# Les techniques du développement informatique sécurisé

Ce programme de formation vise à sensibiliser les équipes de développement aux risques de sécurité liés au développement d'applications web. Ce module présente les attaques couramment utilisées par les pirates informatiques. Les techniques présentées sont approfondies et mises en pratique. Le module détaille les bonnes pratiques à adopter pour se prémunir contre les attaques présentées.

## LES OBJECTIFS

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.**

almond.institute@almond.eu
www.almond.eu

# Les techniques du développement informatique sécurisé

## PUBLIC

Cette formation s'adresse aux :

- 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

## 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.**

almond.institute@almond.eu
www.almond.eu

# Les techniques du développement informatique sécurisé

## PROGRAMME

### INTRODUCTION

- Contexte cybersécurité (CNIL, menaces, attaquants, fuites de données, le marché noir des failles, etc.)
- OWASP
- Matrice MITRE ATT&CK

### TESTS WEB AVANCÉS

Nous proposons d'articuler les sujets abordés en 2 phases.

**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

almond.institute@almond.eu
www.almond.eu

# Les techniques du développement informatique sécurisé

## 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

## LES PLUS DE LA FORMATION

- Une formation dispensée par un expert en sécurité applicative webayant réalisé de nombreux tests d'intrusions web
- Les formations en présentiel comprennent des mises en pratique réalisées par les participants eux-mêmessur un environnement de test

## POUR ALLER PLUS LOIN

Cette formation permet de préparer la formation suivante :

- Techniques des pirates informatiques – Comment s'en protéger

**Durée**
2 jours (14 heures)

**Tarif**
Contactez-nous

**+ prise en charge OPCO**

## SESSIONS DISPENSÉES EN

PRÉSENTIEL

DISTANCIEL

**S'inscrire à une session**

almond.institute@almond.eu
www.almond.eu