LOG8371 : Ingénierie de la qualité en logiciel
Hiver 2023

TP3 :
Sécurité

Remarques & Instructions

Les travaux pratiques constituent une partie importante du cours LOG8371. Leur objectif est de vous inciter à :

- concevoir des plans d'assurance de qualité des logiciels,
- élaborer des stratégies de test,
- utiliser différents outils pour évaluer la qualité des logiciels selon des critères bien déterminés.

Il vous est recommandé de prendre ces travaux au sérieux et de faire appel à votre créativité et à votre pensée critique pour mieux les réussir. La collaboration avec vos collègues est permise durant et en dehors des séances de laboratoire. Cependant, les règlements relatifs au plagiat restent applicables en tout temps.

Ce TP s'intéresse aux sujets de la planification d'assurance qualité des logiciels par rapport à la **sécurité.** Pour répondre aux questions, vous pouvez utiliser n'importe quel outil parmi ceux présentés ou mentionnés dans le labo. On recommande les outils **SonarCloud**(https://www.sonarsource.com/products/sonarcloud/) pour l'analyse statique et **OWASP ZAP**(https://owasp.org/www-project-zap/) pour les tests de pénétration. En tout cas, vous devez explicitement mentionner les outils que vous avez utilisés.

Le livrable final doit être sous la forme d'un rapport professionnel sur la qualité fonctionnelle du système et non pas comme un compte rendu de TP.

Chaque équipe doit soumettre un seul rapport dans lequel il faut mentionner le nom de l'équipe, les noms et matricules de ces membres et toutes les références externes (articles, liens, documentation, outils, ...)

Date de remise des comptes rendus : 19 avril 2023 - 23h59

Objectifs du TP :

Ce TP a comme objectifs la maitrise de :

- La compréhension et la définition des objectifs de la sécurité logicielle.
- L'identification des vulnérabilités par l'analyse statique du code source.
- La performance du testing de pénétration pour assurer la qualité du logiciel.

Préparation :

- Choisissez deux systèmes de la liste « offline » des **applications vulnérables** (sauf DVWA et PyGoat). https://owasp.org/www-project-vulnerable-web-applications-directory/

Question 1 : Analyse statique (45 points)

1) Performez une **analyse statique** du code source des systèmes choisis en utilisant les outils de SonarCloud.
2) 2. Préparez un rapport des résultats de l'analyse en incluant :
   a) le sommaire des résultats par SonarCloud,
   b) des commentaires pour **10 vulnérabilités** (au moins de trois types différents) ou des hotspots de sécurités bloqueurs/critiques/majeurs.
3) Chaque commentaire doit inclure
   a) le nom du fichier où la vulnérabilité se trouve,
   b) la criticité,
   c) le type de vulnérabilité selon l'OWASP, ou le CWE,
   d) une petite description du risque de cette vulnérabilité (vous pouvez utiliser un exemple d'une attaque), et
   e) une recommandation pour la résolution du problème.

SonarQube : https://www.sonarqube.org/downloads/
SonarCloud : https://sonarcloud.io/about/sq

Question 2 : Tests de pénétration (30 points)

1) Déployer vos deux applications localement ou en utilisant Docker.
2) Testez les applications déployées avec l'outil **ZAP**.
3) Concentrez-vous aux vulnérabilités de **l'OWASP Top 10**. Rapportez sur les résultats.
   a) OWASP Top 10 2021 (https://owasp.org/Top10/)

b) OWASP Top 10 2017 (https://owasp.org/www-project-top-ten/2017/Top_10)

c) OWASP Top 10 2013 (https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2013.pdf)

4) ZAP produit aussi des rapports que vous pouvez utiliser pour les statistiques et les visualisations.

a) Vous pouvez utiliser cet add-on aussi https://www.zaproxy.org/docs/desktop/addons/report-generation/

OWASP ZAP : *https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project*

Question 3 : Vérification (25 points)

1) Comparez les résultats de **SonarCloud** avec ceux de **ZAP**.
2) Utilisez le catalogue de CWE pour confirmer vos résultats.
   a) ZAP et SonarCloud n'utilisent pas le même classement. CWE peut être utiliser pour trouver la correspondance entre les deux.
   b) La comparaison doit être faite selon le classement **OWASP Top 10**.
3) Commentez sur les différences entre les deux outils (pourquoi quelques vulnérabilités sont trouvées seulement par un des outils ?)

CWE : https://cwe.mitre.org/

Rapport final

1. Une section par application.

1.1. Une petite introduction (1-2 paragraphes) de l'application (fonctionnalités, langage de développement, déploiement, etc.)

1.2. Résultats d'analyse statique.

1.2.1. Un tableau sommaire avec les vulnérabilités (ou les hotspots) identifiées (voir question 1).

1.2.2. Une description par vulnérabilité

1.2.3. Une recommandation pour corriger chaque instance de vulnérabilité.

1.3. Résultats des tests d'intrusion.

1.3.1. Vous pouvez joindre le rapport générer par ZAP.

1.3.2. Écrivez un petit rapport.

- Quelles sont les vulnérabilités les plus populaires selon ZAP ?

- Quelles sont les vulnérabilités les plus critiques selon ZAP ?

1.4. Comparez les résultats entre SonarCloud et ZAP.

- Quelles vulnérabilités sont identifiées par les deux ? (Les noms pourraient être différents entre les deux, mais vous pouvez utiliser la liste CWE comme le point commun.)
- Est-ce que le niveau de criticité est le même pour les vulnérabilités communes entre les deux utiles ?
- Selon vous, pourquoi les deux outils rapportent des vulnérabilités différentes ?

Remarques de soumission et d'évaluation

Nommez votre rapport « TP3_[nom_équipe].pdf ». L'évaluation du document portera sur l'exactitude et l'exhaustivité des réponses et la qualité de l'écriture. Traitez-le comme un rapport officiel et professionnel. **La note individuelle de chaque membre peut être pondérée selon les évaluations par des pairs qui seront soumises en même temps que le rapport final. Des instructions seront précisées dans un autre énoncé.** Vous pouvez utiliser une annexe à la fin de rapport où vous pouvez nous informer de vos défis pendant le TP et vos actions pour mitiger les problèmes. Le rapport doit rester comme un document officiel, alors l'annexe joue le rôle pour informer les enseignants de vos défis.