OWASP

Public	Administrateurs systèmes, développeurs, responsables sécurité, consultants en cybersécurité et toute personne souhaitant comprendre et renforcer la sécurité informatique en entreprise.
Durée	2 jours - 14 heures
Pré-requis	Une connaissance de base des systèmes d'information et des réseaux (concepts de serveurs, clients, protocoles réseau, etc.). Une compréhension élémentaire des concepts de sécurité informatique (confidentialité, intégrité, disponibilité). Une familiarité avec les environnements web (applications web, navigateurs, bases de données).
Objectifs	Comprendre le paysage actuel des menaces et les enjeux de la sécurité dans les entreprises. Identifier les étapes clés d'une attaque (de la reconnaissance à l'exploitation). Reconnaître les vulnérabilités critiques dans les applications web, notamment celles listées dans le Top 10 de l'OWASP. Utiliser les principales ressources de l'OWASP (guides, cheatsheets, outils) pour évaluer et améliorer la sécurité des applications. Appliquer des bonnes pratiques pour protéger les systèmes et les données contre les attaques courantes. Mettre en œuvre des mesures de protection adaptées aux contextes d'entreprise.
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.

JOUR 1 : LES MENACES D'AUJOURD'HUI ET LES FONDAMENTAUX DE LA SÉCURITÉ

1. SUJET 1 : PAYSAGE DE LA SÉCURITÉ ET NORMES

- Évolution des menaces dans un monde numérique.
- Les trois piliers de la sécurité (Confidentialité, Intégrité, Disponibilité).
- Vue d'ensemble des normes et réglementations clés.
- Les enjeux de la conformité pour les entreprises.

2. SUJET 2 : LA SÉCURITÉ DANS LES ENTREPRISES FRANÇAISES

- Les défis spécifiques aux entreprises françaises (cybercriminalité, conformité,
- sensibilisation).
- Études de cas : Exemples d'attaques récentes.
- Les bonnes pratiques adoptées par les entreprises pour se protéger.
- L'importance de la culture de la sécurité au sein des organisations.

3. SUJET 3 : LE CYCLE D'UNE ATTAQUE : DE LA RECONNAISSANCE À L'EXPLOITATION

- Les étapes d'une attaque : Reconnaissance, discovery, exploitation.
- Techniques de reconnaissance active et passive.
- Découverte des réseaux et des ports (scanning, fingerprinting).
- Identification des vulnérabilités et exploitation (exemples concrets).

4. SUJET 4 : LES VULNÉRABILITÉS WEB ET LES RESSOURCES DE L'OWASP

- Présentation des risques liés aux applications web.
- Focus sur le Top 10 de l'OWASP : Injection SQL, XSS, CSRF, etc.
- Exploration des autres ressources de l'OWASP (guides, cheatsheets, projets).
- Introduction à l'OWASP Testing Guide et à l'OWASP Application Security Verification
- Standard (ASVS).

JOUR 2 : TECHNIQUES D'ATTAQUE ET PROTECTION

1. SUJET 1 : LES TECHNIQUES D'ATTAQUE COURANTES

- Injection de commande et injections SQL : Exemples et démonstrations.
- Cross-site scripting (XSS) et cross-site request forgery (CSRF).
- File inclusion et file upload : Exploitation et conséquences.
- Les attaques « Man in the Middle » (MITM) : Principes et protections.

2. SUJET 2 : DÉCOUVERTE ET EXPLOITATION DES VULNÉRABILITÉS

- Techniques de découverte des vulnérabilités (scanning, outils automatisés).
- Exploitation des vulnérabilités sur un serveur web (exemples pratiques).
- Les outils utilisés par les attaquants et les défenseurs.

3. SUJET 3 : PROTECTION ET BONNES PRATIQUES

- Les solutions techniques pour se protéger (pare-feux, chiffrement, etc.).
- Les bonnes pratiques de développement sécurisé (SDL, DevSecOps).
- L'importance des tests de sécurité (pentest, audit).
- Formation continue et veille en cybersécurité.

4. SUJET 4 : ÉTUDES DE CAS ET MISE EN PRATIQUE

- Analyse de cas réels d'attaques et de leurs conséquences.
- Exercices pratiques : Simulation d'une attaque et mise en oeuvre des protections.
- Discussions et retours d'expérience pour renforcer la sécurité.

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

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

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation