



Introduction au langage de programmation PHP

[Accueil](#) ► [Mes cours](#) ► [Développement logiciel](#) ► [Intro PHP](#) ► [PHP et HTML](#) ► [Affichage des données issues d'un formulaire](#)

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 :

```
1 <!DOCTYPE html>
2 <!--affichage_donnees_1.html-->
3 <html>
4   <head>
5     <meta charset="UTF-8">
6     <title></title>
7   </head>
8   <body>
9     <form action="affichage_donnees_2.php" method="post">
10      <label>Login : <input type="text" id="login" name="login"></label><br>
11      <input type="submit" value="Valider">
12    </form>
13  </body>
14 </html>
```

```
1 <?php
2
3 // affichage_donnees_2.php
4 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 soumetts mon formulaire, une belle pop-up apparaît.

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

```
1 <?php
2
3 // affichage_donnees_3.php
4 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



Intro PHP

Participants

Le langage PHP : introduction

Les types et les variables

Les opérateurs

Les structures de contrôle

Les structure de données

Les fonctions

Les erreurs

Les fichiers

Les expressions rationnelles

PHP et HTML

 [Introduction](#)

 [Syntaxe alternative](#)

 [T.P. tableau de personnes](#)

 [Les formulaires et les superglobales](#)

 [Validation des données de formulaire](#)

 [Détecter les modifications des formulaires](#)

 [**Affichage des données issues d'un formulaire**](#)

 [Les cookies](#)

 [Les sessions](#)

 [L'upload de fichier](#)

 [T.P. formulaire](#)

 [T.P. formulaire et session](#)

Petite application

[Mes cours](#)

ADMINISTRATION



Administration du cours

Réglages de mon profil

Connecté sous le nom « [Arnaud Lemais](#) » ([Déconnexion](#))
[Intro PHP](#)