Practical DevSecOps

# API Security Professional

COURSE


www.practical-devsecops.com

# API Security Professional

Practical DevSecOps


## A Practical Approach to Agile and Automation Techniques in API Security.

### Abstract

APIs now account for 80% of total Internet traffic, from the cloud to your fridge. While APIs bring new ways of developing and distributing applications, they also introduce new ways for malicious actors to attack enterprise systems.

In this course, you will learn how to identify security issues in your APIs, mitigate them with the proper security measures, and design your APIs for maximum efficiency and minimum exposure to risk. You will reinforce your learning using theoretical lectures, demos, quizzes, and secure design practices with realistic case studies and 40+ hands-on exercises.

You will start the course with API basics, core components of API architecture, and ways to interact with the APIs. Once you learn the fundamentals, you will gain hands-on experience with a series of realistic attack scenarios like Server Side Request Forgery, Broken Authentication, Broken Access Control issues, Injection attacks, Privilege escalation, and Security misconfigurations.

Developers, architects, and security professionals tasked with designing and building secure APIs will benefit immensely from this course. This course imparts professionals with deep knowledge of API security, adopting modern security practices and automation to secure APIs with appropriate techniques, catching security issues before they become critical, and alerting relevant engineers in real-time.

The course also prepares you for the Practical DevSecOps Certified API Security Professional (CASP), a vendor-neutral certification program designed to assess an IT professional's API security expertise.

After completing this course, you will be able to:

1. Challenge and earn the Certified API Security Testing Professional Certification by passing a 6-hour practical exam.
2. Demonstrate your API Security Expertises to your peers and colleagues.

# API Security Professional


## A Practical Approach to Agile and Automation Techniques in API Security.

### Course Prerequisites

1. Course participants should have a basic understanding of Linux Commands and OWASP Top 10.
2. Basic knowledge of application development is preferred but is not necessary.

### Learning Objectives

The following are the course's objectives.

1. Identify, exploit, and protect against a wide variety of API security vulnerabilities.
2. Gain a practical understanding of API Security and the tools for automation.
3. Understand and implement the modern ways of scaling API Security Testing.
4. Gain abilities to audit APIs for security measures and provide solutions.
5. Understand, assess, and secure APIs written in different architecture styles.
6. Learn new ways to secure APIs through automation, and DevSecOps practices.

### Course Syllabus

The curriculum focuses on educating students on API Testing methodologies in the hyper-changing landscape of technology. Prepare you for various vulnerabilities one should be aware of while testing APIs and ensure APIs' secure design and operation.

We will cover the following topics in the course:

1. Introduction to API Security
2. API Security tools of the trade
3. Authentication Attacks and Defenses
4. Authorization Attacks and Defenses
5. Input Validation Threats and Defenses
6. Other API Security Threats
7. Other API Security Defenses
8. Implementing Security Defenses
9. API Security, the DevSecOps Way

# API Security Professional


## A Practical Approach to Agile and Automation Techniques in API Security.

### What Will Students be Provided?

We will provide the students with

1. Course videos and Checklists
2. Course Manual
3. 60 days Online Lab Access
4. 30+ Guided Exercises
5. Access to a dedicated Mattermost channel
6. One exam attempt for Certified API Security Testing Professional Certification

### Course Duration

The participant can complete the course in 36 hours. That includes 8 hours of video lectures and 28 hours of hands-on practice. However, a participant will have 3 years access to the on-demand course with 60 days of online lab access

### Who Should Take This Course?

This course is aimed at professionals interested in performing API Security Testing like Security Professionals, Offensive Security Engineers, Red Teamers, Application Security Engineers, Developers, and DevOps Engineers.

### Software and Hardware Requirements

Our state-of-the-art Training Platform works within your browser. You can even do the labs from your mobile devices like iPad and Android phones. All you need is a modern browser on a laptop or desktop.

***Learn more***

To learn more about our courses, certifications and pricing, please visit **our courses** or **contact us**

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

**DAY 1**

### 1 Introduction to API Security

1. Introduction to Application Programming Interface
    a. What is an API?
    b. Need for an API
    c. Why Should You Secure Your APIs?
    d. APIs vs. Web Applications
2. Understanding API Architecture
    a. Overview of the HTTP protocol
        i. Anatomy of a HTTP Request
        ii. Anatomy of a HTTP Response
        iii. HTTP Response Codes and Its Significance
        iv. Stateless and Stateful Requests
    b. Overview of API architecture
        i. API Protocols
        ii. API Data formats
        iii. Different Types of APIs
    c. Simple Architecture
        i. How Are APIs Typically Deployed?
    d. Complex Architecture
3. Strategies To Secure APIs
    a. Threat Modeling of APIs
    b. Traditional VAPT vs API VAPT
4. API Defenses
    a. Input Validation
    b. Identification
    c. Authentication
    d. Authorization
    e. Data Encryption
    f. Transport Security
    g. Error Handling and Logging

# API Security Professional


## Detailed Syllabus

h. Supply Chain Security

**5. Hands-on Exercises**

a. Understanding an API Language (Endpoints, Verbs, and State)
b. Understanding cURL Command
c. Performing CRUD Operations Using API

## 2 API Security Tools of the Trade

1. The Moving Parts in an API
   a. API Gateway
   b. Load Balancer/Reverse Proxy
   c. Message Queues
2. Critical Toolchain for API Development
   a. Source Code Management
   b. CI/CD Tools
   c. Artifact Management
   d. Cloud Platform
   e. Infrastructure as Code
   f. Monitoring and Logging Tools
   g. Collaboration Tools
3. Containerization
4. Ability To Talk to an API
   a. cURL (curl)
   b. Postman
   c. OpenAPI (Swagger)
   d. Python
   e. An MITM Proxy

**5. Hands-on Exercises**

a. Setup the Burp Suite for API Security Testing
b. Understand APIs Using OpenAPI Specifications
c. Performing Reconnaissance on an API
d. Enumerate User Accounts From an API
e. Hunt for Vulnerable APIs With Subdomain Enumerations

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

### 3 Authentication Attacks and Defenses

1. Overview of API Authentication
2. Types of Authentication
    a. No Authentication (Public APIs)
    b. HTTP Basic Authentication
    c. API Token Authentication
    d. OIDC Authentication
    e. JSON Web Tokens (JWTs)
    f. SAML Tokens
    g. Mutual TLS
3. Authentication Attacks
    a. Brute Force
    b. Weak Password Storage
    c. Password Reset Workflows
    d. Account Lockouts
    e. Insecure OpenID Connect Configuration
    f. Insecure JWTs Validation
4. Authentication Defenses
    a. Secure Authentication Workflows
    b. Strong Password and Key Validation
    c. Multi-Factor Authentication
    d. Securely Storing the Tokens
        i. Cookies
        ii. Local Storage and Session Storage
        iii. Token Storage and XSS
    e. Rate Limiting
    f. CAPTCHA

# API Security Professional


## Detailed Syllabus

**5. Hands-on Exercises**

a. Talking to an API Using Basic, API Token and OAuth and JWTs
b. Exploring Broken Authentication Using API Token, Oauth and JWTs
c. Exploiting Weak Passwords
d. Bruteforcing the passwords
e. Exploiting misconfigurations in scope
f. Forging Tokens
g. Abusing JSON Web Token

**DAY 2**

### 4 Authorization Attacks and Defenses

1. Overview of API Authorization
2. Types of Authorization
   a. No Authorization
   b. Role-Based Access Control (RBAC)
   c. Discretionary Access Control (DAC)
   d. Attribute-Based Access Control (ABAC)
   e. Relationship-Based Access Control (ReBAC)
3. Authorization Attacks
   a. Misconfigured Permissions
   b. Broken Object Level Authorization
   c. Broken Function Level Authorization
   d. Horizontal Privilege Escalation
   e. Vertical Privilege Escalation
4. Authorization Defenses
   a. Defending Object & Function Level Access
   b. Attribute-Based Access Control (ABAC) with Roles, and Relations
   c. Decoupling Authorization Decisions With Policy As Code

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

5. Authorizing with OAuth Framework
    a. OAuth Specification
    b. Different Authorization Workflows
    c. Insecure OAuth Configurations
    d. OAuth 2.0 vs OAuth 2.1
    e. Different Types of Tokens
        i. Access Token
        ii. Refresh Token
        iii. ID Token

**6. Hands-on Exercises**

a. Bypassing Access Control
b. Exploiting Broken Object Level Authorization
c. Exploiting Broken Function Level Authorization
d. Exploiting Weak/Default Permissions
e. Finding Another Cell Phone User's Location

## 5 Input Validation Threats and Defenses

1. Introduction to Input Validation
    a. Input Validation
    b. Input Sanitization
2. Injection Vulnerabilities
    a. Cross-Site Scripting (XSS)
    b. SQL Injection
    c. ORM Injection
    d. NoSQL Injection
    e. Server Side Request Forgery
    f. Deserialization Issues
    g. Mass Assignment Issues

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

3. Fuzzing
    a. Fuzzing 101
    b. Fuzzing vs Brute Forcing
    c. Fuzzing APIs Using Open Source and Commercial Tools
        i. Burp Suite Intruder
        ii. OWASP ZAP Fuzzer
        iii. Wfuzz
        iv. FFUF
4. Injection Defenses
    a. Implementing Input Validation
    b. Client-Side vs. Server-Side Validation
    c. Whitelisting & Blacklisting
    d. Implementing Input Sanitization
    e. Validating With Regular Expressions
    f. Output Encoding
        i. HTML Encoding
        ii. HTML Attribute Encoding
        iii. Javascript Encoding
        iv. CSS Encoding
    g. Prepared Statements
    h. Content Security Policy
    i. Trusted Types
**5. Hands-on Exercises**
    a. Input Validation Using Industry Best Practices
    b. Finding a Way To Get Free Coupons Without Knowing the Coupon Code
    c. Using Vulnerability Assessment Approaches Effectively
    d. Fuzzing APIs Using FFUF
    e. Exploiting Mass Assignment Vulnerabilities

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

### 6 Other API Security Threats

1. Introduction to OWASP API Top 10
    a. Broken Object Level Authorization
    b. Broken Authentication
    c. Excessive Data Exposure
    d. Lack of Resources and Rate Limiting
    e. Broken Function Level Authorization
    f. Mass Assignment
    g. Security Misconfigurations
    h. Injection
    i. Improper Asset Management
    j. Insufficient Logging and Monitoring
    k. Broken Object Property Level Authorization
    l. Unrestricted Resource Consumption
    m. Unrestricted Access to Sensitive Business Flows
    n. Server Side Request Forgery
    o. Improper Inventory Management
    p. Unsafe Consumption of APIs
2. Attacking Caching Layers (Memcache, Proxies, etc.,)
3. Attacking GraphQL APIs
4. Attacking SOAP APIs
5. Abusing Micro-services, and REST APIs
6. Post Exploitation in the API World
7. **Hands-on Exercises**
    a. Bypassing Rate-Limiting
    b. Extract Sensitive Data by Abusing Default API Behavior
    c. Finding and Mitigating an IDOR Vulnerability
    d. Exploiting the CORS Misconfigurations
    e. Exploiting Undisclosed API Calls
    f. Attacking GraphQL APIs

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

**DAY 3**

### 7 Other API Security Defenses

1. GraphQL API Security Best Practices
2. SOAP API Security Best Practices
3. REST API Security Best Practices
4. Data Security
    a. Encoding and Decoding
    b. Escaping
    c. Hashing
    d. Encryption and Decryption
    e. Attacking Caching Layers (Memcache, Proxies, etc.,)
5. Securing Data at Rest Using Encryption
    a. Storing Credentials for Service-to-Service Communication
    b. Password Storage and Its Considerations
    c. Picking a Secure Algorithm
6. Securing Data in Transit Using TLS
7. Rate Limiting Best Practices
8. Security Headers
    a. X-XSS-Protection
    b. HTTP Strict Transport Security (HSTS)
    c. Cache-Control
    d. X-Frame-Options
        i. X-Frame-Options vs frame-ancestors
    e. Content Security Policy
        i. Implementing CSP at Scale
        ii. Common Misconfigurations While Using CSP
    f. Cross-Origin Resource Sharing (CORS)
        i. Cookie Based Implementations
        ii. Token Based Implementations

# API Security Professional


## Detailed Syllabus

**9. Hands-on Exercises**

a. Bypassing CSP Header
b. Configuring HSTS To Prevent MITM Attacks
c. Finding the Missing Security Headers and Fixing Them
d. Implementing Rate Limiting Using API Gateway
e. Preventing DOM Based Cross Site Scripting with Trusted Types

## 8 Implementing API Security Mechanisms

1. API Security Design Best Practices
2. Authentication Implementation
3. Authorization Implementation
    a. Designing API Permissions
    b. Designing OAuth Scopes
4. Rate-Limiting Implementation and Best Practices at Different Stages
    a. Reverse Proxy
    b. Load Balancer
    c. API Gateways and WAFs
    d. Request Throttling
5. Securely Store Secrets Using Hashicorp Vault
6. Data Security Implementation
7. Using Transport Layer Security (TLS)
8. Implementing Sufficient Logging & Monitoring
    a. Secure Logging Implementation
    b. Logging Using Syslog Format
    c. Using ELK To Capture the Log Data

**9. Hands-On Exercises**

a. Implementing a WAF for APIs
b. How To Configure TLSv1.2 and Beyond Securely To Achieve A+ on SSLlabs Scans
c. Adding Content Security Policy Header to an API
d. Second-Order Sensitive Information Leakage

# API Security Professional

Practical DevSecOps


## Detailed Syllabus

### 9 API Security, The DevSecOps Way

1. OWASP ASVS Framework
    a. Understanding OWASP ASVS
    b. Using ASVS To Secure Applications and APIs
    c. Creating Checklists With OWASP ASVS
2. Automated Vulnerability Discovery
3. Finding Insecure Dependencies Using Software Component Analysis
4. Finding Vulnerabilities in Code Using Static Application Security Testing
5. Automating API Attacks Using Dynamic Application Security Testing
6. Addressing API Security Issues at Scale
7. **Hands-on Exercises**
    a. Creating a Simple CI/CD Pipeline
    b. Deploying a Microservice/Docker Container to Production
    c. Exploiting a Microservice Using Docker Misconfiguration
    d. Exploiting a Microservice Using API Vulnerabilities
    e. Finding and Fixing API Security Issues Using SCA, SAST, and DAST in CI/CD Pipelines
    f. Securely Store Secrets Using Hashicorp Vault

# API Security Professional

Practical DevSecOps


## Certification Process

### Exam and certification process

Our certifications are well recognized in the industry as we ensure our students gain practical container security skills. We have a rigorous certification program to ensure we deliver on our promise.

**CASP exam** is an online, task-oriented exam where you attempt to solve five challenges (tasks) in **6 hours.** The exam is based on the content covered in the course but might require further research to pass exam. After the exam,  you have 24 hours to send us the exam report.

***Please note***
it's not an MCQ or tests your memory type of exam but practical applicability of the content covered in the course.

### Exam Pass percentage

The student needs to achieve at least 80 points (80%) to achieve the CASP certification.

### Exam Challenges/tasks

The exam has five challenges for the exam, and each of these challenges provides you points based on how complete or partial your solution was. You would need to score 80 points out of 100 (80%) to achieve the CASP certification.

### Exam documentation

After the exam, you have about 24 hours to send us the exam report via email.

### Steps Involved

A typical certification flow involves five steps.

1. The student schedules the exam.
2. The student will receive an exam guide that includes challenges via email. Our instructors will be there to assist you if you face any difficulty while connecting to the exam lab.
3. The student will connect to the exam lab using details from the exam guide and will attempt the practical exam.
4. After the exam, the student will have 24 hours to send us the exam report.
5. The Practical DevSecOps team will evaluate the report and share the result (pass/fail) with the student.

Practical DevSecOps

# About us

Practical DevSecOps (a Hysn Technologies Inc company) offers vendor-neutral, practical, and hands-on DevSecOps training and certification programs for IT Professionals. Our online training and certifications are focused on modern areas of information security, including DevOps Security, Cloud-Native Security, Cloud Security & Container security. The certifications are achieved after rigorous tests (12-24 hour exams) of skill and are considered the most valuable in the information security field.


@pdevsecops

@pdevsecops

Practical DevSecOps

**USA**

+1 (415) 800 4768
trainings@practical-devsecops.com
201 Spear St #1100, San Francisco, CA 94105

**India**

+91 81216 77008
apac@practical-devsecops.com
Hyderabad, India

**Singapore**

+65 85042132
apac@practical-devsecops.com
531A Upper Cross Street #04-95
Hong Lim Complex Singapore 051531