Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

Sécuriser et protéger vos applications web

Mettre en oeuvre la sécurité pour protéger vos applications web

La sécurité est la préoccupation et la responsabilité de tous, en particulier sur le web où le nombre et la complexité des menaces ne cessent de croître.
Cette formation vous apprendra à déceler les points faibles de vos applications web, développer de façon sécurisée et corriger vos vulnérabilités.
Vous apprendrez également à superviser l'activité de vos applications web afin de détecter et réagir aux tentatives d'intrusion.

Détails

- Code : DW-SECU
- Durée : 3 jours (21 heures)

Public
- Chefs de projets
- Developpeurs

Pré-requis

Objectifs
- Découvrir les menaces Web classiques et modernes.
- Repérer vos points faibles.
- Corriger vos vulnérabilités et développer de façon sécurisée.
- Mettre en place et exploiter un système de « monitoring » sécurité afin de détecter et réagir aux tentatives d'intrusion.

Programme

Les applications Web et les menaces
- Comment fonctionne le Web : DNS / HTTP / TLS
- Comment fonctionnent les applications « single-page »
- KYA : « Know Your Attacker ». Connaitre votre attaquant
- Menaces : Man In The Browser / Distribution de Malwares / Advanced Persistent Threat / Ransomware
- Risques

Les vulnérabilités
- Les vulnérabilités présentées ci-dessous seront expérimentées par les stagiaires sous forme d'atelier « ethical hacking » sur une application volontairement vulnérable
- Injection de code
- Injection SQL
- « Broken Authentication and Session Management »
- « Reflected XSS », « Persistent XSS » and « DOM XSS »
- « Insecure Direct Object Reference »
- Erreurs de configuration
- Exposition de données sensibles
- Vérifications insuffisantes des données échangées
- « Cross-Site Request Forgery »
- Utilisation de composants vulnérables
- Redirections non validées

« Single-Page Application » et sécurité des APIs REST
- DOM XSS
- Validation client vs. Validation API
- Fuites et accès non autorisées aux ressources de l'API
- Fuite du token d'authentification

TLS, authentification et authentification forte
- Choix des algorithmes cryptographiques à utiliser
- Authentification avec certificat client et PKCS#11
- Authentification avec « One-Time Password »

ModSecurity
- Mise en place de ModSecurity
- Edition et gestion des règles ModSecurity
- Système de « scoring » ModSecurity
- Le « virtual patching » avec ModSecurity

« Monitoring » sécurité avec ModSecurity et Splunk
- Corrélation d'évènements
- Création de dashboards

Modalités
- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages

Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu