ModSecurity

Cible de sécurité CSPN
Version 0.96

TABLE DES MATIERES

1 IDENTIFICATION

1.1 Identification de la cible de sécurité

La cible de sécurité CSPN du logiciel **ModSecurity 2.5** a été rédigée par **SOGETI ESEC** dans le cadre d'un marché public du **SGDN**.

Cette cible de sécurité a été élaborée en vue d'une évaluation Certification Sécurité de Premier Niveau (CSPN).

1.2 Identification du produit

Catégorie	Identification
Organisation éditrice	Breach Security
Lien vers l'organisation	http://www.breach.com
Nom commercial du produit	ModSecurity
Numéro de la version évaluée	2.5.11
Catégorie de produit	Pare-feu

2 ARGUMENTAIRE (DESCRIPTION) DU PRODUIT

2.1 Description générale du produit

ModSecurity est un module qui s'intègre au serveur Web Apache et qui permet de mettre en place un pare-feu applicatif dédié aux applications Web. Il fournit un moteur permettant de détecter et de se prémunir des attaques avant qu'elles n'atteignent l'application Web protégée.

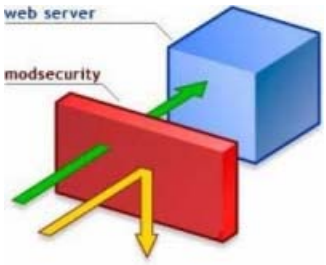

Figure 1 - Fonctionnement globale de ModSecurity[1]

ModSecurity offre les mécanismes suivants :

- Journalisation du trafic HTTP ;
- Surveillance du trafic et détection en temps réel des attaques ;
- Prévention des attaques et correction virtuelle en vue de corriger les vulnérabilités applicatives sans toucher aux applications Web.

Une fois le module ModSecurity installé sur Apache, celui-ci ne fournit que peu de protection par lui-même car il n'intègre pas de règles par défaut. Il faut donc ajouter et configurer les règles nécessaires pour sécuriser les applications Web.

Néanmoins, le projet « **ModSecurity Core Rules Set** » a été créé afin de fournir un jeu de règles fournissant une protection générique contre les attaques les plus employées à l'encontre des applications Web.

[1] Source : http://www.owasp.org/index.php/Category:OWASP_ModSecurity_Core_Rule_Set_Project

2.2 Description de l'utilisation du produit

ModSecurity s'installe comme module sur un serveur Web Apache. Il démarre donc avec le serveur Apache et reste actif en permanence.

Deux modes de configuration sont possibles :

- Intégré directement sur le serveur Web Apache à protéger. Dans ce cas de figure, pour chaque serveur Web Apache à protéger, le module ModSecurity doit être installé ;
- En coupure du réseau installé sur un serveur Web Apache configuré en « **Reverse Proxy** » (relai inverse) en utilisant un second module, *mod_proxy*. Dans ce cas de figure, ModSecurity protège plusieurs serveurs Web, qui peuvent être de type différents (IIS, WAS, JBoss, etc.).

2.3 Description de l'environnement d'utilisation prévu

ModSecurity s'installe sur un serveur Web Apache et fonctionne sur les systèmes d'exploitation suivants : **Linux, Windows, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, Mac OS X** et **HP-UX**.

Le serveur où sera installé ModSecurity sera configuré en mode « **Reverse Proxy** » ; le schéma ci-dessous présente l'architecture cible et les types d'environnement qui seront protégés :

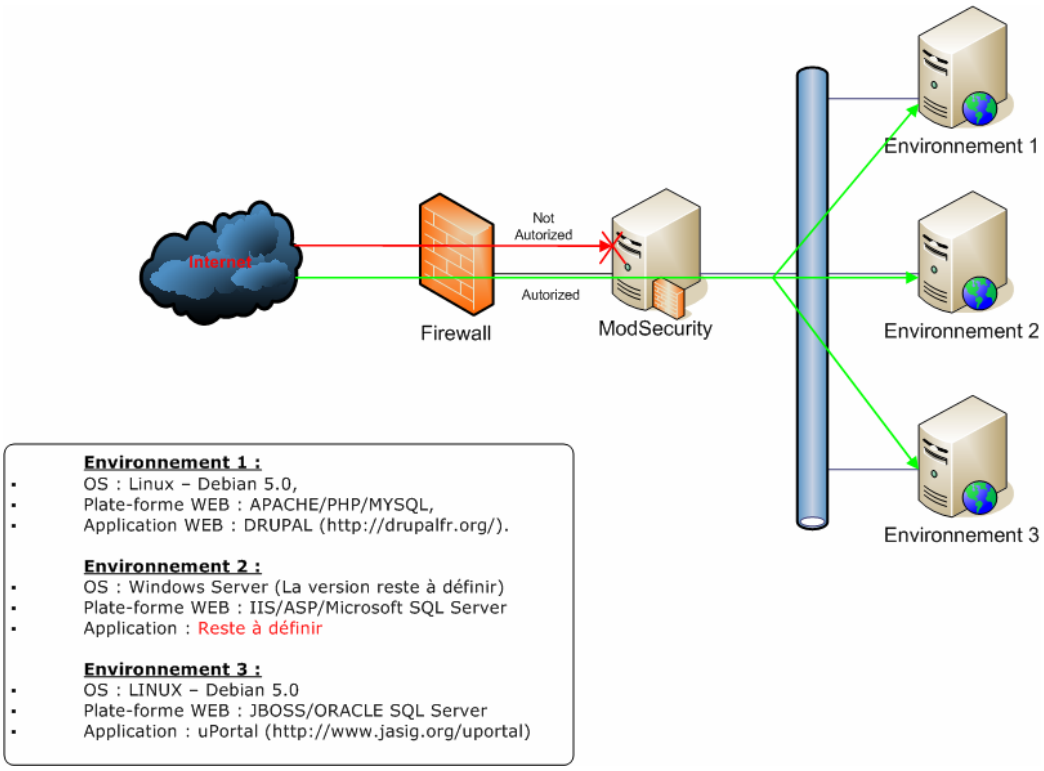

Figure 2 - Architecture Cible

2.4 Description des hypothèses sur l'environnement

Environnement Logique:

- ModSecurity doit être installé sur un système **sain**, correctement mis à jour, en particulier au niveau des correctifs liés à la sécurité. Il convient également de sécuriser le système, par désactivation des services et partages inutiles par exemple.
- Le serveur Web Apache sur lequel est installé ModSecurity est correctement configuré et administré.
- L'administrateur dispose des moyens de contrôler la configuration de ModSecurity par rapport à un état de référence, ou de la régénérer dans un état sûr.

Environnement physique :

- Les équipements contenant le serveur Web Apache avec ModSecurity doivent se trouver dans des locaux sécurisés dont l'accès est contrôlé et restreint aux administrateurs.

Mesures organisationnelles :

- Les administrateurs sont des personnes considérées comme non hostiles. Ils sont formés pour exécuter les opérations dont ils ont la responsabilité et suivent les manuels et procédures d'administration.
- Les administrateurs sont sensibilisés à l'analyse régulière des événements d'audit générés par ModSecurity.
- Les procédures de gestion et traitement des alarmes sont formalisées, documentées et connues par les administrateurs de sécurité de ModSecurity.

2.5 Description des dépendances

Pour fonctionner correctement, le logiciel ModSecurity doit être installé sur un server ayant les pré-requis suivants :

- **Serveur Web :**
  - Version : ModSecurity dans sa version 2.x ne fonctionne qu'avec les versions d'Apache 2.0.x ou supérieures.
  - Configuration : Les modules suivants doivent être activés :
    - *mod_unique_id*
    - *mod_proxy*
- **Librairies :**
  - *libAPR*
  - *libAPR-util*
  - *libPCRE*
  - *libXML2*
  - *libLUA 5.1.x*

- *libCURL 7.15.1* ou ultérieure

Le paragraphe 2.3 identifie les installations prises en compte dans cette cible de sécurité.

2.6 Description des utilisateurs typiques

Le contexte d'utilisation du logiciel ModSecurity fait intervenir l'administrateur qui réalise les activités suivantes :

- L'installation du serveur avec le module ModSecurity ;
- La configuration des règles de sécurité de ModSecurity ;
- La récupération et l'exploitation les journaux (alertes, actions) générés par ModSecurity.

Par ailleurs, les utilisateurs des contenus et applications Web hébergés sur le serveur Apache n'ont pas d'interaction directe avec ModSecurity.

2.7 Définition du périmètre de l'évaluation

L'évaluation porte sur la capacité du logiciel ModSecurity à protéger des applications Web et leurs données avec le jeu de règles « **ModSecurity Core Rule Set** » sur l'environnement cible décrit dans la section **2.3**. Les règles seront adaptées afin que l'application protégée puisse s'exécuter normalement.

N.B : La fonctionnalité d'analyse des documents PDF et l'administration de ModSecurity ne font pas partie du périmètre de cette évaluation.

3 DESCRIPTION DE L'ENVIRONNEMENT TECHNIQUE DE FONCTIONNEMENT

3.1 Matériel compatible ou dédié

Les matériels utilisables sont ceux adaptés pour les systèmes d'exploitation retenus.

3.2 Environnement système retenu

Dans le cadre de cette évaluation CSPN, l'environnement d'utilisation prévu est :

- Système d'exploitation **Linux**, et plus particulièrement la distribution **Debian** dans sa version 5.0.x ;
- Serveur Web **Apache** version 2.2.14 ;
- **ModSecurity** version 2.5.11 ;
- **ModSecurity Core Rule Set** version 2.0.3.

4 DESCRIPTION DES BIENS SENSIBLES QUE LE PRODUIT DOIT PROTEGER

Le produit contribue à protéger des biens utilisateurs de type informations et services de l'application Web, protégés par le filtrage des flux, susceptibles d'être accédés ou modifiés.

Protection : Confidentialité, Intégrité et Disponibilité;

Nota : Les biens sensibles du logiciel ModSecurity (règles, journaux) doivent être protégés par le système d'exploitation et l'environnement d'exploitation sous lequel s'exécute l'application (hors périmètre).

Protection : Confidentialité, Intégrité et disponibilité.

5 DESCRIPTION DES MENACES

Etant donné que les administrateurs ne sont pas considérés comme des attaquants potentiels, l'agent de menace est une entité qui transmet un flux vers le serveur Web.

Description des menaces :

- Un attaquant transmet des requêtes HTTP anormales au serveur Web ; Cette attaque vise à modifier les informations gérées par l'application web.

- Un attaquant tente une attaque de type débordement de tampon ou de manipulation de paramètres ; Cette attaque vise à modifier les informations gérées par l'application web. Celle-ci par effet de bord peut entrainer une indisponibilité du service offert par l'application web.
- Un programme malveillant consomme de la bande passante pour rendre le site inactif ; Cette attaque vise à rendre indisponible le service offert par l'application web.
- Un programme malveillant recueille de manière systématique des informations sur le site Web (scan de vulnérabilités, fingerprinting,.. ;) ; L'objectif de cette démarche entreprise par l'attaquant est de récupérer des informations sur l'application web afin de pouvoir lancer ultérieurement une attaque ciblée.
- Un attaquant cherche à corrompre l'application Web par des attaques applicatives de type : Injections SQL, *Cross Site Scripting* (XSS), Injections de commandes, Injections de code ColdFusion, PHP et ASP, Injections d'E-mail, *HTTP Response Splitting*, modification du contenu XML etc.) ; Cette attaque vise à modifier les informations gérées par l'application web ou prendre le contrôle de celle-ci.
- Un attaquant tente d'établir des connexions avec des chevaux de Troie ou des portes dérobées ; Cette possibilité est réalisable suite à une attaque, précédemment réussie, qui aurait permis d'injecter un cheval de Troie ou une porte dérobées au sein de l'application web. L'application étant corrompu, l'attaquant peut modifier le contenu de l'application web avec du contenu malveillant. L'objectif étant d'attaquer les utilisateurs par rebond depuis l'application web. L'attaquant peut en parallèle récupérer des informations auxquelles il ne devrait pas avoir accès.

6 DESCRIPTION DES FONCTIONS DE SECURITE DU PRODUIT

La fonctionnalité de sécurité principale de ModSecurity est de protéger en disponibilité et en intégrité les applications et les données hébergées par un serveur Web contre tout type d'attaques. Cette protection est assurée par les règles configurées dans le logiciel.

Les fonctions de sécurité de ModSecurity sont donc :

- Mettre en œuvre les règles de sécurité telles que configurées dans l'application :
  - Détecter les événements selon le paramétrage du « ModSecurity Core Rule Set » :
    - Analyse de la conformité protocolaire :
      - Détection des anomalies dans le protocole HTTP ;
      - Vérification du respect des contraintes de l'application (longueur des paramètres envoyés à l'application, etc.).
    - Détection d'attaques :
      - Détection d'outils de collecte d'information : Scanneurs, Robot d'indexation, robots… ;
      - Détection des tentatives de connexions des « *chevaux de Troie* » ou des « *portes dérobées* » déjà déployés au sein du système d'information ;
      - Détection générique des attaques :
        - Injections SQL diverses ;
        - *Cross Site Scripting* (XSS) ;

        - Injection de commandes ;
        - Injection de code ColdFusion, PHP et ASP ;
        - Injection d'E-mail ;
        - *HTTP Response Splitting*;
    - Réaliser des actions préventives (en vue de prévenir une attaque) :
        - Protection du contenu XML ;
        - Surveillance des accès aux sites Web ;
        - Réécriture des messages d'erreur renvoyés par le serveur Web ;
- Bloquer les attaques suite à leur détection,
- Journaliser les événements et les actions.

FIN DU DOCUMENT