Sécurité applicative : intégrer la sécurité dès la conception

Assimiler les bonnes pratiques de conception et développement d'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 par exemple un arrêt de la production ou 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
- Décrire et analyser les étapes d'une attaque afin d'identifier les signaux d'alerte et mettre en place des actions de prévention.

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
- Ops
- Testeur
- Administrateur
- Architecte

PRE-REQUIS

Séminaire en présentiel
Qualité du logiciel - Software Craftsmanship

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 : 1 790,00 € HT / participant

Intra-entreprise :
Tarifs et dates sur demande.

- Pratique des langages de développement Web (A minima : HTML, JavaScript, SQL)
- Connaissance du protocole HTTP
- Idéalement la connaissance d'un framework front de type Angular, React…

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.

La formation se veut résolument tournée vers la pratique: elle alterne les simulations des différentes attaques existantes et les bonnes pratiques pour protéger vos applications.

PROFIL DES INTERVENANTS

Cette formation est dispensée par un·e ou plusieurs consultant·es d'OCTO Technology ou de son réseau de partenaires, expert·es reconnus des sujets traités.

Le processus de sélection de nos formateurs et formatrices est exigeant et repose sur une évaluation rigoureuse leurs capacités techniques, de leur expérience professionnelle et de leurs compétences pédagogiques.

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.

Afin de valider les compétences acquises lors de la formation, un formulaire d'auto-positionnement est envoyé en amont et en aval de celle-ci.

En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués.

Une évaluation à chaud est également effectuée en fin de session pour mesurer la satisfaction des stagiaires et un certificat de réalisation leur est adressé individuellement.

PROGRAMME PEDAGOGIQUE DETAILLE

Jour 1

PRÉSENTATION DE LA DÉMARCHE DE SECURE CODING

SECURE BY DESIGN :

- Présentation des 10 principes de sécurité pour concevoir une application sécurisée
- Challenge offensif en équipe pour simuler une attaque applicative

SÉCURITÉ DU WEB : PRÉSENTATION DES MÉCANISMES DE SÉCURITÉ DES NAVIGATEURS WEB

- SOP (Same Origin Policy)
- CORS (Cross-Origin Resource Sharing)
- CSP (Content Security Policy)

REVUE DU TOP 10 OWASP (OPEN WEB APPLICATION SECURITY PROJECT)

MISE EN PRATIQUE DES PRINCIPALES ATTAQUES AVEC UNE APPLICATION VOLONTAIREMENT VULNÉRABLE.

Les participants doivent, de manière collaborative, exploiter la faille puis en identifier la cause pour ensuite la corriger

- Attaque XSS (Cross Site Scripting)
- Attaque SSTI (Server Side Templating Injection)
- Attaque REDOS (Regular expression Denial of Service)

Jour 2

MISE EN PRATIQUE DES PRINCIPALES ATTAQUES (SUITE DU JOUR 1)

- Attaque IDOR (Insecure Direct Object Reference)
- Attaque Mass Assignment
- Attaque SQL injection
- Attaque CSRF (Cross Site Request Forgery)

BONNES PRATIQUES DE SÉCURITÉ

- Mesures de protection contre les Bot (Captcha)
- Sécurité des Cookies
- Protocole HTTPS: parametres TLS et entêtes HTTP

MISE EN PRATIQUE AU TRAVERS D'UN ATELIER DE SECURE CODING POUR DÉFINIR SA STRATÉGIE DE SÉCURITÉ APPLICATIVE

Identification d'un plan d'action post formation

SYNTHÈSE ET PARTAGE DES RETOURS SUR LA FORMATION

Accessibilité

L'inclusion est sujet important pour OCTO Academy.
Nos référent·es sont à votre disposition pour faciliter l'adaptation de votre formation à vos besoins spécifiques.
Pour les contacter : academy.accessibilite@octo.com