Questions / Réflexions

Prime-Fitness

**Quelle 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 expliquer la moindre partie du code fourni.

**Quelle technologie pour le Front-End ?**

-Je vais utiliser Bootstrap, du HTML, Javascript et 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’utiliser Bootstrap pour s’avancer au maximum sur le côté CSS.

**Côté sécurité que faire ?**

-La première idée qui me vient à l’esprit est d’utiliser en premier lieu Cloudflare. Pour la simple et bonne raison qu’il fournit un service tellement important pour la sécurité, que de passer outre serait aujourd’hui un peu bête. Par exemple, il fournit une bonne protection contre les attaques DDOS, il permet de cacher l’IP réelle du serveur, permet aussi d’ajouter certains filtress dans les requêtes et bien d’autres choses.

-Ensuite dans le site lui-même, toutes les requêtes seront des requêtes préparées. Ainsi il est impossible de détourner une requête SQL afin d’exploiter 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 puisse 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 caractères).

-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 failles XSS potentielles.

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

-Pour les formulaires, on ajoutera côté front des patterns qui permettent de vérifier que les données entrées soient valides même si, en soit, ce n’est pas une protection efficace mais ça démotivera certaines personnes. Côté back on validera les données de la même manière avec les mêmes patterns via des regex. Ainsi on laissera passer seulement les données autorisées et rien d’autre.

-Afin de bien séparer les fonctions 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 envoi un formulaire non conforme, celui-ci serait automatiquement bloqué par le contrôleur avant même d’arriver à la soumission ou au test.