Updated on 27/05/2024

Sign up

vAPI API security training

2 days (14 hours)

PRESENTATION

vAPI security (Vulnerable Adversely Programmed Interface) is an open source platform based on the PHP interface. This tool can be operated as a self-hosted API via PHP, PostMan, MySQL or executed as a Docker image. API security is becoming a major concern. APIs are increasingly used to manage data transfer services. This platform is aimed at security professionals who want to secure their modern Web APIs. It enables developers to see vulnerabilities in their code and consider potential mitigations. It simplifies the task of pentesters, who will see the various API bugs categorized. This course will teach you how to use vAPIs, manage vulnerabilities, subpackages and submodules. You'll also learn about tools such as MitM, Burp Suite and Zap. Following our vAPI security training course, you'll know how to manage the platform, secure your APIs and reduce attack surfaces.

OBJECTIVES

- Control API security with vAPI
- Test your vulnerabilities
- Master vulnerability detection tools
- Securing your APIs

TARGET AUDIENCE

- Developers
- Safety engineers
- Penetration testers
- Cybersecurity professionals

Prerequisites

- Basic knowledge of PHP, Laravel and MySQL
- Basic knowledge of web application security

vAPI safety training program

Fundamentals

- Introduction to vAPI
- vAPI objectives
- Laravel PHP
- Tools with Laravel
- Postman environment
    - Store API calls
  - Migration to an OpeAPI

vAPI security package

- Subpackages
- Submodules
  - Core module
  - Exception module
  - Message module
- Security context analysis through the REST layer
- Create a context for the ID session
- SSO security

vAPI test techniques

- Manipulator proxy (MitM)
- Burp Suite
- ZAP
- Performing tests
- API vulnerability
  - Credential stuffing

vAPI platform

- vAPI roadmap
- Creating a dashboard
- User progress tracking
- The API challenge framework
- Possible opportunities for the platform

Plug-in vulnerability

- Vulnerability with a Wordpress plug-in
  - WP HTML Mail
- REST API
- Save mail theme settings
- TeslaMate vulnerability
- vAPI Endpoint

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.