Sécurité applicative : intégrer la sécurité dès la conception

Pratiques pour concevoir et développer une application sécurisée

DESCRIPTION

Depuis quelques années, les attaques informatiques se sont complexifiées et leurs auteurs se sont professionnalisés. Garantir la sécurité des applications informatiques est une question essentielle non seulement pour maintenir la confiance des utilisateurs et se prémunir contre certains risques aux conséquences économiques importantes comme un arrêt de la production, l'indisponibilité d'un site d'e-commerce…

En parallèle, la réglementation s'est renforcée pour devenir de plus en plus exigeante et la responsabilité de l'entreprise est engagée. Face à ces nouveaux enjeux, les équipes de développement doivent maîtriser la sécurité de leurs applications.

Cette formation a pour objectif de vous transmettre les connaissances nécessaires pour renforcer la sécurité de votre application (sécurité défensive) et mieux appréhender les techniques des attaquants (sécurité offensive).

OBJECTIFS PEDAGOGIQUES

- Concevoir une application “Secure by design”
- Maîtriser les bonnes pratiques de sécurité à toutes les phases de développement
- Identifier les principales failles de sécurité applicative et anticiper les menaces
- Appréhender le déroulement d'une attaque pour mieux la déjouer

PUBLIC CIBLE

Cette formation s'adresse à toute personne concernée par la sécurité des applications au sens large (application web, site, web service, etc.). Sont concernés en particulier :

- Développeur

Séminaire en présentiel
Qualité du logiciel

Code :
SECAP

Durée :
2 jour(s) (14,00 heures)

Exposés : **35 %**
Cas pratiques : **50 %**
Echanges d’expérience : **15 %**

Inter-entreprises :
Prochaines sessions disponibles sur notre site web.
Tarif : 1 680,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

OCTO Academy est une marque d’OCTO Technology, référencé au DATADOCK – 34, avenue de l'Opéra, 75002 Paris France - SAS au Capital de 509 525.30 €
Tél : +33 1 70 36 18 67 – Fax : +33 1 58 56 10 01 – academy@octo.com – https://www.octo.academy – academy@octo.com
SIRET : 418 166 096 00069 – RCS Paris B 418 166 096 - NAF 6202A – Organisme de formation N° 11 75 48 936 75

- Ops
- Testeur
- Administrateur
- Architecte

PRE-REQUIS

- Connaissance d'un langage de programmation.
- Culture du web (HTML, formulaire, serveur web, base de données).

METHODE PEDAGOGIQUE

Formation avec apports théoriques, échanges sur les contextes des participants et retours d'expérience pratique du formateur, complétés de travaux pratiques et de mises en situation.

PROFIL DES INTERVENANTS

Toutes nos formations sont animées par des consultants-formateurs expérimentés et reconnus par leurs pairs.

MODALITÉS D'ÉVALUATION ET FORMALISATION À L'ISSUE DE LA FORMATION

L'évaluation des acquis se fait tout au long de la session au travers des ateliers et des mises en pratique. Une évaluation à chaud sur la satisfaction des stagiaires est réalisée systématiquement en fin de session et une attestation de formation est délivrée aux participants mentionnant les objectifs de la formation, la nature, le programme et la durée de l'action de formation ainsi que la formalisation des acquis.

PROGRAMME PEDAGOGIQUE DETAILLE

JOUR 1

SECURITY BY DESIGN

- Défense en profondeur

- Principe de moindre privilège
- Diminuer la surface d'attaque
- Separation of duties
- Fail securely
- Transparence : éviter la sécurité par l'obscurité
- Programmation défensive
- Sécurité positive

VULNÉRABILITÉS LES PLUS RÉPANDUES (ET COMMENT S'EN PRÉMUNIR)

- Validation insuffisante des entrées/sorties (injection de code, XSS, traversée de répertoire, validation côté client, etc.)
- Problème de configuration de sécurité
- Gestion des droits
- Authentification
- Chiffrement insuffisant
- Déni de service

JOUR 2

BONNES PRATIQUES DE SÉCURITÉ

- Grille d'audit de l'OWASP : ASVS (Application Security Verification Standard)
- HTTP Security Headers
- Stockage de mots de passe dans une application

ANATOMIE D'UNE ATTAQUE

PRATIQUE

- En groupe de deux ou plus
- Mise en pratique des connaissances avec WebGoat (application volontairement vulnérable)
- Exploitation de vulnérabilités spécifiques (injections, protocole HTTP, etc.)

OCTO Academy est une marque d'OCTO Technology, référencé au DATADOCK – 34, avenue de l'Opéra, 75002 Paris France - SAS au Capital de 509 525.30 €
Tél : +33 1 70 36 18 67 – Fax : +33 1 58 56 10 01 – academy@octo.com – https://www.octo.academy – academy@octo.com
SIRET : 418 166 096 00069 – RCS Paris B 418 166 096 - NAF 6202A – Organisme de formation N° 11 75 48 936 75