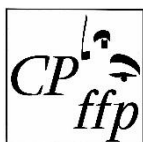


Expert développement d'applications sécurisées & Ethical hacking

PROGRAMME

**UNE FORMATION CERTIFIANTE
(HABILITATION FFP)**



FORMATION CERTIFIANTE

OBJECTIFS DE LA FORMATION

- Comprendre et appliquer les bonnes pratiques en matière de développement sécurisé
- Comprendre quelles sont les causes des vulnérabilités et prendre les mesures pour les prévenir de façon efficace et pertinente
- Préconiser les meilleures solutions possibles pour corriger / remédier aux vulnérabilités des applications
- Déployer les outils permettant d'augmenter le niveau de sécurité des applications de l'entreprise
- Paramétrer, mettre en œuvre et exploiter / interpréter les résultats des outils de test
- Intégrer les concepts de Security & Privacy by Design en profondeur dans le code
- Définir un plan d'audit de sécurité des applications
- Préparer, rédiger et communiquer un compte-rendu des résultats des tests et un plan de remédiation



PROGRAMME

MODULE 1 « MISE A NIVEAU DES CONNAISSANCES SYSTEMES/RESEAUX/LANGAGES » (9H) :

Objectifs :

- Comprendre comment une application interagit avec les composants [Ram, disque, Interfaces E/S, services système] via le système d'exploitation
- Comprendre comment les informations sont acheminées entre applications communicantes à travers le réseau, les mettre en œuvre
- Étudier le référentiel des langages de programmation [quel langage pour quel type d'application]

Contenu :

- Description, rôle, composantes d'un système d'exploitation
- Étude rapide de principaux systèmes d'exploitation WINDOWS/ANDROID/IOS/MAC OS/LINUX
- Différents types d'OS [Operating system] [multi-tâches/temps réel/embarqué]
- Architecture TCP/IP et Infrastructure réseau
- Interactions Applications/OS/Réseau
- Rappels sur les architectures et composants logiciels [Web, API, POO, SOA, N Tiers, Modèle MVC, Web services, etc.]
- Rappels des principes sur les principaux langages PYTHON, JAVA, C, JAVASCRIPT, PHP, etc.
- Travaux pratiques [Projet de développement sur un mois d'une application avec les deux parties Back end et Front end]

MODULE 2 « SÉCURITÉ DU DÉVELOPPEMENT DES APPLICATIONS WEB » (15H) :

Objectifs :

- Sensibiliser sur les risques liés à la sécurité des applications Web
- Comprendre la logique d'attaque sur les couches applicatives
- Assimiler les bonnes pratiques autour des développements
- Prendre conscience des problématiques de sécurité en prenant la place d'un attaquant exploitant les vulnérabilités usuelles, et apprendre les méthodes de défense pour s'en protéger
- Réaliser un défi / challenge de sécurité [audit de code et correction d'une application Web]

Contenu :

- Introduction aux risques et enjeux de la sécurité applicative
- Rappels sur les technologies Web
- Introduction aux techniques d'attaque et aux mécanismes de défense
- Connaissance de l'application
- Authentification
- Gestion de la session
- Gestion des autorisations
- Injection de code - Gestion des entrées utilisateurs
- Attaques ciblant d'autres utilisateurs - Gestion des sorties utilisateurs
- Journalisation des événements de sécurité
- Gestion des erreurs et des exceptions
- Introduction à la cryptographie
- Sécurité des Services Web

MODULE 3 « SÉCURITÉ DES DÉVELOPPEMENTS MOBILES » (12H) :

Objectifs :

- Sensibiliser autour des risques liés à la sécurité des applications mobiles
- Comprendre la logique d'attaque sur les couches applicatives pour mobiles
- Assimiler les bonnes pratiques autour des développements pour mobiles
- Prendre conscience des problématiques de sécurité en prenant la place d'un attaquant exploitant les vulnérabilités usuelles sur applications mobiles, et apprendre les méthodes de défense pour s'en protéger
- Réaliser un défi / challenge de sécurité [audit de code et correction d'une application mobile]

Contenu :

- Introduction aux risques et enjeux de la sécurité applicative pour les mobiles
- Introduction aux techniques d'attaque et aux mécanismes de défense
- Sécurité native des OS mobiles
- Interaction avec le serveur d'application
- Sécurité des applications mobiles
- Environnement mobile
- Déploiement

MODULE 4 « ETHICAL HACKING » (24H) :

Objectifs :

- Identifier les différentes phases d'une attaque
- Découvrir et mettre en œuvre les outils du pentesteur
- Définir un plan de tests d'intrusion, savoir interpréter et rédiger un rapport sur les résultats
- Mettre en œuvre la démarche de Pentest sur différents types d'attaques [réseaux et systèmes]
- Réaliser un défi / challenge de sécurité [tests d'intrusion et rédaction d'un rapport d'audit ciblant une application Web et une application mobile]

Contenu :

Découverte et cartographie de la cible (6h)

- Introduction
- Les informations publiques
- La cartographie réseau

Exploitation système et réseaux (6h)

- Introduction
- Exploitation système
- Attaques réseaux

Exploitation avancée (6h)

- Persistance et Portes dérobées
- Évasion de défense
- Attaques sur les mots de passe
- Pivot et rebond

Challenges de sécurité (6h)

- Tour d'horizon des différents types de défis [Script/Système/Crypto etc.]
- Session dédiée à l'attaque d'une infrastructure vulnérable

MODULE 5 « SÉCURITÉ DU CYCLE DE DÉVELOPPEMENT LOGICIEL » (4H) :

Objectifs :

- Sensibiliser autour des risques liés à la sécurité des développements applicatifs
- Évaluer les pratiques en sécurité des logiciels de votre entreprise
- Construire un plan d'assurance qualité des logiciels équilibré comprenant des étapes concrètes et bien définies
- Définir / Mesurer les actions liées à la sécurité au travers de l'entreprise et démontrer les améliorations concrètes dues à l'application d'un plan de qualité en sécurité

Contenu :

- Sécurité du cycle de développement logiciel
- Sécurisation de la gouvernance
- Sécurisation de la conception et des développements
- Tests et audits de sécurité
- Sécurisation du déploiement



Public visé

Personnes ayant un profil technique [développeurs / architectes / chefs de projet] souhaitant acquérir les connaissances suffisantes pour sécuriser leurs développements d'applications



Prérequis techniques

Expérience en programmation [entre 2 à 5 ans], idéalement en développement Web et Mobile
Connexion ADSL a minima (>1Mps)
[test ou entretien préalable]



Équipe pédagogique

Professionnels experts dans le développement sécurisé des applications et Ethical hacking



Durée

64 heures de formation sur 4 mois, soit 4h / semaine [2 sessions de 2h] en soirée



Validation des acquis

QCM
Certification Expert développement d'applications sécurisées & Ethical hacking - habilitation FFP



Frais individuels

3 800 € HT

Période et lieu de formation : Janvier à Avril 2020 à Villeurbanne



LES PLUS

UNE MÉTHODOLOGIE INNOVANTE

Un format mixte présentiel/téléprésentiel

Vous suivez nos cours en « direct-vidéo », ou en présentiel, animés par nos formateurs [experts reconnus dans le domaine de la sécurité applicative], depuis leur poste de travail ou dans les locaux de l'INSA Lyon. Nos sessions de formation sont adaptées à un public composé de professionnels du développement qui disposent d'un emploi du temps très chargé. Nous vous proposons deux sessions par semaine sur 4 mois [64h].

Une interactivité forte

Chaque cours se veut interactif, nos formateurs prennent le temps de répondre aux questions posées pendant les cours par les participants. Une plateforme de discussion privée permet à ces derniers de continuer à échanger avec leur formateur ou avec le reste des participants après les cours.

Un laboratoire d'expérimentation complet en ligne [24/7]

Des exercices et travaux pratiques vous permettent de participer activement à la formation. Tout est accessible sans avoir à installer le moindre logiciel au préalable [un simple navigateur suffit]. Pas de risque donc d'enfreindre votre politique de sécurité pour installer des outils d'attaques et/ou des applications vulnérables sur vos postes de travail.

FORMATION CERTIFIANTE
Expert développement
d'applications sécurisées
& Ethical hacking

Information générale et inscription :

Tél. : +33 (0)4 72 43 83 93

Email : formation@insavalor.fr

INSAVALOR Formation continue

66, Boulevard Niels Bohr

CS 52132

69603 Villeurbanne Cedex

Contact pédagogique :

Email : omar.gaouar@insa-lyon.fr

www.insavalor.fr



INSA
VALOR

APPSEC
ACADEMY