Sécurité informatique

CTI FORMATION
Créateur de compétences

Public visé :
Développeurs, concepteurs, personnes qui gérent des sites web.

Pré-requis :
Connaissances du code (PHP, Merise, Java...).

Modalités de suivi / Appréciation des résultats :
Attestation de fin de stage.

Encadrement :
La formation sera assurée par un formateur expert en sécurité informatique.

OBJECTIF

Prendre conscience de l'existence d'un grand nombre de failles web. Exploiter et corriger les failles les plus récurrentes et/ou impactantes. Bénéficier d'outils, de ressources pour la mise en place d'un site web sécurisé.

PROGRAMME

MÉTHODOLOGIE POUR SÉCURISER UN SITE WEB (OWASP)
. Top 10 des failles les plus importantes

INTRODUCTION AU BUG BOUNTY
. Connaître les plateformes existantes (HackerOne, Bugcrowd, OpenbugBounty...) et savoir en tirer parti.

LES CONNAISSANCES EN LIEN AVEC LA SÉCURITÉ
. Défensif ou offensif (Web Application Firewall, Content Security Policy, fonctions PHP dangereuses...)

LA PRISE EN COMPTE DE L'INFRASTRUCTURE DANS LES INCIDENTS DE SÉCURITÉ
. Vulnérabilité logiciel, mauvaise configuration et implémentation de module
. Lister les différentes couches de sécurité.

AVOIR UNE VISION PLUS LARGE DES VULNÉRABILITÉS PRÉSENTES
. Exploiter d'autres vulnérabilités actuelles via des sites vulnérables développés à cet effet.

LES « BEST PRACTICES » À APPLIQUER

MISE EN PRATIQUE
Développer (un à deux modules par jour) un site web comprenant :
. Authentification (SQL injection, XSS)
. Upload de fichier/image (File upload, RCE, Directory traversal, etc.)
. Gestion d'utilisateurs, ajout, suppression... (CSRF, XSS, IDOR, Sensitive data)
. Gestion de profil (CSRF, XSS)
. Post de messages (XSS, XXE)
. Fonction « se déconnecter » (tester la partie « session management »).

ENRICHISSEMENT DU VOCABULAIRE ET DE LA CULTURE GÉNÉRALE EN SÉCURITÉ INFORMATIQUE