Projet CASSIOPEE® :
« Database Firewall »
Compte rendu d'avancement n°03

Liste de diffusion : Grégory Blanc, Grégoire Menguy, Baptiste Polvé

Ordre du jour

- **Développement du système de journalisation (achevé)**
- **Gestion des tautologies dans l'analyseur (en cours)**

Développement du système de journalisation

Baptiste a mis en place le système de Monitoring / journalisation.
Ce système permet de lancer un système de journalisation qui travaille dans un thread autonome en gérant l'écriture des logs dans le fichier de logs. Ainsi, l'application « abonne » son message de logs en le classant selon son type et le thread de journalisation le traite dès que possible.
Cette architecture a l'avantage de ne pas ralentir de façon trop importante l'application puisque l'ouverture/fermeture/écriture de fichiers se fait en parallèle du fonctionnement de l'application.
Il paraît difficile de traiter les alertes pour la multiplication de requête sensible à partir de ce module, le traitement via des compteurs sur des points spécifiques devrait être plus efficace dans l'analyseur. Cependant pour améliorer de manière intelligente l'application, l'étude des fichiers de journalisations sera nécessaire.

Gestion des tautologies dans l'analyseur

Grégoire poursuit la lecture de l'article An Analysis Framework for Security in Web Applications de Gary Wassermann et Zhendong Su qui explique le fonctionnement (la théorie) de leur Framework permettant de reconnaître les tautologies. Cela reste très théorique pour l'instant et ne sera sûrement pas suffisant pour éliminer tous les risques. En effet, celui-ci ne traite que les tautologies linéaires (opérateurs logiques et comparaisons d'expressions arithmétiques linéaires). Il faudra donc combiner la méthode proposée avec un système de signatures.

Ce CR sera considéré comme validé lundi 02/05/2017 en l'absence de remarque.