

Échange de données avec l'utilisateur en PHP

Techniques et précautions

Mohammad Ghoniem
Université de Bretagne Sud



Plan

1. Les cookies
2. Les sessions PHP
3. Les « magic quotes »

I. Les cookies



Pourquoi utiliser des cookies ?

- Évolution vers les sites dynamiques
- HTTP est un protocole sans état (stateless)
 - Nécessité de renvoyer des données au serveur à chaque requête
 - Éviter la répétition de saisies côté utilisateur
- Exemple
 - Se remémore l'ID d'un visiteur sur un site d'abonnés
 - Conserver un liste articles sélectionnés par l'utilisateur
 - Générer un profil de visiteur

Qu'est-ce qu'un cookie ?

- Un cookie est une chaîne de caractères stockée de façon permanente ou provisoire côté client.
- Les cookies permettent de maintenir un état entre des visites successives, et au sein d'une même visite.
- Les cookies sont mis en place par le navigateur.
- Chaque cookie est associé à une URL.

Limitations

- Nombre total de cookies ≤ 300
- Nombre de cookies par site ≤ 20
- 4 ko par cookie
- Les cookies sont envoyés uniquement aux serveurs autorisés à les recevoir.
- La portée d'un cookie :
 - Date d'expiration
 - Chemin d'accès
 - Domaine
 - Paramètre de sécurité

Cookies en PHP

- `setcookie(nom, valeur, duree, chemin, domaine, sécurisé)`
 - Création / mise à jour
 - Première opération du script PHP
- Le cookie est détruit automatiquement à la fin de chaque session sauf instruction contraire.
- Contenu du cookie disponible à l'aide de
 - `$HTTP_COOKIE_VARS["nom_cookie"]` (php 3)
 - `$_COOKIE["nom_cookie"]` (php 4 et +)
- Suppression du cookie à l'aide de `setcookie("nom")`

Pièges classiques

- Ne rien envoyer au navigateur avant un `setcookie()`
- Nécessité de recharger la page avant d'accéder au cookie
- Les appels à `setcookie()` sont réalisés en ordre inverse

II. Les sessions PHP



Définition des sessions

- Mécanisme permettant de suivre l'utilisateur tout au long d'une visite, ou d'une visite à la suivante,
- Basé sur un identifiant de session unique,
- Passage de l'identifiant :
 - dans un cookie
 - dans l'URL (explicitement ou de manière transparente)
- Les données sont stockées côté serveur
- Possibilité de stockage personnalisé en BDD.
- Apparition des sessions dans PHP à partir de la version 4.

Sessions et sécurité

- Possibilité d'usurpation d'identifiant
 - Utilisation conjointe avec les cookies (activé à l'aide de *session.use_only_cookies*, mais insuffisant)
 - Utilisation d'un chiffrement

Fonctions PHP liées aux sessions

- `session_id();`
- `session_name();`
- `session_start();` // appelée en premier *
- `session_encode();` // encode les données
// de session avant stockage
- `session_decode();`
- `session_register();` // enregistre une variable
- `session_unregister();`
- `session_destroy();` // détruit la session mais pas
// le cookie associé

III. Usage des « magic quotes »

Barrer le chemin aux
visiteurs malveillants...



Le problème

- Réception de données peu fiables de la part de l'utilisateur
- Possibilité d'injection de code
- Existence de caractères spéciaux pour SQL
- Nécessité de protéger les scripts

Conversion des caractères spéciaux

- Caractères spéciaux SQL : \ , " , NULL.
- Fonction PHP addslashes() :
 - \ ⇒ \\ , " ⇒ \" , NULL ⇒ \0 , ' ⇒ \'
 - Mode magic_quotes_sybase :
 - NULL ⇒ \0
 - ' ⇒ "
- Les MQ peuvent s'appliquer soit données envoyées par le client web, soit aux données lues sur le serveur
 - magic_quotes_gpc (GPC : GET, POST, COOKIES)
 - magic_quotes_runtime

Application des MQ

```
<?php
    $sql = "INSERT INTO table VALUES('
        . addslashes($foo) . ' ', ".time().")";
?>
```

Après activation des magic quotes :

```
<?php
    $sql = "INSERT INTO table
    VALUES('$foo', ".time().")";
?>
```

Les magic quotes

- Ne sont pas activées pas défaut.
- Détection
 - boolean `get_magic_quotes_gpc()`
 - boolean `get_magic_quotes_runtime()`
- Neutralisation de l'effet de `addslashes()`
 - `stripslashes()`

Liens complémentaires

- Cookies

- http://wp.netscape.com/newsref/std/cookie_spec.html
- <http://www.cookiecentral.com/>
- <http://www.tactika.com/cookie/>

- Sessions PHP

- <http://www.php.net/manual/fr/ref.session.php>
- <http://www.phpfreaks.com/tutorials/41/0.php>
- <http://www.toutestfacile.com/php/cours/printables/PHPFacile.com-sessions.php>
- <http://cyberzoide.developpez.com/php4/faqsession/>