



SECURITE DES APPLICATIONS, SERVICES ET SERVEURS WEB

- Public** Ce cours s'adresse à toute personne désireuse de protéger ses applications Web d'attaques potentielles. Il concerne plus particulièrement les personnes directement impliquées dans le développement, la maintenance ou l'audit d'applications Web, y compris les développeurs d'applications Web, le personnel chargé de l'Assurance Qualité sur les logiciels, les testeurs et les auditeurs de la sécurité des applications Web, ainsi que les administrateurs de la sécurité.
- Durée** 4 jours - 28 heures
- Pré-requis** Des connaissances de base du fonctionnement des applications web et de l'administration de serveurs web sont supposées acquises.
- Objectifs** Les entreprises s'appuient aujourd'hui de plus en plus sur Internet et les systèmes en réseau. Or, la cybercriminalité et les violations de sécurité laissent planer une menace toujours plus importante sur leurs données et fonctions vitales. Si vos applications Web ne sont pas dotées des parades de sécurité appropriées, des intrus peuvent s'immiscer et compromettre l'intégrité des informations qu'elles envoient et reçoivent. La menace est particulièrement sérieuse pour les entreprises qui partagent des données propriétaires sur Internet, des intranets ou d'autres réseaux publics.
- Méthodes pédagogiques** Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
- Moyens techniques** 1 poste de travail complet par personne
 De nombreux exercices d'application
 Mise en place d'ateliers pratiques
 Remise d'un support de cours
 Passage de certification(s) dans le cadre du CPF
 Remise d'une attestation de stage
- Modalité d'évaluation des acquis** Evaluation des besoins et objectifs en pré et post formation
 Evaluation technique des connaissances en pré et post formation
 Evaluation générale du stage
- Délai d'accès** L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
- Accessibilité handicapés** Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. DÉMARRAGE

- Définir les menaces contre vos atouts web
- Recueil de données sur la légalité et le droit à la vie privée

2. MODÉLISATION DE LA SÉCURITÉ WEB

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

3. CHIFFREMENT ET HACHAGE

- Différentiation cryptographie à clé publique et à clé privée
- Vérification de l'intégrité des messages

4. CONFIGURATION DE LA SÉCURITÉ POUR DES SERVICES HTTP

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

5. SÉCURISATION DES COMMUNICATIONS AVEC SSL/TLS

- Obtention et installation de certificats de serveurs
- Mise en place de HTTPS sur le serveur web

6. DÉTECTION DE MODIFICATIONS NON AUTORISÉES DU CONTENU

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

7. UTILISATION DES RESSOURCES DE L'OWASP

- Les dix principales vulnérabilités de l'OWASP
- Identification des risques dans la cybersécurité

8. GESTION DE L'AUTHENTIFICATION DE SESSIONS

- Protection contre le détournement de sessions
- Blocage de la falsification de requêtes inter-sites

9. CONTRÔLE DES FUITES D'INFORMATIONS

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

10. VALIDATION DES SAISIES

- Établissement de limites de confiance
- Déceler et supprimer les menaces de XSS
- Exposer les dangers de la validation côté client
- Mettre en œuvre une validation des données côté serveur robuste avec les expressions régulières

11. FONCTIONNALITÉS AJAX

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

12. ÉVALUATION DES RISQUES ET DES MENACES

- Gestion des interactions imprévisibles
- Identification de vulnérabilités JSON

13. DIAGNOSTIC DES VULNÉRABILITÉS XML

- Repérage des balises non terminées et des dépassements de champs, révéler les faiblesses de services web

14. 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

15. CONFIGURATION ET UTILISATION DE SCANNERS

- Recherche par motifs pour identifier les erreurs
- Découverte de vulnérabilités inconnues grâce au « fuzzing »

16. DÉTECTION DES DÉFAUTS DANS LES APPLICATIONS

- Scans d'applications à distance
- Trouver les vulnérabilités dans les applications Web grâce aux outils de test d'intrusion de l'OWASP et de tiers

17. ADOPTION DES NORMES

- Réduction des risques en mettant en œuvre des architectures éprouvées
- Gestion des données personnelles et financières

18. GESTION DE LA SÉCURITÉ RÉSEAU

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

NOUS CONTACTER

Siège social

16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone

04 76 23 20 50 - 06 81 73 19 35

Centre de formation

87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

E-mail

contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !



ACF Audit Conseil Formation



@ACF_Formation



ACFauditconseilformation