Makina Corpus Formation
49 grande rue Saint-Michel
31400 Toulouse
Email: formation@makina-corpus.com
Tel: 0661342710

Formation Sécurité Web

Mise à jour janvier 2024

Inter 1800€ HT/participant
Intra 4500€ HT* groupe de 6 participants
*hors frais de déplacement et de personnalisation de formation sur-mesure

Apprenez à mieux gérer la sécurité d'une application LAMP.

Durée: 21.00 heures (3.00 jours)

À QUI S'ADRESSE CETTE FORMATION ?

Profil du stagiaire

- Développeurs web
- Architectes web

Prérequis

- Connaissances de PHP (niveau simple)
- Connaissances des commandes UNIX de base
- Connaissances des technologies des applications web (JavaScript, CSS et HTML)

OBJECTIFS PÉDAGOGIQUES

1. Comprendre les principales attaques de sécurité pour apprendre à mieux développer des applications web
2. Comprendre les règles principales de développement sécurisé
3. Comprendre les principaux éléments de configuration des services LAMP afin de mieux protéger les applications

Makina Corpus Formation
49 grande rue Saint-Michel
31400 Toulouse
Email: formation@makina-corpus.com
Tel: 0661342710

CONTENU (PROGRESSION PÉDAGOGIQUE)

Révisions : le protocole HTTP

- HTTP/1.0 HTTP/1.1
- codes HTTP (200,404,302,301,503,500,100,...)
- Proxy et reverse proxy caches
- Tunneling HTTP
- Authentification HTTP
- Cookies et Sessions
- GET vs POST
- Entêtes spécifiques (Vary, Content-Lenght, Content-Encoding, Mime, etc.)
- HTTPS : HTTP over TLS
- Autres protocoles : DNS et TCP/IP

Apache

- Portée de la configuration : VirtualHosts (IP et Noms), Directory, Location
- mod_rewrite : les bases
- Les mpm : prefork, worker, event
- Exemples de configuration

Nginx

- Pincipes de fonctionnement
- Portée de la configuration (Server, http, location, ...)
- Exemples de configuration

LAMP

- Linux - Apache - PHP – MySQL
- Architectures classiques, séparation n-tiers, caches, montée en charge
- PHP, mod_php ou php-fpm
- Cloisonnements de configuration
- Ajax : Json, jsonp, XMLHttpRequests

Analyser les failles

- CVE
- Vecteurs d'attaque, vulnérabilités, impacts et exploitations
- Évaluation des risques

Étude théoriques du TOP-10 OWASP

- Injections - Sessions et Authentification
- Cross Site Scripting – XSS
- Références Directes non sécurisées à un objet
- Mauvaise configuration de sécurité
- Exposition de données sensibles
- Manque de contrôle d'accès fonctionnel
- Falsification de requêtes interdites (CSRF)
- Utilisations de composants vulnérables
- Redirections et renvois non validés

Makina Corpus Formation
49 grande rue Saint-Michel
31400 Toulouse
Email: formation@makina-corpus.com
Tel: 0661342710

Autres failles importantes

- Déni de Service
- Protection de la vie privée
- Fuite d'information
- XXE : XML external Entity Processing
- Clickjacking

Étude pratique du top-10 OWASP

- Injections HTML
- Injections JavaScript
- Injections SQL
- CSRF
- Open redirect
- Escalade de privilèges
- Information disclosure
- DOS
- Cache poisonning

Principes de sécurisations

- Robustesse et Rigueur
- KISS
- Validation des Entrées, Filtrage des Sorties
- Sécurité en profondeur

Cas pratique

- Corrections de l'application
- Blindages de configuration :
  - Apache
  - Nginx
  - PHP
  - MySQL/PostgreSQL
  - mod_security : exemples.
  - Entêtes HTTP (X-Frame-Options, Content-Security-Policy, ...)

Retours sur les points clefs

- Authentification
  - Stockage
  - Complexité des mots de passe
  - Authentification multi-facteurs
  - Transmission de mots de passe
  - NTLM/CAS/Oauth/OpenID/SAML
- XSS
  - Types d'XSS (Dom-based, reflected, etc)
  - Techniques d'obfuscation avancées
- Injections SQL

Makina Corpus Formation
49 grande rue Saint-Michel
31400 Toulouse
Email: formation@makina-corpus.com
Tel: 0661342710

- time-based, blind injections
- Injection de second ordre

La sécurité d'un point de vue plus large

- Social engineering
- Procédures humaines
- Sécurité physique
- Tolérance aux pannes, backups
- Supervision
- Détection d'intrusion

Makina Corpus Formation
49 grande rue Saint-Michel
31400 Toulouse
Email: formation@makina-corpus.com
Tel: 0661342710

ORGANISATION

Formateur
Formation assurée par un expert-formateur PostgreSQL

Moyens pédagogiques et techniques

- Accueil des stagiaires dans une salle dédiée à la formation.
- Documents supports de formation projetés.
- Exposés théoriques
- Étude de cas concrets
- Quiz en ligne
- Mise à disposition en ligne de documents supports à la suite de la formation.

Dispositif de suivi de l'exécution de d'évaluation des résultats de la formation

- Feuilles de présence dématérialisées.
- Questions orales ou écrites (QCM).
- Mises en situation.
- Formulaires d'évaluation de la formation.

Délais d'accès
La convocation est envoyée 7 jours avant le début de la formation après réception du bon de commande signé.

Coordonnées de l'équipe pédagogique
- Responsable formation, handicap et votre formateur : Cécile Chardonneau formation@makina-corpus.com
- Suivi facturation : Nathalie Carles Salmon administration@makina-corpus.com