

PHP – Semaine 6/6 – Séance d'exercices 1/3

Exercice n°36 – Sécurisation d'un répertoire avec Apache

Nous vous demandons de mettre en œuvre la sécurisation d'un répertoire `/36.secret` présent dans `/www` par la technique « `.htaccess` et `.htpasswd` » décrite sur le site d'openclassrooms à l'adresse <https://openclassrooms.com/fr/courses/918836-concevez-votre-site-web-avec-php-et-mysql/918580-protégez-un-dossier-avec-un-htaccess>.

Créez un simple script `test.php` dans ce répertoire :

```
<?php
    echo realpath("test.php");
?>
```

Le serveur Apache permet l'usage de plusieurs techniques de cryptages. Lire à ce sujet https://httpd.apache.org/docs/2.4/fr/misc/password_encryptions.html. Nous allons utiliser la technique de cryptage de mot de passe `bcrypt` (blowfish).

Pour générer un mot de passe crypté, vous pouvez utiliser Apache server's `htpasswd.exe` en ligne de commande, mais cela n'est pas vraiment pratique.

Écrivez votre propre script PHP et utilisez la fonction suivante :

```
$hash = password_hash($votremotdepasse, PASSWORD_BCRYPT);
```

ou encore, trouvez un générateur de mot de passe crypté (`htpasswd generator`) sur Internet, comme par exemple <http://aspirine.org/htpasswd.html>.

Remarque : attention à l'utilisation d'un générateur en ligne, celui-ci pourrait capturer vos informations (*phishing*). Il est recommandé de faire fonctionner un générateur trouvé en ligne hors ligne.

Un même mot de passe peut donner plusieurs *hashes* valides selon la technique blowfish. Par exemple 3PO peut donner comme *hashes* :

```
$2y$10$7sGuz66Pq09297v7QtzcMuKBrMq/VwyakdvsHFNux6W03e4bjQSOe
```

```
$2y$10$0HKdpsDgYzpPgPX1JXX8K.AMB94tJAJ5APKP891yWgDp2.gq1NfNa
```

```
$2y$10$mXAYakdOCc3GY.6rfDR8VeqxVazQZgsFvMQji3cZopt1eL7Ya9Nkq
```

Les systèmes d'exploitation Windows ne permettent pas de renommer un fichier en `.htaccess` via la GUI. Pour créer un fichier `.htaccess`, il faut créer un nouveau fichier à l'aide d'un éditeur de texte et sélectionner Enregistrer sous... dans le menu Fichier. Dans la fenêtre de sauvegarde, il faut entrer `".htaccess"` (en rajoutant les guillemets) puis cliquer sur Enregistrer.

Les systèmes d'exploitation MacOS ne permettent pas de voir un fichier `.htaccess` via le Finder. Pour créer un fichier `.htaccess`, créez un fichier `htaccess` de type texte et puis à l'aide du terminal, renommez-le avec la commande `mv htaccess .htaccess`. Le fichier `.htaccess` correctement nommé ne sera plus visible dans le Finder. Pour le voir dans le terminal, écrivez la commande `ls -a`. Faites la même chose pour le fichier `.htpasswd`.

Remarque : pour cet exercice, il vaut mieux utiliser le serveur Apache de Wampserver que le moteur *build-in* dans l'IDE PhpStorm.

Exercice n°37 – Gestion des utilisateurs et *upload* d'image

Nous vous demandons de créer une nouvelle table « utilisateurs » dans la base de données « bdbn ».

Cette table contient 4 champs :

1. Un entier « no » qui est la clé primaire auto incrémentée.
2. Une chaîne de 30 caractères « pseudo » qui représente un login.
3. Une chaîne de 60 caractères « mdp » qui représente un mot de passe crypté selon la méthode blowfish.
4. Une chaîne de 255 caractères « photo » qui représente l'URL vers une photo.

Seul le champ n°4 peut être NULL.

Vous pouvez utiliser la technique que vous voulez pour créer cette table, par exemple, à l'aide de phpMyAdmin :

Nom de table: Ajouter colonne(s)

| Nom | Type | Taille/Valeurs* | Valeur par défaut | Interclassement | Attributs | Null | Index | A.I |
|--------|---------|-----------------|-------------------|-----------------|-----------|-------------------------------------|---------|-------------------------------------|
| no | INT | | Aucun(e) | | | <input type="checkbox"/> | PRIMARY | <input checked="" type="checkbox"/> |
| pseudo | VARCHAR | 30 | Aucun(e) | utf8_general_ci | | <input type="checkbox"/> | --- | <input type="checkbox"/> |
| mdp | VARCHAR | 60 | Aucun(e) | utf8_general_ci | | <input type="checkbox"/> | --- | <input type="checkbox"/> |
| photo | VARCHAR | 255 | Aucun(e) | utf8_general_ci | | <input checked="" type="checkbox"/> | --- | <input type="checkbox"/> |

Commentaires de table : Interclassement : Moteur de stockage :

| # | Nom | Type | Interclassement | Attributs | Null | Valeur par défaut | Commentaires | Extra |
|---|---------------|--------------|-----------------|-----------|------|-------------------|--------------|----------------|
| 1 | no | int(11) | | | Non | Aucun(e) | | AUTO_INCREMENT |
| 2 | pseudo | varchar(30) | utf8_general_ci | | Non | Aucun(e) | | |
| 3 | mdp | varchar(60) | utf8_general_ci | | Non | Aucun(e) | | |
| 4 | photo | varchar(255) | utf8_general_ci | | Oui | NULL | | |

Insérez un administrateur à l'aide de phpMyAdmin. Le mot de passe doit être crypté selon la technique blowfish. C'est le *hash* du mot de passe qui est à stocker dans le champ mdp. Laissez le champ « photo » vide pour l'instant.

| no | pseudo | mdp | photo |
|----|--------|---|-------|
| 1 | C | \$2y\$11\$QMmBV2iEr6879r/cT.eypuPMd.pzxsUKX63DFBFJqK... | NULL |

Dans la zone d'administration du site, affichez un second tableau avec les pseudos et les photos des utilisateurs. Pour l'instant, il n'y a aucune photo de référencée dans la table des utilisateurs, nous vous demandons d'afficher une image générique quand il y a la valeur NULL dans le champ « photo ».

Zone d'Administration


Bienvenue C

[Se déconnecter](#)

| Titre | Auteur | | |
|-------------------------------------|-----------------|---------|---------------|
| L'instant présent | Main Tenant | Effacer | Mettre à jour |
| Terre: ma Nature | V. du Ciel | Effacer | Mettre à jour |
| Manger jeune, sain et bio | KidsinCuisine | Effacer | Mettre à jour |
| Vivre chaque instant | A. Bonsplans | Effacer | Mettre à jour |
| Le secret du bonheur: aimer | Jolie Joanne | Effacer | Mettre à jour |
| Le grand livre des bonnes nouvelles | M. Youpie Lavie | Effacer | Mettre à jour |

Pseudo

Photo



Ajouter un nouvel utilisateur

Pseudo :

Mot de passe :

Photo : Aucun fichier choisi

Excellente journée qu'aujourd'hui le 27/02/2019 :: 5.001ms pour exécuter le script PHP du client cv55996a54d243b51g7p8p40qv

Tableau avec images génériques (150 pixels de large)

L'étape suivante vous demande de créer un formulaire dans la page d'administration pour ajouter un nouvel utilisateur et, bien sûr, veillez à prévoir la possibilité d'*upload* d'une image.

En cliquant sur le bouton Ajouter, les informations doivent être ajoutées dans la table utilisateurs et l'image copiée dans le répertoire `views/images/` du site Web. Le pseudo et le mot de passe ne peuvent pas être laissés vides. Dans le cadre de cet exercice, il ne vous est pas demandé de gérer les failles possibles de sécurité lors de l'*upload*.