Documentation des mesures de sécurités

# Navigation des pages :

Une image contenant texte

Description générée automatiquement

Une image contenant texte

Description générée automatiquement

# Mesures de sécurité implémentées :

* **Se protéger contre les attaques de force brute :**
  + Si 3 tentatives de connexion échouent, le processus de connexion sera bloqué pendant 1 minutes.
* **Se protéger contre les injections SQL :**
  + Le ‘username’ et le ‘password’ saisis seront protégés par la fonction *htmlSpecialChars()* avant toute échange avec la base de données.
  + L'utilisation de prepared statements SQL.
* **Mesures de sécurité liées au système d’authentification :**
  + Une connexion ne sera possible que si le ‘username’ saisi existe dans la base de données.
  + Si le ‘username’ saisi existe dans la base de données (BD), une comparaison du ‘password’ saisi avec celui haché et enregistré dans BD sera effectuée.

* **Mesures de sécurité liées au système d’authentification :**
  + Une inscription n’est possible que si le ‘username’ saisi n’existe pas dans la BD (‘username’ doit être unique).
* **Hachage du Mot de passe :** 
  + Un ‘password’ ne sera jamais enregistré en texte clair dans la BD. Il sera donc crypté avant d’être enregistré dans la BD :

*$hashed\_password = password\_hash($password, PASSWORD\_BCRYPT);*

* **Se protéger contre les injections SQL :**
  + Le ‘username’ et le ‘password’ saisis seront protégés par la fonction *htmlSpecialChars()* avant toute échange avec la base de données.
  + L'utilisation de prepared statements SQL.
* **Éviter les mots de passe simples et faciles à deviner :**
  + Le ‘password’ doit contenir des lettres.
  + Le ‘password’ doit contenir des chiffres.
  + Le ‘password’ doit contenir des caractères spéciaux.
  + Le ‘password’ doit avoir une longueur minimale de 5 caractères.
* **Implémentation de sessions utilisateurs. De ce fait, on garantit :**
  + L’authentification d’utilisateur
  + Stockage sécurisé des informations de session
  + Expiration automatique des sessions
  + Sécurité contre la duplication de sessions

# D’autres mesures de sécurités à implémenter :

* L’authentification à deux facteurs.
* Hébergement du site web et l’utilisation du protocole TLS pour sécuriser la page web au sein du serveur.