



Séminaire du Laboratoire de Physique Corpusculaire Réseau AuDACES

Sécurité Logicielle Web

Thomas LALLART (INRA - Avignon)
Vincent MAZENOD (CNRS - Clermont)

Jeudi 12 Mars 2015, 14h00, Salle 9109

A destination des développeurs-testeurs, des ASR, des chefs de projets et des utilisateurs d'applications Web, l'objectif de ce séminaire est d'échanger sur les notions de sécurité logicielle dans le monde du Web. Dans un contexte où les applications sont majoritairement ouvertes sur Internet, doivent être accessibles depuis différents terminaux et réalisées de plus en plus rapidement, les développeurs - ou plus généralement les parties prenantes d'un développement logiciel - manquent souvent de temps, d'informations ou de formations pour répondre aux enjeux actuels relatifs à la sécurité.

Sous la forme de démonstrations et d'exemples concrets, nous verrons les principales vulnérabilités, les moyens de les détecter et les types d'attaques possibles sur les applications de type Web. Nous vous proposons de jouer aux apprentis hackers et de découvrir comment exploiter des failles telles que XSS, CSRF, Injections, directory traversal ou le vol de sessions. Nous discuterons ensuite des pratiques permettant de se protéger au mieux de ces menaces et aborderons aussi les aspects juridiques liés à la protection des données.



Enfin, nous verrons comment intégrer ces exigences de sécurité dans les équipes et dans les projets, plus particulièrement avec une approche agile. En s'appuyant sur des ressources de référence, tels que les guides de l'OWASP, nous présenterons une approche pragmatique et itérative de mise en oeuvre de tests d'intrusion dans les projets dans le but d'augmenter leur niveau de sécurité.