Sécurité des Applications Web

DURÉE
4 jours (28h)

RÉFÉRENCE
SEC131

CATÉGORIE
Sécurité des Applications

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Prendre connaissance des bonnes pratiques de développement permettant d’éviter de rendre une application vulnérable.
- Installer, configurer et utiliser des outils permettant d’analyser vos applications

POUR QUI ?

- Chefs de projets
- Développeurs

Programme détaillé

1/ Introduction

- Les technologies web, les risques
- Mythes et réalités
- Statistiques et évolutions

2/ Attaquants et défenseurs

- Le profil des "pirates", leur arsenal
- La défense (politique de sécurité, législation, réponse des éditeurs...)
- Le Bug Bounty ; avantages et inconvénients

3/ Les applications Web et les menaces

- Comment fonctionne le Web : DNS / HTTP / TLS
- Comment fonctionnent les applications “single-page”
- KYA : “Know Your Attacker”. Connaitre son attaquant
- Menaces : Man In The Browser, Distribution de Malwares, Advanced Persistent Threat, Ransomware
- Risques

4/ 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

5/ Protocole HTTP

- 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
- Mécanismes d'authentification HTTP
- L'accélération HTTP, proxy, le Web balancing
- Attaques protocolaires HTTP Request Smuggling et HTTP Response splitting

6/ Vulnérabilités des applications Web

- L'exposition des applications Web
- Classement des risques majeurs selon l'OWASP et le CWE
- Analyse des vulnérabilités et des conséquences de leur exploitation
- Les principales attaques :
- "Cross Site Scripting” (XSS)
- Les attaques en injection
- Les attaques sur les authentifications et sessions
- CSRF...
- Les vulnérabilités des frameworks et CMS

7/ Outils de détection et d’exploitation

- Les scanners de vulnérabilités Web
- L'analyse statique de
- Les outils d’analyse manuelle
- Exploitation SQL
- Brute-force et fuzzing

8/ Le pare-feu réseau dans la protection d'applications HTTP

- Le pare-feu réseau, son rôle et ses fonctions

- Combien de DMZ pour une architecture N-Tiers ?
- Limite du pare-feu réseau pour la protection d'une application Web

9/ 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 ?
- Autorité de certification à 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

10/ 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 ?
- La façon de configurer Apache et IIS pour une sécurité optimale
- Le cas du Middleware et de la base de données

11/ Principe du développement sécurisé

- Les écueils
- La sécurité dans le cycle de développement
- Application à AGILE/SCRUM
- Le budget
- Le rôle du code côté client
- Le contrôle des données envoyées par le client
- Les règles de développement à respecter

12/ L'authentification des utilisateurs

- L'authentification via HTTP
- 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...)

13/ 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

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

28 au 31 Juil. 2026	Casablanca
22 au 25 Sep. 2026	
17 au 20 Nov. 2026	

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Scannez pour accéder
à la fiche en ligne