Philippe CHAUVELIN - François-Guillaume Ribreau

CSII 3e année

Les attaques XSS

E.P.S.I - NANTES

114 rue des Hauts Pavés

BP 41903

44019 NANTES CEDEX 01

Sommaire

Introduction

L'expansion de l'informatique conduit de plus en plus de gens à développer leurs propres programmes, que ça soit pour une entreprise ou pour une utilisation personnelle (ex : site web). Cette expansion est aussi une porte ouverte au piratage, de plus en plus courant en raison du nombre de développeurs qui augmente chaque année. Les Exploits, faisant partie de nos jours des logiciels malveillants les plus utilisés par les pirates, sont de plus en plus virulents. Ce thème est très intéressant car il nous permettra, en tant que développeur, de comprendre les failles que l'on peut générer en programmant nos logiciels et comment y remédier. La sécurité logicielle étant une compétence de choix au vue des constatations dites précédemment. Il nous amènera également à nous poser la problématique suivante : Comment protéger nos programmes des Exploits ? Dans une première partie, nous verrons ce que sont réellement les exploits, leurs objectifs, leur fonctionnement général. Comme pour les virus (Worm, chevaux de Troie etc.) il existe plusieurs types d'exploits. Par conséquent, nous aborderons les différences entre chacun, ainsi que leurs caractéristiques, de plus il sera expliqué pour chacun d'entre eux, les causes, conséquences et contexte dans lequel ils se situent. Nous tenterons dans une seconde partie d'expérimenter le concept de « faille logicielle » en créant un programme simple et en y insérant l'une des failles qui sera détaillée dans la partie précédente. Nous pourrons donc par la suite tester un Exploit spécifique à la faille choisie. Un développeur spécialisé dans la sécurité logicielle doit savoir exploiter les failles visibles d'un programme afin de pouvoir y remédier. Nous expliquerons donc dans cette troisième partie les différentes étapes de construction d'un Exploit qui nous permettront par la suite de créer le nôtre puis ensuite de le tester. Nous verrons dans une dernière partie des méthodes appropriées pour protéger son programme contre les Exploits. Nous expliquerons dans un premier temps les erreurs à ne pas commettre dans un code source, afin d'éviter l'ouverture d'une faille. Puis nous présenterons les différents logiciels permettant de lutter contre le piratage. La résultante de cette dernière partie nous permettra de conclure quant aux différentes solutions que le développeur peut mettre en place dans son code afin d'éviter l'ouverture d'une faille de sécurité.

Chapitre

1 Approche théorique

1.1 Définition

Le XSS est une attaque visant les sites web qui affichent dynamiquement du contenu côté client et ce sans effectuer de contrôle des informations saisies par les utilisateurs. Les exploits Cross-Site Scripting consistent à forcer un site web à afficher du code HTML ou des scripts non autorisés et saisis par les utilisateurs. Le XSS est donc une attaque menée dans le but d'exécuter un code Javascript directement sur le poste de la victime. Cette technique est particulièrement utilisée par les pirates pour voler la session d'un utilisateur connecté. Si le pirate arrive à identifier un site web vulnérable, il a donc la possibilité d'insérer un script au sein d'une URL et de l'envoyé à une victime. Si cette dernière est connectée sur ce site web vulnérable, elle enverra immédiatement, et à son insu, son cookie de session au pirate. L'attaquant pourra alors utiliser ce cookie et voler la session de la victime pour mener des actions frauduleuses.

1.2 Recherche de faille

1.3 XSS réfléchi

Contenu Section

1.4 XSS stocké

Contenu Section

1.5 Solutions envisageable

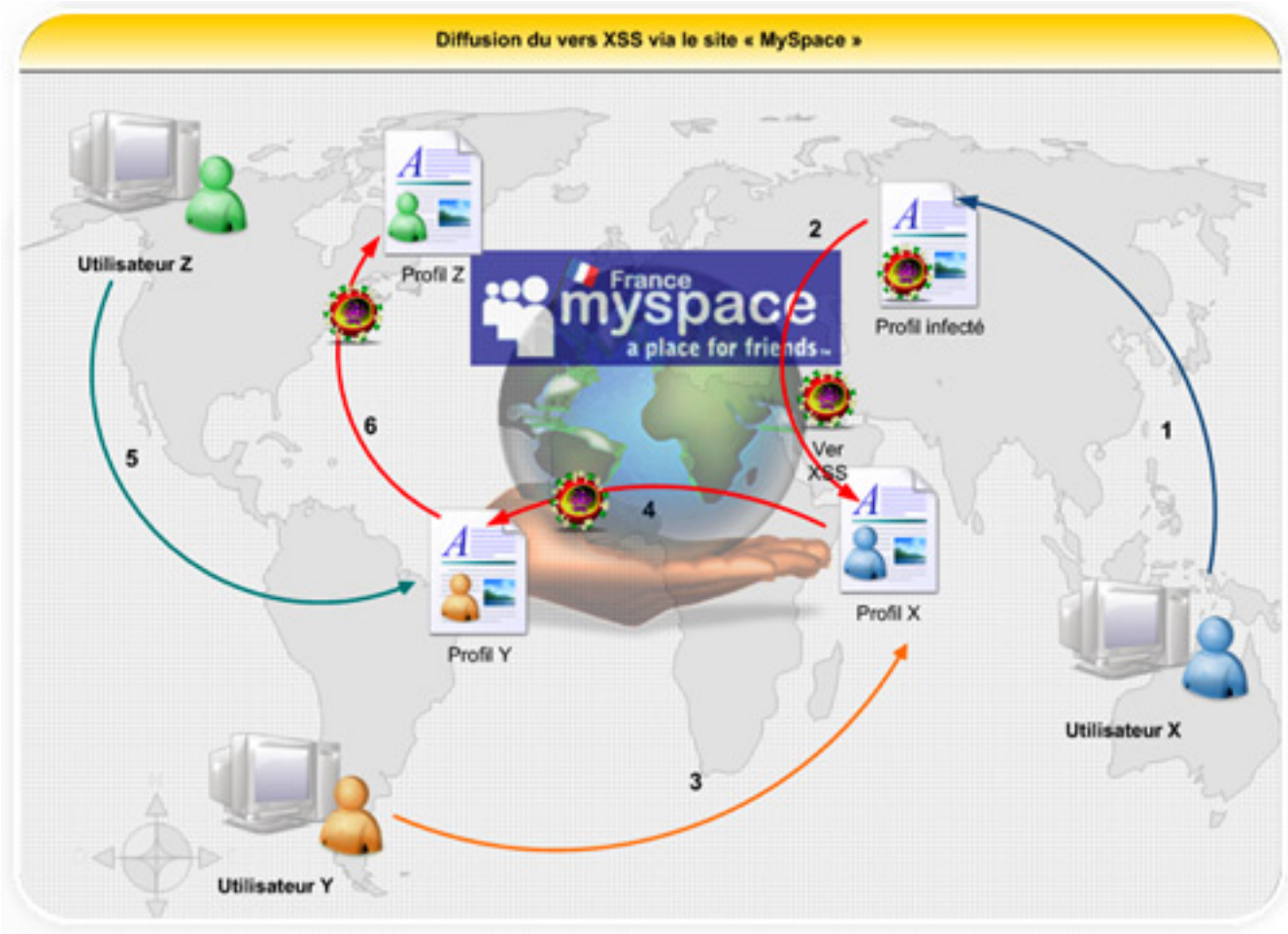
Contenu Section

Chapitre

2 Approche pratique

2.1 Cas MySpace

Le premier ver XSS a été créé en 2005 sur le réseau social mondial MySpace. Sans gravité et nommé «Samy » il avait pour but d'ajouter à la liste d'amis de la victime un contact appelé Samy, pour ensuite se répliquer. Au final Samy a contaminé près de 1 000 000 de profils.



Comment le pirate a-t-il découvert la faille ? Il a tout d'abord remarqué que l'insertion de code HTML au sein de son profil était possible. En théorie si l'injection de code HTML

est possible, il est également possible d'injecter du code Javascript, c'est à ce niveau que le pirate s'est heurté à un problème. En effet le site Myspace dispose d'une forte restriction en ce qui concerne le terme « javascript » (Ex : <script language= ''text/javascript") par conséquent l'insertion de ce dernier semblait très délicate. Il a donc trouvé une solution pour contourner ce problème, qui consistait à séparer ce terme en deux parties par retour chariot, ce qui lui a permis ensuite d'exploiter cette faille au maximum. Ce code JS envoyait discrètement et à l'insu de la victime des requêtes POST et GET via AJAX, la seule condition était que la victime visite le profil de l'utilisateur Samy. Le plus compliqué dans la mise en place de cette faille était la génération de requête http automatique sans la moindre intervention. La victime ne se rendait pas compte que lors de sa visite du profil Samy le navigateur lançait des requêtes http, simplement parce que la validation se faisait automatiquement (très dur à réaliser en JS). Samy n'a pas été le seul ver à se propager à si grande échelle, il y a eu également le ver « Yammaner » (crée en 2006). Celui-ci a contaminé un grand nombre de serveur web-mail, notamment Yahoo. S'appuyant sur le même principe que Samy, Yammaner avait pour but de voler la liste de contact de la victime. Pour cela cette dernière recevait un email qui une fois ouvert s'envoyait lui-même à tous les contacts de la victime.

Conclusion

Contenu Conclusion

Bibliographie

[1] Monsieur Barbu. *La Belle thèse*. PhD thesis, Université, 2002.

[2] Fernand Dupont. *Les choux farcis*. Un gros éditeur, 2004.

[3] Nestor Dupont. *réparer son vaisseau*. l'Alliance, 2009.

[4] Patrick Durand and René Durand. Les tomates tueuses. *Le beau journal*, page 24, jan 2007.

[5] Monsieur Mauvais. Mon roman inachevé. il est chouette mon roman, feb 2000.

[6] Les Zéros. Le site du zéro, jun 2009. www.siteduzero.com.

Table des figures

Annexes

Table des matières