LOG6302A — Analyse d'applications et Cyber-sécurité

Laboratoire #1

Donné le : Jan 18 2024, 09 :30 AM
Échéance : Feb 01 2024, 09 :30 AM

- Il s'agit d'un travail 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)

Objectifs

— Comprendre et utiliser un AST

— Rechercher des patterns dans la structure de code source

— Détecter de possible vulnérabilités connues

Lecture d'un AST

Ouvrez l'archive et analysez le code d'exemple (README.pdf / README.py) pour comprendre le fonctionnement d'un visiteur d'AST. Puis vérifier que le code fonctionne chez vous avec les exemples.

Détection de patterns

Vous trouverez dans l'archive des sources du framework wordpress, ainsi que les AST correspondant :

— wordpress_source contient les sources PHP

— wordpress_ast contient les AST correspondant, avec un index nommé *filelist* à la racine.

Le but de cette partie est de créer un visiteur capable de sélectionner tout les lignes de code faisant appel à une base de données dans le code de Wordpress 4.8.1. En PHP il existe plusieurs façons de faire de tel appels, voici la liste à considérer :

```
1 mysql_query( * );
2 mysqli_query( * );
3 $object->execute();
4 $object->mysql->exec( * );
```

Si vous trouvez d'autre manières de faire des requêtes SQL, vous pouvez les ajouter.

Detection de vulnerabilités connues

Vous trouverez dans le dossier "test_cve" des fichiers PHP implémentant chacun une vulnérabilité connue. De la même manière que précédemment, vous devez implémenter des visiteurs permettant de les détecter sur les fichiers de test (dossier "test_cve"), puis essayer de trouver ces vulnérabilités dans le code de Wordpress 4.8.1.

Groupe	**CVEs**
1	2017-7189, 2021-21705, 2020-7071
2	2017-7189, 2021-21705, 2020-7069
3	2017-7189, 2021-21707, 2019-9025
4	2017-7189, 2021-21707, 2019-11039