Introduction au langage de programmation PHP

Affichage des données issues d'un formulaire

L'affichage de données issues d'un formulaire ou d'une base de données ou d'une autre ressource peut être la source d'attaques, notamment l'injection de script. Pour éviter ces injections il suffit de demander à PHP de convertir certains caractères en entité HTML. Ainsi les caractères seront affichés correctement mais ne seront plus évalué comme les caractères d'un script. La fonction htmlentities() permet de convertir en entité HTML tous les caractères qui peuvent l'être. La fonction htmlspecialchars() permet de convertir en entité HTML tous les caractères spéciaux.

Voici un exemple simplissime d'injection de script :

```
<!DOCTYPE html>
<!--affichage_donnees_1.html-->
<html>
    <head>
        <meta charset="UTF-8">
        <title></title>
    </head>
    <body>
        <form action="affichage_donnees_2.php" method="post">
            <label>Login : <input type="text" id="login" name="login"></label><br>
            <input type="submit" value="Valider">
        </form>
    </body>
</html>
```

```
<?php

// affichage_donnees_2.php
echo $_POST['login'];
```

Nous affichons juste la valeur de la saisie... Sans aucune validation... Je peux réaliser une petite injection en écrivant <script>alert('Injection !)</script> dans le champ texte. Et lorsque je soumets mon formulaire, une belle pop-up apparaît.

Pour empêcher cette injection je vais utiliser htmlentities() pour convertir les caractères.

```
<?php

// affichage_donnees_3.php
echo htmlentities($_POST['login']);
```

Cette fois la chaîne <script>alert('ici')</script> est écrite en toutes lettres mais le code n'a pas été exécuté.

Fin

NAVIGATION

Accueil
- Ma page
  - Pages du site
  - Mon profil
  - Cours actuel