LOG6302A — Analyse d'applications et Cyber-sécurité

Laboratoire #3

Donné le : Feb 15 2024, 09 :30 AM
Échéance : Mar 07 2024, 09 :30 AM

- Un notebook ou une archive contenant le code et un rapport (PDF) doit être rendu sur Moodle 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 Implémentation de PTFA

En utilisant les algorithmes vu en cours (pdf), implémenter la ou les versions d'analyses de flux par traversement de patron ("Pattern Traversal Flow Analysis" ou PTFA) permettant de résoudre les problèmes ci-dessous.
Validez les performance de votre implémentation sur les graphes de différentes tailles fournis, en excluant les temps de lectures et impressions (complexité $\mathcal{O}(|V| + |E|)$). Les patterns à considérer sont tout les nœud ayant pour type "Pattern".

- dossier perf/ -

2 Utilisation sur un CFG

fopen - fclose : A l'aide des algorithmes que vous avez implémenté ci-dessus, vérifier que tout appel a *fopen* sont toujours suivi d'un appel a *fclose* au sein d'une même procédure.
Si un chemin ne respecte pas cette suite d'appels, détailler le dans le rapport et justifier.

- dossier part_1/ -

Protections De la même manière, assurez vous que tout appel de base de données est protégés par une vérification de privilège (*if (has_cap('use_db'))*) en amont ou sein d'une même procédure.
Si un chemin n'est pas protégé, détailler le dans le rapport et justifier.

- dossier part_2/ -

3 Réparation automatique

Protections Lorsque vous détectez un appel de base de données non protégé, ajouter automatiquement une vérification de privilège à la ligne d'avant dans le code source. Un fichier PHP doit être créé contenant le nouveau code source.

- dossier part_2/ -

4 Justifier

Discuter des limitations de l'analyse implémentée. Et proposer des pistes pour résoudre les problèmes restants ou pour améliorer l'analyse