





























# INTERNET / INTRANET

## PHP – LES SESSIONS

### TP : Authentification

L'objectif est de mettre en place un système qui permet de protéger l'accès à un certain nombre de page d'un site. Pour cela, nous allons utiliser le concept de sessions.

Pour définir les utilisateurs autorisés à accéder au site, nous utiliserons une table d'une base de données qui ressemblera à celle-ci :

	Champ	Type	Interclassement	Attributs	Null	Défaut	Extra	Action
<input type="checkbox"/>	id	int(11)			Non		auto_increment	      
<input type="checkbox"/>	login	varchar(50)	latin1_swedish_ci		Non			      
<input type="checkbox"/>	password	varchar(50)	latin1_swedish_ci		Non			      
<input type="checkbox"/>	level	int(11)			Non	9		      

Le login et le mot de passe sont utilisés pour s'authentifier. Le mot de passe est enregistré en clair (sans hachage). Le champ level peut être utilisé pour distinguer des groupes d'utilisateurs.

Quand un utilisateur accède à une page protégée quelconque du site, s'il n'est pas authentifié, il sera redirigé vers un formulaire d'authentification « **login.php** » :

```
<?php
session_start();
?>
<html>
  <head></head>
  <body>
    <h3 align="left"><?php echo $_SESSION["msg"]; ?></h3>
    <form method="post" action="auth.php">
      Login : <input type="text" name="log" /><br />
      Password : <input type="password" name="pass" /><br />
      <input type="submit" value="Entrer" />
    </form>
  </body>
</html>
```

L'utilisateur sera alors invité à entrer son login et son mot de passe. Les données du formulaire sont envoyées à la page « **auth.php** » :

```
<?php
// démarrage de la session
session_start();
// récupération des paramètres du formulaire
$login = $_POST["log"];
$password = $_POST["pass"];
// Connexion la base de données
mysql_connect("localhost","root","");
mysql_selectdb("mabase");
$sql = "SELECT * FROM user WHERE login='$login' AND
password='$password'";
// Exécution de la requête
$result = mysql_query($sql);
$row = mysql_fetch_assoc($result);
// Vérifier si les données fournies sont correctes
if (!$row){
    // ici l'utilisateur n'est pas reconnu
    $_SESSION["msg"] = "Votre login ou mot de passe est incorrect";
    header("location:login.php");
} else {
    // Ici l'utilisateur a fourni les bonnes informations
    $_SESSION["login"] = 1;
    $_SESSION["msg"] ="Bienvenu M. " . $row["login"];
    header("location:index.php");
}
?>
```

Si l'utilisateur n'entre pas les bonnes informations, il sera redirigé vers le formulaire tout en lui affichant un message d'erreur. Dans le cas contraire, il sera redirigé vers la page d'accueil « **index.php** ».

Voici la page d'accueil qui est protégée :

```
<?php
// on démarre la session et on s'assure que
// l'utilisateur est authentifié.
session_start();
if (empty($_SESSION["login"]) ){
    // ici l'utilisateur n'est pas authentifié
    // on le redirige vers le formulaire d'authentification
    header("location:login.php");
    exit();
}
?>
<html>
    <head></head>
    <body>
        <div class="bienvenu"></div>
        <h2>Ma page protégée</h2>
        <a href="logout.php">Logout</a>
    </body>
</html>
```

Quand l'utilisateur est authentifié, il pourra à tout moment se désauthentifier en cliquant sur un lien qui appelle le fichier « **fermer.php** ». Ce fichier a pour rôle de fermer la session et revenir au formulaire d'authentification.

Voici le code du fichier « **fermer.php** » :

```
<?php

    session_start();

    session_destroy();

    header("location:index.php");

?>
```