Formation Sécurité des applications Web, synthèse

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Ce séminaire dresse un panorama des menaces du Web. Il détaille les failles des navigateurs, réseaux sociaux et du Web 2.0, les nouvelles vulnérabilités sur SSL/TLS et certificats X509, ainsi que des applications Java EE, .NET et PHP. Il présente les solutions pour protéger et contrôler la sécurité des applications.

Référence	SEW
Durée	2 jours (14h)
Tarif	2 140 €HT
Repas	repas inclus

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 5 au 6 juin 2025

du 18 au 19 novembre 2025

PARIS

du 14 au 15 octobre 2025

VOIR TOUTES LES DATES

Objectifs

| Identifier les menaces de sécurité sur les applications Web
| Connaître les protocoles de sécurité Web
| Identifier les typologies d'attaque
| Sécuriser les applications Web

Public

| SI
| RSSI
| responsables sécurité
| développeurs
| concepteurs
| chefs de projets intégrant des contraintes de sécurité
| responsables ou administrateurs réseau, informatique, système

Prérequis

| connaissances de base en informatique et en réseaux

Programme de la formation

Menaces, vulnérabilités des applications Web
| Risques majeurs des applications Web selon IBM X-Force IBM et OWASP.
| Attaques de type Cross Site Scripting (XSS), injection et sur sessions.
| Propagation de faille avec un Web Worm.
| Attaques sur les configurations standard.

Protocoles de sécurité SSL, TLS
| SSL v2/v3 et TLS, PKI, certificats X509, autorité de certification.
| Impact de SSL sur la sécurité des firewalls UTM et IDS/IPS.
| Failles et attaques sur SSL/TLS. Techniques de capture et d'analyse des flux SSL.
| Attaque HTTPS stripping sur les liens sécurisés.
| Attaques sur les certificats X509, protocole OCSP.
| SSL et les performances des applications Web.

Attaques ciblées sur l'utilisateur et le navigateur
| Attaques sur les navigateurs Web, Rootkit.
| Sécurité des Smartphones pour le surf sur le Net.
| Codes malveillants et réseaux sociaux.
| Les dangers spécifiques du Web 2.0.
| Les techniques de Social Engineering.

Attaques ciblées sur l'authentification
| Authentification via HTTP, SSL par certificat X509 client.
| Mettre en oeuvre une authentification forte, par logiciel.
| Solution de Web SSO non intrusive (sans agent).
| Principales attaques sur les authentifications.

Sécurité des Web Services
| Protocoles, standards de sécurité XML Encryption, XML Signature, WS-Security/Reliability.
| Attaques d'injection (XML injection...), brute force ou par rejeu.
| Firewalls applicatifs pour les Web Services.
| Principaux acteurs et produits sur le marché.

Sécuriser efficacement les applications Web
| Durcissement, hardening : sécuriser le système et le serveur HTTP.
| Virtualisation et sécurité des applications Web.
| Environnements .NET, PHP et Java. Les 5 phases du SDL.
| Techniques de fuzzing. Qualifier son application avec l'ASVS.
| WAF : quelle efficacité, quelles performances ?

Contrôler la sécurité des applications Web
| Pentest, audit de sécurité, scanners de vulnérabilités.
| Organiser une veille technologique efficace.
| Déclaration des incidents de sécurité.
| Démonstration Mise en oeuvre d'un serveur Web avec certificat X509 EV : analyse des échanges protocolaires. Exploitation d'une faille de sécurité critique sur le frontal HTTP. Attaque de type HTTPS Stripping.

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

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.