

Sécurité des applications web

Parcours : Applied (Applications web et big data)

Public concerné

► Niveau Bac +3 et Bac +4 en informatique, statistiques, mathématiques et/ou expérience professionnelle requise en lien avec la formation visée

Durée

► 5 jours, 35 heures

Dates

► Voir sur le site les dates des sessions
formation-continue.parisnanterre.fr

Tarif

► 2 000 euros TTC

Nombre de places

► 15 places

Inscription

► En ligne sur le site, rubrique Formations courtes
formation-continue.parisnanterre.fr

En savoir plus

Responsable de la formation : Reda BENDRAOU
rbendraou@parisnanterre.fr

Objectifs pédagogiques

- Fondamentaux de la sécurité informatique au sein des organisations ;
- Méthodes et analyses de gestion des risques ;
- Identification et sélection des outils techniques permettant de déjouer des attaques ;
- Sécurité du web.

Modalités pédagogiques

- Formation en présentiel ;
- Phases d'apports théoriques, d'échanges, de partage d'expériences et des ateliers réalisés au travers de cas pratiques.

Compétences visées

- Mettre en oeuvre des processus opérationnels afin de sécuriser un SI interne ;
- Identifier et proposer des technologies sécurisées adaptées aux utilisateurs ;
- Mesurer les risques d'une organisation ;
- Détecter les types d'attaque ;
- Appréhender la sécurité liée aux technologies JAVA.

Prérequis

- Langage Java, développement d'applications



Intervenants

► Enseignants-chercheurs de l'université Paris Nanterre, intervenants professionnels

Modalités de validation

► Mise en pratique

Certification

► Cette formation donne lieu à la délivrance d'une attestation de compétences

Parcours de formation

Cette formation fait partie du parcours Applied Formations associées :

- Projet d'intégration d'une application (3 jours) ;
- Développement d'applications web en Java (9 jours) ;
- Technologie du Big Data (6 jours) ;
- Test des applications web (5 jours) ;
- Traitement statistique des données (3 jours) ;
- Développement d'applications Android (3 jours).

La validation de l'ensemble du parcours peut permettre la délivrance du diplôme d'université.

Le point fort de la formation

► Formation conçue en cohérence avec les besoins identifiés sur le marché du travail

Programme

- Présentation des notions de sécurité : contexte, risques, méthodes de gestion des risques
- Les différents types d'attaque : attaques ciblées sur l'utilisateur ou le navigateur, techniques de Social Engineering
- Les outils de la sécurité : fondamentaux de la cryptographie, techniques cryptographiques, législation et principales contraintes d'utilisation
- L'authentification: authentification biométrique, aspects juridiques, authentification forte
- Les certificats et leurs utilisations : utilisation de SSH, OpenSSL, protocoles sécurité TLS, notions de signature
- Sécurité et langage Java : Créer ses permissions avec Java Security, Java Cryptography, architecture du module d'authentification JAAS
- Sécurité et le Web : sécurité des web services, protocoles, standards de sécurité XML, Firewalls, audit de sécurité

« *Se former tout au long de la vie* »

Lieu

Université Paris Nanterre
Bâtiment de la Formation Continue
200 avenue de la République
92001 Nanterre Cedex



MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE



Cette formation fait partie de la gamme « Formations courtes » développée en commun par l'université Paris Nanterre, l'université Paris 8 et le Cnam Île-de-France. Elle est soutenue par le Ministère de l'enseignement supérieur, l'université Paris Lumières et le CESI dans le cadre de l'AMI « Pilotes FTLV 2017 ».