Best

Sécurité des applications

Mettre en oeuvre les règles et bonnes pratiques liées au développement sécurisé d'applications

★★★★★ **4,1/5 (21 avis)**

Présentiel ou en classe à distance

3 jours (21 h)

Prix inter : 2.250,00 € HT
Forfait intra : 6.990,00 € HT

Réf.: DEV303

Idéal en Distanciel

Les applications web sont de plus en plus exposées aux tentatives de piratages. La sécurisation d'une application et des données qu'elle véhicule fait dorénavant partie intégrante de tout nouveau projet de développement. Tous les acteurs IT ont pris conscience de cette nécessité et intègrent dans leurs solutions des éléments et des outils offrant un niveau de sécurisation à la hauteur des enjeux et attentes du marché. Durant cette formation de 3 jours, les participants aborderont dans le détail chaque brique de sécurisation qu'il est possible de considérer et s'approprieront les techniques à employer pour renforcer la sécurité de leurs prochaines applications.

A qui s'adresse cette formation ?

Pour qui

- Architectes
- Développeurs
- Analystes
- Chefs de projets...

Prérequis

- Disposer d'une bonne connaissance de la programmation objet et de la programmation d'applications Web
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Sécurité dans le Framework et du code

- Concepts fondamentaux
- Sécurité d'accès du code et des ressources
- Sécurité basée sur les rôles
- Le principe du W^X
- Services de chiffrement
- Validation et contrôle des entrées / sorties
- Gestion et masquage d'erreurs
- Gestion sécurisée de la mémoire
- Contrôle d'authenticité et d'intégrité d'une application/d'un code

- Offuscation du code
- Reverse engineering sur : bundle C#, application Java, binaire Windows
- Contrôle des droits avant exécution du code
- Sécuriser les données sensibles présentes dans un binaire
- Stack/Buffer/Heap overflow

2 - Les bases de la cryptographie

- Cryptographie - Les définitions
- Types de chiffrement : chiffrement à clés partagées, chiffrement à clé publique
- Symétrique vs. asymétrique, combinaisons symétrique / asymétrique
- Fonctions de hachage
- Utilisation des sels
- Signatures numériques, processus de signature, processus de vérification

3 - Chiffrement, hash et signature des données

- Cryptographie Service Providers (CSP)
- System, security, cryptographie
- Choix des algorithmes de chiffrement
- Chiffrement symétrique : algorithme (DES, 3DES, RC2, AES), chiffrement de flux, mode de chiffrement (CBC, ECB, CFB)
- Algorithmes asymétriques
- Algorithme : RSA, DSA, GPG
- Algorithme de hachage : MD5, SHA1 / SHA2 / SH3

4 - Vue d'ensemble d'une infrastructure à clé publique (PKI)

- Certificat numérique : certificat X.509
- PKI - Les définitions
- Les fonctions PKI
- PKI - Les composants
- PKI - Le fonctionnement
- Applications de PKI : SSL, VPN, IPSec
- IPSec et SSL en entreprise
- Smart Cards (cartes intelligentes)
- Autorité de certification

5 - SSL et certificat de serveur

- Certificat de serveur SSL : présentation, autorité de certification d'entreprise, autorité de certification autonome

6 - Utilisation de SSL et des certificats clients

- Certificats clients
- Fonctionnement de SSL : phase I, II, III et IV
- Vérification de la couverture d'utilisation d'un certificat (lors du handshake)
- Vérification des dates d'utilisation d'un certificat

7 - Sécurité des services Web

- Objectifs de la sécurisation des services Web : authentification, autorisation, confidentialité et intégrité
- Limitations liées à SSL
- Sécurité des services Web : WSE 2.0, sécurisation des messages SOAP / REST

8 - Jetons de sécurité

- Jetons de sécurité : User-Name Token, Binary Token, XML Token, JWT (JSON Web Tokens), Session-based Token
- Intégrité d'un jeton (MAC / HMAC)
- Cycle de vie d'un jeton, expiration automatique (ou pas), contexte d'utilisation d'un jeton
- Habilitations suivant le contexte du jeton
- Certificats X.509
- Signature des messages SOAP / REST : création d'un jeton de sécurité, vérification des messages (MAC / HMAC), chiffrement des messages, déchiffrement du message

9 - Sécurité et développement Web

- Classification des attaques : STRIDE, OWASP
- Les erreurs classiques
- Authentification par jeton et gestion des habilitations
- Les handlers et méthodes HTTP
- Séparation des handlers par contexte de sécurité
- Attaque par injection
- Injection HTML
- Injection CSS

- Injection JS
- Injection SQL
- XSS (Injection croisée de code) : XSS réfléchi, XSS stocké
- XSS Cookie Stealer
- CSRF : Cross-Site Request Forgery

10 - Organiser la veille

- Top 10 de l'OWASP
- Le système CVE
- Le système CWE

Les objectifs de la formation

- Comprendre les problématiques de sécurité des applications
- Connaitre les principales menaces et vulnérabilité
- Appréhender les méthodologies / technologies de protection et de contrôle de la sécurité des applications
- Mettre en place une stratégie de veille

Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Au-delà des apports théoriques indispensables, cette formation intègre de nombreux ateliers qui apporteront aux participants une expérience pratique de la sécurisation d'applications.
- Des conseils pratiques et méthodologiques sont proposés pour chaque thème évoqué.
- 80% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.

Dates et villes 2026 - Référence DEV303

Dernières places disponibles Session garantie

A distance

du 19 janv. au 21 janv.	du 6 juil. au 8 juil.	du 14 déc. au 16 déc.
du 13 avr. au 15 avr.	du 5 oct. au 7 oct.	

Toulouse

du 19 janv. au 21 janv.	du 13 avr. au 15 avr.	du 5 oct. au 7 oct.

Strasbourg

du 19 janv. au 21 janv.	du 6 juil. au 8 juil.	du 14 déc. au 16 déc.

Sophia Antipolis

du 19 janv. au 21 janv.	du 6 juil. au 8 juil.	du 14 déc. au 16 déc.

Rouen

du 19 janv. au 21 janv.	du 6 juil. au 8 juil.	du 14 déc. au 16 déc.

Bordeaux

du 19 janv. au 21 janv.	du 6 juil. au 8 juil.	du 14 déc. au 16 déc.

Rennes

du 19 janv. au 21 janv.	du 13 avr. au 15 avr.	du 5 oct. au 7 oct.

Paris

du 19 janv. au 21 janv. du 13 avr. au 15 avr.	du 6 juil. au 8 juil. du 5 oct. au 7 oct.	du 14 déc. au 16 déc.

Nantes

du 19 janv. au 21 janv.	du 13 avr. au 15 avr.	du 5 oct. au 7 oct.

Lyon

du 19 janv. au 21 janv.	du 6 juil. au 8 juil.	du 14 déc. au 16 déc.

Marseille

du 13 avr. au 15 avr.	du 5 oct. au 7 oct.	du 14 déc. au 16 déc.

Aix-en-Provence

du 13 avr. au 15 avr.	du 5 oct. au 7 oct.	du 14 déc. au 16 déc.

Lille

du 13 avr. au 15 avr.	du 5 oct. au 7 oct.	du 14 déc. au 16 déc.