Orange Cyberdefense

SensePost Training

Pragmatic API Exploration

INTERMEDIATE LEVEL

Overview

The threat landscape of organizations increases with the adoption of APIs. The content of the course creates awareness around the various attack vectors used to target APIs and provides actionable mitigation strategies.

The aim of this course is to empower you to conduct a risk assessment of an API. This hands-on course covers API basics, API threat model, API protocols and architectures, typical vulnerabilities, enumerating an attack surface and best practices around security.

Moreover, it focuses on gaining practical experience of the OWASP Top 10 for APIs. In addition, you would be gaining practical experience on exploiting typical vulnerabilities on RESTful (REST) APIs and GraphQL. The course concludes with a capture the flag (CTF) to apply knowledge gained during the course.

Who should attend

This course is ideal for any developer looking to further their understanding of security in practise and to widen their understanding of vulnerabilities in APIs.

This course is also ideal for penetration testers looking to advance their API testing skills or those starting out in penetration testing of web and APIs.

Skills you'll learn

- Best Practices
- Exploiting APIs
- OWASP Top 10
- Enumeration

Training in a glance

6 core training modules

26 sub-modules and learning objectives

20 hands-on practicals

16 hours of training

Why our training is great

- Our training is provided by active penetration testers and security analyst
- Our training is hands-on with a course spilt of 40% theory and 60% practical
- We teach offensive methodologies to proactively enhance defensive thinking
- Each student gets their own lab environment during the course to practice real-world attacks

training@orangecyberdefense.com

orangecyberdefense.com

Orange
Cyberdefense

SensePost Training

Pragmatic API Exploration

INTERMEDIATE LEVEL

Course Modules

1. Introduction to APIs
    - Fundamentals of APIs and Web Applications
    - The API ecosystem
    - Threat model of an API
2. Engaging and exploring APIs
    - Understanding the required toolsets
    - Unpacking the base structure of APIs
3. Enumerate the API Attack Surface
    - Finding and exploring target APIs
    - Fuzzing and hidden endpoints
    - Wordlists and toolsets required
4. Demystifying the OWASP Top 10 for APIs
    - API vulnerability classes
    - Exploring and finding vulnerabilities
    - Practical exploitation of vulnerabilities
    - Identification of mitigation strategies
5. Exploring GraphQL
    - Introduction to GraphQL
    - Known vulnerabilities
    - Securing GraphQL
6. Capture The Flag Exercise
    - Combining all the skill taught in the course to discover and exploit an API

All modules contains several practical exercises and sub-objectives.

The above provides a summarised course outline, full course outline available on request.

Key take-aways

Understanding the usage and business context around APIs

Assess and analyse real world APIs with a leading methodology

Understand API security best practises in an applied approach

Prerequisites

A strong familiarity with Linux command line usage and basic security concepts.

No security related experience is required but a technical understanding of computers, networks, Linux and Windows are a must.

What you'll need

A laptop with a modern browser (Chrome or Firefox)

Zoom and/or Microsoft Teams installed

A Discord account

What you'll get

Lifetime access to our online class portal with the course resources and practical answer guides.

Access to our realistic lab environment and attack network during the training

Value for your organisation

Understanding the potential risks associated to APIs and the threats your organization may be susceptible to.

Increased security mindset and best practice knowledge that can actively be applied to the security and defense of APIs and web applications.

training@orangecyberdefense.com
orangecyberdefense.com