Attaques XSS sur Facebook !

par Pascal Couturiaux, samedi 10 septembre 2011, 17:12

Le **cross-site scripting**, abrégé **XSS**, est un type de faille de sécurité des sites Web, que l'on trouve typiquement dans les applications Web qui peuvent être utilisées par un attaquant pour provoquer un comportement du site Web différent de celui désiré par le créateur de la page (redirection vers un site, vol d'informations, etc.). Il est abrégé XSS pour ne pas être confondu avec le CSS (feuilles de style) étant une abréviation commune pour « *cross* » (croix) en anglais.

Les risques

L'exploitation d'une faille de type XSS permettrait à un intrus de réaliser les opérations suivantes :

- Redirection (parfois de manière transparente) de l'utilisateur.
- Vol d'informations, par exemple sessions et cookies.
- Actions sur le site faillible, à l'insu de la victime et sous son identité (envoi de messages, suppression de données, etc.)
- Rendre la lecture d'une page difficile (boucle infinie d'alertes par exemple).

Une faille de ce type était à l'origine de la propagation des virus Samy sur MySpace en 20052 et Yamanner sur Yahoo! Mail en 2006.

Solution contre les failles XSS

Une parade efficace contre les failles XSS serait de ne pas naviguer sur des sites malveillants. Malheureusement, compte tenu des divers actes de piratage à moyenne et grande échelles, même un logiciel de protection à jour ne permet pas d'éviter toutes les failles. En revanche, les systèmes d'exploitation les plus populaires disposent de navigateurs web multiples.

Par conséquent, **la *solution* simple contre les *failles XSS* consiste à utiliser un navigateur web dédié aux sites de confiance nécessitant une identification préalable et peu susceptibles de contenir des failles de sécurité en eux-mêmes** (tels les sites de votre FAI, de votre webmail ou de votre banque), **et un autre navigateur web pour tous les autres usages.**

Une solution alternative consisterait à utiliser des comptes (de préférence *non administrateurs*) distincts de votre système d'exploitation, les navigateurs web stockant chacun les informations de chaque utilisateur dans des emplacements distincts. Cependant, cette deuxième solution est beaucoup plus contraignante et difficile à exploiter à l'usage, en particulier lorsqu'on se connecte fréquemment sur les sites de confiance.

L'ULTIME SOLUTION

Ce serait de faire désinfecter et nettoyer votre PC par un professionnel !!