Etude sur les contrôles de la Sécurité Applicative

Contexte

Ces dernières années ont vu un véritable accroissement des attaques sur les applications avec des impacts importants. Les dernières études montrent que :

- 84% des attaques ciblent la couche applicative.
- 75% des vulnérabilités se retrouvent dans la couche applicative.
- 70% des applications ont au moins une vulnérabilité dans le top 10 OWASP.
- 15% des applications web ont une vulnérabilité critique ou élevée.

La sécurité constitue un enjeu majeur pour les clients de CGI, la majorité des projets sur le site de Rennes contiennent des clauses portant sur la sécurité. Des formations destinées aux collaborateurs, des locaux à accès restreint pour certains projets et des contrôles sécuritaires représentent des procédures que CGI veuille à appliquer dans le cadre de l'évolution du domaine des services du numérique et ses défis notamment ceux centrés sur la sécurité.

Ces efforts constituent une très bonne base, mais nécessitent aujourd'hui une complémentarité dans le domaine de la sécurité applicative. C'est dans ce contexte que CGI lance un projet d'étude sur la construction et l'amélioration des contrôles de la sécurité applicative.

Travail demandé

L'objectif de cette étude se présente sous forme de quatre missions principales :

- Faire une analyse des vulnérabilités des projets applicatifs de CGI sur plusieurs axes : code source, protocoles utilisés, respect des bonnes pratiques du développement, contrôles d'accès et de sessions, sécurité des données et vulnérabilité aux attaques qui pourra être étudiée via des tests d'intrusion.
- Proposer une procédure bien détaillée (démarches d'intégration, corrections et recommandations) et s'appuyant sur une ou plusieurs solutions logicielles résolvant (ou minimisant) les problèmes trouvés dans la phase d'analyse.
- Mise en œuvre de la solution proposée sous forme d'un POC (Proof of Concept) sur un projet ciblé puis faire les améliorations nécessaires.
- Diffusion de la solution sur tous les autres projets CGI puis la formation d'une équipe sur la prise en main de la solution proposée pour le maintien du bon fonctionnement.

Bibliographie

- Hongzhe Li, Jaesang Oh, Heejo Lee: Detecting Violations of Security Requirements for Vulnerability Discovery in Source Code. IEICE Transactions 99-D(9): 2385-2389 (2016)
- Antonio Nappa, Richard Johnson, Leyla Bilge, Juan Caballero, Tudor Dumitras: The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching IEEE Symposium on Security and Privacy 2015: 692-708
- Gavin Watson Andrew Mason Richard Ackroyd : Executing Social Engineering Pen Tests, Assessments and Defense. Social Engineering Penetration Testing, Syngress (ISBN: 9780124201248). April 2014.

Contact : Salah Sadou (Salah.Sadou@irisa.fr)