Corrigé du sec17b

Le mot de passe n'est pas haché

Les mots de passe doivent être hachés pour éviter qu'on puisse les voler si on a accès à la base de données où ils sont stockés. Pour cela, il faut :

1. Agrandir le champ "password" dans la table "user"
2. Modifier "inscription.php" pour hacher les mots de passe avec "password_hash()"
3. Modifier "connexion.php" pour vérifier les mots de passe avec "password_verify()"

Un fichier csv visible depuis Internet contient le user, le mot de passe et le nom de la base de données MySQL

Le fichier CSV peut être ouvert dans le navigateur si on connait son nom. Pour éviter cela, il faut :

1. Supprimer le fichier CSV
2. Ajouter le user, le mot de passe et le nom de la base de données dans le fichier "init.php" ou "functions.php"

Les champs du formulaire d'inscription ne sont pas vérifiés

Il faut vérifier les champs pour éviter par exemple qu'on puisse s'inscrire sans mot de passe ou que l'email n'ait pas le bon format. Pour cela, il faut :

1. Vérifier les champs obligatoires
2. Vérifier les formats des champs (email, textes, nombres,...)

L'inscription n'est pas protégée contre les injections SQL

On peut ajouter du code SQL dans les champs du formulaire d'inscription. Pour éviter cela, il faut :

1. En PDO, remplacer les "query" par des "prepare"/"execute" dans "inscription.php"

La page "profil.php" peut potentiellement afficher tous les profils alors qu'elle ne devrait afficher que celle de l'utilisateur connecté

On peut accéder à n'importe quel profil en changeant l'ID dans l'URL. Pour éviter cela, il faut :

1. Enlever l'ID de l'URL dans "menu.php"
2. Enlever la lecture de l'ID de l'URL ($_GET) dans "profil.php"
3. Ajouter la lecture de l'ID dans la session car celui-ci est renseigné dés la connexion