I**ntroduction**

Aujourd’hui nous avons un défi ! Nous devons travailler sur la partie sécurités de notre application Calorie Traqueur. Pour cela nous allons écrire ici toutes notre stratégie de sécurités et listé également les axes primordiaux de protection

Cette application aura pour but de venir en aide à toutes les personnes souhaitant venir à bout de leurs objectifs physiques.

**LES 3 GRANDS AXES**

Les trois grands axes sur lequel nous allons nous concentrer aujourd’hui sont...

- La protection des données personnelles.

* L’identification.
* La protection de la partie client.

**LA MISE EN PLACE**

**LA PROTECTION DES DONNÉES PERSONNELLES.**

* Utiliser le principe de Moindre Privilège ( Pour limiter les vols ainsi que la destruction de données ).
* HTTPS ( Pour sécuriser les échanges de données ).
* CSP ( Permet de sécuriser les échanges avec l’API )

**LA SÉCURITÉ LIÉ AU MOTS DE PASSE**

Nous allons dans un premier temps définir notre plan d’actions dans la partie authentification et mots de passe car c’est le premier élément à laquelle notre client utilisateur sera confronter.

* Interdire l’accès après trop de tentative échouer (8) de mots de passe pour contrer les attaques en ligne.
* Hacher le mot de passe ainsi que rajouter un salage pour contrer les attaques hors ligne.
* Utiliser des caractères spéciaux dans les mots de passe pour contrer les attaques par dictionnaire.
* Utiliser un canal sécuriser comme un flux encapsuler pour un protocole TLS pour contrer les attaques par homme du milieu.
* Complexité et longueur minimale requises.
* Notifications d’activités suspect.

**LA SÉCURITÉS LIÉ À L’EXPERIENCE UTILISATEUR**

Dans cette partie nous allons nous intéresser à la partie de la sécurité au moment où l’utilisateur interagie avec l’application.

* Défense en profondeur.
* Réduction de la surface d’attaques.
* HSTS ( Pour limiter les risques d’attaque ‘ man in the middle ‘ ).
* SOP
* CORS
* Utilisation de la balise HTML <template> contre les vulnérabilités XSS.
* Dissocier clairement la composition des pages web ( HTML, CSS, JAVASCRIPT ).
* Utiliser le X-XSS protection
* Utiliser XMLHttPRequest ( Pour encoder )
* Choisir une API selon ça méthode HTTP
* Audit.