

Formation Python : Tests d'intrusion

Durée :	3 jours
Public :	Testeurs d'applications, Développeurs Python
Pré-requis :	Avoir suivi la formation Python Initiation ou connaissances équivalents
Objectifs :	Maîtriser les tests d'intrusion d'applications en utilisant Python
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	PYT100596-F
Note de satisfaction des participants:	Pas de données disponibles

Comprendre le principe des tests d'intrusion

Découvrir le Pentesting, vulnérabilités d'applications et réseaux
Fondements des attaques : réseau, web, SQL
Failles courantes de sécurité

Atelier : installation de l'environnement de développement - présentation des types d'attaques courantes

Introspecter le réseau

Gestion du réseau, principes d'attaque
Interception de paquets réseau (bibliothèque Scapy)
Manipulation de sockets
Frameworks de Fuzzing (bibliothèque Sulley)

Atelier : Interception de paquets - fuzzing de services

Tester une application web

Attaques web
Présentation de la bibliothèque Request
Proxy2 et l'interception applicative
BurpSuite : modèle, développement
Contournement de captcha
Détection de firewalls
Injection SQL
Attaque Slowloris, altération HTTP
MITMProxy
SSL Striping
Forensics

Atelier : réalisation de tests d'intrusion sur une application web

Maîtriser la cryptographie

Cryptographie symétrique, asymétrique
Itérateurs sur des chaînes (bibliothèque itertools)
Attaques cryptographiques en Python

Atelier : attaque cryptographique en Python

Antivirus et portes dérobées

Principe des portes dérobées
Cython : module antivirus et backdoors
Shellcodes

Atelier : Création d'une porte dérobée avancée