Attaques CSRF et XSS sur Facebook !

par Pascal Couturiaux, samedi 10 septembre 2011, 17:04

Les attaques de type **Cross-Site Request Forgery** (abrégées **CSRF**) utilisent l'utilisateur comme déclencheur, celui-ci devient complice sans en être conscient. L'attaque étant actionnée par l'utilisateur, un grand nombre de systèmes d'authentification sont contournés.
En bref, une personne utilise des liens (qui est en fait un script). L'URL de ce lien vers le script permettant de faire des action malveillante désiré. Via ce stratagème cette personne à les Authentifications nécessaire pour réaliser ces méfaits.

Comment se protéger ?

Il est assez difficile de détecter une attaque CSRF même en utilisant un antivirus ou un firewall, alors là l'antivirus c'est vous! L'objectif est d'empêcher le navigateur à effectuer des actions à l'insu du client ou sans accord préalable de ce dernier.
Pour cela voici des mesures à prendre en compte :

- Ne pas suivre les liens suspects
- Ne pas sauvegarder vos identifiants dans votre navigateur
- Toujours se déconnecter à la fin d'utilisation de vos comptes
- Utilisez un deuxième navigateur pour les sites suspects (Firefox et ces modules complémentaires)
- Désactiver l'interprétation (traduction) du code HTML dans vos client WEBMail

Suite Article "Attaques XSS sur Facebook !"