Questions / Réflexions

Prime-Fitness

**Qu’elle technologie choisir pour le Back-End ?**

-Je vais partir sur du PHP, car je connais assez bien PHP pour espérer sortir un projet exploitable sans trop de problème.

**Framework ou non pour le Back-End ?**

-J’ai envie de la faire sans Framework afin d’avoir un contrôle TOTAL sur le code et pouvoir expliquez le moindre parti du code fourni.

**Qu’elle technologie pour le Front-End ?**

-Je vais utiliser Bootstrap et du HTML, Javascript, Css en plus quand cela sera nécessaire

**Framework ou non pour le Front-End ?**

-Oui Bootstrap dernière version seulement, pas de jQuery ou autre, Le but est d’utilisé Bootstrap pour s’avancer au maximum sur le coté CSS

**Coté sécurité que faire ?**

-La première idée qui me viens à l’esprit est d’utilisé en premier lieux Cloudflare, pour la simple et bonne raison qu’il fourni un service tellement important pour la sécurité que de passer outre serait aujourd’hui un peut bête, par exemple il fournit une bonne protection contre les attaques DDOS, il permet de cacher l’IP réelle du serveur, ça permet aussi d’ajouter certain filtre dans les requêtes et bien d’autre chose.

-Ensuite dans le site lui-même toutes les requêtes seront des requêtes préparées ainsi il est impossible de détourner une requête afin d’exploité une potentielle faille injection SQL

-Pour les mots de passe TOUS les mots de passe seront hash dans la base de données, et aucun mot de passe ne sera envoyé par mail, nous enverrons un lien pour modifier le mot de passe avant même que l’utilisateur puissent se connecter, Les mots de passe seront OBLIGATOIREMENT des mots de passe fort (au moins 1 lettre majuscule, 1 lettre minuscule, 1 chiffre, 1 caractère spécial et au minimum 8 caractère)

-Pour tout ce qui est affichage le moindre texte qui aurai pu être entré par l’utilisateur devra être échappé et non pas interprété comme du html, ainsi on évitera les faille XSS qui pourrait potentiellement venir de là.

-Pour améliorer la sécurité on passera les cookies en http only ainsi javascript ne devrais théoriquement pas pouvoir récupérer de cookie même avec une attaque XSS.

-Pour les formulaires on ajoutera coté front des patterns qui permettent de vérifier que les données entrer soit valide même si, en soit, ce n’est pas une protection efficace mais ça démotivera certaine personne, coter back on validera les données de la même manière avec les mêmes patterns via des regex, ainsi on devrait bloquer quasiment la totalité des attaques par formulaire possible

-afin de bien séparé les fonction administrateur d’un utilisateur on va aussi créer un contrôleur admin afin de ne laisser passer que les administrateurs accédés à la soumission des formulaires, cela aura pour effet que même si un utilisateur enverrez un formulaire comme par magie celui-ci serai automatiquement bloqué par le contrôleur avant même d’arriver à la soumission ou au test

**Combien de café j'ai bu aujourd'hui ? :**

- Après moulte réflexion j'en ai déduit qu'il valait mieux attendre le lendemain pour avoir un compte sur et avoir à les comptez une seule fois, dans un soucis de n'oubliez aucun café j'ai décidé de noter sur une ardoise d'école de ma grande avec un bâton par café bu au marqueur rouge ! ainsi aucun oublie possible et à J+1 il suffit de compter le nombre de bâtons !