Sécurité des Applications Web

VOTRE FORMATION

DURÉE : 5 JOURS

35 heures

PROCHAINE SESSION :

6, 7, 8, 15 et16 juillet 2020

LIEU : En distanciel

PRIX : 1 495 €

net de taxes

LE PUBLIC

Les développeurs Web, les experts sécurité de développement, les responsables sécurité

Les administrateurs réseaux, systèmes et applications, les architectes

LES OBJECTIFS

Mettre en œuvre la sécurité dans un environnement Web

Auditer à la recherche des faiblisses et opérer les mesures pour sécuriser vos applications Web.

Sécuriser vos services et environnements Web

PRÉ-REQUIS

Connaissance en développement Web sous Java

RESSOURCES

- Support de cours
- 70% d'exercices pratiques

MODALITES

Formation 100 % à distance

De 4 à 16 participants

9h –17h30

Financement éligible au FNE Formation pour tout salarié d'entreprise en activité partielle

VOTRE CONTACT :

Andrea FALLOURD
Conseillère en formation
06 74 51 44 97
afallourd@itescia.fr

ITESCIA - Campus de Pontoise
8 rue Pierre de Coubertin
95300 PONTOISE

www.itescia.fr

VOTRE PROGRAMME

Cette formation dresse un panorama complet des menaces du Web et les techniques et mesures de sécurisation d'un environnement Web. Elle présente un aperçu de l'ensemble des outils et des mécanismes de sécurité permettant de protéger les applications Web contre les actes malveillants et répondre ainsi répondre aux différents risques cités dans l'OWASP Top 10. Elle donne une vision globale des moyens, actions et solutions permettant de garantir la sécurité des applications Web. Avec des travaux pratiques et des études de cas réels, elle présente les solutions les plus efficaces pour protéger et contrôler la sécurité des applications Web.

Introduction aux fondamentaux Web

Rappels des bases de l'architecture Client – Serveur

Notions sur le protocole HTTP (Headers, méthodes, cookie, token)

Notions sur les API serveur (Rest VS SOAP)

Notions sur les architectures N-tiers (Serveur d'application, SGBD, DNS, proxy, …)

Principes clés liés aux applications web

Les mécanismes d'authentification Web
- Faiblesses
- Attaques et mesures préventives

Gestion des entrées/sorties
- Faiblesses
- Attaques et mesures préventives

Contrôle d'accès
- Faiblesses
- Attaques et mesures préventives

Principes Web et méthodologie de pentest

Modèle MVC

Communication entre les briques Serveur et Base de données

Enumération et fuzzing du contenu de l'application

Analyse des fonctionnalités de l'application

OWASP TOP 10
- A1 – Injection
- A2 – Broken Auth
- A3 – Sensitive Data Exposure
- A4 – XML External Entities (XXE)
- A5 – Broken Access Control
- A6 – Security Misconfig
- A7 – Cross-Site Scripting (XSS)
- A8 – Insecure Deserialization
- A9 – Using components with known vulns
- A10 – Insufficient logging & monitoring

Autres vulnérabilités
- Cross Site Request Forgery (CSRF)
- …

Outillage

Outils de découverte

Burp Suite
- Interception de trafic
- Rejeu de requêtes
- Brute force

SQLmap pour les injections SQL

Rédaction de rapport d'audit

Elaboration de tableau récapitulatif

Description de la méthodologie d'audit réalisée

Vulnérabilités Web

Outils d'analyse

Enumération des vulnérabilités

↳Les travaux pratiques seront réalisés sur la plateforme d'entrainement **SECURITY DOJO** unique en son genre. Les scénarii de LABs de SEC-DOJO sont tirés de cas réels avec des vulnérabilités récentes et d'actualité.

Avec les LABs de Sec-Dojo, pour monter l'infrastructure nécessaire aux travaux pratiques, vous n'avez ni à télécharger des iso, ni à installer, ni à configurer, ni à paramétrer et ni à déboguer. Vous êtes directement au cœur du sujet « la sécurité ».