Développement sécurisé

Durée 2 jour(s) (SECU-DEV)

La sécurité des devs par la pratique

Description

La formation d'introduction au développement sécurisé est mise au point et animée par l'équipe de pentesters de Zenika. Le contenu du cours inclut les principes et mécanismes importants du développement sécurisé, nécessaires à la conception et au développement de produits et systèmes sécurisés. Cette formation est un moyen pour nous de faire un pont entre le monde de l'infosec (sécurité de l'information) et le monde du développement. Ces deux mondes sont généralement dissociés alors que leur collaboration pourrait beaucoup leur bénéficier. En s'appuyant sur des vulnérabilités récentes et de la modélisation de risque, nous verrons les principes liés à la grande partie d'une surface d'attaque, en réfléchissant autant du point du vue d'un attaquant qu'un "défenseur". Notre objectif est de donner les clés à un public de développeurs pour qu'ils puissent être à l'aise et comprendre un maximum possible la sécurité de leurs futurs projets en gagnant un regard objectif sur leur surface d'attaque. Grâce aux petits systèmes développés en interne que les stagiaires attaqueront ainsi qu'à l'accompagnement des formateurs, ils/elles auront d'autant plus de bases pour démystifier les potentiels attaques que leurs applications peuvent risquer. Nous pourrons travailler sur les réponses aux questions comme "Mon produit est-il sécurisé ?" ou bien "Quelle est la surface d'attaque de mon produit ?". Nos systèmes de TP fonctionnent à la manière de challenges de hacking (ou CTF : Capture The Flags) via l'implémentation volontaire des vulnérabilités, mais avec l'accompagnement en plus. Les cours exposent de même les différents types de menaces et acteurs potentiels, qu'ils soient de jeunes personnes utilisant aléatoirement des outils de hacking, des groupes criminels, activistes, ou organisations Étatiques.

Objectifs

- Un socle solide de sécurité applicative
- La connaissance de la facilité d'attaques possibles depuis près de 20 ans
- Des bases en test d'intrusion permettant d'automatiser des recherches de vulnérabilités
- Des connaissances générales sur la sécurité de l'information d'aujourd'hui et des menaces actuelles

Public

- Développeurs Juniors, Confirmés
- Chefs de projet

Prérequis

- Programmeur

Répartition

50% Théorie, 50% Pratique

Programme

Introduction

- Menaces
- Objectifs de sécurité : CIDT / CIDP
- Principes de la sécurité applicative :
  - Vue globale
  - Minimiser la surface d'attaque
  - Établir une configuration par défaut sûre
  - Principes de moindre privilège
  - Défense en profondeur
  - Gestion sûre des erreurs
  - Le principe de moindre confiance
  - Segmentation
  - La sécurité par l'obscurité
  - Keep it Simple and Stupid (KISS)
  - Corriger les problèmes de sécurité de manière perenne
- Mécanismes de sécurité
- Lier les mécanismes aux objectifs de sécurité
- Mini démo + mini challenge d'introduction

Authentification

- Préceptes de la sécurité liée à l'authentification
- Pour chaque précepte :
  - Exemples de cas réels (contournement, bruteforce)
  - Application concrète
  - Démonstration d'exploitation et challenge

Permissions

- Préceptes de la sécurité liée aux permissions et autorisations
- Pour chaque précepte :
  - Exemples de cas réels (élevation de privilèges verticales, horizontales, et en diagonale)
  - Application concrète
  - Démonstration d'exploitation et challenge

Gestion de sessions

- Préceptes de la sécurité liée à la gestion de session
- Pour chaque précepte :
  - Exemples de cas réels (vol de session, contournements de sécurité)
  - Application concrète
  - Démonstration d'exploitation et challenge

Validation de données

- Préceptes de la sécurité liée la validation de données
- Pour chaque précepte :
  - Exemples de cas réels (injections de code)
  - Application concrète
  - Démonstration d'exploitation et challenge

Gestion des erreurs

- Préceptes de la sécurité liée à la gestion d'erreur
- Pour chaque précepte :
    - Exemples de cas réels (fuites d'informations)
    - Application concrète
    - Démonstration d'exploitation et challenge

Journalisation

- Préceptes de la sécurité liée à la journalisation
- Pour chaque précepte :
    - Exemples de cas réels (analyses forensics, SOCs)
    - Application concrète
    - Démonstration d'exploitation et challenge

Chiffrement

- Préceptes de la sécurité liée au chiffrement
- Pour chaque précepte :
    - Exemples de cas réels (POODLE, DROWN, Cryptographie faite maison)
    - Application concrète
    - Démonstration d'exploitation et challenge

Intégration

- Préceptes de la sécurité liée à l'intégration d'une application
- Pour chaque précepte :
    - Exemples de cas réels (Attaques relatives aux conteneurs, au Cloud)
    - Application concrète
    - Démonstration d'exploitation et challenge