Formation **Sécurité applicative : attaque, défense et anticipation des failles logicielles**

Les failles de programmation sont au cœur de la sécurité informatique. Cette formation Sécurité applicative vise l'acquisition de compétences et connaissances clés en sécurité offensive, défensive, et dans l'anticipation des vulnérabilités au sein des applications. Les apprenants comprendront les fondamentaux théoriques et pratiques des principales failles logicielles d'aujourd'hui, seront en mesure de les identifier et de mettre en œuvre les meilleures pratiques pour éviter leur apparition lors de leurs développements. A l'issue de la formation Sécurité applicative, ils ont compris le contexte et la réalité de la sécurité logicielle. Les journées de formation s'organisent autour de cours théoriques le matin et de séquences plus pratiques l'après-midi, afin de permettre une mise en application des acquis de la formation dès le retour en entreprise des stagiaires !

Durée
4 jours

Objectifs pédagogiques

- Comprendre les principes fondamentaux de la sécurité applicative
- Identifier les principales vulnérabilités des applications
- S'approprier les méthodes, techniques et outils de protection
- S'entraîner à protéger ses applications contre les failles logicielles
- Connaître les processus d'audit de code

Public
Développeurs, chefs de projet

Prérequis
Bonnes connaissances en développement logiciel

Programme de formation

Introduction à la formation Sécurité applicative
Présentation générale de la formation Sécurité applicative
Vue d'ensemble des failles logicielles dans la sécurité informatique : enjeux, principes et concepts fondamentaux

Les différentes classes de vulnérabilités : failles de code, de conception, de déploiement, d'administration...
Pourquoi une faille apparaît-elle ? Cycle de vie d'une application et de ses failles
Les grands principes de sécurisation à connaître

Mise en application sur les principales failles logicielles

Cross-site scripting, ou XSS
Failles d'injection (SQL, commandes...)
Dépassement de tampon : buffer overflow, ou BOF

Security et Privacy by design : la sécurité dès la conception

Les concepts de Security by design : risques et menaces, surface d'attaque, gestion des privilèges...
La défense en profondeur
Privacy by design : la protection de la vie privée dès la conception

Mise en application sur des failles logicielles de plus haut niveau

Problématiques d'authentification et de droits
Redirections ouvertes
Failles de conception et de design

Sécurité et gestion de projet

Surveillance des dépendances
Attaques tierces parties
DevSecOps
Logs et traces applicatives

Mise en application

Les processus d'audit de code
Découverte de failles existantes

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques.
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d’évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l’auto-positionnement, permettant ainsi une analyse détaillée de leur progression.