

## TP 2

Distribué à distance le mercredi 23 août 2023  
Date de remise : le vendredi 8 septembre 2023

## Blog multi-usagers

### Objectif pédagogique

Ce travail pratique porte sur l'intégration PHP/MySQL. L'étudiant(e) doit démontrer ses aptitudes à écrire des programmes simples en PHP qui intègrent une base de données MySQL. Les concepts importants à évaluer sont la programmation HTTP, l'écriture de requêtes SQL simples, l'utilisation de la librairie MySQLi de PHP, le processus d'authentification, la gestion des rôles et l'utilisation des tableaux, des fonctions et des fichiers inclus.

### Ce qu'il faut accomplir

Vous devez développer un système de gestion de contenu de type blog supportant plusieurs usagers différents. Un ARTICLE (contenu du blog) possèdera un Titre, un Texte, un Auteur (qui sera un usager du système). Tous les usagers (authentifiés ou non) peuvent voir tous les articles contenus sur le site web. Cependant, seuls les usagers authentifiés peuvent faire l'ajout d'un article, et seul l'usager ayant écrit un article peut modifier celui-ci.

Voici donc les fonctionnalités que vous devez implémenter.

a) **Page d'authentification**

La page d'authentification devra être accessible à partir de la page d'affichage des articles. Cette page sera une page d'authentification typique, qui devra implémenter l'algorithme de validation sécuritaire que nous avons vu en classe. Lorsque l'usager est authentifié, il est redirigé vers la page d'affichage des articles.

b) **Page d'affichage des articles**

La page d'affichage des articles affichera par défaut les articles dans l'ordre inverse de celui dans lequel ils ont été insérés (en se basant sur les IDs auto-générés), c'est-à-dire que l'article le plus récent sera affiché en premier. Pour chaque article, on affichera dans l'ordre le titre de l'article, le texte de l'article et le nom de l'auteur.

De plus, si l'usager est authentifié, pour tous les articles dont il est l'auteur, un lien MODIFIER CET ARTICLE sera affiché à côté du titre de l'article. Ceci l'amènera vers la page de modification de l'article. Pour ces mêmes articles, un lien SUPPRIMER CET ARTICLE sera lui aussi affiché pour l'usager qui l'a rédigé seulement.

Un lien vers la création d'articles s'affichera aussi pour un usager authentifié.

c) **Formulaire de recherche des articles**

Dans le haut de la page d'affichage des articles se trouvera un petit formulaire permettant d'effectuer une recherche dans les titres et les textes des articles. Lorsque l'usager (authentifié ou non) cliquera sur le bouton Rechercher, seuls les articles répondant à la recherche seront affichés.

d) **Pages de création et de modification des articles**

La page de création permet à un usager authentifié de créer un article, alors que la page de modification d'un article, accessible seulement par l'auteur de cet article, permettra à l'usager de modifier un article. On donne dans les 2 cas un titre et un texte à l'article en question.

Il y aura aussi 20% du TP d'accordé pour les pratiques de programmation. Produisez donc un code clair, commenté, et modulaire qui gère les exceptions en affichant les messages appropriés, en respectant la structure fournie en classe. Vous devez aussi vous assurer qu'il n'y a pas de trous de sécurité dans votre code (par exemple, qu'il est vraiment impossible pour un utilisateur non-authentifié d'ajouter un article, pour un usager de modifier l'article de quelqu'un d'autre...). Votre code doit être protégé contre les attaques par injection SQL et le XSS (cross-site scripting).

De plus, sans faire l'objet d'un effort gargantuesque, la présentation doit tout de même être soignée, le HTML et le CSS devant être réalisé selon les pratiques que vous avez apprises jusqu'à maintenant.

**Ce qu'il faut remettre**

Sauvegardez votre application complète dans un répertoire identifié par votre nom et déposez ce dernier dans LEA avant minuit à la date d'échéance.

**De plus, votre application doit être installée sur WEBDEV, et votre répertoire de remise remis sur LÉA doit contenir un fichier README.txt contenant l'URL de votre site sur WEBDEV ainsi qu'une liste d'au moins deux usagers (username / password) que je pourrai utiliser pour tester votre TP.**

**Votre TP devrait aussi être mis à ma disposition sur GitHub.**

**Barème :**

Gestion de l'authentification et de la sécurité (15%)

Utilisation adéquate des requêtes SQL (20%)

Traitement de requêtes, affichage des données dynamiques en PHP (25 %)

Fonctionnement correct de l'application (20 %)

Pratiques de programmation et gestion des versions (20%)