



# ORGANISME DE FORMATION AUX TECHNOLOGIES ET METIERS DE L'INFORMATIQUE

## Formation Sécurité des applications et des serveurs web *Sécurisez vos sites Internet et Intranet*

N° ACTIVITÉ : 11 92 18558 92

TÉLÉPHONE : 01 85 77 07 07

E-MAIL : inscription@hubformation.com

Avec Internet, les réseaux sont dorénavant ouverts et par conséquent, beaucoup plus exposés aux attaques virales ou autres actes de piratage. Il est donc primordial de savoir faire face à ces différents risques pour protéger les données de l'entreprise et garantir l'intégrité et le bon fonctionnement de son système d'information. L'objectif de cette formation est de permettre aux participants d'identifier les risques liés à internet puis de comprendre comment sécuriser les serveurs web, les applicatifs et les données associés en recourant aux méthodes et technologies ad hoc.

### Objectifs

- | Évaluer les risques internes et externes liés à l'utilisation d'Internet
- | Identifier les différentes solutions pour mettre en oeuvre la sécurité d'un serveur Web
- | Identifier comment garantir la fiabilité et la confidentialité des données grâce aux différentes solutions sécurisantes
- | mettre en oeuvre une politique de sécurité fiable sur un serveur Apache ou IIS

### Public

- | Responsable sécurité
- | Chef de projets
- | Développeur Web
- | Administrateur de serveur Web

### Prérequis

- | Connaissance en administration Unix
- | Connaissance des réseaux et protocoles TCP/IP

### Programme de la formation

#### Introduction au protocole HTTP

- | Format des requêtes
- | Mécanismes d'authentification HTTP
- | Génération de requêtes HTTP
- | Découverte passive d'informations
- | HTTP : protocole de transport

#### Introduction au protocole HTTPS

- | Généralités
- | Authentification par certificats X.509
- | Méthodes d'audit HTTPS
- | Historique des failles de sécurité

#### Qualité des développements WEB

- | Erreurs classiques
- | Classification OWASP : exemples, démonstrations
- | Injections : exemple avec SQL
- | XSS (Injection croisée de code)

Référence	RES212
Durée	3 jours (21h)
Tarif	2 150 €HT

### SESSIONS PROGRAMMÉES

#### A DISTANCE (FRA)

- du 10 au 12 juin 2025
- du 28 au 30 juillet 2025

#### PARIS

- du 10 au 12 juin 2025
- du 28 au 30 juillet 2025

#### AIX-EN-PROVENCE

- du 10 au 12 juin 2025
- du 13 au 15 octobre 2025

#### BORDEAUX

- du 10 au 12 juin 2025
- du 13 au 15 octobre 2025

#### GRENOBLE

- du 10 au 12 juin 2025
- du 13 au 15 octobre 2025

#### LILLE

- du 10 au 12 juin 2025
- du 28 au 30 juillet 2025

#### LYON

- du 10 au 12 juin 2025
- du 13 au 15 octobre 2025

#### NANTES

- du 28 au 30 juillet 2025
- du 13 au 15 octobre 2025

[VOIR TOUTES LES DATES](#)

## Apache

- | Présentation du serveur phare du marché Web
- | Sécurisation d'un serveur Apache
- | Mettre en place https avec mod\_ssl
- | Apache en relais-inverse
- | Relayage applicatif avec mod\_proxy/mod\_rewrite
- | Filtrage applicatif avec mod\_security
- | Application à l'intégration Apache / Tomcat

## Internet Information Services (IIS)

- | Architecture
- | Installation
- | Sécurisation
- | Outils
- | HTTPS

## Méthode pédagogique

Une formation complète durant laquelle s'alternent les phases d'apports théoriques, d'échanges, de partage d'expériences et de mises en situation.

Une formation qui accorde une large place à la mise en oeuvre concrète des acquis à travers la réalisation d'une série d'ateliers amenant les participants à assurer la sécurité d'un serveur Web.

## Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

---

## Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

- | Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
- | Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
- | Privilégier une connexion filaire plutôt que le Wifi.
- | Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
- | Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
- | Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
- | Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
- | Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
- | Horaires identiques au présentiel.

---

## Accessibilité



Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.

Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.