Zen'Etude : mesures de sécurités

Dans le cadre de la réalisation du projet tuteuré, nous avons établis plusieurs mesures de sécurités, afin d'assurer des protections de bases.

I) Protection anti-XSS (injection de Javascript)

Les attaques de type XSS permettent d'injecter du code Javascript dans une page Web quelconque. Ainsi, une personne mal intentionnée pourrait injecter du code Javascript dans une page web, l'envoyer à un responsable (professeur par exemple, ou administrateur), et voler son cookie de session (cookie garantissant l'authenticité de l'utilisateur).

Mesure : Utiliser la fonction PHP strip_tags() et htmlspecialchars() , permettant de sécuriser une chaine de caractère et ainsi d'éviter l'injection de code malveillant.

II) Protection anti injection SQL

Les attaques de type injections SQL fonctionnent de telle sorte qu'un utilisateur mal intentionné puisse injecter du code SQL, et ainsi récuperer voir alterer des informations confidentielles (absences, notes, mot de passe, adresses …).

Mesure : Utiliser la fonction PHP mysql_real_escape_string(), premettant de filtrer les requettes SQL malveillantes

III) Protection contre les failles « file upload »

L'utilisateur pourrra effectivement changer sa photo de « profil ». Cette fonctionnalité nécéssite un script PHP d'upload de fichiers. En cas de mauvaise gestion de l'upload, l'utilisateur pourrait aisement mêttre en ligne des fichiers (PHP par exemple) malveillants, et ainsi prendre le contrôle de la plateforme.

Mesure : Afin de palier à ce problème, le fichier uploadé devra respecter certaines normes : être au format JPG ou PNG, ne pas dépasser X octets, etc.

IV) Protection contre les usurpations d'identité

Chaque utilisateur sera identifié par un identifié (ID) unique, qui ne dépendra ni du nom, ni du prénom. L'email de la personne est une valeure sûre, car celle-ci ne peut être identique pour deux personnes.

Mesure : Identifier chaque personne par un numéro.