



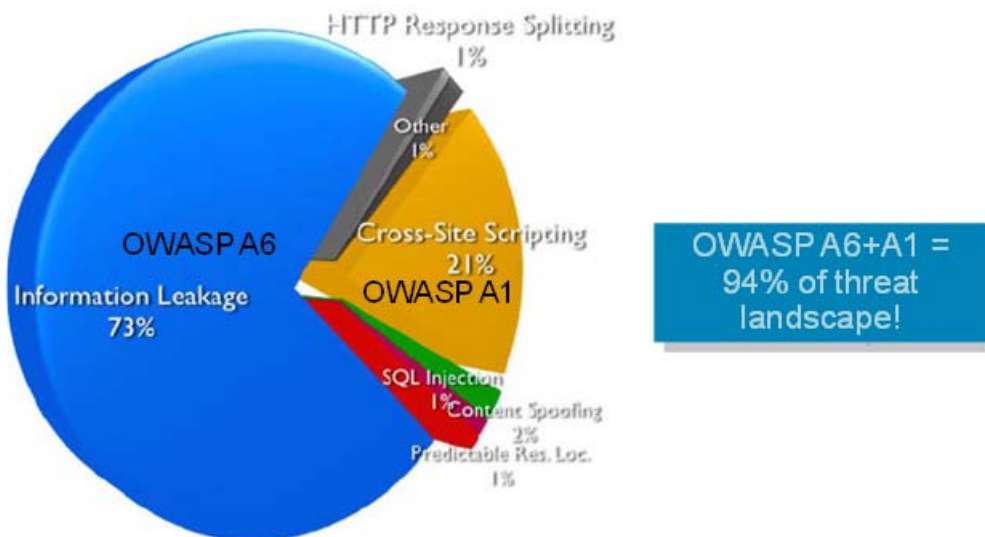
La sécurité des applications Web

Introduction

Les technologies déployées dans les environnements Web ont fortement évolué ces dernières années. L'avènement du Web 2.0 a changé la manière de présenter et d'accéder aux ressources accessibles via le protocole HTTP. Ces nouvelles architectures ont considérablement augmenté la surface d'attaque et rendu bon nombre de serveurs plus vulnérables.

De nombreuses études publiques, comme celle de la communauté [OWASP](#), nous révèlent que la grande majorité des vulnérabilités sont d'ordres applicatifs. Aussi, ces vulnérabilités proviennent le plus souvent du code spécifique des applications, plus que des « frameworks » utilisés pour les développer.

Vulnérabilités les plus communes des applications WEB par catégories



Top 5 vulnerability classes in the overall population.

Source: WhiteHat Security, 2007

Les vulnérabilités les plus répandues permettent à un attaquant d'obtenir des informations censées n'être accessibles que par des utilisateurs dûment identifiés.

D'autres ont pour but de modifier le contenu délivré aux utilisateurs du serveur. Actuellement, ces pratiques ont surtout pour ambition de compromettre les machines clientes, plutôt que de modifier le

contenu visible. Ceci rend d'autant plus difficile la découverte d'une attaque réussie. Lors de l'utilisation du serveur, le contenu semble intact pour ses utilisateurs. Un bon exemple est la découverte par SOPHOS, en septembre 2008, de contenu « JavaScript » malicieux dans les pages du site web de BusinessWeek. Plusieurs milliers de pages ont été modifiées lors d'une attaque de type « SQL Injection », dans le but d'y introduire des « JavaScript » malicieux, afin de compromettre les machines des nombreux lecteurs. Sans la découverte de ces contenus malicieux par SOPHOS, ces derniers auraient pu rester actifs très longtemps, car l'aspect des pages n'était absolument pas altéré.

Une simple recherche sur Google du type « BusinessWeek SQL Injection » permet d'obtenir plus d'informations sur cette attaque.

Web Application Firewall

Les technologies traditionnelles, comme les Firewalls, sont malheureusement peu efficaces contre ces attaques au niveau applicatif. Une nouvelle génération de Firewalls, les Web Application Firewalls (WAF) a donc vu le jour, avec l'ambition de répondre à ces nouveaux risques.

La plupart de ces vulnérabilités proviennent d'un contrôle insuffisant effectué par le serveur, sur le contenu des requêtes. Le rôle d'un Web Application Firewall est donc de pallier cette insuffisance, par une fonction appelée « Virtual Patching ». Chaque requête est contrôlée avant d'être envoyée au serveur. Si la requête est considérée comme valide, elle sera relayée au serveur. En revanche, si le WAF découvre un contenu dangereux dans cette requête, il y répondra sans solliciter le serveur concerné.

Le consortium PCI a rappelé en avril 2008, dans ses recommandations PCI DSS, que les technologies Web Application Firewall ne devaient pas être confondues avec les technologies Firewall traditionnelles et que ces dernières étaient une réponse efficace aux problèmes de vulnérabilité applicative des serveurs Web.

Human Assisted Learning

La technologie Web Application Firewall contient un ensemble de règles de type « Black List » définissant les contenus illicites. Comme dans toute technologie de type « Black List », certaines règles peuvent produire, de manière exceptionnelle, des faux positifs. Notre technologie WAF utilise une technique appelée « Human Assisted Learning (HAL) » afin de permettre à l'administrateur d'adapter très rapidement la politique de sécurité à son environnement.

Ceci passe par une étape d'apprentissage. Pendant cette étape, le WAF est configuré de manière à alerter l'administrateur lors de la découverte d'un contenu malicieux, sans pour autant bloquer le trafic (Monitor Mode). A charge pour l'administrateur de vérifier si ce contenu est effectivement impropre pour le serveur concerné, ou s'il est nécessaire de créer une exception pour ce contexte particulier. A la fin de cette période d'apprentissage, la technologie WAF sera en mesure de sécuriser les accès aux serveurs avec l'assurance de ne pas perturber les requêtes légitimes.

Pour les administrateurs les plus expérimentés, il est aussi possible de recourir à une configuration de type « White list », référençant de manière explicite et exhaustive, l'ensemble des requêtes considérées comme acceptables par les serveurs.

ACE XML Gateway / Web Application Firewall



Face aux évolutions du Web, comme par exemple AJAX, les technologies Web Services et les services Web classiques sont de plus en plus utilisés conjointement. Quoi de plus naturel donc, que d'implémenter notre solution Web Application Firewall dans notre offre existante d'accélération et de sécurisation des Web Services « ACE XML Gateway (AXG) ».

L'AXG accueille des fonctions d'accélération comme le offloading SSL, la transformation XSLT, la validation de la conformité des requêtes au schéma du service, etc. ainsi que le filtrage des requêtes XML afin d'en assurer l'accès de manière sécurisée.

Depuis le mois de mai de cette année, l'AXG supporte aussi la technologie Web Application Firewall (WAF) avec la sortie de la version 6. Il est donc à présent possible d'obtenir une licence permettant l'activation de cette fonction en plus des fonctions XML. Si les fonctions XML ne sont pas nécessaires, une licence WAF uniquement est aussi disponible.

Dans le cas des technologies AJAX, il est intéressant de noter que l'intégration des deux services (XML & WAF) en une seule appliance, simplifie grandement le développement d'une politique de sécurité globale.

La politique de sécurité livrée a été développée par Cisco pour répondre aux recommandations PCI DSS 1.1 section 6.5 et 6.6 (OWASP Top 10).

Cette offre comporte donc trois éléments : un manager, un gateway XML et un gateway WAF. Ils peuvent être configurés sur une seule appliance ou distribués, un manager étant capable de gérer plusieurs gateways. Des fonctions avancées de « monitoring » et de « reporting » apportent encore un peu plus de valeur à cette offre, comme le « Performance Monitor » permettant une analyse fine des temps de réponse, de la latence et la visualisation de la taille des requêtes/réponses.

Pour aller plus loin

Point d'entrée sur Cisco.com

<http://www.cisco.com/go/waf>

Documentation

http://www.cisco.com/en/US/partner/products/ps9586/products_installation_and_configuration_guides_list.html



Contactez-nous :

www.cisco.fr

0800 907 375

Siège social Mondial
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France
Cisco Systems France
11 rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie Mexique • Nouvelle Zélande • Norvège • Pays-Bas • Pérou Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine • Russie Singapour • Slovaquie • Slovénie • Suède Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe



Copyright © 2008 Cisco Systems, Inc. Tous droits réservés. CCSP, CCVP, le logo Cisco Square Bridge, Follow Me Browsing et StackWise sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, et iQuick Study sont des marques de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, le logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0502R) 205534.E_ETMG_JD_10/08

