Travail pratique : Site PHP MVC/POO avec une interface d'administration sécurisée (pondération 20%)

Le travail consiste à reprendre le code produit par le TP2 en ajoutant une interface MVC d'administration pour gérer la table utilisateur, sécuriser l'accès à l'interface d'administration avec un formulaire d'authentification, et exploiter le profil de l'utilisateur.

Si besoin, vous pouvez consulter ce site de démonstration du travail demandé : https://cjouhannet.webdev.cmaisonneuve.qc.ca/31B/TP3/admin

Ajout d'une interface MVC d'administration pour gérer la table utilisateur (16 points)

Le script de chargement SQL de la table utilisateur et de 3 utilisateurs dans cette table, est fourni.

Codez cette interface en complétant le contrôleur Admin qui récupère les URIs structurées par exemple ainsi (avec une logique similaire à la gestion de la table auteur vue en cours) :

admin?entite=utilisateur
admin?entite=utilisateur&action=a
admin?entite=utilisateur&action=m&utilisateur_id=4
admin?entite=utilisateur&action=s&utilisateur id=4

page de liste des utilisateurs (action=l par défaut) formulaire d'ajout d'un utilisateur formulaire de modification de l'utilisateur d'id 4 traitement de suppression de l'utilisateur d'id 4

1 Page de liste des utilisateurs (2 points)

Affichez par exemple la page :



Les liens encadrés en rouge ont une structure similaire à ceux utilisés pour gérer l'entité "auteur" vue en cours, avec en plus le lien de l'action "générer mdp" qui permet de générer un nouveau mot de passe et de l'envoyer par courriel à l'utilisateur concerné :

admin?entite=utilisateur&action=generer mdp&utilisateur=1

2 Page formulaire d'ajout d'un utilisateur (3 points)

Affichez par exemple la page :



3 profils sont définis dans la select :

- Utilisateur (défaut) de valeur "utilisateur",
- Editeur de valeur "editeur",
- Administrateur de valeur "administrateur".

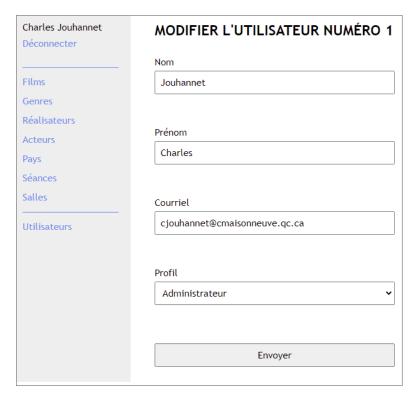
Lorsque la saisie est sans erreur, l'utilisateur est ajouté dans la table utilisateur, en générant un mot de passe aléatoire (par exemple 10 caractères avec alternance d'un caractère alphabétique et d'un chiffre) encrypté avec la fonction de hachage SHA2 dans le champ utilisateur mdp.

Le mot de passe généré (en clair avant encryptage) est envoyé à l'utilisateur dans un courriel d'information.

Revenez sur la page de liste en ajoutant un message de compte-rendu au-dessus de la liste.

3 Page formulaire de modification d'un utilisateur (3 points)

Affichez par exemple la page :



Mêmes champs à gérer que pour le formulaire d'ajout avec un champ caché supplémentaire utilisateur_id qui contient la clé de l'utilisateur à modifier dans la table SQL.

Le mot de passe n'est pas concerné par ces modifications et reste inchangé.

Comme pour le formulaire d'ajout, revenez sur la page de liste en ajoutant un message de compterendu au-dessus de la liste.

4 Suppression d'un utilisateur (1 point)

Revenez sur la page de liste en ajoutant un message de compte-rendu au-dessus de la liste.

5 Génération d'un nouveau mot de passe pour un utilisateur (1 point)

Comme pour l'ajout d'un utilisateur, générez un mot de passe aléatoire, modifiez le dans la table SQL et envoyez le à l'utilisateur dans un courriel d'information.

Revenez sur la page de liste en ajoutant un message de compte-rendu au-dessus de la liste.

6 Page d'authentification d'un utilisateur s'il n'est pas déjà connecté (3 points)

Affichez par exemple la page :



Comme vu en cours, utilisez le mécanisme de session PHP pour tester puis mémoriser la connexion d'un utilisateur.

Le mot de passe saisi est encrypté avec le même algorithme de hachage pour être comparé à celui enregistré dans la table utilisateur pour ce courriel.

Si la saisie est correcte, l'utilisateur est enregistré dans une variable de session et la page d'administration par défaut est affichée en fonction du profil de l'utilisateur.

7 Exploitation du profil de l'utilisateur (2 points)

7-1 Adaptez le menu au profil de l'utilisateur :



7-2 Générez une erreur http 403 si le profil n'est pas autorisé en accès direct à une page, par exemple avec l'URI admin?entite=utilisateur&action=a si l'utilisateur connecté a le profil éditeur.

8 <u>Déconnexion de l'utilisateur</u> (1 point)

En cliquant sur le lien "Déconnecter" du menu, supprimez la variable de session de l'utilisateur et affichez la page d'authentification.

L'URI du lien "Déconnecter" pourrait être par exemple : admin?entite=utilisateur&action=d

Barème:

Interface MVC d'administration pour gérer la table utilisateur (10 points) :

Page de liste des utilisateurs 2 points Page formulaire d'ajout d'un utilisateur 3 points Page formulaire de modification d'un utilisateur 3 points Suppression d'un utilisateur 1 point Génération d'un nouveau mot de passe pour un utilisateur 1 point Page d'authentification d'un utilisateur s'il n'est pas connecté 3 points Exploitation du profil de l'utilisateur 2 points Déconnexion de l'utilisateur 1 point

Qualité du code : 4 points

POO, respect de l'architecture MVC, indentation, nommage (variables, méthodes, etc.) et commentaires

Consignes:

- Vous devez utiliser la POO pour tous les composants MVC.
- Comme pour le TP2, utilisez Twig pour les vues des pages à afficher, et également pour le message HTML d'information envoyé à l'utilisateur (avec son mot de passe).
- Indentez bien votre code.
- Commentez votre code lorsque c'est nécessaire; chaque méthode doit avoir un en-tête PHPDoc.
- Vous pouvez utiliser et modifier le code CSS fourni ou faire votre propre mise en page.

Remise:

Remettez votre dossier compressé avec tous les composants sur Léa.