LOG8371: Ingénierie de la qualité en logiciel
Hiver 2022

TP3 : Sécurité

Remarque :

Les travaux pratiques constituent une partie importante du cours et ont pour objectif de vous pousser à concevoir des plans d'assurance de qualité des logiciels, à élaborer des stratégies de test et à vous servir des différents outils disponibles pour évaluer la qualité des logiciels selon des critères donnés. 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 les séances de laboratoire, cependant les règlements relatifs au plagiat restent tout de même applicables en tout temps.

Ce travail pratique se concentre sur les sujets de la planification d'assurance qualité 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 pour l'analyse statique et OWASP ZAP pour les tests de pénetration. En tout cas, vous devez explicitement mentionner les outils que vous avez utilisés.

Le livrable final sera un rapport professionnel sur la sécurité du système. *Ne pas répondre directement aux questions suivantes en tant qu'un TP*. Supposez que vous soumettez le rapport au cadre d'un projet et qu'il sera lu par des développeurs, des architectes ou des gestionnaires du projet. Vous devez soumettre un seul document par équipe, incluez le nom de votre équipe, les noms et matricules des membres de l'équipe, et toutes les références externes telles que des articles, des liens, de la documentation et des outils.

Date de remise : 24 avril, 23h59

Objectifs du TP :

Les objectifs de ce deuxième TP sont de maitriser:

- 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

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

Question 1 : Analyse statique (45 points)

1. Performez une analyse statique du code source de OneDev en utilisant les outils de SonarCloud.

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 SANS, ou le CWE,
    d. une petite description pour le risque (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 pénetration (30 points)

1. Utiliser le déploiement existent de vos deux applications ou déployez les systèmes vous-mêmes.
2. Testez l'application déployée 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/export-report/

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.
    a. Une petite introduction (1-2 paragraphes) par rapport à l'application (fonctionnalités, langage de développement, déploiement, etc.)
    b. Résultats d'analyse statique.

i. Un tableau sommaire avec les vulnérabilités (ou les hotspots) identifiées avec l'informations requises à la question 1.
ii. Une description par vulnérabilité
iii. Une recommandation pour corriger chaque instance de vulnérabilité.
iv. REMARQUE : La description est fournie pour la vulnérabilité en général (alors au moins 3) et la recommandation pour chaque instance de vulnérabilité (alors 10 au total).

c. Résultats des tests d'intrusion.
    i. Vous pouvez joindre le rapport générer par ZAP.
    ii. Écrivez un petit rapport.
        1. Quelles sont les vulnérabilités les plus populaires selon ZAP?
        2. Quelles sont les vulnérabilités les plus critiques selon ZAP?

d. Comparez les résultats entre SonarCloud et ZAP.
    i. Quelles vulnérabilités sont identifiées par les deux? (pas nécessaire de se concentrer sur les 10 que vous avez rapporté pour SonarCloud).
        1. Les noms pourraient être différents entre les deux, mais vous pouvez utiliser la liste CWE comme le point commun.
    ii. Est-ce que le niveau de criticité est le même pour les vulnérabilités communes entre les deux utiles?
    iii. Selon vous, pourquoi les deux outils rapportent des vulnérabilités différentes?

Remarques de soumission et d'évaluation

- Nommez votre rapport comme « TP3_[nom_équipe].pdf ».
- Le document sera évalué pour 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.