Sécurisation de faille XSS simple

Dans ce premier article sur les failles de sécurité web php nous allons entrevoir comment sécuriser un minimum (mais pas complètement) un type de faille xss simple.
La première chose à savoir est qu'il existe des failles de deux types:
les failles xss non permanentes
les failles xss permanentes.
Les failles non permanentes sont en général bien moins graves que les failles permanentes même si avec un peu d'ingénierie sociale il est possible d'en agrandir la portée. Rappelons-le, le maillon le plus faible de la chaîne représente le niveau général de sécurité d'un système et souvent il est plus facile de s'attaquer à un maillon humain faible qu'a une machine sécurisée.
Je vous laisse le loisir de vous renseigner sur Wikipédia qui fournit quelques informations de culture générale:
http://fr.wikipedia.org/wiki/Cross-site_scripting
Pour revenir à l'article nous allons voir comment sécuriser une faille simple qui pourrait apparaître sur un forum ou tout autre site qui permet d'enregistrer des données et de les faire afficher par d'autres utilisateurs.
Cas d'usage
Imaginons que dans notre site les données entrées par les utilisateurs ne soient pas traitées avant d'être soit enregistrées soit ré affichée…
Cela pourrait être le cas par exemple pour un script de ce genre:
dans inscription.php:
1
et par exemple plus tard dans l'affichage des informations de cet utilisateur:
1
Ce script pourrait exister sur un site imaginaire par exemple www.exemple.fr Innocemment si je rentre dans mon navigateur l'url suivante: www.exemple.fr/inscription.php?mail=<script type= 'text/javascript'> alert('XSS!'); </script>&password=pass
D'une part le script va enregistrer un utilisateur avec un mail exécutant un code JavaScript et à chaque affichage de cet utilisateur nous aurons une popup avec le text « XSS ! » qui va s'affiche. De prime abord c'est un piratage anodin. Mais cela découvre la faille XSS. A la place de la fenêtre d'affichage on aurait très bien pu exécuter n'importe quel script javascript…
Mettons que maintenant l'attaquant veuille aller plus loin… et injecte dans l'url :
1
Son domaine mycorsaire site peut avoir récupéré tous les cookies de votre site. Notamment les cookies de session. Il est vrai que dans ce cas plusieurs failles sont cumulées mais ce n'est pas un cas rare.
Quelle parade contre le xss ?
Une parade assez simple contre ce genre d'attaques (qui ne résoudra pas tout mais répond aux cas basiques) est l'utilisation de la fonction php htmlspecialchars… elle convertit les caractères spéciaux et les encode en HTML ce qui empêche l'interprétation du script comme du code et ne l'affichera que comme un banal texte.
Cette fonction répond à la protection MINIMALE de script surtout si vous hébergez des données sensibles. La protection minimale implique de contrôler toutes les variables fournies par l'utilisateur. Et ce au niveau du serveur car un client est tout à fait modifiable. Il est tout à fait possible par exemple de transformer les variables passées en POST dans une requête PHP et cela de façon très simple…
Rappelons le la protection minimale d'un site implique le contrôle rigoureux et systématique de toutes les variables utilisateurs (cookies, entrées de formulaires etc.).