Sécurité offensive

Techniques de hacking du Web

3 jours (21h00) | 9 4,6/5 | SEC-HACKWEB | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 13/10/2023. Document téléchargé le 27/07/2024.

Objectifs de formation

A l'issue de cette formation, vous serez capable de :

- Développer des compétences avancées en test d'intrusion et en évaluation de la sécurité des applications Web
- Utiliser les techniques de détection et d'exploitation de vulnérabilités
- Identifier et résoudre les failles de sécurité spécifiques aux applications Web.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* *nous consulter pour la faisabilité en distanciel*

** *ratio variable selon le cours suivi*

Prérequis

Avoir suivi la formation SEC-HACK "Techniques de hacking - Niveau 1" ou avoir les connaissances équivalentes. Avoir une connaissance de base des commandes Linux et en développement, ainsi qu'une familiarité avec les langages Web courants.

Public concerné

Pentesters et professionnels de la sécurité cherchant à approfondir leurs compétences en test d'intrusion Web et développeurs souhaitant comprendre les vulnérabilités courantes dans les applications Web pour les corriger.

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 M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1 - Matin

Introduction au Pentest Web

- Introduction au Pentest Web
- Rôles et responsabilités du pentester
- Méthodologie du Pentest Web
- Utilisation des outils de test d'intrusion

Jour 1 - Après-midi

Préparation du laboratoire et reconnaissance

- Configuration du laboratoire de test
- Collecte d'informations sur la cible
- Utilisation d'outils comme Shodan, Dorks et DirBuster pour la recherche de failles

Jour 2 - Matin

Détection de vulnérabilités

- Scan de vulnérabilité avec WPScan, Nikto, OpenVAS et Nmap
- Utilisation de Burp Suite et ZAP pour l'analyse de sécurité
- Détection des vulnérabilités courantes

Jour 2 - Après-midi

Exploitation de vulnérabilités Web

- Attaques par force brute
- Attaques de l'injection de code
- Exploitation de vulnérabilités SQL Injection

Jour 3 - Matin

Exploitation de vulnérabilités Web - Suite

- Attaques de script côté client
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - XXE (XML eXternal Entity)
  - Vulnérabilité SSRF (Server Side Request Forgery)

Jour 3 - Après-midi

Techniques de défense

- Modélisation des menaces (Threat Modeling)
- Sécurisation de l'authentification (CAPTCHA et protection anti-brute force)
- Gestion des mots de passe (salage dynamique, gestion des politiques de mot de passe)
- Sécurisation des fonctionnalités d'upload de fichiers
- Utilisation de DAST (Dynamic Application Security Testing), SAST (Static Application Security Testing), WAF (Web Application Firewall)
- Utilisation de ressources et guides de sécurité :
  - L'OWASP Testing Guide
  - ASVS (Application Security Verification Standard)

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités d’évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation

Accessibilité de la formation

Le groupe M2i s'engage pour faciliter l'accessibilité de ses formations. Les détails de l'accueil des personnes en situation de handicap sont consultables sur la page Accueil et Handicap.

Modalités et délais d’accès à la formation

Les formations M2i sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.