TESTS D'INTRUSION DES SERVEURS ET DES APPLICATIONS WEB

Public	Personnes ayant un profil technique souhaitant acquérir les connaissances suffisantes pour sécuriser leurs développements Web : DevSecOps, Programmeurs, Développeurs, Architectes, Chefs de projet, Consultants cybersécurité
Durée	5 jours - 35 heures
Pré-requis	Expérience en programmation, idéalement en développement Web Connaissance de base en cybersécurité, par exemple suivi de la formation SECUCYBER est un plus
Objectifs	Éduquer vos équipes de développement aux risques et aux enjeux de la sécurité applicative en mettant en application l'ensemble des points clés du standard OWASP Être en mesure d'augmenter rapidement la qualité et la sécurité de leurs développements de façon pertinente et efficace.
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 AUX RISQUES ET AUX ENJEUX DE LA SÉCURITÉ APPLICATIVE

- Quelques idées reçues
- La couche applicative – Une surface d'attaque de choix
- Prise en main de l'environnement de travaux pratiques

2. RAPPELS SUR LES TECHNOLOGIES WEB

- Encodages (URL, HTML, Base64)
- HTTP / HTTPS
- Utilisation d'un proxy Web pour intercepter, analyser et modifier les échanges HTTP(S)

3. INTRODUCTION AUX TECHNIQUES D'ATTAQUE ET AUX MÉCANISMES DE DÉFENSE

- Présentation de l'OWASP (guides, outils et TOP 10 de l'OWASP Web)
- Attaques et mécanismes de défense
- Utilisation du scanner de vulnérabilité OWASP ZAP

4. LA PHASE DE RECONNAISSANCE UTILISÉE AVANT D'ATTAQUER UNE APPLICATION

- Axes de fuite d'informations techniques
- Utilisation d'outils de "Crawling" et d'outils de collecte d'information

5. LE MÉCANISME DE GESTION DE L'AUTHENTIFICATION (ATTAQUE ET DÉFENSE)

- Mécanismes d'authentification les plus rencontrés
- Failles / Attaques qui ciblent le mécanisme d'authentification
- Moyens de défense permettant de sécuriser le mécanisme d'authentification
- "Brute-force" d'un mécanisme d'authentification
- Interception de données en transit (Sniffing)

6. LE MÉCANISME DE GESTION DE LA SESSION (ATTAQUE ET DÉFENSE)

- Rappel autour des sessions
- Failles / Attaques qui ciblent le mécanisme de gestion de la session
- Moyens de défense permettant de sécuriser le mécanisme de gestion de la session
- Exploitation de la faille permettant la fixation de session

7. LE MÉCANISME DE GESTION DES AUTORISATIONS (ATTAQUE ET DÉFENSE)

- Droits horizontaux et droits verticaux
- Failles / Attaques qui ciblent le mécanisme de gestion des autorisations
- Attaques de type Cross-Site Request Forgery (CSRF)
- Attaques de type File Inclusion (RFI / LFI) et Path Traversal
- Moyens de défense permettant de sécuriser le mécanisme de gestion des autorisations
- Exploitation d'une faille de type Path Traversal

8. LA GESTION DES ENTRÉES UTILISATEURS (INJECTION DE CODE)

- Les différents types d'attaques permettant l'injection de code (SQL, HQL, LDAP, commandes, etc.) et le principe général de ce type d'attaque
- Moyens de défense permettant de sécuriser vos entrées utilisateurs
- Exploitation de failles de type Injection SQL manuellement et de façon automatique (via l'utilisation d'un outil)

9. LES ATTAQUES CIBLANT LES AUTRES UTILISATEURS (ATTAQUE DE TYPE CROSS-SITE)

- Attaques de type Cross-Site Scripting (XSS)
- Le cas des clients riches JavaScript (AngularJS, Backbone, Ember, NodeJS, ReactJS, etc.)
- Moyens de défense permettant de sécuriser la navigation de vos utilisateurs et de se protéger contre l'injection de code HTML / JavaScript
- Mise en œuvre de différents scénarios d'attaques reposant sur l'exploitation d'une faille de type Cross-Site Scripting (modification de l'affichage, vol de session, redirection arbitraire, etc.)

10. SÉCURITÉ DE LA JOURNALISATION, DE LA GESTION DES ERREURS ET DES EXCEPTIONS

- Principe et enjeux de la journalisation des évènements de sécurité
- Stockage d'informations sensibles dans les journaux et attaques de type injection de "logs"
- Principe et enjeux de la gestion des erreurs et des exceptions
- Axes de prévention et bonnes pratiques dans le domaine

11. SÉCURITÉ DES SERVICES WEB (FRONT END JAVASCRIPT, API SOAP & REST)

- Front-end à base de clients riches JavaScript
- Les failles des clients riches JavaScript
- Services Web SOAP et REST
- Failles des Services Web SOAP et des Services REST
- Axes de prévention et bonnes pratiques dans le domaine

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