

PHP – Semaine 6/6 – Séance d'exercices 2/3

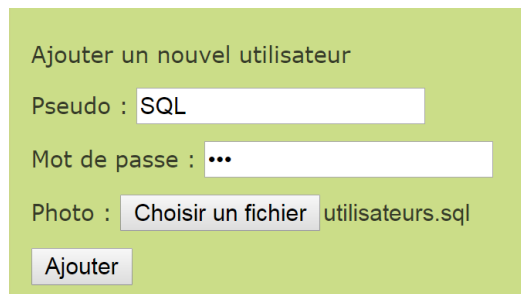
Exercice n°38 – Pallier les failles de l'*upload*

Lisez le document intitulé « Semaine 6 - Les Failles de l'Upload en PHP par Guillaume LAUMAILLET - Licence Libre sur Homeofscience.net.pdf ».

Il est important de garder à l'esprit dans le développement d'un site Web professionnel qu'il faut pallier les failles de sécurité et ce, autant que possible.

Mettez à jour le code du site des bonnes nouvelles pour pallier les failles de l'upload en implémentant la vérification classique du type du fichier et la vérification du mime-type par la fonction `getimagesize`.

Le fichier doit être une image de type `.jpg` ou `.png` uniquement, dont le mime-type correspondant est `'image/jpeg'` ou `'image/png'`.



Ajouter un nouvel utilisateur

Pseudo :

Mot de passe :

Photo : utilisateurs.sql

Le fichier uploadé doit être une image `.jpg` ou `.png` !

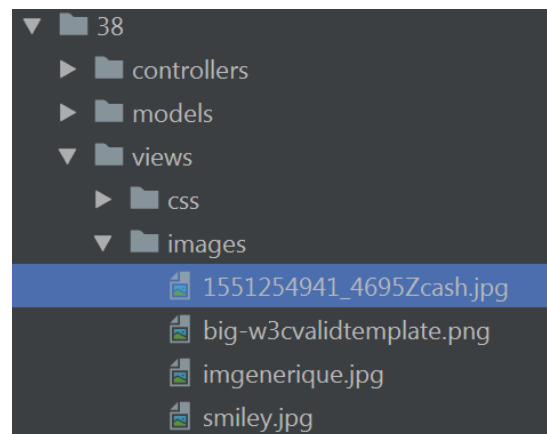
Rajoutez au nom du fichier enregistré dans la base de données un horodatage à la microseconde près. Ainsi, la probabilité d'écraser une image existante (portant un même nom) tend vers zéro.

Ajouter un nouvel utilisateur

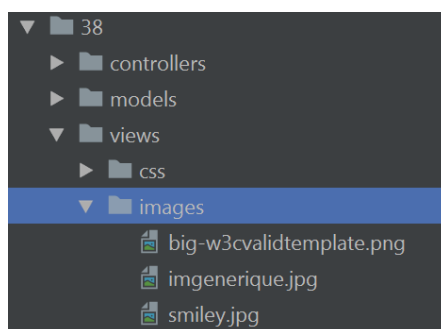
Pseudo :

Mot de passe :

Photo : Zcash.jpg



Pensez aussi au fait que l'image pourrait être effacée du disque serveur... affichez alors l'image générique.



Exercice n°39 – S’authentifier avec les informations en base de données

Nous allons maintenant modifier le code concernant le login vers la zone d’administration pour offrir la possibilité à tout utilisateur enregistré dans la table des utilisateurs de se connecter.

Vous aurez besoin d’écrire notamment une méthode `bd_valider_utilisateur` pour vérifier les données d’authentification. Cette fonction prend comme paramètres un nom d’utilisateur et un mot de passe et renvoie vrai ou faux selon que les données d’authentification se trouvent dans la table « utilisateurs » ou pas.

Rappel : le mot de passe est crypté selon la méthode **blowfish**.

Dans la zone d’administration, vérifiez qu’il s’affiche bien « Bonjour » suivi du pseudo de l’utilisateur authentifié.

Pour conclure, offrez la possibilité à l’utilisateur connecté de changer son mot de passe. Pour ce faire, affichez un formulaire classique qui demande l’ancien mot de passe et deux fois le nouveau.

Notifiez l'utilisateur clairement :

- Votre ancien mot de passe n'est pas correct
- Le nouveau mot de passe n'est pas encodé deux fois correctement
- Votre mot de passe a bien été changé

Questions à réfléchir :

- Est-ce possible que deux utilisateurs aient le même pseudo ?
- Que se passera-t-il si deux utilisateurs ont le même pseudo ?

Que faire pour que tout se déroule bien ?

Faites les modifications nécessaires pour pallier ce cas problématique de deux pseudos identiques.