

Sécuriser des applications, services et serveurs Web - 4 jours *formation 940*

- Vous apprendrez à**
- Mettre en œuvre et tester des applications Web dans votre entreprise
 - Configurer un serveur Web dans le but de chiffrer le trafic Web avec HTTPS
 - Identifier, diagnostiquer et corriger les 10 principales vulnérabilités définies par l'OWASP
 - Protéger des applications Web 2.0 Ajax
 - Sécuriser des services Web XML avec WS-Security
 - Réaliser un audit de la sécurité des applications Web grâce au scan manuel et automatisé

Objectif Aujourd'hui, la cybersécurité est un véritable défi, les attaques ciblant précisément les vulnérabilités des applications Web. Ces vulnérabilités peuvent être exploitées pour obtenir des informations confidentielles et compromettre l'intégrité de l'entreprise. Par conséquent, les entreprises doivent mettre en place des mesures de sécurité strictes dans le processus de développement d'applications Web. Cette formation vous apporte une expérience pratique approfondie de la sécurisation d'applications et serveurs hôtes Web.

À qui s'adresse cette formation À ceux qui souhaitent mettre en œuvre, tester et déployer des applications Web sécurisées. Des connaissances de base du fonctionnement des applications Web et de l'administration de serveurs Web sont supposées acquises. Des connaissances en développement des applications Web et en sécurité sont utiles mais non requises.

Travaux pratiques Dans ce cours, des exercices approfondis basés sur une étude de cas évolutive vous apportent une expérience pratique de la sécurisation d'applications. Les exercices comprennent :

- Interception et modification d'un message SOAP signé
- Détection de modifications non autorisées du système de fichiers
- Mise en place de HTTPS sur un serveur Web
- Éviter les failles XSS (Cross-site scripting)
- Prévention contre l'injection de code avec la validation des saisies
- Mise en place de restrictions d'accès aux URL
- Protection des services Web avec WS-Security
- Identification des vulnérabilités avec un scanner d'applications

Sécuriser des applications, services et serveurs Web - 4 jours

formation 940

Démarrage

- Définir les menaces contre vos atouts Web
- Recueil de données sur la légalité et le droit à la vie privée
- Explorer les vulnérabilités courantes

Bases de la sécurité

Modélisation de la sécurité Web

- Le triangle CIA (Confidentialité, Intégrité et Disponibilité)
- Authentifications et autorisations

Chiffrement et hachage

- Différentiation cryptographie à clé publique et à clé privée
- Vérification de l'intégrité des messages avec les empreintes, signatures et certificats numériques

Accroissement de la sécurité Web

Configuration de la sécurité pour des services HTTP

- Gestion des mises à jour de logiciels
- Restriction des méthodes HTTP

Sécurisation des communications avec SSL/TLS

- Obtention et installation de certificats de serveurs
- Mise en place de HTTPS sur le serveur Web
- Protection de l'échange des identités

Détection de modifications non autorisées du contenu

- Configuration correcte des permissions
- Scanner pour détecter les changements du système de fichiers

Sécurité des applications Web

Utilisation des ressources de l'OWASP

- Les dix principales vulnérabilités de l'OWASP (Open Web Application Security Project)
- Identification des risques dans la cybersécurité
- Correction des failles identifiées

Sécurisation des interactions entre les bases de données et les applications

- Déceler et empêcher les injections SQL
- Protection des références d'objets directs
- Limites du chiffrement du contenu de bases de données

Gestion de l'authentification de sessions

- Protection contre le détournement de sessions
- Mise en place du contrôle d'accès aux URL
- Blocage de la falsification de requêtes inter-sites

Contrôle des fuites d'informations

- Messages d'erreurs édulcorés sur l'écran de l'utilisateur
- Gestion des erreurs de requêtes et sur les pages

Validation des saisies

- Établissement de limites de confiance
- Déceler et supprimer les menaces de XSS (Cross-site scripting)
- Exposer les dangers de la validation côté client
- Prévention contre le vol électronique

Développement de la sécurité Ajax

Fonctionnalités Ajax

- Identification des éléments principaux d'Ajax
- Échange d'informations de façon asynchrone

Évaluation des risques et des menaces

- Gestion des interactions imprévisibles
- Identification de vulnérabilités JSON

Sécurisation des services Web XML

Diagnostic des vulnérabilités XML

- Repérage des balises non terminées et des dépassements de champs
- Révéler les faiblesses de services Web

Protection de l'échange de messages SOAP

- Validation des saisies avec un schéma XML
- Chiffrement des échanges avec HTTPS
- Mise en œuvre d'un cadre de sécurité des services Web
- Authentification de l'accès aux services Web

Scans d'applications pour identifier les faiblesses

Configuration et utilisation de scanners

- Recherche par motifs pour identifier les erreurs
- Découverte de vulnérabilités nouvelles ou inconnues grâce au "fuzzing"

Détection des défauts dans les applications

- Scans d'applications à distance
- Stratégies de scans et de tests

- Test d'applications Web avec Netcat, Cryptcat et Wget
- Interception du trafic avec WebScarab de l'OWASP

Bonnes pratiques pour la sécurité Web

Adoption des normes

- Réduction des risques en mettant en œuvre des architectures éprouvées
- Gestion des données personnelles et financières
- Recommandations pour la journalisation

Gestion de la sécurité réseau

- Modélisation des menaces pour diminuer les risques
- Intégration d'applications à votre architecture réseau