Projet CASSIOPEE® :
« Database Firewall »
Compte rendu d'avancement n°04

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

Ordre du jour

- **Gestion des ERROR_BASED_INJECTION (achevé)**
- **Gestion des attaques en général (en cours)**
- **Gestion des tautologies (achevé)**
- **Élargissement de la grammaire MySQL (en cours)**
- **Base de données pour les tests de sécurité et de performances (en cours)**

Gestion des ERROR_BASED_INJECTION

Comme convenu lors de la précédente réunion, Baptiste a mis en place la gestion des error based injection à travers le remplacement de l'erreur reçu par une erreur générique indiquant de contacter l'administrateur du site si l'erreur persiste.

Gestion des attaques en général

Baptiste va gérer la contre attaque en affichant le même type de message que pour les error_based_injection lorsqu'une attaque est détectée, en plus de la notification dans le fichiers de logs.

Gestion des tautologies

Grégoire a fini d'intégrer la gestion des tautologies au sein de l'analyseur. Pour l'instant, les tests sont fructueux. La méthode nécessite cependant l'utilisation d'une base de données de signatures importantes que nous n'avons pas encore.

Élargissement de la grammaire MySQL

Grégoire poursuit l'élargissement de la grammaire MySQL acceptée pour limiter le nombre de faux positifs. En effet, pour l'instant, le parser n'autorise que les requêtes simples – SELECT et close WHERE avec des sous requêtes. Grégoire étend donc la grammaire pour y intégrer les fonctions MySQL, ainsi que l'utilisation des opérandes ORDER BY, GROUP BY, LIMIT, OFFSET.

Base de données pour les tests performance/sécurité

Une première collecte a été faite par Baptiste, avec la participation de Grégoire et implémentée aux Google Test pour automatiser les tests. Cependant, il est actuellement difficile de trouver des bases complètes. Sqlmap sera certainement utilisé pour tester le temps de traitement (test de performance).

Ce CR sera considéré comme validé lundi 16/05/2017 en l'absence de remarque.