

# Sécuriser ses applications en PHP

Cette formation vous permettra de connaître les failles de sécurité les plus courantes et surtout la façon de sécuriser vos applications afin de ne pas y être confronté.

## Modalité

Formation en centre de formation sur Colmar

## Durée totale

14 heures (2 jours)

## Tarif

1410.00€ TTC / pers.

## Modalités Pédagogiques

- Méthodes : Expositive, démonstrative et active
- Moyens : Cas pratique, mise en situation
- Ressources : Support de cours et Programme de formation
- Moyens techniques : Teams

## Prérequis

Bonnes connaissances en PHP, SQL et javascript.  
Validation du test de positionnement (QCM)

**Pour les séances en distanciel, un serveur local comprenant PHP 7 (ou plus) et un serveur de BDD (MySQL ou MariaDB) sont obligatoires.**

## Public cible

Développeurs PHP souhaitant sécuriser leurs applications

## Délai et Modalités d'accès

Délai d'accès 10 jours après la signature du contrat. Dates à convenir entre le client et l'organisme de formation.

## Objectifs

À l'issue de la formation, le stagiaire doit être capable de maîtriser les compétences suivantes :

- Comprendre les différents éléments de sécurité du système d'information
- Analyser et réagir aux attaques sur le serveur
- Identifier les failles pour y appliquer des correctifs pour les éviter
- Déterminer les failles potentielles d'un utilisateur de logiciel et appliquer les bons correctifs pour empêcher les attaques
- Adapter son code aux failles potentielles lors du téléchargement de fichiers via un site web

## Déroulé du parcours de formation

### Introduction

- La cybercriminalité et les risques
- Les organisations de sécurité
- Les principes de la sécurité des données
- Les failles de sécurité les plus courantes
- Les exigences de sécurité

### Les attaques sur le serveur

- Les attaques par Déni de Service (DoS et DDos)
- Les outils permettant d'auditer les failles de sécurité du serveur
- Anonymiser les informations

### Les formulaires et leurs failles

- Validation des entrées, assainissement
- Les attaques XSS (Cross Site Scripting)
- Les jetons

### L'utilisateur

- Les mots de passe
- Attaque Brut Force
- L'injection SQL

### Le téléchargement de fichiers

- Les types MIME
- Traiter le fichier reçu

### Évaluations formatives

Le suivi de la progression pédagogique est assuré par des quiz de validation des connaissances à la fin des modules et des exercices d'application pratiques (mises en situation).

### Modalités d'évaluation

Le formateur évalue la progression en cours de formation à l'aide de cas pratiques, mises en situation, QCM...  
Un test de positionnement sera complété en amont et en aval afin de valider les compétences acquises.

### Formateurs

Tous les formateurs de CE FORMATION sont des professionnels en activité, à leur compte ou salarié, ils conservent ainsi "les mains dans le cambouis".  
Ils ont chacun leur spécialité, mais également une vision globale du métier et sont dotés d'un niveau BAC+3 ou supérieur.  
Ils sont tous également formateurs dans d'autres centres de formation, depuis au minimum 2 ans, et sont connus et respectés pour leur engagement, leur pédagogie et leur humilité face au métier et à sa constante évolution.

### Contacts

CE FORMATION  
07.68.48.96.63  
[contact@ce-formation.com](mailto:contact@ce-formation.com)  
CE FORMATION

### Accessibilité aux PSH

Cette formation est accessible aux personnes en situation de handicap.  
Si la situation nécessite des aménagements spécifiques, le candidat peut contacter notre référent handicap :  
Christel EHRHART  
07.68.48.96.63  
[christel@ce-formation.com](mailto:christel@ce-formation.com)

### Indicateurs

Taux de satisfaction : 75 %

Taux d'accomplissement : 100 %