Formation Sécurité Web | Sécuriser ses développements d'applications

La formation Sécurité Web sensibilise à la sécurisation des développements d'applications.

Fiche en date du 29/01/2023.(Voir sur le site)

Informations pratiques

Voir nos formateurs

3 rue de Tolbiac, 75013
Voir le plan

2 jours

1 540 €

Prochaines sessions :

Contactez-nous à training@soat.fr

Nombre de participants maximum : 10

Objectifs

- Sensibilisation à la sécurité informatique
- Comprendre les menaces et les risques
- Aborder les notions sur les éléments de sécurité

Public

- Architectes, lead développeurs, développeurs tous niveaux

Prérequis

- Pratiques du développement C# ou Java
- Bonnes connaissances du Web (HTTP, HTML, JavaScript)

Méthodes pédagogiques

100% théorie

Description

Face à l'augmentation du risque numérique, les entreprises doivent intégrer la sécurité dans leur cycle de développement et de livraison. Il n'est plus possible de se passer de la sécurité au sein de nos applications. Pendant trop longtemps, les projets ont intégré la sécurité trop tardivement. Cela doit désormais être adressé dès le début d'un projet. Les développeurs doivent ainsi être sensibilisés à la sécurité au sein de leurs développements et comprendre les risques encourus pour les entreprises. La formation Sécurité Web vous donnera les fondamentaux de la sécurisation des développements d'applications.

Programme

Introduction

- Ce qui chance dans la réglementation : RGPD
- Security by design
- Privacy by design

Les fondamentaux de la sécurité informatique

- Analyse des risques et sensibilisation de vos utilisateurs
- Authentification (LDAP, Active Directory, SSO, OAuth)
- Composants réseaux (Firewall, proxy, tunneling)
- Théorie de la cryptographie (identification, signature, chiffrement, certificats)
- Protocoles (HTTPS, SSH, IPsec)

Principales failles de sécurité présentes dans les applications et contre-mesures

- OWASP : Vulnérabilités les plus importantes
- Injection (SQL, Commande, LDAP)
- Authentification de mauvaise qualité
- Exposition de données sensibles
- Violation de contrôle d'accès
- Mauvaise configuration sécurité
- Cross-Site-Scripting (XSS)
- Désérialisation non sécurisée
- Utilisation de composants présentant des vulnérabilités connues
- Journalisation et surveillance insuffisantes
- Mise en pratique avec une DVWA
- Les spécificités des Web services, des API REST et du Web 2.0
- Cas pratiques et Post Mortems

Bonnes pratiques de développement

- Architecture des applications (n-tiers, rupture de protocole, proxy)
- Gestion des mots de passe et tokens
- Filtrage des entrées utilisateurs
- Gestion des cookies et de la session
- Spécificité des WS (WSSE)
- Des outils pour vos développements
- Transformations de votre organisation (audit, Pentest de vos applications, sensibilisation de vos utilisateurs…)
- Mise en pratique avec une DVWA
- Les spécificités des Web services, des API REST et du Web 2.0
- Cas pratiques et Post Mortems

Évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de quizz, mises en situation, travaux pratiques… En fin de formation, il est également demandé aux participants de mesurer leur satisfaction vis-à-vis de de la formation suivie. SOAT Training dispose d'un processus qualité qui prend en considération les éventuels dysfonctionnements rencontrés par les participants afin d'être proactif quant à la solution corrective adaptée tant sur le contenu de la formation elle-même que les conditions de son déroulement.