API101 - DEFENDING WEB APIS

Course Learning Objectives

This course is part of a series for defending web applications and web services.

In five modules, we'll explore modern practices for protecting public and private RESTful APIs from security risks in authentication and authorization, for performing both input validation and output sanitization, for preventing sensitive data exposure in objects, error messages, and log files, for securing communication, for reducing the attack surface of by preventing common attacks like CSRF, DoS, and DDoS, and for deploying Web APIs and updating them to new versions.

Description

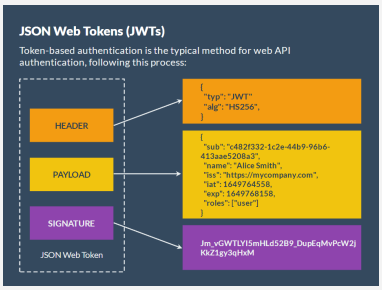
Defending Web APIs is for software developers, architects, and security architects. This course focuses on best practices for securing Web APIs throughout the software development lifecycle.

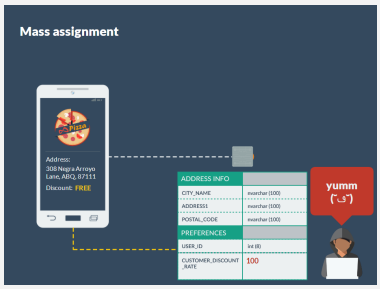
Audience

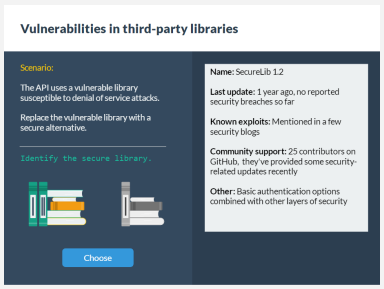
Software Developers
Architects
Software Architects

Time Required

Tailored learning - 70 minutes total







API101 - DEFENDING WEB APIS

Course Outline

1. Choosing an Authentication Strategy

- Private, public, and partner APIs
- Splitting functionalities
- Choosing an authentication type
- Evaluate authentication strategies
- Planning for the future
- API keys
- Best practices for using API keys
- JSON Web Tokens (JWTs)
- JWT security
- Best practices for using token-based authentication
- Stolen tokens
- OAuth
- When to use OAuth

2. Authorizing API Actions

- Authentication and authorization
- Authorization checks
- Best practices for securing an API
- Broken access control
- Preventing broken access control
- Cross-Origin Request Sharing (CORS)
- CORS configuration
- CORS configuration options
- CORS security mistakes

3. Protecting Data

- Transport Layer Security (TLS)
- Excessive data exposure
- Best practices for avoiding excessive data exposure
- Mass assignment
- Best practices for avoiding mass assignment
- Data validation
- Best practices for data validation
- Error messages
- Sending a malicious code
- Avoid vulnerabilities
- Error messages
- Secure handling of error messages

4. Protecting Availability

- About availability
- Traffic-based attacks
- Message size limits
- Strategic endpoint limits and traffic-based defense
- Rate limiting
- Rate limiting policies
- Brute force attacks
- Resource use
- Reviewing code for availability

5. Secure Deployment

- The secure SDLC
- Operational risk analysis
- Version management
- API versioning
- Asset management
- Defense against improper asset management
- Application usage monitoring
- Best practices for keeping your logs safe

SecurityCompass