Francois-Guillaume RIBREAU - Philippe Chauvelin
CSII 3eannée

Les différents vecteurs d'attaque et de protection des applications web

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. 4. Présentation 4.1 Définition

Un Exploit est un programme informatique mettant en œuvre l'exploitation d'une vul-

nérabilité liée à un logiciel. Chaque exploit est spécifique à une version d'une application car il permet d'en exploiter les failles. Ils sont utilisés la plupart du temps pour les raisons suivantes : • Augmentation des privilèges : les Exploits les plus redoutables permettent de prendre le contrôle sur les programmes exécutés avec les privilèges d'administrateur (root sous les systèmes de type UNIX) ; • Provocation d'une erreur système : certains Exploits ont pour objectif la saturation d'un programme informatique afin de le faire « planter ». Lorsqu'une faille est détectée, le pirate peut l'exploiter en injectant dans des zones non contrôlées, du code arbitraire. Cependant cela nécessite un minimum de connaissances du système cible.

1

Théorie

Comment se déroule l'attaque

2

Technique

Comment s'en protéger (technique)

2.1 Le spoofing de variable

3

Pratique

Exemple d'entreprise, startup qui ont eu des attaques XXX ou YYYY et comment elles s'en sont prémunies.
Exemple Brin.gr avec l'attaque SSH. (changer le port 22).

4

Discussions

5

Conclusion