LOG8371: Ingénierie de la qualité en logiciel

Hiver 2019

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 permis durant et en dehors les séances de laboratoire, cependant les règlements relatifs au plagiat restent tout de même applicable en tout temps.

I) 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.

II) Énoncé :

Q1) Performez une analyse statique du code source de WEKA REST en utilisant les outils de SonarQube. Préparez un rapport des résultats de l'analyse en incluant : a) le sommaire des résultats par SonarQube, b) des commentaires pour 10 vulnérabilités (au moins de trois types différents) ou des hotspots de sécurités bloqueurs/critiques/majeurs. Chaque commentaire doit inclure le fichier de la vulnérabilité, la criticité, le type de vulnérabilité selon l'OWASP, ou le SANS, ou le CWE, une petite description pour le risque (vous pouvez utiliser un exemple d'une attaque), et une recommandation pour la résolution du problème. (45 points)

SonarQube : https://www.sonarqube.org/downloads/

SonarCloud : https://sonarcloud.io/about/sq

Q2) Déployez une version REST de Weka en utilisant des containeurs Docker. Testez l'application déployée avec l'outil ZAP. Concentrez-vous aux vulnérabilités de l'OWASP Top 10. Rapportez sur les résultats. (45 points)

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

Q3) Comparez les résultats de SonarScanner avec ceux de ZAP. Utilisez le catalogue de CWE pour confirmer vos résultats. Commentez sur les différences entre les deux outils (pourquoi quelques vulnérabilités sont trouvées seulement par un des outils?) (10 points)

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

Remise :

Le travail doit être fait par équipe de 3-5 personnes et doit être remis via Moodle au plus tard le :

- 19 Avril avant 23h59 pour les trois groupes.

Veuillez envoyer un fichier de type *.pdf avec vos rapports. Le fichier portera le nom :

log8371_TP3_NomÉquipe.pdf

Les travaux en retard seront pénalisés de 10 % par jour de retard. (Aucun travail ne sera accepté après 4 jours de retard. Si votre dépôt ne respecte pas la nomenclature définie ci-dessus, 0.5 point de pénalité sera appliqué). Tous les livrables doivent être de haute qualité et être traité en façon professionnelle.

Bonne chance.