‘Huit des dix plus grands sites Internet sont vulnérables’ estiment WhiteHat

Le groupe WhiteHat security vient de publier une étude mettant en exergue le faible niveau de sécurité de huit des dix plus grands sites du 3W. Selon eux les hackers peuvent les utiliser pour récupérer des données confidentielles.

Jeremiah Grossman, le fondateur de la société WhiteHat indique : » *Nous procédons régulièrement à des balayages (ndlr : scan) des sites Web les plus populaires avec des trafics très importants. Généralement, ce sont des sites d’e-commerce, de banque en ligne…30% des sites scannés contiennent une vulnérabilité à corriger de toute urgence.* »

Aussi surprenant que cela puisse paraître, certains sites autorisent un accès direct à sa base de données contenant des informations sur ses clients.

2 sites sur trois sont victimes d’une faille ou plus de type cross-site scripting (XSS). Ces attaques profitent des failles de programmation des sites et sont de plus en plus utilisées dans les attaques de phishing ou hameçonnage.

Un scam récent sur le site de vente aux enchères eBay utilisait le cross site scripting pour rediriger les acheteurs sur un site de phishing. Un bogue qui a depuis été corrigé.

Les autres menaces

Un tiers des sites scannés par WhiteHat s’exposent a des risques importants en donnant des informations trop précises sur le site et sa programmation facilitant ainsi grandement l’attaque. Un site sur quatre est vulnérable au spoofing (ndlr : usurpation d’adresse ARP et IP.

« Une autre vulnérabilité très dangereuse concernant les bases de données et qui permettait l’injection de requêtes SQL est pour sa part de moins en moins commune » indique le document.

Moins d’un site sur cinq est encore vulnérable à ce bogue. Reste que correctement exploitée, cette porte ouverte peut faire dégâts assez colossaux.

Avec le langage de programmation utilisé par les sites dits de Web 2.0, en l’occurrence l’Ajax, il est possible de positionner les lignes de CSS Cascading Style Sheet (les feuilles de styles) dans une couche encore plus invisible du code source de la page *« le risque est donc encore plus grand «* considère Grossman.

Enfin, les réseaux communautaires comme Myspace et Youtube, ainsi que les blogs sont aussi de formidables sources d’informations pour les pirates.

Le rapport publié par WhiteHat est disponible au téléchargement sur cette page, l’étude a été menée entre le premier janvier 2006 et le 31 mars 2007.