Sécurité des applications Web

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Développement

Action collective : Non

Filière : Action collective ATLAS "Java, .Net, C++"

Rubrique : Tronc commun

Code de formation : F28041

PRÉSENTATION

Objectifs & compétences

- Comprendre les différentes sécurités existantes autour des serveurs WEB, navigateurs, etc.
- Savoir gérer des tests de pénétration sur une application WEB Secure coding
- Avoir les bonnes méthodes et pratiques dans la conception d'une application WEB
- Acquérir les compétences nécessaires pour créer un programme de sécurité des applications
- Savoir couvrir les exigences demandées par les ISO 27001/2 à savoir
- Utiliser la norme ISO 27034 - sécurité des applications

Public visé

Manager en sécurité de l'information RSSI Chef de projet Développeur, Lead Dev

Pré-requis

Avoir les bases de la direction des systèmes d'information et de développement

PROGRAMME

1er Jour :

Chapitre 1 Les chiffres du WEB
Panorama de la sécurité WEB
Les normes, lois
Les référentiels
Les groupes de réflexions
Complément d'E-learning Web security scanning

Chapitre 2 Le top 10 des menaces selon l'OWASP
Les injections
Violation de gestion d'authentification et de session Cross-Site Scripting (XSS)
Références directes non sécurisées à un objet (IDOR)
Contrôle d'accès brisé
Mauvaise configuration de sécurité
Exposition de données sensibles
Protection contre les attaques insuffisantes CSRF (Cross site request forgery)
Exploitation de vulnérabilités connues API non protégée

2ème Jour :

Chapitre 3 Concevoir sécuriser (secure coding)
Conception sécurisée Les bases du respect des données personnelles
Réduction des attaques de surfaces
Défense en profondeur
Séparation des privilèges
Sécurisation par défaut

€ Tarifs

Prix public : 2275 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
Le plan de développement des compétences de votre entreprise : rapprochez-vous de votre service RH.
Le dispositif FNE-Formation.
L'OPCO (opérateurs de compétences) de votre entreprise.
France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
CPF -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

Lieux & Horaires

Durée : 35 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Chapitre 4 Bugs bar Modélisation de menaces (Threat modeling)
Système de ticketing et tableau de bord Créer ses standards avec ASVS

3ème Jour (Journée) :

Chapitre 5 Ajout de services de sécurité en IC (intégration continue)

Analyse statique
Analyse dynamique
WAF
Test de montée de charge

Chapitre 6 Durcissement des serveurs et bonnes pratiques ANSSI

Bonnes pratiques pour les SGRB®
Bonnes pratiques sur un serveur WEB et CMS
Configuration de la x-frame, xss-protection, csp, flag secure, HTTPOnly, etc

Chapitre 7 Test d'intrusion sur une application WEB
Utilisation de Burp suite
Aperçu des APIs et fonctionnalités de Burp et SQLMAP
Utilisation de l'OWASP Testing guide
Mise en application d'un test d'intrusion (scoring, reporting, analyse des besoins)

4ème Jour (Journée) :

Chapitre 8 Récapitulatif des acteurs autour de la sécurité application tels que (OWASP, MITRE, PCI-DSS, SAFECODE, HIPAA, etc.)
État des lieux sur les différentes sécurités autour de la sécurité applicative et DevOps telles que les navigateurs, serveurs, prestataires, outils (WAF, SAST, DAST, Cloudflare)
Les avantages et les défauts en termes de sécurité du DevOps et des méthodes Agile
Utiliser un modèle CAMS (Culture, Automation, Measurement, and Sharing)
Analyser les prérequis pour commencer un cycle de développement sécurisé avec :
Quelles sont les existants en matière de sécurité (PSSI, SMSI, etc.)
Quelles sont les lois concernées par la sécurité applicative

Chapitre 9 Établir in PIA (privacy impact assessment)
Permettant de définir la criticité des informations stockées par les applications et établir les risques et potentiels contrôles à prévoir. Affectation des responsabilités aux parties prenantes du projet

Chapitre 10 "Secure by design" et la mise en place d'un plan d'action pour le durcissement des infrastructures
Préparation à la réduction des surfaces d'attaques
Modélisation des menaces et analyse avec les exigences de l'entreprise

Chapitre 11 Préparation au "Secure code" avec : Analyse statique du code (démonstration des différents produits du marché) et automatisation du processus
Code review et analyse de fonctions non utiles
Vérification des exigences de l'organisation et du cycle de développement sécurisé en place

5ème Jour (Journée) :

Chapitre 12 Introduction au "Process model" et "Maturity model"

Étude du SDL (Microsoft Securiy developpement) de Microsoft
Préparation d'une formation pour les parties prenantes d'une application
Définir les exigences en termes de sécurité d'une organisation pour une application
Mettre en place l'architecture de l'application de manière sécurisée
Créer les procédures pour la mise en application d'une analyse statique et dynamique automatisée
Mettre un tableau de bord avec métrique
Créer un plan de réponse à incident

Chapitre 13 Présentation de BSIMM, OPENSAMM
Comparaison des différents Frameworks
Quand appliquer un modèle de maturité ?
Mise en place de OPENSAMM
État de l'art des différentes fonctions de la gouvernance SSI
Comprendre le processus OWASP OPENSAMM
Objectif, activité, granularité proposée par le Framework
Appliquer un score à l'aide des "scorecard"
Créer un tableau de bord avec les différentes métriques proposées par OPENSAMM

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

Méthode

Fin de formation : entretien individuel.
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.
Assiduité : certificat de réalisation.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.