Ecole d'ingénieurs
du Canton de Vaud
Route de Cheseaux 1
CH-1401 Yverdon-les-Bains
Tél : +41 24 423 21 11
Fax : +41 24 425 00 50

Travail de diplôme 2003

Sécurité des applications Web

Développement d'un firewall applicatif HTTP

Problématique

La sécurité des applications Web est critique car celles-ci sont généralement publiquement accessible sur Internet, et donc la moindre vulnérabilité pourra être exploitée par n'importe quel *hacker* dans le monde.

Au même titre qu'une application de bureau ou qu'un système d'exploitation, une application Web est sujette à un certain nombre de failles de sécurité, dues à des négligences de programmation. Les développeurs Web, pressés par le temps et souvent peu sensibilisés au problème de la sécurité, ne sont pas conscient des failles de sécurité qu'ils peuvent laisser dans leur code.

L'étude des principales vulnérabilités rencontrées dans les applications Web montre que la plupart des attaques se font par simple manipulation d'URL ou en injectant des paramètres dans un formulaire pour, par exemple, contourner un mécanisme d'authentification. Ces attaques empruntent toutes le port TCP 80 et ne sont par conséquent pas bloquées par les firewalls IP conventionnels.

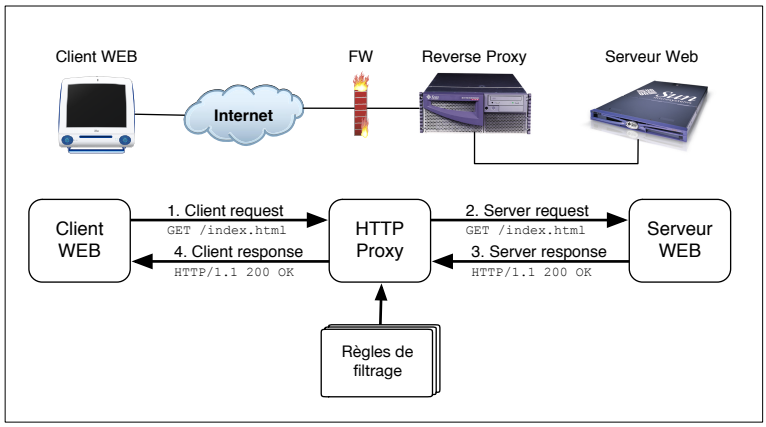
Mandat

Le travail consiste à développer un firewall applicatif spécialisé dans le protocole HTTP, permettant de filtrer les principales attaques avant même qu'elles ne parviennent au serveur Web. Le filtrage se fait sur la base de l'URL, des paramètres de scripts, de la méthode (GET, POST, etc...) et des entêtes HTTP, aussi bien en entrée qu'en sortie.

Fonctionnement

Le logiciel joue le rôle d'un *reverse proxy*. Situé entre le client et le serveur Web, généralement sur la zone publique (DMZ) d'un firewall d'entreprise, il reçoit les requête en provenance du client, les filtre et les transmet ensuite au serveur Web. Le *reverse proxy* est un intermédiaire obligé pour atteindre le serveur Web : un firewall IP empêche un accès direct au serveur Web depuis l'extérieur.

La configuration se fait au moyen de règles permettant d'indiquer au *reverse proxy* quelles sont les requêtes autorisées, et quelles sont les requêtes qui doivent être bloquées. Les modes de fonctionnement *White list* (filtrage inclusif) et *Black list* (filtrage exclusif) sont supportés.



Technologies

ProxyFilter, comme a été baptisé le fruit de ce travail de diplôme, prend la forme d'un module venant se greffer sur le serveur Web Apache. Le langage de programmation utilisé est Perl, et la syntaxe de configuration est basée sur XML. *ProxyFilter* est un projet *open source* sous license GPL.

http://proxyfilter.sourceforge.net

Auteur : Sylvain Tissot
Expert externe : Gérald Litzistorf, EIG
Prof. reponsable : Stefano Ventura, EIVD
Sujet proposé par : Sylvain Maret, e-Xpert Solutions SA

Haute Ecole Spécialisée
de Suisse Occidentale