+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 26/07/2023

S'inscrire

Formation Sécurité des Applications Web

3 jours (21 heures)

PRÉSENTATION

Cette formation Sécurité des applications Web se concentre sur les vulnérabilités Web les plus fréquentes afin que vous puissiez détecter les attaques et sécuriser vos applications Web. Grâce à notre formation, votre équipe apprendra à identifier les vulnérabilités les plus courantes des applications Web, comprendre le déroulement des différentes attaques afin de prévenir les risques pour votre entreprise. Mais aussi, elle saura mettre en place plusieurs mesures de sécurisation simples et tester la sécurité de vos applications. Vous pourrez aussi configurer un serveur Web pour chiffrer le trafic Web avec HTTPS. Cette formation va permettre à votre entreprise d'apporter un niveau de sécurité aux applications déployées comme les services extranet et les messageries. Vous aurez à disposition après cette formation les clés de la protection d'un service en ligne grâce à des exemples de ripostes et attaques adaptées. En fonction de l'avancement, les thématiques suivantes pourront en particulier être parcourues : attaques par force brute et fuzzing, cloisonnement et contrôle d'accès, exploitation d'injections SQL à l'aveugle, Cross-Site Scripting (XSS).

OBJECTIFS

- Connaître les failles de sécurité
- Comprendre les déroulements des attaques
- Tester la sécurité de ses applications web

PUBLIC VISÉ

- Développeurs
- Chefs de projets
- Administrateurs réseaux/système
- Pentesteurs
- Hackers éthiques

Pré-requis

- Connaissance de base en sécurité web
- Connaissance d'un langage de programmation

PROGRAMME DE NOTRE FORMATION SÉCURITÉ DES APPLICATIONS WEB

INTRODUCTION

- L'écosystème de la sécurité web
- Les différentes normes
- Les différentes lois
- Les référentiels
- Présentation des menaces
- Les vulnérabilités
  - Les risques majeurs
  - Attaque en injection
  - Attaque sur les sessions
  - Attaque sur les configurations standard
- Les attaques côté client
  - Cross Site Scripting (XSS)
  - Gestion de session et authentification
  - Phishing

LES DIFFÉRENTS CONSTITUANTS D'UNE APP WEB

- Qu'est-ce que le serveur frontal HTTP ?
  - Son rôle
  - Ses faiblesses
- Protocole HTTP
  - Les requêtes
  - Les réponses
  - Codes HTTP
  - HTTPS
- Les risques intrinsèques
- Les différents acteurs du marché
- Le Client
- Le Serveur
- Les URLs
  - L'anatomie d'une URL
  - Les failles de type open redirect
- Les headers
- Les différentes méthodes
- Les status code

DÉVELOPPEMENT SÉCURISÉ

- Qu'est-ce que le développement sécurisé ?
- Rôles
  - Côté client
  - Côté sécurité
  - Côté ergonomie
- Attaque type "Buffer Overflow"
- Les différentes règles de développement à respecter
- Les risques résiduels
  - Headers
  - URL malformée
  - Cookie Poisoning

HARDENING APPLICATIF

- Sécuriser une authentification
- La gestion des mots de passe
  - Modification des status code
  - Salage dynamique
- Encodage
  - Des entrées
  - Des sorties
- Management
  - Des logs
  - Des sessions

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.