Audit de Sécurité de Sites Web

Lien : https://innov-systems.com/formation/audit-de-securite-de-sites-web-

DURÉE
4 jours (28h)

RÉFÉRENCE
DEV143

CATÉGORIE
Développement D'applications (Java, Eclipse, Windows 10, Spring, Jquery, Labview, Testsand)

OBJECTIFS DE LA FORMATION

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

- Auditer une application Web par un test de pénétration à l'aide d'outils automatiques mais aussi manuellement
- Mettre en place des contres mesures pour se prémunir des attaques

POUR QUI ?

- Développeurs
- Administrateurs de sites et serveurs Web

Innov Systems

Programme détaillé

1 / Tour d'horizon des attaques sur le Web

- Qui ? Pourquoi ? Comment ?
- Les cibles les plus courantes

2 / Classification des attaques Web

- Présentation de l'OWASP
- Classification des dix attaques les plus courantes

3 / Technologies liées à la sécurité

- Firewalls, panorama des outils, techniques de base réseaux
- Filtres des requêtes HTTP
- Empreinte de message, les algorithmes SHA-x et MD5
- Signature numérique, Clé publique/ clé privée, Coffre à clé et coffre de confiance, Autorités de certification
- Chiffrement de données, les algorithmes AES et RSA
- Protocoles SSL v2/v3 et TLS, PKI, certificats X509
- Techniques d'authentification HTTP, authentification par certificat

4 / Passage des contrôles côté client

- Les outils inclus dans les navigateurs
- Utilisation d'un proxy local (ZAP, BurpSuite)
- Utilisation d'addons (Tamper Data, Web developper, etc)
- Débogage de JavaScript (principe d'obfuscation)
- Bonne pratique et règle de sécurité pour les contrôles côté client

5 / Technique d'hameçonnage par injection dans l'URL

Innov Systems

6 / Les failles XSS

- Faille XSS reflétées
- Faille XSS stockées
- Exemple de récupération de session
- Se prémunir des failles XSS

7 / Passage d'authentification

- Les bonnes pratiques
- Gérer correctement les IDs de session
- Politiques des mots de passe
- Les authentifications HTTP

8 / Les injections SQL classiques

- Rappels sur les bases de données
- Principe des injections SQL

9 / Les injections SQL en aveugle

- Principe
- Exploitation

10 / Détection et exploitation des injections SQL

- Par des outils automatiques
- Manuellement

11 / Se prémunir des injections SQL

12 / La faille Include

- Exploitation d'une faille include

Inov Systems

- Bonnes pratiques pour se prémunir des failles includes

13 / La faille Upload

- Passage des extensions et types MME
- Mise en place d'un shell
- Saturation du serveur
- Contre mesure

14 / Les outils d'audit automatiques

- ZAP
- W3AF
- Acunetix
- Burpsuite

15 / Interprétation et vérification des résultats

- Interpréter les résultats d'un outil automatique
- Vérifier la véracité des alertes remontées

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

Innov Systems

Prochaines dates programmées

05 au 08 Jan. 2027	Présentiel - Casablanca
02 au 05 Mars 2027	Présentiel - Casablanca
27 au 30 Avr. 2027	Présentiel - Casablanca
22 au 25 Juin 2027	Présentiel - Casablanca
24 au 27 Août 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés

Innov Systems