SECURE SPHERE by EPITA

EPITA ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

SECURE DEV WEB

Développez et programmez de manière cyber sécurisée

Objectif

Former les développeurs à l'intégration des bonnes pratiques cyber pour sécuriser les applications dès leur conception.

Destinataires

Développeurs, éditeurs logiciels et chefs de projets.

Prérequis

La connaissance d'au moins un langage de programmation Web (Java, Node.js, PHP, Python, etc.) est nécessaire.

Des notions dans le fonctionnement des systèmes d'exploitation et en cryptographie sont un plus.

Méthode pédagogique

Une pédagogie immersive qui allie apports théoriques, retours d'expériences et cas pratiques pour un ancrage durable des compétences.

Les cas pratiques sont réalisés sur un système vulnérable fourni par SECURESPHERE.

Formateurs

Consultants-Formateurs spécialistes de la sécurité informatique.

Compétences acquises

- Sécuriser la conception des applications web afin d'éviter les intrusions et limiter les failles dans les systèmes d'information en intégrant la sécurité dans les spécifications fonctionnelles et en implémentant les fonctions de sécurité dans les spécifications techniques
- Développer des logiciels et des applications capables d'écarter les intrusions dans les systèmes d'information en caractérisant les vulnérabilités
- Écarter les intrusions dans les systèmes d'information en développant des logiciels et des applications qui incluent les contre-mesures existantes dans les mécanismes intégrés aux noyaux spécifiques du développement web
- Tester le logiciel ou l'application pour éviter les intrusions et limiter les failles dans les systèmes d'information en mettant en oeuvre des tests de robustesse sur les éléments développés
- Sécuriser le déploiement des applications pour éviter les intrusions et limiter les failles dans les systèmes d'information en vérifiant leur intégration dans l'environnement existant

Moyens techniques

Salle de formation équipée de postes de travail informatiques disposant de tous les logiciels nécessaires au déroulement de la formation.

DURÉE
3 jours - 21 heures

TARIF INTER
2 250 € HT
par stagiaire

TARIF INTRA
Nous contacter

LIEU
Campus Cyber
Tour Eria,
5 rue Bellini
92800 Puteaux

ou dans vos locaux

ACCESSIBILITÉ
Cette formation est accessible aux personnes en situation de handicap.

Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE

SECURESPHERE
est détenteur de la certification Qualiopi au titre de la catégorie d'actions de formation.

PROGRAMME

INTRODUCTION

Concepts génériques liés aux vulnérabilités web
- Exemples réels et conséquences
- Identification des vulnérabilités (CVE)
- Criticité des vulnérabilités (CVSS) et politique de communication par les éditeurs logiciels

Gestion de projets
- Principe de l'analyse de risques (OWASP A04)
- Intégration de la sécurité dans les projets (OWASP A04)

Spécificités de l'hébergement dans le cloud et des offres Sofware as a service (SAAS)

CONCEPTION

Spécifications fonctionnelles
- Principe de sécurité par défaut (OWASP A04)
- Transparence vs sécurité par l'obscurité
- Protection des données sensibles et concepts cryptographiques (OWASP A02)
- Traçabilité (OWASP A09)
- Fonctionnalités dangereuses
- Gestion des mises à jour (OWASP A06

Spécifications techniques et implémentation des fonctions de sécurité
- Authentification (OWASP A07)
- Gestion des mots de passe
- Gestion des sessions
- Autorisation / Gestion des droits (OWASP A01)
- Cryptographie appliquée (OWASP A02)
- Gestion des erreurs

PROGRAMMATION (IN) SÉCURISÉE

Vulnérabilité (dont OWASP TOP 10) liées au développement et contre-mesures
- Injections OWASP A03, OWASP A10 :
  - SQL, LDAP
  - Commandes système
  - Arguments de commandes
  - Code interprété
- ReDoS
- Injections XML - XXE (OWASP A05)
  - Cross-site scripting – XSS
  - Désérialisation (OWASP A08)
  - Directory transversal
- Cross-site request forgery (CSRF)

Outils et recette sécurité
- Tests manuels de sécurité
- Tests unitaires, audit statique de code
- Configuration de l'environnement (OWASP A05)
- Tests automatisés de sécurité
- Fuzzing et tests d'intrusion applicatifs

Protection au niveau de l'environnement
- Filtrage réseau et NIDS
- Relais et Web Application Firewall (WAF)

ÉVALUATION
L'évaluation est réalisée tout au long de la formation, sous la forme d'exercices ou de mises en situation.

ATTESTATION
Une AACE, Attestation d'Acquisition des Compétences de l'EPITA, est délivrée aux stagiaires ayant validé l'ensemble des compétences visées par le stage.