Fiche de formation
Les techniques du développement informatique sécurisé

CONTACT POUR CETTE FORMATION

Miora RAHARINIRINA
Chargée de mission formation
almond.institute@almond.eu
07 64 42 71 56

- Version 1.0
- 29/01/2024

Les techniques du développement informatique sécurisé

Les objectifs pédagogiques

Cette formation vise à sensibiliser vos équipes aux risques informatiques et à leurs conséquences. Ce module présente les techniques couramment utilisées par les pirates informatiques en vulgarisant le sujet pour un auditoire non technique. Il détaille les bonnes pratiques à adopter pour se prémunir contre la plupart des attaques.

01. Connaître **les principales failles** liées aux applications web (Top 10 OWASP).

02. Savoir détecter **la présence des failles présentées.**

03. Acquérir les **bonnes pratiques de développement.**

Les techniques du développement informatique sécurisé

Informations pratiques

Public

- Développeurs et développeuses d'applications web, quelle que soit la technologie utilisée

Prérequis

Connaissance basique des environnements web :

- 1 langage web : PHP, JAVA, ASP .NET, Python, etc.
- 1 langage de base de données : SQL et/ou NoSQL
- 1 système d'exploitation : Linux et/ou Windows

Évaluation des acquis

- Réalisation d'un questionnaire en ligne final recouvrant l'ensemble des notions apprises
- En cas de formation en présentiel : réalisation d'exercices pratiques

Modalités et délai d'accès

Le stagiaire est considéré inscrit lorsque :

- Les prérequis et besoins sont identifiés et validés
- La convention de formation signée

Les demandes d'inscription peuvent être envoyées jusqu'à 10 jours ouvrés avant le début de la formation.

Accessibilité

Que vous soyez reconnu en situation de handicap ou pas, rendre notre formation accessible à toutes et à tous fait partie de notre engagement.

Si vous avez besoin d'une compensation ou adaptation pour le contenu, les supports, le « lieu », le matériel utilisé, les horaires, le rythme, **nous sommes à votre écoute.**

Les techniques du développement informatique sécurisé

La formation en présentiel ou distanciel

Programme

Introduction	Tests web avancés
→ Contexte cybersécurité (CNIL, menaces, attaquants, fuites de données, le marché noir des failles, etc.) → OWASP → Matrice MITRE ATT&CK	→ **La 1ère phase permet d'aborder l'essentiel des sujets importants et le top 10 OWASP sur 1,5j :** • Authentification/Stockage des mots de passe / HTTP (Utilisation de Burp Suite) / Manipulation de champs HTTP / Gestion de la session / Path Traversal, LFI / Déni de service applicatif / Mise en cache / RCE / XSS / Injections SQL / CSRF / Open Redirect / XXE / SSRF → **La 2e phase sur 0,5j permet d'aborder certains sujets choisis en concertation avec le public de la formation selon les technologies utilisées, ses compétences et appétences. Les sujets possibles sont :** • Désérialisation non sécurisée (PHP et/ou JAVA) / Type Juggling (PHP) / Log forging / En-têtes de sécurité / Dependency Confusion / OAuth/OpenID / Angular et XSS / SAMLv2 / Configuration TLS / Injection NoSQL / Sécurité des API

Les plus de la formation

→ Une formation dispensée par un expert en sécurité applicative web ayant réalisé de nombreux tests d'intrusions web.

→ Les formations en présentiel comprennent des mises en pratique réalisées par les participants eux-mêmes sur un environnement de test.

Tarifs et infos

→ **Durée:** 2 jours (14 heures)

→ **Tarif:** Contactez-nous

→ **Financement:** Prise en charge OPCO