Développement sécurisé

Durée 2 jour(s) (SECU-DEV)

La sécurité des applications web par la pratique de l'attaque

Description

La formation au développement sécurisé est mise au point et animée par l'équipe de pentesters de Zenika. Le contenu du cours inclut les mécaniques importantes de la sécurité des applications web, nécessaires à la conception et au développement de produits et systèmes sécurisés. Cette formation est un moyen de se mettre dans la peau d'un attaquant et de comprendre comment des personnes malveillantes s'introduisent dans une application web non sécurisée. Notre objectif est de donner les clés à un public de développeurs pour qu'ils puissent être à l'aise et comprendre au mieux la sécurité de leurs futurs projets en gagnant un regard objectif sur leur surface d'attaque. 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.

Objectifs

- Comprendre les motivations des attaquants et les vecteurs d'intrusion
- Connaitre les vulnérabilités les plus communes, ainsi que leur exploitation et comment s'en prémunir
- Utiliser des outils pour tester la sécurité de son application

Public

- Développeurs Juniors, Confirmés
- Chefs de projet

Occuper ou avoir occupé un poste lié au développement facilitera la compréhension globale de la formation

Prérequis

Aucun

Répartition

30% Théorie, 70% Pratique

Evaluations des acquis

L'évaluation des acquis de la formation se fera en séance au travers d'ateliers, d'exercices et/ou de travaux pratiques. Dans le cas d'une formation officielle éditeur, veuillez nous consulter afin que nous vous fassions part des modalités d'évaluation.

A l'issue de la formation, vous sera transmis une évaluation à chaud de l'action de formation qui vous permettra de nous faire part de vos retours quant à votre expérience apprenant avec Zenika.

Ressources pédagogiques

Les ressources pédagogiques proviennent de productions des équipes Zenika et/ou de la documentation éditeur dans le cas d'une formation "Officielle". Les documents sont en français ou en anglais.

RQTH et ma formation Zenika

Si vous êtes sujet à un handicap, prenez contact avec nos équipes pour que nous puissions définir ensemble comment nous pourrons aménager la session afin que vous puissiez vivre une expérience en formation inchangée.

Programme

Introduction

- Menaces
- Objectifs de sécurité : CIDT / CIDP
- Bonnes pratiques de 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 pérenne

Chiffrement

- Vulnérabilités liées au chiffrement
- Stockage des mots de passe

Authentification et session

- Vulnérabilités liées à l'authentification

Pour chaque vulnérabilité :

- Exemples de cas réels (contournement, bruteforce)
- Application concrète
- Démonstration d'exploitation et challenge

Permissions

- Vulnérabilités liées aux permissions et autorisations

Pour chaque vulnérabilité :

- Exemples de cas réels
- Application concrète
- Démonstration d'exploitation et challenge

Validation de données

- Vulnérabilités liées à la validation de données

Pour chaque vulnérabilité :

- Exemples de cas réels (injections de code)
- Application concrète
- Démonstration d'exploitation et challenge

Gestion des erreurs, Journalisation et Monitoring

- Préceptes de la sécurité liée à la gestion d'erreur

Pour chaque précepte :

- Retours d'expérience