Sécurité défensive

Techniques défensives et offensives des applications Web

5 jours (35h00) | ★★★★☆ 4/5 | SEC-SAW | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Contenu mis à jour le 18/10/2024. Document téléchargé le 08/12/2024.

Objectifs de formation

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

- Intégrer la sécurité dès le début du cycle de développement (DevSecOps)
- Analyser les attaques pour identifier les vecteurs et les méthodes utilisés
- Identifier les principales menaces et vulnérabilités auxquelles les applications Web sont exposées
- Décrire les différentes techniques d'attaques utilisées par les pirates
- Appliquer des pratiques de codage sécurisé pour prévenir les vulnérabilités courantes
- Utiliser des frameworks et des bibliothèques de sécurité pour renforcer la protection des applications
- Implémenter des mécanismes d'authentification et de gestion des sessions sécurisées
- Mettre en place des contrôles d'accès pour protéger les données sensibles
- Effectuer des audits de sécurité réguliers pour identifier les vulnérabilités
- Effectuer des tests pour confirmer les vulnérabilités
- Assurer la conformité avec les réglementations et les normes de sécurité (comme RGPD, OWASP Level 2, PCI-DSS...)
- Encourager la collaboration entre les équipes de développement et de sécurité pour intégrer la sécurité dès le début du cycle de développement
- Promouvoir une culture de sécurité au sein de l'organisation en sensibilisant les employés aux bonnes pratiques de sécurité.

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 des connaissances généralistes en programmation Web.

Public concerné

Développeurs, ingénieurs DevOps, pentesters et RSSI en sécurité applicative.

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 à la cybersécurité

- Les enjeux d'un système d'information
- Le panorama des risques actuels
- Les profils des attaquants et leurs objectifs
- Les méthodes et les outils des attaquants
- Les vecteurs d'attaque d'un système d'information
- Les grandes familles d'attaques
- Les différentes phases d'une attaque (Cyber Kill Chain)

Le pilotage et la maîtrise des risques

- La prise de conscience de l'importance de la sécurité au sein de l'Etat et des entreprises
- Organismes d'Etat et indépendants (ANSSI, SGDSN, CERT, OWASP...)
- Exigences légales et contexte juridique (Article 323, Loi Godfrain, RGPD...)
- Les référentiels et normes de la sécurité des systèmes d'information (ISO 270xx, IEC 62443, OWASP, HDS, PCI-DSS...)
- Les standards de gestion de vulnérabilités (MITRE, NVD, CVE, CVSS, CWE, IOC, OTX, Exploit, TTp...)
- Le "Threat Modeling" et le framework ATT&CK
- Les principaux enjeux de la sécurité des applications Web

Exemple de travaux pratiques (à titre indicatif)

- *Modélisation des enjeux de sécurité d'un site Web*

Introduction au DevSecOps

- Le rôle de la sécurité dans le cycle de développement
- La méthodologie DevSecOps
- Les principes de sécurité dans le développement
- Les outils DevSecOps (Jenkins, GitLab CI/CD, SonarQube...)
- Les frameworks sécurisés (Spring Security, Express.js avec Helmet...)
- L'intégration continue de la sécurité (SAST, DAST)

Rappels sur les technologies du Web

- Le protocole HTTP
- Les headers
- Les status codes
- Les méthodes

Exemples de travaux pratiques (à titre indicatif)

- *Affichage et analyse d'une requête GET et d'une requête POST dans les DevTools d'un navigateur*

Les technologies de sécurisation

- Les techniques d'authentification (LM, Challenging, Kerberos, LDAP, MFA...)
- L'authentification centralisée et unique (CAS, SSO, WebSSO, OAuth, OpenID...)
- Les techniques de hash (MD5, AES, RSA, SSL, TLS...)
- Les techniques de chiffrement (symétrique, asymétrique, AES, TLS...)
- Les clés et les certificats numériques
- Les protocoles de vérification (WindBind, SASL, GSSAPI...)
- Les modèles de définition des autorisations (ACL 1.x, ACL 2.x)
- Les normes de gestion des groupes et les rôles (RBAC, PDP, PEP...)

Exemples de travaux pratiques (à titre indicatif)

- *Mise en oeuvre de l'environnement de formation avec une image virtuelle contenant un serveur Web, une base de données et différents scripts*

Jour 2

Les vulnérabilités du développement

- Introduction au Top 10 OWASP, Top 25 SANS et à Veracode
- Présentation des principales catégories de vulnérabilité
  - 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 (SSRF)

Exemples de travaux pratiques (à titre indicatif)

- *Mise en évidence et exploitation d'une vulnérabilité de type :*
  - *"Broken Access Control" sur la base d'un script livré par le formateur*
  - *"Injection" sur la base de scripts livrés par le formateur*
  - *"Insecure Design" sur la base d'un script livré par le formateur*
  - *"Security Misconfiguration" sur l'environnement de formation*
  - *"Vulnerable and Outdated Components", en déployant un outil de scan de vulnérabilité (Nessus, OpenVAS...) sur l'environnement de formation*
  - *"Vulnerable and Outdated Components", en déployant un outil de scan de vulnérabilité spécifique aux applications Web (Acunetix, Netsparker, Nikto, Wapiti, Qualys WAS...) sur l'environnement de formation*
  - *"Identification and Authentication Failures", sur la base d'un script livré par le formateur en déployant des outils spécialisés (Hydra, Medusa, Burp Suite, Wfuzz, Patator...)*
  - *"Software and Data Integrity Failures" sur la base d'un script livré par le formateur*
  - *"Security Logging and Monitoring Failures" sur l'environnement de formation*
  - *"Server-Side Request Forgery (SSRF)" sur la base d'un script livré par le formateur*

Jour 3

Les classes d'outils populaires exploités par les attaquants

- Les scanners de vulnérabilité Web (Burp Suite, Netsparker, Acunetix, WPscan, Nikto...)
- Les outils d'injection SQL (Sqlmap, Havij, SQLNinja...)
- Les outils de fuzzing (Wfuzz, Skipfish, Arachni...)
- Les outils de brute-force (Hydra, Medusa, Patator...)
- Les outils de manipulation de requêtes (Burp Suite, Postman...)
- Les outils de contournement de l'authentification (Hydra, Burp Suite, Cain & Abel...)
- Les outils d'exploitation des failles XSS (XSSer, Xenotix, BeEF...)
- Les outils de déni de service (LOIC, HOIC, Slowloris...)

Exemples de travaux pratiques (à titre indicatif)

- *Mise en oeuvre et utilisation d'un outil :*
  - *De scan de vulnérabilité*
  - *D'injection SQL*
  - *De fuzzing*
  - *De brute-force*
  - *De manipulation de requêtes*
  - *De contournement de l'authentification*
  - *D'exploitation des failles XSS*
  - *De déni de service*

Les attaques avancées

- Les LFI et RFI
- Les Wrappers
- L'écriture d'un Shell code de type RCE

Exemple de travaux pratiques (à titre indicatif)

- *Exploitation d'une LFI pour créer un Shell code de type RCE*

Jour 4

La sécurité du développement

- Les apports de l'OWASP
  - Les objectifs
  - Les ressources (Testing Guide, Security Guide, Code Review Guide, WebGoat, Juice Shop...)
  - Le Level 2 et ses directives
- Les bonnes pratiques de sécurisation
  - 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
- La validation et le filtrage des données en entrée et en sortie
- Les tokens anti-CSRF
- La sécurité des sessions et des cookies
- L'utilisation de CSP (Content Security Policy) pour limiter les risques
- L'impact de SOP (Same-Origin Policy)
- L'utilisation de CORS (Cross-Origin Resource Sharing)
- L'utilisation de HSTS (HTTP Strict Transport Security)
- L'option X-Frame
- La sécurité des API et des WebServices
- L'obfuscation et la minification

Exemples de travaux pratiques (à titre indicatif)

- *Sécurisation d'un script fourni par le formateur contre les attaques de type*
  - "*Broken Access Control*"
  - "*Injection*" *côté serveur*
  - "*Injection*" *côté client*
  - "*Identification and Authentication Failures*"

L'automatisation de la sécurisation

- Automatisation des tests de sécurité
- Intégration de la sécurité dans les pipelines DevOps
- Méthodes de détection des vulnérabilités dans le code
- Utilisation d'outils de test d'intrusion automatisés
- L'analyse statique du code (SAST)
- L'analyse dynamique du code (DAST)

Jour 5

Exemples de travaux pratiques (à titre indicatif)

- *Réalisation d'une analyse statique de code à l'aide d'outils de SAST (SonarQube, Checkmarx, Veracode, RIPS...)*
- *Réalisation d'une analyse dynamique de code à l'aide d'outils de DAST (OWASP ZAP, Burp Suite, Acunetix, Netsparker, AppSpider, W3af...)*
- *Proposition de solutions pour corriger les problèmes identifiés*

La sécurité du chemin d'exécution

- Limiter la phase de reconnaissance
- Limiter les risques et conséquences de la phase de compromission
- Limiter les possibilités de l'attaquant après l'intrusion
  - Eléments fondamentaux nécessaires sur un système
  - Eléments à supprimer d'un environnement de production
- Le durcissement du système d'exploitation
  - Gestion de l'authentification et des comptes utilisateurs
  - Politique de mot de passe et écueils courants
  - Politique de gestion des pare-feux
  - Configuration système
  - Mise en place et surveillance du système de fichiers
  - Limiter les droits d'exécution
- Le durcissement des applications serveurs
  - Bonne pratique d'installation et de maintenance
  - L'exposition de données sensibles
  - Les défauts de paramétrage de sécurité
  - Vérifier les failles connues sur les composants utilisés
  - Le manque d'historique et de monitoring
  - Les serveurs Web
  - Le langage côté serveur
  - Les bases de données

Exemples de travaux pratiques (à titre indicatif)

- *Sécurisation de l'environnement de formation contre les vulnérabilités de type :*
  - "*Security Misconfiguration*"
  - "*Vulnerable and Outdated Components*"
  - "*Security Logging and Monitoring Failures*", *en déployant un IPS, un IDS ou une politique d'écoute du système de fichiers*

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. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Accueil PSH.

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.