Projet CASSIOPEE® :
« Database Firewall »
Compte rendu de réunion n°06

Motif :	Lieu :	Date : 23 mai 2017
Réunion de projet	D101-01	**Heure de début :** 17h00 **Durée :** 1h

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

Ordre du jour

- **Avancement**
  - **Gestion des attaques**
  - **Tests DVWA**
  - **Améliorations de la grammaire MySQL**
  - **Utilisation du barème**
  - **Rapport de synthèse**
- **Prévisions**
- **Échange avec le client**

Avancement du projet

- **Gestion des attaques**
  - **Le DBF détecte et gère les requêtes malveillantes**
  - **Le système de logs montre les requêtes bloquées**

- **Tests avec DVWA**
  - **Les premiers tests ont été réalisés**
    → Le DBF fonctionne bien

- **Amélioration de la grammaire MySQL**
  - **Rajout de méthodes MySQL dans la grammaire**
    → Moins de faux positifs mais plus de faux négatifs
  - **Ajout d'une whitelist pour gérer les exceptions**

- **Utilisation du Barème**
  - **Barème implémenté et fonctionnel**

- **Rapport de synthèse**
  - **Le plan est validé**
  - **rendu pour le client : archive avec les sources du projet et notice d'installation**

Prévisions

- **Faire d'autres tests avec SQLmap**
- **Trouver une base de données de requêtes légitimes et faire les tests**
- **Améliorer le système de log (cf. Échange avec le client)**
- **Résoudre la faille de la whitelist (cf. Échange avec le client)**

Échanges avec le client

- **Amélioration du système de logs :**
  - **Écrire pourquoi la requête a été bloquée**

- **Whitelist :**
  - **Résoudre le problème de la complétude des signatures (Cf : UNION)**

- **Tests :**
  - **Tests temporels : faire de nombreux tests et faire la moyenne des temps**
  - **Tests performance : charge CPU et RAM sur l'hôte**

- **Mettre les éléments suivants sur le poster :**
  - **Les motivations du projet**
  - **Les politiques de sécurité utilisées (blacklist, barème)**
  - **Les moyens, techniques employés**
  - **Les résultats**
  - **Pour aller plus loin**
  - **Il faut surtout faire comprendre les différentes phases du projet**

Ce CR sera considéré comme validé mardi 30/05/2017 en l'absence de remarques.