HACKING ET SÉCURITÉ DES APPLICATIONS WEB

Public	Développeurs et administrateurs système
Durée	3 jours - 21 heures
Pré-requis	Expérience en programmation, idéalement en développement Web (des bases en HTML, JavaScript et SQL sont nécessaires pour les exercices). Installations nécessaires sur votre machine : des droits d'administration suffisants pour installer les outils nécessaires à la réalisation des travaux pratiques.
Objectifs	Prendre connaissance des bonnes pratiques de développement permettant d'éviter de rendre une application vulnérable. Installer, configurer et utiliser des outils permettant d'analyser efficacement vos applications
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. INTRODUCTION : LE PAYSAGE DE L'INSÉCURITÉ NUMÉRIQUE

- Les technologies Web, les risques
- Mythes et réalités
- Statistiques et évolutions
- Retours d'expériences

2. ATTAQUANTS ET DÉFENSEURS

- Le profil des "pirates", leur arsenal
- La défense (politique de sécurité, législation, réponse des éditeurs...)
- Le Bug Bounty ; avantages et inconvénients

3. ARCHITECTURE D'UNE APPLICATION WEB ET VECTEURS D'ATTAQUE

- Architecture générale : client et serveur HTTP
- Navigateurs Web, serveurs HTTP : fonctionnement, faiblesses

4. LE PROTOCOLE HTTP

- Format des requêtes standards et malicieuses
- Génération de requêtes HTTP
- Découverte passive d'information
- Comprendre les étapes d'une attaque

5. VULNÉRABILITÉS DES APPLICATIONS WEB

- L'exposition des applications Web
- Classement des risques majeurs selon l'OWASP et le CWE (MITRE)
- Analyse des vulnérabilités et des conséquences de leur exploitation
- Les principales attaques : "Cross Site Scripting" (XSS) / Les attaques en injection / Les attaques sur les authentifications et sessions / CSRF...
- Les vulnérabilités des frameworks et CMS

6. OUTILS DE DÉTECTION ET D'EXPLOITATION

- Les scanners de vulnérabilités Web
- L'analyse statique de code
- Les outils d'analyse manuelle
- Exploitation SQL
- Brute-force et fuzzing

7. PRINCIPE DU DÉVELOPPEMENT SÉCURISÉ

- Les écueils
- La sécurité dans le cycle de développement
- Application à AGILE/SCRUM
- Le budget
- Le rôle du code côté client
- Le contrôle des données envoyées par le client
- Les règles de développement à respecter

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