TD Méthodologie d’analyse des systèmes d’information

# Projet Audit sécurité automatisé

**Contexte projet**

Fortify Static Code Analyser (SCA) développé par HP est un logiciel permettant de tester la sécurité des applications par l'analyse statique de leur code (SAST). Les failles de sécurité logicielles sont identifiées, puis hiérarchisées par niveau de risque. De bonnes pratiques sont données pour corriger les lignes de code et remédier ainsi aux vulnérabilités.

Fortify est capable d’analyser les applications développées en interne, avec de nombreux langages dont COBOL et JAVA, ainsi que les applications mobiles pour smartphone.

**Fonctionnement**

Les grandes fonctionnalités de HP Fortify SCA sont les suivantes :

* Compréhension de 22 langages différents ;
* Détection plus de 669 vulnérabilités ;
* Support de nombreux IDE (Eclipse, Intellij, IBM RAD, Visual Studio, …) ;
* Possibilité de lancer jusqu'à 10 revues de code en parallèle ;
* Client web accessible depuis le réseau interne ;
* Client lourd, permettant la modification de code, installé sur le poste du responsable de la sécurité.

Fortify génère des artéfacts lors de la réalisation d’une revue de code qui contient toutes les données de l’analyse. Depuis cet artefact, un rapport d’audit est généré pour être compréhensible par les responsables applicatifs et les développeurs.

**Choix techniques**

Elle est composée de :

* Une base de données (MySQL);
* Deux serveurs virtualisés (Fortify 360 et Fortify SCA) ;
* Un poste, sur lequel est installé le client lourd.

L'application dispose donc d'un compte unique disposant de droit administrateur qui permet de réaliser la revue de code et transmet le rapport d'audit généré aux demandeurs. Le compte administrateur est utilisé par deux personnes.

L’application n’est pas connectée à Internet et est uniquement utilisée sur le réseau interne.

**Objectif du projet**

Il est prévu dans la stratégie de sécurité de l’entreprise qu'une revue de la sécurité des codes développés en interne soit réalisée pour chaque projet applicatif. La solution HP Fortify a été identifiée pour répondre à ce besoin pour les applications de l’entreprise.

Question :

Identifier les données manipulées/créées/utilisées par le projet.

Définir les enjeux de sécurité du projet et justifier en termes de besoins et d’impacts.