

DESR4 : Programmation dynamique

TP5. Administration du site Web

I. Administration du site

Le but de ce manipulation est de créer le back office c'est à dire l'espace administrateur du site web de commerce en ligne pour permettre d'administrer la base de données des articles. Les pages seront accessibles par le lien Admin en bas à droite du site

I.1. Création de l'espace Admin

- Créez dans l'arborescence de votre site web (sous Filezilla) un dossier « admin » qui contiendra tout votre espace d'administrateur
- Créez dans ce répertoire un fichier ajout.php qui contient dans un div identifié « container » le titre `<h1> Administration du site OpenShop</h1>` . Liez ce fichier avec le fichier styleadmin.css que vous trouverez sous moodle.
- Créez le formulaire identique au fichier « iajout.png ».
Remarques
 - la validation du formulaire fera appel de nouveau au fichier ajout.php du dossier admin, l'envoi se fera part par la méthode POST
 - le contenu du select (c'est à dire vêtements accessoires ect...) est issu d'une requête permettant de récupérer les enregistrements de la table « Catégorie »,
- Au dessus du formulaire, vous allez faire le traitement de celui-ci, vous devez :
 - Vérifiez si tous les champs ont été définis (fonction isset()) si c'est le cas vous devez récupérer la valeur de chaque champ dans une variable sinon mettre cette variable comme une chaîne vide.
 - Vérifiez également si tous les champs ne sont pas vides. Si c'est le cas, les informations saisies seront stockées dans la base de données et l'image sera téléchargée sur le serveur. Un message devra être affiché si l'enregistrement a bien été effectué. Le téléchargement de l'image sera réalisé avec la fonction : `move_uploaded_file()`. Vous avez le droit d'insérer cet élément uniquement si le produit n'existe pas dans la base de données.

1.2. Sécurisation de l'espace Admin

2 méthodes peuvent être utilisées :

- identification par fichiers .htaccess et .htpasswd
- identification par information issue d'une base de données

2.a) Via une base de données

- Créez dans votre base de données, une table nommée « *compte* » qui contient les champs id (int auto incrémenté), login (varchar 24) et mot de passe (varchar 8)
- Ajoutez un compte en chiffrant le mot de passe en md5 (<http://www.md5.fr/>)
- Créez Le fichier « index.php » dans le dossier admin qui contient le formulaire permettant à l'utilisateur de saisir son login et son mot de passe. Si l'utilisateur saisi un compte existant dans la table compte alors l'utilisateur sera redirigé vers la page «ajout.php » sinon l'utilisateur reste sur la page «index.php »
- Modifiez le fichier « footer.php » du front office, pour permettre d'accéder au back office c'est à dire au fichier index.php du dossier admin.

2.b) .htaccess et .htpasswd (Ne pas faire c'est de l'information)

Il est parfois nécessaire de protéger l'accès à un répertoire sur un serveur web (ex : répertoire d'administration, contenant des données sensibles) afin d'éviter que n'importe qui puisse y accéder.

Il y a différentes méthodes, on peut utiliser des langages comme le PHP, ASP, PERL ...), mais la méthode la plus simple est d'utiliser le mécanisme de protection d'Apache.

C'est-à-dire effectuer une protection à l'aide des fichiers « .htaccess » et « .htpasswd ».

- Créez le fichier .htaccess (n'oubliez pas le point devant le nom) à la racine du dossier admin et écrivez les lignes suivantes :

```
AuthName "PHRASE D'ACCUEIL"  
AuthType Basic  
AuthUserFile "adresse absolue de fichier .htpasswd "  
Require valid-user
```

AuthUserFile : c'est le nom et le chemin d'accès du fichier qui contiendra les noms des utilisateurs et les mots de passe associés. Ce chemin doit partir de la racine du site sauf dans le cas de test local avec easyphp il est nécessaire de mettre l'adresse absolue

On peut, et il est même conseillé de choisir un autre nom que .htpasswd pour le fichier qui contiendra le couple utilisateur/mot de passe. Le point précédent le nom de fichier permettra de cacher (au sens Unix /linux du terme).

Il est également recommandé de mettre le fichier des mots de passe en dehors de l'arborescence du site si l'on en a la possibilité.

AuthGroupFile : permet de définir un droit d'accès à un groupe d'utilisateur. Cette solution n'est que rarement utilisée pour un site Web. Le reste du temps il pointe vers /dev/null. Il faut que cette ligne soit présente.

AuthName : c'est le texte qui apparaîtra dans la fenêtre demandant le mot de passe.

AuthType : L'authentification est en générale « basic ». Les mots de passe sont alors envoyés en clair sur le réseau. Pour sécuriser davantage l'accès, on peut utiliser la méthode d'authentification « digest » qui crypte les mots de passe en MD5 . Ce système n'est supporté que par certains navigateurs.

Require valid-user : accepte tous les utilisateurs qui ont un login : mot de passe dans .htpasswd.

Require herve jacques : limite l'accès à un ou plusieurs utilisateurs précis, ici herve et jacques. A noter que les utilisateurs sont séparés par des espaces.

- Créez le fichier .htpasswd (n'oubliez pas le point devant le nom) à la racine du dossier admin et écrivez les lignes suivantes :

```
login1:motDePasseNonCrypte  
login2:motDePasseNonCrypte
```

ce qui correspond au nom d'utilisateur (login1) et son mot de passe . Il y aura une ligne pour chaque utilisateur. Le mot de passe ne doit pas être crypté lorsqu'on travaille sous windows. Bien sur lorsque vous placerez un site sur un serveur, il sera nécessaire de crypter le mot de passe.

Si l'on n'a pas accès à l'utilitaire htpasswd, on peut se rendre sur l'un des deux sites suivant proposant le cryptage d'un mot de passe.

<http://home.golden.net/generator/> (il génère le couple login/password)

<http://www.ovh.net/cgi-bin/crypt.pl>

le fichier .htpasswd étant terminé, il suffit de le mettre à sa place (celle définie dans le fichier .htaccess).

- Vous devez à présent tester le fonctionnement de cette restriction. Modifiez le nom du fichier index.php du front office contenu dans le dossier siteWebShop (Pas celui de l'admin) en index2.php. En cliquant sur l'alias vous devez voir apparaître tous vos dossiers et fichiers **sauf** le dossier « admin ». Supprimez un cours instant votre fichier .htaccess et vérifiez que le dossier « admin » est visible.
- Remplacez votre fichier .htaccess
- Renommez index2.php en index.php et cliquez sur le lien admin du footer.
- Vous devez accéder directement à votre admin. La restriction ne fonctionne pas. Vous travaillez en local avec easyphp, il est nécessaire de modifier le fichier httpd.conf d'apache. Cliquez sur l'icone easyphp puis faites : Configuration-> Apache Le fichier s'ouvre. Il est nécessaire de modifier la ligne AllowOverride none en AllowOverride all de votre alias qui doit se trouver tout en bas du fichier.
- Redémarrez le serveur et testez le fonctionnement

1.3. Administration avancée

Pour l'instant, l'administrateur du site doit rentrer les articles un à un. Il serait intéressant pour lui d'envoyer un fichier XML contenant une liste d'articles à ajouter à la base de données.

- Créez un fichier XML contenant une liste d'article.
- Ajoutez dans l'index de l'Admin, le titre « Insertion d'articles via fichier XML »
- Créez un formulaire permettant d'envoyer au serveur le fichier XML
- Traiter ce fichier XML en insérant chaque article dans la base de données. Vous utiliserez la classe SimpleXML pour parcourir votre fichier
-

Remarque :

- La partie XML est un plus, je préfère que tout fonctionne correctement avant de vous attaquer à cette partie