Rapport de réunion 6

Ivan Baheux

14h30 : 24/octobre/2022

1 Presence

- Oum-El-Kheir Aktouf
- Baheux Ivan

2 Résumé

Les sujets de cette semaine étaient :

- Point global sur le travail de la semaine
- Point sur le rapport écrit (pre-study/SotA)
- Point sur les DSL pour la sécurité
- Point sur la contribution

3 Point global sur le travail de la semaine

Le travail de la semaine s'est orienté sur trois axes :

- Travailler sur les DSL liés à la sécurité
- Finir le SotA
- Construire la démonstration de vulnérabilité sur laquelle on construira l'outil
- Avancer un modèle pour la contribution à venir

4 Point sur le rapport écrit (pre-study/SotA)

L'état de l'art est fini, par rapport à la dernière fois, à été rajouté :

- La fin de la partie introduction
- La partie sur l'adversaire
- La partie sur les MBST et les DSL pour la sécurité
- Quelques corréctions

5 Point sur les DSL pour la sécurité

Les recherches sur les DSL pour la sécurité dans la littérature ont montré que les DSL n'étaient qu'un outil plus qu'une réelle méthode.

Le DSL est utilise soit pour générér un modèle sur lequel faire du test de comportement (donc un modèle haut-niveau) soit en tant qu'outil de "script" pour écrire des patterns/tests d'intrusion. Les examples apportés sont : lopez et al. [1] et wolschke et al.[2].

6 Point sur la contribution

Une proposition d'architecture à été faire, l'idée résumée de celle-ci était de faire communiquer trois acteurs :

- Un script(DSL) de test de penetration
- La machine à état, résultat du DSL d'Abdallah, enrichie avec les fonctions presentes dans chaque état.
- Un outil (comme FlowDroid) d'analyse des flots de données

Le but était de faire une passe d'analyse rapide du DSL d'abdallah afin de détécter des pattern puis d'utiliser l'analyse de flots de données pour générer les tests.

Cette architecture est trop complexe, ainsi une solution plus simple et plus efficace à été proposée et sera suivie ces prochains jours.

La solution est comme suit :

- Générer le modèle via le DSL d'abdallah
- Enrichir le DSL via le flot de données (ex : blocD(Sink x)-¿blocA(Source y)).
- Détecter les pattern du DSL/script et générer les tests en fonction.

7 Point sur la suite

La prochaine réunion étant dans deux jours, il faudra travailler sur la solution proposée.

Le but est de faire un petit programme de test sur lequel batir la contribution. Au vu du DSL d'Abdallah, ce n'est pas grave si le test n'est pas attaqué depuis une autre fonction (via un intent) pour l'instant un script (test) que devra éxecuter un utilisateur (pentesteur) est suffisant.

References

[1] M. López, H. Ferreiro, L. Castro, and T. Arts, "A DSL for Web Services Automatic Test Data Generation," Aug. 2013.

[2] C. Wolschke, S. Marksteiner, T. Braun, and M. Wolf, "An Agnostic Domain Specific Language for Implementing Attacks in an Automotive Use Case," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ser. ARES 21. New York, NY, USA: Association for Computing Machinery, Aug. 2021, pp. 1–9. [Online]. Available: https://doi.org/10.1145/3465481.3470070