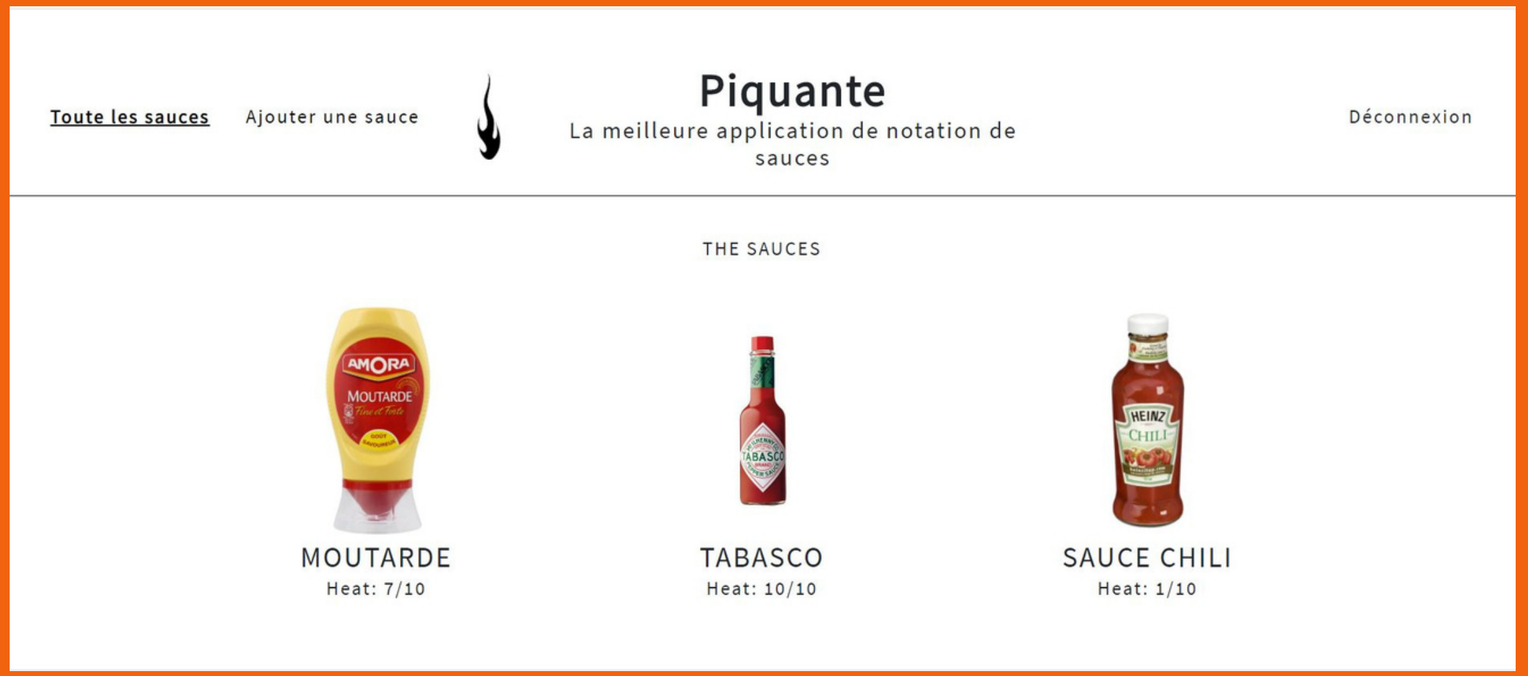
Création de l'application web "Piquante"

Auteur: Claire-Lise Démettre

Présentation du projet

- La marque So Pecocko crée des sauces piquantes avec un succès considérable
- Création d'une aplication web qui évalue les sauces piquantes de So Pekocko
- Chaque utilisateur peut ajouter sa sauce préférée et liker/disliker celles des autres utilisateurs

Présentation de l'application web "Piquante"



Les fonctionnalités

- Création d'un utilisateur
- Accès à toutes les sauces entrées dans l'application
- Création d'une sauce
- Modification de la sauce créée
- Suppression de la sauce créée
- Like/Dislike d'une sauce d'un autre utilisateur
- Déconnexion et reconnexion au compte utilisateur

Création d'une API REST pour le Backend

Application Programming Interface:
Moyen de communication entre client et données

Representational State Transfer:
se base sur le protocole de requête http

Create
Read
Update
Delete

Des lignes directrices architecturales spécifiques

Des avantages importants:
Séparation client/serveur
Stateless
Mise en cache

Technologies utilisées

Node.js

Runtime qui permet d'écrire toutes les tâches côté serveur en JavaScript

Express

Framework reposant sur Node qui facilite la création et la gestion des serveurs Node

MongoDB Atlas

Base de données
Création de shémas de données stricts (utilisateurs et sauces)

La Sécurité

RGPD

Le Réglement Général sur la Protection des Données encadre le traitement des données personnelles sur le territoire de l'Union européenne.

OWASP

L'Open Web Application Security (OWASP) est un organisme à but non lucratif mondial qui milite pour l'amélioration de la sécurité des logiciels. Il évalue les dix principaux risques pour la sécurité des applications web et préconise un développement logiciel sécurisé.

Mesures de sécurité mises en place

- Hashage du mot de passe utilisateur avec bcrypt
- Manipulation sécurisée de la base de données avec mongoose
- Vérification que l'email utilisateur soit unique dans la base de données avec mongoose-unique-validator
- Authentification de l'utilisateur par token avec jsonwebtoken
- Protection des headers avec helmet
- Validation des inputs email
- Authentification sur les routes requises
- Sécurisation du nom d'utilisateur et mot de passe de la base de données dans le fichier config.js (voir le Read.me)
- Mise en place d'une politique de confidentialité
- Deux types de droits administrateur sur la base de données

Pour tester l'API

1. Installer la version 4 de node-sass

2. Cloner le frontend ici => https://github.com/OpenClassrooms-Student-Center/dwj-projet6
   Le frontend du projet a été généré avec Angular CLI version 7.0.2.
   - Dans un terminal accéder au frontend
   - Installer : npm install
   - Lancer: ng serve

3. Cloner le backend ici => https://github.com/ClaireLise-dev/So_Pekocko

4. Ajouter un fichier config.js en suivant l'exemple config_exemple.js. Vous y entrerez l'adresse srv "secrète" de la base de données que voici:
"mongodb+srv://Clairelise86:Cl121186@cluster0.sxv0c.mongodb.net/Cluster0?retryWrites=true&w=majority"

5. Dans un autre terminal:
   - Accéder au dossier backend
   - Lancer: node server

6. Le frontend est accessible à l'adresse http://localhost:4200