Mécanismes de sécurité utilisés

L’application est sécurisée de différentes manières :

Des attributs « required » sont utilisés en HTML sur chaque balises « Input », afin de vérifier l’envoi correct de la totalité des données réclamées dans les formulaires.

Ensuite, en backend, les données passent par une méthode « Filter\_var » fournie par PHP, qui me permettra de vérifier que les données sont valides.

Les requêtes sont préparées avec PDO afin d’éviter les injections SQL.

L’application effectue également un hachage sur les mots de passe, cela ajoute une couche de sécurité en stockant des hachages sécurisés au lieu de mots de passe en texte brut dans la base de données.

Des vérifications d’existences sont aussi utilisés pour s’assurer qu’il n’y ait pas de doublons.

La gestion des erreurs se fait avec des blocs TRY-CATCH pour capturer les exceptions et renvoyer des messages d’erreur appropriés.

L’application gère également les sessions grâce à la variable superglobale « $\_SESSION » fournie par PHP.