Sécurité défensive

La sécurité des frameworks JavaScript

2 jours (14h00) | ★★★★½ 4,6/5 | SEC-FRAM | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Document mis à jour le 09/12/2023

Objectifs de formation

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

- Ecrire un code participant à la sécurité d'une application Web
- Expliquer les vulnérabilités affectant les applications Web
- Créer des tests visant à éprouver la sécurité des applications Web, notamment en JavaScript
- Développer des applications sécurisées en utilisant les frameworks JavaScript
- Formuler des exigences de sécurité aux autres corps de métiers.

Modalités, méthodes et moyens pédagogiques

Formation délivrée en présentiel ou distanciel* (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 les 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 des connaissances en développement d'application en langage JavaScript.

Public concerné

Pentesters et développeurs.

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

Introduction

- Panorama de la sécurité Web
- Les normes et lois
- Les référentiels
- Les principaux groupes de réflexion et de travail sur la sécurité des applications Web
- L'évolution des langages Web, des technologies et des usages du Web
- L'apport du Full Stack

Protocole HTTP avec JavaScript

- Rappels des fondamentaux sur les protocoles HTTP et HTTP/2
  - La pile applicative
  - Les méthodes
  - Les codes erreurs
  - Les principaux champs
- Le fonctionnement d'AJAX
- L'architecture des applications Web (monolithe, n-tiers, SOA / ROA...)
- Le cas des API
- Contrôler la permissivité des interfaces Web

Les outils connexes

- Faire des tests et des validations
  - Les tools des navigateurs
  - La capture via proxy
  - La capture via tcpdump ou Wireshark
  - Les tests avec Postman
  - Les "vulnerability scanners" (Burp Suite, Accunetix, les outils spécialisés CMS, les sites Web d'analyse)

L'OWASP

- Présentation de l'OWASP et de ses projets
- Les Security Cheat Sheets
- Le Top 10
- Le Top 25 du SANS
- Les Google Dorks
- Les guides de l'OWASP (Test Guide, Dev Guide...)
- L'ASVS (Application Security Verification Standard)
- Les grandes familles d'attaques

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

Jour 2

Sécurité du client

- Protéger les clients des attaques Cross-Site Scripting (XSS)
- Les protections apportées par Angular JS, NodeJS et React contre les XSS
- Protéger les clients des attaques Cross-Site Request Forgery (CSRF)
- Les protections apportées par Angular JS, NodeJS et React contre les CSRF
- Le cas jQuery
- La gestion de l'origine
- Filtrer la saisie utilisateur
- Limiter l'expérience utilisateur
- Surveiller le parcours de l'utilisateur
- L'obfuscation et le chiffrement du code
- La signature du code
- La gestion de la sécurité des bibliothèques tierces
- Le "pruning"

Exemples de travaux pratiques (à titre indicatif)

- *Démonstration des attaques XSS et CSRF*
- *Sécurisation d'une interface HTML avec JavaScript*
- *Création d'un contrôle et d'un suivi utilisateur*

Gestion des sessions

- Les méthodes d'authentification Web
- L'apport du JavaScript sur l'authentification
- Exploitation de la méthode HTTP basic
- "Forms Authentication Module"
- "Integrated Windows Authentication"
- La méthode Application_Authenticate Request
- Le contrôle des rôles et permissions
- L'utilisation de l'URL Authorization Module
- Les "security attributes"

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.