Programme de formation

Sécurité WEB

Bases sécurité offensive pour les développeurs
Comprendre les attaques pour mieux se défendre

Durée

2 jours / 14 heures

Description

La Cybersécurité tient une place de plus en plus importante dans les préoccupations actuelles des concepteurs de site et applications web. Une application se doit d'être à la fois robuste, scalable et sécurisée.
Durant cette formation, nous vous présentons quelques-unes des failles de sécurité les plus présentes sur le web ainsi que les méthodes employées pour les exploiter et les prévenir.

Objectifs pédagogiques

- Appréhender les failles de sécurité web les plus communes (TOP 10 OWASP)
- Apprendre à les détecter
- Effectuer des exercices simples pour les comprendre et les éviter

Public

Développeur web, Admin Système, Chef de projet / directeur de projet technique

Pré-requis

Connaissances générales en programmation web (php/js notamment), connaissances générales en ligne de commande shell, connaissances générales en réseau

Méthodes pédagogiques

60 % théorie / 40 % pratique

Profil intervenant

L'ensemble de nos formations est animé par des formateurs expérimentés possédant une expérience terrain éprouvée.

Modalités d'évaluation

L'évaluation des acquis se fait tout au long de la session au travers d'ateliers de mise en pratique des notions et concepts abordés pendant la formation

Programme

Introduction

- Introduction
- OWASP top 10
- Concepts fondamentaux
- Fonctionnement HTTP
- Entrées utilisateurs
- Mots de passe

Failles communes

- Web Server
    - SQLI
    - Template injection
    - Commandes Injection
    - LFI/RFI
    - Upload de fichier
    - Unserialize
    - SSRF
    - XXE
    - Logical bugs
    - Type juggling
- **Web Clients**
    - XSS
    - CSRF
- **Privilèges escalation**
    - Cron
    - Sudo
    - Kernel

Cas concret client anonymisé

- Revue de pentest réels