navixia
information security

Cours SecDev pour développeurs

Les applications web et mobiles constituent une vulnérabilité potentielle dans un réseau d'entreprise et sont souvent utilisées comme point d'entrée par les pirates. Ce cours permet aux développeurs de comprendre le mode opératoire des attaquants et de prendre en compte les impératifs de sécurité en écrivant leur code.

La formation, spécialement développée par Navixia, vous permet à vous, développeur, d'acquérir des connaissances opérationnelles en sécurité de l'information dans le cadre du développement d'applications. Le cours, interactif et pratique, inclut divers labos reflétant des cas concrets. Il vous donne la possibilité de vous confronter pratiquement aux différents risques que peut présenter le code, d'expérimenter leurs conséquences, d'apprendre à les corriger et d'adopter de manière générale une approche du développement axée sur la sécurité.

Des modules de formation pertinents

Le cours est conçu pour traiter les aspects de la sécurité auxquels vous êtes confronté chaque jour en tant que développeur. La sélection de modules qui forment le cours vous permet de traiter en toute connaissance de cause les aspects les plus importants de la sécurité en lien avec les applications. Vous abordez les vulnérabilités du point de vue de l'attaquant (hacker) et/ou du défenseur (développeur).

Une protection accrue pour l'entreprise

La sécurité de l'infrastructure IT est grandement renforcée lorsque vous, développeur, prenez conscience des risques potentiels liés au code et savez comment les éviter. C'est une protection efficace pour l'entreprise.

Pourquoi ce cours

Pour coder des logiciels ou des applications sûrs, un développeur doit savoir quelles faiblesses sont visées par les pirates. Ce cours lui apprend à penser comme un hacker et lui donne les outils nécessaires pour améliorer de manière significative la sécurité du code.

A qui s'adresse ce cours

Ce cours est particulièrement indiqué pour les **développeurs**, les **architectes software**, et toute personne appelée à coder ou à intégrer des applications web ou mobiles dans le cadre de ses activités.

Des instructeurs chevronnés

Les instructeurs de Navixia allient une expérience étendue de pentesteurs et de développeurs.
Ils ont ainsi une vision pragmatique et concrète des modes opératoires d'attaque ou de défense, ce qui leur permet de donner des conseils pertinents adaptés à la réalité du terrain.

Organisation logistique

- **Durée**: 2 jours
- **Lieu**: le centre de formation de Navixia à Ecublens
- **Langue**: Français (anglais sur demande)
- **Coût**: CHF 2'500 / pers., incluant: (a) Formation dispensée par un instructeur qualifié; (b) Equipement matériel et logiciel utilisé durant le cours; (c) Documentation de cours; (d) repas de midi, incl. boissons; (e) Pauses-café; (f) Attestation de cours.

La formation a lieu dès 4 participants.

Route du Bois 1 | CH-1024 Ecublens | Tél. +41 (0)21 324 32 00 | Fax +41 (0)21 324 32 01 | info@navixia.com | www.navixia.com

navixia
information security

Programme du cours

Footprinting

Comprendre l'importance de restreindre au maximum les informations disponibles sur l'infrastructure interne, le framework et les technologies utilisées afin de ne pas fournir à un attaquant d'informations exploitables pour lancer des attaques spécifiques à des outils ou vulnérabilités. Apprendre à limiter les informations fournies par le code.

Injections (SQL / NOSQL)

Comprendre comment un attaquant peut exploiter certaines propriétés d'une application pour communiquer directement avec la base de donnée et ainsi récupérer ou injecter des données normalement non accessibles. Analyser les méthodes qui permettent de contrôler la saisie des entrées utilisateurs (*sanitize input data*). Apprendre comment un codage approprié permet d'éviter ces risques.

Authentification

Comprendre comment un attaquant peut exploiter les fonctionnalités liées aux procédures de connexion et d'identification des utilisateurs afin d'accéder aux ressources protégées. Apprendre comment éviter ce type de risque dans le code.

Exposition des données sensibles

Comprendre comment et où stocker les informations confidentielles d'une application. Appréhender la différence entre ce qui est accessible par l'utilisateur et les données qui restent exclusivement côté serveur.

Utilisation de composants vulnérables

Comprendre quel type d'attaque peut être exécuté à partir de failles publiques connues et comment prévenir ces risques.

Violation du contrôle d'accès

Comprendre comment un attaquant peut tirer parti de failles dans la procédure de contrôle d'accès pour atteindre des ressources normalement protégées par une authentification. Apprendre à mettre en place les parades nécessaires lors du développement.

Crypto : fonction de hachage

Comprendre pourquoi le hachage des mots de passe est essentiel dans les bases de données. Analyser la robustesse de différentes fonctions de hachage existantes et apprendre en faire usage efficacement.

Crypto : maîtriser les paramètres SSL

Analyser les paramètres d'une configuration SSL et les propriétés d'un certificat SSL.

API sécurisées

Comprendre comment construire une interface de programmation applicative (API) robuste sur le plan de la sécurité. Analyser les différentes méthodes d'authentification d'une API (mot de passe, clé, token). Mettre ces éléments en pratique.

Gestion de session

Comprendre comment gérer les sessions côté serveur et les bonnes pratiques liées au cycle de vie (création, vérification, expiration). Analyser les différents moyens de gérer la session côté client et ses propriétés (longueur, entropie, contenu).

Route du Bois 1 | CH-1024 Ecublens | Tél. +41 (0)21 324 32 00 | Fax +41 (0)21 324 32 01 | info@navixia.com | www.navixia.com