LOG6302A — Analyse d'applications et Cyber-sécurité

Laboratoire #4

Donné le : Feb 29 2024, 09 :30 AM
Échéance : Mar 21 2024, 09 :30 AM

- Vous pouvez travailler sur ce laboratoire en équipe de deux.
- Chaque groupe doit rendre sur Moodle une archive contenant leur code et un rapport (PDF) avant la date limite.
- Le rapport doit rendre compte de ce que vous avez fait et les problèmes rencontrés. Vous pouvez discuter de tout autre élément que vous jugeriez pertinent.
- Chaque jour de retard entraîne une pénalité de 50%.
- Si vous avez des questions, vous pouvez demander des clarifications sur Discord (#lab-question)

1 Extraction du DataFlow

Extrayez le dataflow intra-procédural (moodle) des exemples de code fournis :

— pour chaque référence de variable, déterminer la/les définitions qui corresponde

— pour chaque définition, déterminer la/les références qui corresponde

Dans le cadre de ce laboratoire vous devez considérer uniquement les définitions simple de la forme (Variable = Expression $\wedge$ Literal).
Vérifiez votre implémentation en vous assurant que l'ensemble des pairs définitions / références correspond à l'ensemble des pairs références / définitions. Puis extrayez ces ensembles pour les fichiers dans le dossier *part_1*.

2 Utilisation du DataFlow

2.1 Variable vive / morte

Appliquer votre algorithme aux fichiers du dossier *part_2* :

— chercher des références non définies

— chercher des définitions non référencées

2.2 Filtration des données utilisateur

En utilisant les information extraites du dataflow, vérifier que, dans le dossier *part_3*, tout paramètres de la méthode *prepare_query* est filtré en amont par le biais *filter_var*. Dans le cadre de ce laboratoire, on se contentera de vérifier que toutes les définitions possible des paramètres de *prepare_query* sont des appels à *filter_var*.

2.3 Rapport

Détailler dans le rapport les résultats de votre analyse, et justifier les anomalies détectées.