# Formation Sécurité des applications Web

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

L'intrusion sur les serveurs de l'entreprise représente un risque majeur. Il est essentiel de comprendre et d'appliquer les technologies et les produits permettant d'apporter le niveau de sécurité suffisant aux applications déployées et plus particulièrement aux applications à risque comme les services extranet et la messagerie. Résolument pragmatique, ce stage vous apportera les clés de la protection d'un service en ligne à partir d'exemples concrets d'attaques et de ripostes adaptées.

| | |
|---|---|
| Référence | SER |
| Durée | 3 jours (21h) |
| Tarif | 2 440 €HT |
| Repas | repas inclus |

## Objectifs

| Identifier les vulnérabilités les plus courantes des applications Web
| Identifier le déroulement d'une attaque
| Tester la sécurité de ses applications Web
| Configurer un serveur Web pour chiffrer le trafic Web avec HTTPS
| Mettre en place des mesures de sécurisation simples pour les applications Web

## Public

| Administrateurs réseaux, systèmes
| Webmasters

## Prérequis

| Connaissances de base en systèmes, réseaux et d'Internet.

## Programme de la formation

**Introduction**
| Statistiques et évolution des failles liées au Web selon IBM X-Force et OWASP.
| Evolution des attaques protocolaires et applicatives.
| Le monde des hackers : qui sont-ils ? Quels sont leurs motivations, leurs moyens ?

**Constituants d'une application Web**
| Les éléments d'une application N-tiers.
| Le serveur frontal HTTP, son rôle et ses faiblesses.
| Les risques intrinsèques de ces composants.
| Les acteurs majeurs du marché.

**Le protocole HTTP en détail**
| Rappels TCP, HTTP, persistance et pipelining.
| Les PDU GET, POST, PUT, DELETE, HEAD et TRACE.
| Champs de l'en-tête, codes de status 1xx à 5xx.
| Redirection, hôte virtuel, proxy cache et tunneling.
| Les cookies, les attributs, les options associées.
| Les authentifications (Basic, Improved Digest...).
| L'accélération HTTP, proxy, le Web balancing.
| Attaques protocolaires HTTP Request Smuggling et HTTP Response splitting.
| Travaux pratiques  Installation et utilisation de l'analyseur réseau Wireshark. Utilisation d'un proxy d'analyse HTTP spécifique.

## SESSIONS PROGRAMMÉES

A DISTANCE (FRA)
du 18 au 20 juin 2025
PARIS
du 11 au 13 juin 2025
AIX-EN-PROVENCE
du 18 au 20 juin 2025
BORDEAUX
du 18 au 20 juin 2025
LILLE
du 18 au 20 juin 2025
LYON
du 18 au 20 juin 2025
NANTES
du 18 au 20 juin 2025
SOPHIA-ANTIPOLIS
du 18 au 20 juin 2025
STRASBOURG
du 18 au 20 juin 2025
TOULOUSE
du 18 au 20 juin 2025

VOIR TOUTES LES DATES

**Les vulnérabilités des applications Web**
| Pourquoi les applications Web sont-elles plus exposées ?
| Les risques majeurs des applications Web selon l'OWASP (Top Ten 2010).
| Les attaques "Cross Site Scripting" ou XSS - Pourquoi sont-elles en pleine expansion ? Comment les éviter ?
| Les attaques en injection (Commandes injection, SQL Injection, LDAP injection...).
| Les attaques sur les sessions (cookie poisonning, session hijacking...).
| Exploitation de vulnérabilités sur le frontal HTTP (ver Nimda, faille Unicode...).
| Attaques sur les configurations standard (Default Password, Directory Transversal...).
| Travaux pratiques  Attaque Cross Site Scripting. Exploitation d'une faille sur le frontal http. Contournement d'une authentification par injection de requête SQL.

**Le firewall réseau dans la protection d'applications HTTP**
| Le firewall réseau, son rôle et ses fonctions.
| Combien de DMZ pour une architecture N-Tiers ?
| Pourquoi le firewall réseau n'est pas apte à assurer la protection d'une application Web ?

**Sécurisation des flux avec SSL/TLS**
| Rappels des techniques cryptographiques utilisées dans SSL et TLS.
| Gérer ses certificats serveurs, le standard X509.
| Qu'apporte le nouveau certificat X509 EV ?
| Quelle autorité de certification choisir ?
| Les techniques de capture et d'analyse des flux SSL.
| Les principales failles des certificats X509.
| Utilisation d'un reverse proxy pour l'accélération SSL.
| L'intérêt des cartes crypto hardware HSM.
| Travaux pratiques  Mise en oeuvre de SSL sous IIS et Apache. Attaques sur les flux HTTPS avec sslstrip et sslsnif.

**Configuration du système et des logiciels**
| La configuration par défaut, le risque majeur.
| Règles à respecter lors de l'installation d'un système d'exploitation.
| Linux ou Windows. Apache ou IIS ?
| Comment configurer Apache et IIS pour une sécurité optimale ?
| Le cas du Middleware et de la base de données. Les V.D.S. (Vulnerability Detection System).
| Travaux pratiques  Procédure de sécurisation du frontal Web (Apache ou IIS).

**Principe du développement sécurisé**
| Sécurité du développement, quel budget ?
| La sécurité dans le cycle de développement.
| Le rôle du code côté client, sécurité ou ergonomie ?
| Le contrôle des données envoyées par le client.
| Lutter contre les attaques de type "Buffer Overflow".
| Les règles de développement à respecter.
| Comment lutter contre les risques résiduels : Headers, URL malformée, Cookie Poisoning... ?

**L'authentification des utilisateurs**
| L'authentification via HTTP : Basic Authentication et Digest Authentication ou par l'application (HTML form).
| L'authentification forte : certificat X509 client, Token SecurID, ADN digital Mobilegov...
| Autres techniques d'authentification par logiciel : CAPTCHA, Keypass, etc.
| Attaque sur les mots de passe : sniffing, brute force, phishing, keylogger.
| Attaque sur les numéros de session (session hijacking) ou sur les cookies (cookie poisoning).
| Attaque sur les authentifications HTTPS (fake server, sslsniff, X509 certificate exploit...).
| Travaux pratiques  Attaque "Man in the Middle" sur l'authentification d'un utilisateur et vol de session (session hijacking).

**Le firewall "applicatif"**
| Reverse proxy et firewall applicatif, détails des fonctionnalités.
| Quels sont les apports du firewall applicatif sur la sécurité des sites Web ?
| Insérer un firewall applicatif sur un système en production. Les acteurs du marché.
| Travaux pratiques  Mise en oeuvre d'un firewall applicatif. Gestion de la politique de sécurité. Attaques et résultats.

## Méthode pédagogique

Des sites en ligne sécurisés et protégés (firewall multi-DMZ) seront déployés, une accélération SSL, un proxy d'analyse du protocole HTTP, un injecteur de flux HTTP(S), une authentification forte par certificat, des outils d'attaques sur les flux HTTPS...

## 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.