



Éditorial

Quand XSS rime avec compromission massive

Guillaume Lehembre 

Les Cross-Site Scripting (XSS) sont un type de vulnérabilités Web très fréquentes, dont l'impact n'est pas forcément bien connu. D'une manière générale, on peut considérer que la plupart des applications Web sont sinistrées (authentification parfois faible, inclusion de fichier locale et distante, injections SQL) et au vu du nombre de XSS découverts chaque jour dans les applications Web, les administrateurs ont tendance à se dire que c'est un problème bénin - comparé à d'autres - valant rarement le coup d'être corrigé.

Mais depuis quelques temps, ce type de vulnérabilités n'est plus seulement utilisé pour voler un simple cookie d'un utilisateur peu attentionné, mais permet de réaliser des actions de plus grande envergure. L'association des XSS permanents avec d'autres attaques comme les Cross-Site Request Forgery (CSRF ou XSRF), combinés à quelques subtilités HTML et aux techniques d'infections virales, permettent de réaliser des Cross-Site Scripting évolués sur des sites très fréquentés. L'appât du gain généré par l'installation de programme de type spyware/malware est aussi une motivation supplémentaire pour des personnes malveillantes, sans parler de la *facilité* à trouver des XSS permanents sur des sites très populaires [1]. Plusieurs exemples récents assez médiatisés sont très représentatifs du problème. En octobre 2005, le ver Samy (ou ver MySpace) [2] a permis à son créateur de se connecter - en s'ajoutant automatiquement dans les contacts - à près d'un million de personnes sur le site de MySpace en moins de 20 heures (environ 1/35 des utilisateurs à l'époque), site visité quotidiennement par plusieurs millions d'utilisateurs. Toi aussi deviens mon ami :-). Cet exemple fait sourire mais d'autres personnes ont pensé utiliser le potentiel de tels vers XSS à des fins plus illicites. C'est le cas d'un des vers de Flash exploitant ce type de faille et ayant une nouvelle fois touché le site de MySpace en juillet 2006 ; ce dernier exploite la possibilité de charger du code Javascript dans des objets Flash, redirigeant la victime vers un code malveillant exploitant la très *populaire* faille WMF (MS06-01), tout en se répliquant dans le blog MySpace de quelqu'un d'autre. L'inclusion d'exploit dans du Flash a aussi été utilisée par la suite dans des campagnes publicitaires malveillantes.

Les webmails sont souvent une cible privilégiée pour la recherche de XSS, ces sites populaires ont aussi eu

leur lot de XSS *utiles* et exploités massivement. Ce fut par exemple le cas de Yahoo avec le ver Yamaner qui, au travers d'un mail HTML incluant du Javascript, exploitait une vulnérabilité dans le rafraîchissement automatique des emails, pour se propager à tous le carnet d'adresse de la victime comportant des adresses Yahoo, tout en reportant l'ensemble des adresses mails infectées à un site externe. Votre adresse devenait alors spammée en un rien de temps sans que vous en soyez responsable !

D'autres sites de grande envergure - considérés comme de confiance - ont aussi été touchés par des vulnérabilités XSS à des échelles différentes : Google, Microsoft, Paypal, etc. [4], les XSS deviennent donc un vecteur de propagation très intéressant. De nouvelles possibilités intéressantes peuvent être utilisées au travers de XSS, comme des injections dans des flux Atom/RSS ou l'utilisation astucieuse de Javascript pour scanner des réseaux internes en accédant à des données sensibles comme l'ont montré plusieurs chercheurs lors de la conférence BlackHat USA 2006. La technologie Ajax n'est pas en soi une technologie dangereuse, mais permet des attaques plus complexes en rendant certaines actions non imputables aux utilisateurs, vis à vis du serveur Web. Les articles de ce numéro sur les XSS et la sécurité Ajax vous aideront à y voir plus clair !

- <http://www.f-secure.com/weblog/archives/archive-072006.html#00000930> [1]
- <http://fast.info/myspace/> [2]
- http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html [3]
- <http://www.webappsec.org/projects/whid/> [4]

À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants - <http://www.hsc.fr>). Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une expérience certaine dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques sur ce sujet et a publié plusieurs articles dont un article dans le numéro 14 de Hakin9 intitulé *Sécurité Wi-Fi - WEP, WPA et WPA2*. Contact : Guillaume.Lehembre@hsc.fr