Projet CASSIOPEE® :
« Database Firewall »
Compte rendu de réunion n°02

Motif :	Lieu :	Date : 07 mars 2017
Deuxième réunion	D101-01	**Heure de début :** 14h00 **Durée :** 1h30min

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

Ordre du jour

- **Retour sur la semaine**
  - **Planification**
  - **État de l'art parsers**
  - **État de l'art DBF**
  - **État de l'art IDS**
- **Prévisions**

Avancement du projet

- **Présentation du planning**
- **Déroulement des recherches :**
  - **état de l'art parsers : terminé**
  - **état de l'art IDS : en cours**
  - **état de l'art DBF : en cours**

Nous avons présenté l'avancée de ces différents travaux.

Questions prévues pour le client

- **Faut-il poursuivre les recherches générales ? → Se centrer sur MySQL.**
- **Retour sur la structure de notre DBF à la lumière de nos recherches.**

Définition des objectifs pour la semaine suivante :

Il faut arrêter les recherches générales sur les parsers et les IDS et les centrer sur le protocole MySQL. Il est donc nécessaire de commencer la phase de pré-étude du développement pour pouvoir centrer nos recherches sur MySQL.

Remarques :

Parsing de requêtes SQL :

- **Attention à ne pas se fonder sur de la documentation trop ancienne. Il est peut-être possible de trouver de nouvelles failles dans le parsing avec Yacc.**
- **Penser à tester le parser créé en utilisant une liste de tests importante et en analysant les résultats reçus.**

État de l'art DBF :

- **Faire une comparaison entre le DBF et le WAF pour montrer les apports et les limites d'un DBF.**
- **Rechercher les performances de GreenSQL et trouver un moyen de les améliorer.**

Implémentation de l'analyseur :

- **Faut-il filtrer en entrée et en sortie du serveur MySQL ?**
  - **Définir les exploitations possibles.**
  - **Définir le coût de l'*Output traffic validation* en terme de performances temporelles.**
  - **Définir l'apport de *l'Output traffic validation* en terme de sécurité.**
- **Possibilité d'appliquer une blacklist sur les flux sortants**
  - **ex : Interdiction de renvoyer les passwords.**

Liste d'attaques pour réaliser les tests de sécurité : ne pas utiliser la banque de donnée ARPA 1999 qui est devenue obsolète.

Ce CR sera considéré comme validé jeudi 09/03/2017 en l'absence de remarque.