Mission 4 sécurisation d'une application Web

Compétence visée : Mettre à disposition des utilisateurs un service informatique

Sous-compétence cochée : Réaliser les tests d'intégration et d'acceptation d'un service

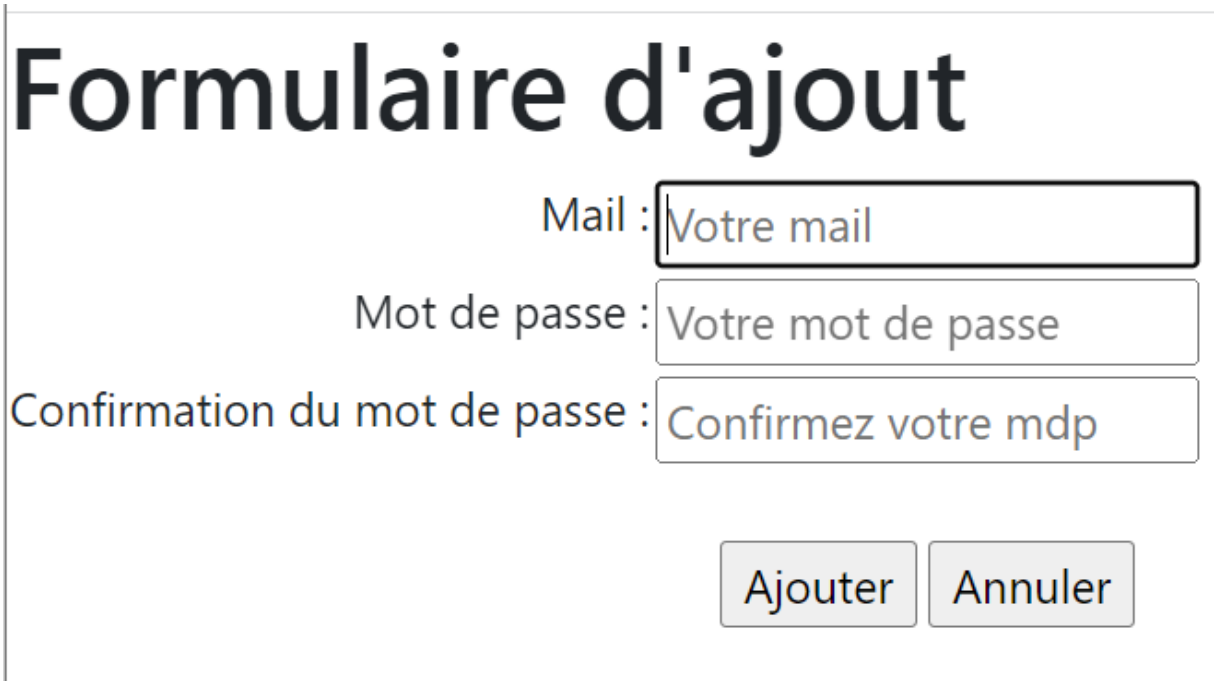
Travail demandé : Créer un formulaire d'ajout d'utilisateur en vérifiant les tests suivants :

- tous les champs doivent être complétés

- vérification de l'existence de l'utilisateur déjà dans la BD et les mots de passe se correspondent

- le cryptage de mot de passe.

- si on a évité les injections SQL et XSS



```php
<?php
$bdd = new PDO('mysql:host=localhost;dbname=utilisateurs', 'root', '');

if(isset($_POST['forminscription'])) {

   $email = htmlspecialchars($_POST['email']);//test 4
   $mdp = $_POST['mdp'];
   $mdp = htmlspecialchars($mdp);//test4
   $mdp2 = $_POST['mdp2'];



   if(!empty($_POST['email']) AND !empty($_POST['mdp']) AND
!empty($_POST['mdp2'])) {


            if(filter_var($email, FILTER_VALIDATE_EMAIL)) {
               $reqmail = $bdd->prepare("SELECT * FROM users WHERE email = ?
");
               $reqmail->execute(array($email));
               $mailexist = $reqmail->rowCount();
               if($mailexist == 0) {// test2
                  if($mdp == $mdp2) {
                     $mdph = password_hash($mdp,PASSWORD_DEFAULT) ; //test 3
                     $insertmbr = $bdd->prepare("INSERT INTO users(email, mdp)
VALUES(?, ?)");
                     $insertmbr->execute(array($email, $mdph));
                     $erreur = "Votre compte a bien été créé !";
                  } else {
                     $erreur = "Vos mots de passes ne correspondent pas !";
                  }
               } else {
                  $erreur = "Adresse mail déjà utilisée !";
               }
            } else {
               $erreur = "Votre adresse mail n'est pas valide !";
            }


    } else {
      $erreur = "Tous les champs doivent être complétés !";
   }
   echo $erreur;
}
?>
```