DOCAPOSTE Institute

Formation Sécurité des applications

Présentation

Cette formation de trois jours (21 h) donne aux développeurs et chefs de projet les bases indispensables pour concevoir des applications Web et mobiles robustes. Elle explore d'abord les enjeux et attaques emblématiques, puis fait appliquer les bonnes pratiques OWASP au travers d'un refactoring guidé, avant de conclure par l'utilisation d'outils SAST/DAST et d'une « IA légère » pour détecter et corriger les failles.
Les participants repartent avec des check-lists, des scripts d'audit et un pipeline de tests sécurité facilement réutilisables.

Durée : 21,00 heures (3 jours)
Tarif INTRA : Nous consulter

Objectifs de la formation

A l'issue de la formation, le stagiaire sera capable de développer des applications web et mobiles sécurisées

- Comprendre les problématiques de la sécurité des applications
- Identifier les principales menaces et vulnérabilités affectant les applications web et mobiles
- Appliquer les bonnes pratiques de sécurité dans le développement d'applications
- Utiliser des outils et techniques pour détecter et corriger les failles de sécurité
- Découvrir les principes de base de la cybersécurité et leur impact sur la sécurité des applications

Prérequis

Posséder une bonne connaissance de la programmation objet et de la programmation d'application Web

Public

Architectes, développeurs, analystes, chefs de projets

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

DOCAPOSTE Institute

Programme de la formation

Jour 1 – Comprendre les problématiques de sécurité des applications
Objectifs :

- Expliquer les enjeux et spécificités de la sécurité pour le web et le mobile
- Situer l'impact des failles sur la confidentialité, l'intégrité et la disponibilité des données

Introduction aux enjeux de sécurité

- Panorama des risques dans les applications web et mobiles
- Différences et complémentarités entre sécurité applicative et cybersécurité
- Étude de cas : incidents réels et conséquences (fuite de données, interruption de service)

Atelier révélateur de menaces

- Analyse guidée d'un scénario d'attaque (ex. injection, vol de session)
- Identification des vecteurs de menace et discussion des impacts

Jour 2 – Identifier vulnérabilités et appliquer les bonnes pratiques
Objectifs :

- Cartographier les principales vulnérabilités OWASP et mobiles
- Mettre en œuvre les standards et recommandations de développement sécurisé

Menaces et vulnérabilités

- Top 10 OWASP pour le web (Injection, XSS, CSRF…) et vulnérabilités mobiles (stockage, permissions)
- Cycle de vie d'une vulnérabilité : de la découverte au correctif

Bonnes pratiques de développement

- Défense en profondeur : principes W^X, least privilege, secure defaults
- Sécurisation des entrées/sorties, gestion des erreurs et logs
- Authentification, autorisation et gestion des sessions/token (JWT, OAuth)

Atelier implémentation

- Refactoring d'une application de démonstration pour y intégrer les contrôles de sécurité

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

- Mise en place de tests de non-régression sécurité (scénarios OWASP)

Jour 3 – Outils de détection, IA et principes de cybersécurité
Objectifs :
- Utiliser des outils, y compris IA légère, pour scanner et corriger les failles
- Comprendre les bases de la cybersécurité et leur application au développement

Outils et techniques de détection
- Présentation des scanners statiques (SAST) et dynamiques (DAST)
- Utilisation d'outils open source et commerciaux (ex. OWASP ZAP, MobSF)
- Introduction à l'IA légère pour la sécurité : LLM et modèles ML pour l'analyse de code et détection de vulnérabilités
- Intégration de l'analyse dans le CI/CD

Correction et remédiation
- Processus de gestion des vulnérabilités (tri, patch, validation)
- Automatisation des tests de sécurité dans le pipeline de déploiement

Principes de cybersécurité
- IA & RGPD : risques et bonnes pratiques
- Concepts clés : Confidentialité, Intégrité, Disponibilité (CIA)
- Gouvernance, veille et mise à jour des dépendances

Atelier IA/sécurité
- Utiliser un outil IA (ex. prototype LLM ou scanner ML) pour analyser un extrait de code et identifier des vulnérabilités
- Comparaison manuelle vs IA et discussion des apports

Organisation

Formateur
Les formateurs de Docaposte Institute sont des experts de leur domaine, disposant d'une expérience terrain qu'ils enrichissent continuellement. Leurs connaissances techniques et pédagogiques sont rigoureusement validées en amont par nos référents internes. Riches de leur expérience sur le sujet, ils sauront accompagner vos collaborateurs dans leur montée en compétences.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Moyens pédagogiques et techniques

- Apports des connaissances communes.
- Mises en situation sur le thème de la formation et des cas concrets.
- Méthodologie d'apprentissage attractive, interactive et participative.
- Équilibre théorie / pratique : 60 % / 40 %.
- Supports de cours fournis au format papier et/ou numérique.
- Ressources documentaires en ligne et références mises à disposition par le formateur.
- Pour les formations en présentiel dans les locaux mis à disposition, les apprenants sont accueillis dans une salle de cours équipée d'un réseau Wi-Fi, d'un tableau blanc ou paperboard. Un ordinateur avec les logiciels appropriés est mis à disposition (le cas échéant).

Dispositif de suivi de l'exécution et de l'évaluation des résultats de la formation

En amont de la formation :

- Recueil des besoins des apprenants afin de disposer des informations essentielles au bon déroulement de la formation (profil, niveau, attentes particulières...).
- Auto-positionnement des apprenants afin de mesurer le niveau de départ.

Tout au long de la formation :

- Évaluation continue des acquis avec des questions orales, des exercices, des QCM, des cas pratiques ou mises en situation...

A la fin de la formation :

- Auto-positionnement des apprenants afin de mesurer l'acquisition des compétences.
- Evaluation par le formateur des compétences acquises par les apprenants.
- Questionnaire de satisfaction à chaud afin de recueillir la satisfaction des apprenants à l'issue de la formation.
- Questionnaire de satisfaction à froid afin d'évaluer les apports ancrés de la formation et leurs mises en application au quotidien.

Accessibilité

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France

Nos formations peuvent être adaptées à certaines conditions de handicap. Nous contacter pour toute information et demande spécifique.

Docaposte Institute
ACI 3A3-303 - 45-47 Boulevard Paul Vaillant Couturier, 94200 IVRY SUR SEINE
Tél : Variable non renseignée - Email : hello.institute@docaposte.fr
SIRET : 813 058 542 00032 - Code APE : 8559A - N TVA Intra : FR 58 813 058 542
Déclaration d'activité enregistrée sous le numéro 11941117994 auprès du préfet de région d'Ile-de-France