Piquantee HotTakes

Shmuel Bitan

Fonctionnement du site : Connexion

L'utilisateur va pouvoir créer un compte avec un mail valide et unique (donc avec lequel aucun compte est créé) et un mot de passe sécurisé (je reviendrai dessus dans un second temps) .

Le mot de passe est crypté grâce a la fonction hash puis envoyé vers la base de données mongodb .

Lorsque l utilisateur va se connecter on va chercher son mail dans la bdd et si il y apparait on va le comparer avec le mot de passe est stocké dans la bdd .

Fonctionnement du site : ajout de sauce

Après que l'utilisateur se soit inscrit ou connecté il a la possibilité d'ajouter une sauce sur le site .

Pour cela il a juste à renseigner le nom le producteur une description une image et l'ingrédient principale .

Ensuite l'utilisateur a la possibilité de liker ou disliker les sauce (on peut le faire sur toute les sauces du site même si elles ont été ajoutée par un autre utilisateur) et les utilisateurs peuvent voir le nombre de like par sauce .

Fonctionnement du site : modification de la sauce

Apres avoir ajouté une sauce l'utilisateur pourra la modifier ou la supprimer mais chaque utilisateur ne peut modifier que les sauces ajoutées par lui.

Lors de la modification de la sauce il pourra modifier tous les champs remplis lors de l'ajout et cela va modifier la sauce dans la bdd (pareil lors de la suppression)

Sécurisation du site mot de passe

D après la CNIL

D’après une étude de Verizon de 2021, 81 % des notifications de violations de données mondiales seraient liées à une problématique de mots de passe. **En France, environ 60 % des notifications reçues par la CNIL depuis le début de l’année 2021 sont liées à du piratage** et un grand nombre aurait pu être évité par le respect de bonnes pratiques en matière de mots de passe.

J ai donc mis en place un schéma de mot de passe pour le renforcer .

Le mot de passe devra donc comporter au minimum 8 caractères et au maximum 30 .

Il devra comporter 2 chiffres , au moins une majuscule et une minuscule et aucun espace .

Sécurisation du site owasp

Ajout de helmet pour sécuriser les headers http et éviter la fuite d'information sur express qui pourrait compromettre l'api .Voir:

https://www.veracode.com/blog/secure-development/fasten-your-helmetjs-part-1-securing-your-express-http-headers#:~:text=li-,Helmet.,from%20the%20end%2Duser%20perspective.

Ajout de mongo sanitize pour éviter les injection sql et la fuite d'information . Voir:

https://owasp.org/www-project-proactive-controls/v3/en/c3-secure-database

Ajout d un nombre maximale d essaie de mot de passe par adresse ip . Voir:

https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Amélioration future: vente en ligne rgpd

Sécurisez les données en ligne :

- l'ensemble du parcours de vente doit être en https ;
- ne transmettez pas de données personnelles par email (exemple : mot de passe, coordonnées personnelles) ;
- ne conservez pas les coordonnées bancaires de vos clients ;
- sécurisez la transaction bancaire.