+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 27/05/2024

S'inscrire

Formation vAPI sécurité des API

2 jours (14 heures)

PRÉSENTATION

vAPI sécurité (Vulnerable Adversely Programmed Interface) est une plateforme open source basée sur l'interface PHP. Cet outil peut être exploité en tant qu'API autohébergé via PHP, PostMan, MySQL ou exécutée en tant qu'une image de Docker. La sécurité des APIs devient un sujet de préoccupation important. Les API sont de plus en plus utilisées pour gérer des services de transferts de données. Cette plateforme s'adresse aux professionnels de sécurité voulant sécuriser leurs APIs Web modernes. Elle permet aux développeurs d'apercevoir les vulnérabilités de leur code et d'envisager des atténuations potentielles. Elles simplifient les tâches des pentesters qui verront les différents bugs d'API catégorisés. Cette formation vous enseignera l'utilisation de vAPI, la manière de gérer les vulnérabilités, les subpackages et les submodules. Vous découvrirez également les outils tels que MitM, Burp Suite ou Zap. À la suite de notre formation vAPI sécurité, vous saurez gérer la plateforme, sécuriser vos APIs et réduire les surfaces d'attaques.

OBJECTIFS

- Maîtriser la sécurité des API à travers vAPI
- Tester vos vulnérabilités
- Maîtriser des outils de détection de vulnérabilités
- Sécuriser vos APIs

PUBLIC VISÉ

- Développeurs
- Ingénieurs de sécurité
- Testeurs de pénétration
- Professionnels en cybersécurité

Prérequis

- Connaissance de base en PHP, Laravel et MySQL
- Connaissance de base en sécurité des applications web

Programme de notre formation vAPI sécurité

Fondamentaux

- Introduction à vAPI
- Les objectifs de vAPI
- Laravel PHP
- Outils avec Laravel
- Environnement Postman
  - Stocker des appels d'API
- Migration vers une OpeAPI

Package vAPI sécurité

- Subpackages
- Submodules
  - Core module
  - Exception module
  - Message module
- Analyser le contexte de sécurité par la couche de REST
- Créer un contexte pour la session ID
- SSO sécurité

Techniques de test vAPI

- Proxy manipulateur (MitM)
- Burp Suite
- ZAP
- Faire les tests
- Vulnérabilité d'API
  - Credential stuffing

Plateforme vAPI

- Feuille de route vAPI
- Création d'un tableau de bord
- Suivie de progression des utilisateurs
- Le cadre de défis d'API
- Opportunités envisageables de la plateforme

Vulnérabilité dans les plug-ins

- Vulnérabilité avec un plug-in Wordpress
  - WP HTML Mail
- REST API
- Enregistrer les paramètres du thème messagerie
- Vulnérabilité de TeslaMate
- vAPI Endpoint

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.