



MANICODE

SECURE CODING EDUCATION





WEB & API SECURITY CLASSES | JIM MANICO, INSTRUCTOR 3

IronClad Development: Building Secure Web & Web Service Applications 4

Application for Security Managers 6

Application Security for User Interface Developers & Designers 7

ADVANCED WEB SECURITY CLASSES | PHILIPPE DE RYCK, INSTRUCTOR 8

Mastering OAuth 2.0 and OpenID Connect 9

A Builder's Guide to React Security 10

A Builder's Guide to Angular Security 11

Web Application Security Fundamentals 12

Securing Modern REST APIs in NodeJS / Spring Boot 13

JAVASCRIPT WEB SECURITY CLASSES | RON PERRIS, INSTRUCTOR 14

Securing Express Applications 15

Securing React Applications 16

SECURE DESIGN & .NET CLASSES | AVI DOUGLEN, INSTRUCTOR 17

Threat Modeling Workshop 18

.NET Security 19

ESSENTIAL KUBERNETES SECURITY | ABHAY BHARGAV, INSTRUCTOR 21

Essential Kubernetes Security 22

ADVANCED MOBILE SECURITY | SVEN SCHLEIER, INSTRUCTOR 23

iOS Security 24

Android Security 25



WEB & API SECURITY CLASSES

Jim Manico

Jim Manico is the founder of Manicode Security where he trains software developers on secure coding and security engineering. He is also the co-founder of the LocoMoco Security Conference and is a investor/advisor for BitDiscovery and Signal Sciences. Jim is a frequent speaker on secure software practices and is a member of the JavaOne rockstar speaker community. He is the author of *"Iron-Clad Java: Building Secure Web Applications"* from McGraw-Hill. For more information, visit <http://www.linkedin.com/in/jmanico>.

IRONCLAD DEVELOPMENT: BUILDING SECURE WEB & WEB SERVICE APPLICATIONS | 2-3 DAYS, HANDS ON
APPLICATION SECURITY FOR MANAGERS | 1 DAY, LECTURE
APPLICATION SECURITY FOR USER INTERFACE DEVELOPERS & DESIGNERS | 1 DAY, LECTURE

"Jim is a high energy talented programmer. I worked with him on a number of complex coding projects and he did show great skill in organizing and implementing these projects. He does understand the concepts of web development very well, in particular the need for and implementation of security measures. In addition, Jim communicates well and is a great team player."

JOHANNES ULLRICH

"Jim is extremely charismatic, energetic and highly technical. He has unparalleled skill in developing J2EE applications, which are both robust and secure. His knowledge of application security and security architecture is phenomenal, and he is leading a vigorous campaign to change the J2EE spec to make it more secure. I recommend Jim for any development, security or training project."

JERRY HOFF

"Jim taught one of the more recent security classes, and having observed many classes in action I can honestly say he really stood out as an instructor. He very successfully engaged the diverse demographics in the class and convinced all of them why the security issues pertained to their immediate job, and were the concerns of all information employees."

JOSH BROWN

IRONCLAD DEVELOPMENT: BUILDING SECURE WEB & WEB SERVICE APPLICATIONS



Instructor: Jim Manico

Course Length: 2 Days, Hands On

Skill Level: Intermediate

Student Requirements: Familiarity with the technical details of building web applications and web services from a software engineering point of view.

Laptop Requirements: Any laptop that can run a web browser and updated client-side JVM.

Jim's secure coding training classes are designed to benefit any web developer, architect, security professional or other software development professional who needs to build and maintain secure web and web service software. Classes taught by Jim Manico are custom built from the following learning modules. (Please note times are approximate.)

USER INTERFACE SECURITY

XSS Defense <i>Client side web security</i>	2 hr
Content Security Policy <i>Advanced Client side web security</i>	1 hr
Content Spoofing and HTML Hacking <i>HTML based client-side injection attacks</i>	.5 hr
Angular and AngularJS Security <i>Coding Angular applications securely</i>	.5 hr
React Security <i>Coding React applications securely</i>	.5 hr
Vue.js Security <i>Coding Vue.js applications securely</i>	.5 hr

IDENTITY & ACCESS MANAGEMENT

Authentication Best Practices <i>Best practices of web authentication</i>	1 hr
Session Management Best Practices <i>Best practices of web session management</i>	1 hr
Secure Password Storage <i>How to store user passwords for authentication securely</i>	1 hr
Access Control Design <i>How to design modern multi-tenant access control</i>	1 hr
OAuth Security <i>Introduction to the OAuth authorization protocol</i>	2 hr
OpenID Connect Security <i>Introduction to the OpenID connect federation protocol</i>	1 hr

PROCESS

Secure SDLC and AppSec Management <i>Processes around building secure software</i>	1hr
DevOps Best Practices <i>Introduction to DevOps and DevSecOps with a CD/CI focus</i>	1hr

Continued on page 5

Continued from page 4

CORE MODULES

Introduction to Application Security <i>Broad Introduction to Application Security</i>	.5 hr
Introduction to Security Goals and Threats <i>Application Security Terminology Definitions</i>	.5 hr
HTTP Security Basics <i>HTTP Response/Request Headers, Verbs, Secure Transport Basics</i>	1.5 hr
CORS and HTML5 Considerations <i>LocalStorage, HTML5 Sinks, CORS</i>	1 hr
API and REST Security <i>REST Design, XML, XXE, JSON, API Access Control</i>	1 hr
Microservice Security <i>Microservice Security Architectures</i>	1 hr
JSON Web Tokens <i>JWT Security Challenges</i>	.5 hr
SQL and other Injection <i>Parameterization, Database Config, Command/LDAP Injection</i>	1.5 hr
Cross Site Request Forgery <i>CSRF Defenses for multiple architecture types (stateless, API, etc)</i>	1.5 hr
File Upload and File IO Security <i>Multi-Step Secure File Upload Defense, File I/O Security Basics</i>	1 hr
Deserialization Security <i>Safe Deserialization Strategies</i>	.5 hr
Input Validation Basics <i>Whitelist Validation, Safe Redirects</i>	.5 hr

CRYPTO MODULES

Cryptography Fundamentals <i>Introduction to applied cryptography</i>	2 hr
HTTPS/TLS Best Practices <i>Introduction to transport security</i>	1 hr

STANDARDS

OWASP Top Ten 2017 <i>Top Ten Web Security Risks</i>	1 hr
OWASP ASVS 4.0 <i>Comprehensive Secure Coding Standard</i>	1 hr
GDPR <i>European Data Privacy Law</i>	1 hr

ADDITIONAL TOPICS

3rd Party Library Security Management <i>How to detect and manage insecure 3rd party libraries</i>	.5 hr
Application Layer Intrusion Detection <i>How to help detect application layer attacks</i>	.5 hr
Web/Webservice Threat Modeling <i>Introduction to Threat Modeling (Security Design)</i>	1 hr
Multi-Form Workflow Security <i>How to handle complex form workflows securely</i>	.5 hr
Java 8/9/10/11 Security Controls <i>Advances in Java Security</i>	1 hr
Introduction to Cloud Security <i>Introduction to AWS, Docker and Kubernetes</i>	1 hr
Competitive Hacking LABS <i>Hands on Labs!</i>	4 hr

APPLICATION FOR SECURITY MANAGERS



Instructor: Jim Manico

Course Length: 1 Day, Lecture

Skill Level: Intermediate

Course Goals:

- Understand the various stages of a secure SDLC
- Understand the types of attacks specific to application security
- Prepare managers to build contracts and procure software with application security considerations
- Build a business case for application security investment

Student Requirements: Experienced software engineering managers or other software development leaders will benefit most from this class.

Laptop Requirements: Need only to take notes.

Application security excellence requires a wide range of management involvement and activity. From managing procurement, contracts, software development activities and more, application security management touches many aspects of business operations.

Managers need a solid understanding of both the technical and business justifications for these activities in order to be successful.

This one day course will prepare managers to take on a wide variety of challenges in order to successfully guide your organization towards application security excellence.

Classes are custom built from the following learning modules. (Please note times are approximate.)

APPLICATION SECURITY MANAGEMENT TRAINING MODULES

Secure SDLC and AppSec Management	2 hr
Introduction to Threat Modeling	1 hr
OWASP Top Ten 2017	1 hr
OWASP ASVS 3.1	1 hr
3rd Party Library Security Management	.5 hr
Legal and Contract Issues	.5 hr
DevOps Best Practices	1 hr
GDPR, PCI and other Compliance Issues	1 hr

APPLICATION SECURITY FOR USER INTERFACE DEVELOPERS & DESIGNERS



Instructor: Jim Manico

Course Length: 1 Day, Lecture

Skill Level: Beginner

Student Requirements: Familiarity with the technical details of designing and building the user interface portion of web applications (HTML/CSS and some JavaScript).

Laptop Requirements: Any laptop that can run a web browser and updated client-side JVM.

This class is designed to teach web based designers how to build secure user interfaces. This class is primarily for the UI software engineer but any web developer, architect, security professional or other software development professional who needs to build and maintain secure web user interfaces will benefit.

We'll cover the many defensive strategies needed to defeat Cross Site Scripting. We'll also take a close look at building modern Content Security Policies as well as explore defending modern JS frameworks such as React and Angular.

Classes are custom built from the following learning modules. (Please note times are approximate.)

USER INTERFACE SECURITY TRAINING MODULES

Content Spoofing and HTML Hacking	1 hr
XSS Defense	2 hr
Content Security Policy	1 hr
Angular.JS Security	1 hr
React.JS Security	1 hr
XSS Labs	2 hr



ADVANCED WEB SECURITY CLASSES

philippe de Ryck

Philippe De Ryck helps developers protect companies through better web security. As the founder of Pragmatic Web Security, he travels the world to train developers on web security and security engineering. His Ph.D. in web security from KU Leuven lies at the basis of his exceptional knowledge of the security landscape. Philippe is a Google Developer Expert and an Auth0 Ambassador/Expert for his community contributions on securing web applications and APIs.

PRAGMATIC WEB SECURITY | 1-3 DAYS, HANDS ON

"The Advanced Application Security training was amazing! I would definitely take any class taught by Philippe again. He was the best instructor I've ever had (including a \$5000 CISSP boot camp led by ISC2).

All the topics were extremely relevant, educational, and the hands-on labs were beneficial to put all the material we covered in class to practice. Excellent work!!"

SOFTWARE ENGINEER
FORTUNE 500 COMPANY

"Mastering OAuth2 and OpenID Connect was one of the best courses I attended. Philippe is a great instructor. He has the gift of explaining complex topics in a very understandable and structured way. The presentations were perfectly prepared.

I can recommend this course to anyone who is professionally involved with this topic. I am looking forward to the next course from Philippe. Great work. Thank you very much."

JOCHEN HAMMANN
TECHNICAL LEAD, SERVICETRACE

"Dr. Philippe De Ryck is a stellar secure coding instructor. He brings an immense body of web security knowledge to the classroom when teaching his various class offerings. His style is both focused yet inviting which encourages students to participate in class.

It's rare to find professionals who have both the technical ability and presentation skills it takes to be a successful instructor-led-trainer.

Dr. Philippe De Ryck has both and more in spades!"

JIM MANICO
FOUNDER, MANICODE SECURITY

MASTERING OAUTH 2.0 AND OPENID CONNECT



Instructor: Philippe De Ryck

Course Length: 1-2 Days

Skill Level: Advanced

Student Requirements: Familiarity with engineering modern API-based applications

Laptop Requirements: Any device with a browser

OAuth 2.0 and OpenID Connect (OIDC) are crucial for securing web applications, mobile applications, APIs, and microservices. Unfortunately, getting a good grip on the purpose and use cases for these technologies is insanely difficult. As a result, many implementations use incorrect configurations or contain security vulnerabilities.

This course takes you on a step-by-step journey into the latest best practices in the world of OAuth 2.0, OAuth 2.1, and OpenID Connect. This course helps students understand the problems OAuth 2.0 and OpenID Connect solve, and how to use these technologies to address concrete application security requirements. Throughout the course, we discuss the various design and implementation decisions you will face, along with their trade-offs and current recommendations

This course is the product of hundreds of hours spent advising architects and developers on integrating, implementing, and securing OAuth 2.0 and OpenID Connect. After taking this course, students will be able to analyze their systems for potential weaknesses and apply the latest best practices.

The course format is a mixture of lectures, use case analysis, live demos, and interactive quizzes. All demos rely on real-world scenarios and OAuth 2.0/OIDC implementations.

CONTENT

Introduction to OAuth 2.0 and OIDC	3 hr
<i>Overview of the technologies, security challenges and current best practices</i>	
User Authentication with OpenID Connect	2 hr
<i>Designing and building a (federated) identity system</i>	
Using OAuth 2.0 and OIDC in Single Page Applications	1 hr
<i>Recent changes in flow recommendations for frontend web applications</i>	
Securing Tokens in Single Page Applications	1 hr
<i>Security patterns to enhance token security in the browser</i>	
Using Scopes, Roles, and Permissions	1.5 hr
<i>Pitfalls and recommendations on handling authorization with OAuth 2.0</i>	
Securing APIs with OAuth 2.0	1.5 hr
<i>Practical guidelines on making API security decisions with access tokens</i>	
Hardening an OAuth 2.0 and OIDC Architecture	2 hr
<i>Advanced architectural patterns to improve security</i>	
Advanced Attacks Against OAuth 2.0 and OpenID Connect	2 hr
<i>Analysis of advanced attack scenarios and recommended mitigations</i>	

A BUILDER'S GUIDE TO REACT SECURITY



Instructor: Philippe De Ryck

Course Length: 2 Days + Hands-on Labs

Skill Level: Intermediate

Student Requirements: Familiarity with engineering modern React-based applications backed by APIs

Laptop Requirements: Any computer with a browser



React applications disrupt the traditional web security landscape. Techniques such as clientside templating and server-side rendering reshape how vulnerabilities manifest themselves. Additionally, React applications often conflict with advanced browser-based defenses, such as Content Security Policy.

This course covers the changes in the security model of React applications, common threats to an application, framework features that increase security, and state-of-the-art security technology you should start using. This course offers practical and immediately applicable security advice for React developers.

In the first part of the course, students will learn secure coding guidelines for React applications. The course also explains how to leverage existing browser security mechanisms to enhance the security of React applications.

The second part of the course focuses on the interaction between the React application and its APIs. The content of this course will help developers make decisions on managing state, figuring out how to handle Cross-Origin Resource Sharing policies, and clear up any confusion about handling OAuth 2.0/OpenID Connect in React applications.

The course format is a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing students to gain hands-on experience with offensive and defensive technologies.

CONTENT

The Security Model of React Applications <i>Understanding the power and limitations of React security</i>	1 hr
Essential XSS Attacks and Defenses in React <i>Secure coding techniques to avoid pitfalls with React's XSS defenses</i>	1 hr
Mitigating Advanced XSS Attacks in React Applications <i>Finding and fixing advanced XSS problems in React applications</i>	1 hr
Defending React Applications with Content Security Policy <i>Concrete guidelines on using CSP in React applications</i>	1 hr
Content Security Policy Beyond XSS <i>Use cases for CSP as an effective defense-in-depth mechanism</i>	1 hr
Preventing Unauthorized Access in React <i>Avoiding common authorization pitfalls with client-side routing</i>	1 hr
Securing Isomorphic and Server-side Rendered React <i>Overview of security concerns with server-side rendering</i>	1 hr
REST APIs, Sessions and Security <i>In-depth look at challenges with managing authentication state</i>	1 hr
Using JSON Web Tokens for Security <i>Security challenges and patterns of using signed/encrypted JWTs</i>	1 hr
Understanding Cross-Origin Resource Sharing <i>Practical guidelines for deploying a secure CORS policy</i>	1 hr
Introduction to OAuth 2.0 and OIDC <i>Overview of the technologies, security challenges and current best practices</i>	2 hr
Using OAuth 2.0 and OIDC in Single Page Applications <i>Recent changes in flow recommendations for frontend web applications</i>	1 hr
Securing Tokens in Single Page Applications <i>Security patterns to enhance token security in the browser</i>	1 hr
Offensive and Defense Hands-on Labs <i>Guided labs exploiting and solving application vulnerabilities</i>	4 hr

A BUILDER'S GUIDE TO ANGULAR SECURITY



Instructor: Philippe De Ryck

Course Length: 2 Days + Hands-on Labs

Skill Level: Intermediate

Student Requirements: Familiarity with engineering modern Angular-based applications backed by APIs

Laptop Requirements: Any computer with a browser



Angular applications disrupt the traditional web security landscape. Techniques such as client-side templating and server-side rendering reshape how vulnerabilities manifest themselves. Additionally, Angular applications often conflict with advanced browser-based defenses, such as Content Security Policy.

This course covers the changes in the security model of Angular applications, common threats to an application, framework features that increase security, and state-of-the-art security technology you should start using. This course offers practical and immediately applicable security advice for Angular developers.

In the first part of the course, students will learn secure coding guidelines for Angular applications. The course also explains how to leverage existing browser security mechanisms to enhance the security of Angular applications.

The second part of the course focuses on the interaction between the Angular application and its APIs. The content of this course will help developers make decisions on managing state, figuring out how to handle Cross-Origin Resource Sharing policies, and clear up any confusion about handling OAuth 2.0/OpenID Connect in Angular applications.

The course format is a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing students to gain hands-on experience with offensive and defensive technologies.

CONTENT

The Security Model of Angular Applications <i>Understanding the power and limitations of Angular security</i>	1 hr
Essential XSS Attacks and Defenses in Angular <i>Secure coding techniques to leverage Angular's built-in defenses</i>	1 hr
Defending Angular applications with Content Security Policy <i>Concrete guidelines on using CSP in Angular applications</i>	1 hr
Content Security Policy beyond XSS <i>Use cases for CSP as a effective defense-in-depth mechanism</i>	1 hr
Preventing Unauthorized Access in Angular <i>Avoiding common authorization pitfalls with client-side routing</i>	1 hr
Securing Server-side Rendered Angular Pages <i>Overview of security concerns with server-side rendering</i>	1 hr
REST APIs, Sessions and Security <i>In-depth look at challenges with managing authentication state</i>	1 hr
Using JSON Web Tokens for Security <i>Security challenges and patterns of using signed/encrypted JWTs</i>	1 hr
Understanding Cross-Origin Resource Sharing <i>Practical guidelines for deploying a secure CORS policy</i>	1 hr
Introduction to OAuth 2.0 and OIDC <i>Overview of the technologies, security challenges and current best practices</i>	2 hr
Using OAuth 2.0 and OIDC in Single Page Applications <i>Recent changes in flow recommendations for frontend web applications</i>	1 hr
Securing Tokens in Single Page Applications <i>Security patterns to enhance token security in the browser</i>	1 hr
Offensive and Defense Hands-on Labs <i>Guided labs exploiting and solving application vulnerabilities</i>	4 hr

WEB APPLICATION SECURITY FUNDAMENTALS



Instructor: Philippe De Ryck

Course Length: 1-2 Days + Hands-on Labs

Skill Level: Beginner-Intermediate

Student Requirements: Familiarity with basic engineering concepts of web applications (HTTP, HTML, ...)

Laptop Requirements: Any computer with a browser

Building secure web applications requires developer knowledge on security pitfalls and secure coding guidelines. This course provides developers with practical hands-on knowledge to build more secure web applications.

Academic-level security lectures ensure that developers grasp the causes of vulnerabilities and understand how mitigations work. Rather than providing developers with textbook solutions, this course empowers them to analyze the problem and apply the proper mitigation strategy.

During the hands-on lab sessions, developers are challenged to process and apply the learned concepts. In a custom-built competitive lab environment, developers need to solve offensive and defensive challenges against training applications. Doing so helps them understand the mechanics of both attacks and defenses. Hands-on labs are critical to ensure optimal retention of the security material.

At the end of this course, students are guaranteed to be able to find and fix vulnerabilities in their applications. They will have developed a security mindset and will have obtained an invaluable amount of practical security knowledge.

Various companies use this course as the starting point for their AppSec program. While many students are junior developers being introduced to secure coding, even senior developers have indicated that they have learned a ton of new information. In a nutshell, this course is a must-follow for every web developer in your organization.

The course format is a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing students to gain hands-on experience with offensive and defensive technologies.

CONTENT

The Security Model of the Web <i>Foundational security principles for web applications</i>	1 hr
Security Fundamentals for HTTP Applications <i>Common mistakes and best practices for securing web applications</i>	1 hr
Preventing Server-side Injection Vulnerabilities <i>Deep-dive into injection vulnerabilities (SQLi, command injection, ...)</i>	1 hr
Configuring Modern Security Headers <i>Overview of security headers, their configuration, and their effect</i>	1 hr
Best Practices for End-user Authentication <i>Common authentication pitfalls and modern best practices</i>	1 hr
Secure Password Storage <i>Concrete guidelines for securely handling password-based secrets</i>	1 hr
Modern Multi-factor Authentication <i>Modern MFA mechanisms, their security properties, and trade-offs</i>	1 hr
Best Practices for Session Security <i>Defending against common threats, such as session hijacking and session fixation</i>	1 hr
The Impact of HTTPS on an Application <i>Achieving 100% HTTPS deployments in modern browsers</i>	1 hr
The Modern TLS Certificate Ecosystem <i>Modern certificate security techniques, such as transparency and key pinning</i>	1.5 hr
Essential XSS Attacks and Defenses <i>Secure coding techniques to avoid introducing XSS vulnerabilities</i>	1 hr
Mitigating Advanced XSS Attacks <i>Finding and fixing advanced XSS problems</i>	1 hr
Preventing XSS with Content Security Policy <i>Concrete guidelines on using CSP as a second line of defense against XSS</i>	1 hr
Content Security Policy Beyond XSS <i>Use cases for CSP as an effective defense-in-depth mechanism</i>	1 hr
Offensive and Defense Hands-on Labs <i>Guided labs exploiting and solving application vulnerabilities</i>	8 hr

SECURING MODERN REST APIS IN NODEJS/ SPRING BOOT



Instructor: Philippe De Ryck

Course Length: 1-2 Days + Hands-on Labs

Skill Level: Intermediate-Advanced

Student Requirements: Familiarity with building REST APIs and JSON-based APIs

Laptop Requirements: Any computer with a browser



API security is more important than ever, as illustrated by a dedicated OWASP top 10 for common API security vulnerabilities. This course provides API developers with the necessary knowledge to avoid these common vulnerabilities, but also goes a lot further than that.

The academic-level lectures in this course ensure students fully grasp the cause and consequences of each attack. The lectures also explain various mitigation strategies, along with potential trade-offs and best practices.

Unique hands-on lab sessions allow students to gain practical experience with attacks and defenses. A custom-built lab environment guides students as they solve challenges related to the course contents, all in a friendly competitive atmosphere.

At the end of this course, students will be able to assess their APIs' security and identify potential security vulnerabilities. Additionally, students will be able to make informed decisions about proper countermeasures and their impact on the system.

This course is the perfect follow-up for the "Web application security fundamentals" course. This course is available in a NodeJS Express version, and in a Java Spring Boot version.

The course format is a mixture of lectures, demos, interactive quizzes, and hands-on labs. The lectures provide in-depth knowledge of attacks and defenses. The hands-on labs are conducted in a custom-built competitive training environment, allowing students to gain hands-on experience with offensive and defensive technologies..

CONTENT

API Authentication Techniques <i>Strategies for secure user and service authentication</i>	1 hr
Enforcing API Authorization <i>Designing and implementing robust authorization policies</i>	1 hr
REST APIs, Sessions and Security <i>In-depth look at challenges with managing authentication state</i>	1 hr
Understanding Cross-Origin Resource Sharing <i>Practical guidelines for deploying a secure CORS policy</i>	1 hr
Using JSON Web Tokens for Security <i>Security challenges and patterns of using signed/encrypted JWTs</i>	1 hr
Configuring Modern Security Headers for APIs <i>Overview of security headers, their configuration, and their effect on APIs</i>	1 hr
Preventing API Injection Vulnerabilities <i>Deep-dive into API injection vulnerabilities (SQLi, JSON, ...)</i>	1 hr
Advanced API Injection Attacks <i>Defending against modern attacks, such as Server-Side Request Forgery (SSRF)</i>	1 hr
Introduction to OAuth 2.0 and OIDC <i>Overview of the technologies, security challenges and current best practices</i>	2 hr
Using Scopes, Roles, and Permissions in OAuth 2.0 <i>Pitfalls and recommendations on handling authorization with OAuth 2.0</i>	1.5 hr
Securing APIs with OAuth 2.0 <i>Practical guidelines on making API security decisions with access tokens</i>	1.5 hr
Offensive and Defense Hands-on Labs <i>Guided labs exploiting and solving application vulnerabilities</i>	4 hr



JAVASCRIPT WEB SECURITY CLASSES

Ron Perris

Ron provides secure code training and specific remediation guidance through in-person workshops and online courses. As a member of the Node.js Security WG, Ron provides source code review and code remediation guidance to the JavaScript developer community. He authors secure code training courses used by hundreds of organizations worldwide. Ron has taught over 10,000 hours of software developer training with a focus on modern web application construction. Ron founded the Loco Moco Product Security Conference, where industry leaders from Google, GitHub, and Facebook share best practices in software security.

SECURING MODERN WEB APPLICATIONS: APPLIED PATTERNS FOR BUILDING SECURITY IN | 1-3 DAYS, HANDS ON

"I greatly enjoy working with Ron. He is one of those rare people who is deeply knowledgeable about the technical side of things, without losing sight of business requirements and customer needs. He's not afraid of asking (and answering) the hard questions."

BOUKE VAN LAETHEM

"There is really no doubt that Ron knows his Javascript and has an impressive background. Ron really gives detailed breakdowns of all the considerations when you have a problem or a proposed solution you are thinking about. Ron is excellent about making sure his students understand how to attack problems in a variety of ways and the pros/cons of various approaches. He is great about trying to impart a holistic sense of how to think and reason about problems."

ARUN GOPAL

"Ron combines in depth understanding of security with broad technical knowledge and an intimate understanding of business drivers and needs, illustrating his talent and breadth of knowledge in security operations and customer requirements. Ron is unwavering in his commitment to establishing a higher standard of security solutions which sets him apart from his peers. He is a visionary who recognizes industry trends and technological innovations and is able to easily communicate these to wide audiences."

AZIZ MAAKAROUN

SECURING EXPRESS APPLICATIONS



Instructor: Ron Perris

Course Length: 1-3 Days, Hands On

Skill Level: Intermediate

Student Requirements: Familiarity with the technical details of building web applications and web services from a software engineering point of view.

Laptop Requirements: Any laptop that can run a web browser.

Building security into Express applications requires a firm understanding of secure code best practices in the Node.js environment, knowledge of HTTP security mechanisms, and Express framework specific security techniques. This course is for software developers who want to quickly learn best practices they can use immediately. Each aspect of Express security hardening will be shown through real-world examples that will be memorable and relevant to you and your team.

Each module in this course is the product of reviewing hundreds of codebases for security weaknesses and distilling the resulting remediation efforts into patterns that can be applied to any Express application.

The course format is a mixture of lectures, live code review, and hands-on lab work.

An understanding of JavaScript and modern web application construction techniques is recommended to get the most value out of this course.

CORE MODULES

Introduction to Securing Express <i>Overview of the Key Techniques for Building Security In</i>	1h
Defensive Node.js <i>Avoiding Common Attacks with Secure Coding Patterns</i>	1h
HTTP Security Headers in Express <i>Using Helmet.js to Enhance Security</i>	1h
Encrypted Transport with HTTPS/TLS with Express <i>Introduction to transport security concerns in Express applications.</i>	1h
Introduction to REST-based Web Service Security <i>Overview of key techniques and patterns when building RESTful APIs.</i>	1h
IAM features with Express & Node.js <i>User Identity, Authentication and Access Control</i>	1h

ADDITIONAL TOPICS

Intro to Template & Server-side Rendering Security <i>Overview of Template Engine Security Features and SSR Controls</i>	2h
3rd Party Library Security Management <i>How to detect and manage insecure 3rd party libraries.</i>	2h
SQL & noSQL Datastore Security with Express <i>Secure coding patterns for communicating with MySQL, Postgres and MongoDB.</i>	2h
Security Events and Logging <i>Enabling Intrusion Detection, Forensic Analysis, and Regulatory Compliance</i>	1h

LABS

Instructor-led Cooperative Code Remediation Labs <i>Fix code level vulnerabilities live with instructor guidance!</i>	4h
Hacking the OWASP Top 10 <i>Live hacking with Cross Site Scripting, SQL Injection and the rest.</i>	4h

SECURING REACT APPLICATIONS



Instructor: Ron Perris

Course Length: 1-3 Days, Hands On

Skill Level: Intermediate

Student Requirements: Familiarity with the technical details of building web applications and web services from a software engineering point of view.

Laptop Requirements: Any laptop that can run a web browser.

Building security into React applications requires a firm understanding of secure code best practices in both the Node.js and browser JavaScript execution environments. This course is for developers who are familiar with React and want to quickly learn security best practices they can use immediately.

Each module in this course is based on real-world examples from production code that leverages React and its associated tooling and companion libraries. The patterns you will learn in this course were discovered through remediation of these real-world vulnerabilities.

The course format is a mixture of lectures, live code review, and hands-on lab work.

An understanding of React, JavaScript and modern web application construction techniques is recommended to get the most value out of this course.

CORE MODULES

Introduction to Securing React <i>Overview of the Key Techniques for Building Security In</i>	1h
Defensive Browser Executed JavaScript <i>Avoiding Common Attacks with Secure Coding Patterns</i>	1h
XSS Defense in React <i>Powers and Limits of React's XSS Builtin Defense</i>	1h
Content Spoofing and React Component Injection <i>Avoiding Injection Attackers</i>	1h
Isomorphic and Server-side Rendered React <i>Security Concerns when Rendering Server-side</i>	1h

ADDITIONAL TOPICS

Securing React Hooks, Portals and Refs <i>Avoiding Common Mistakes that Lead to XSS</i>	1h
Redux Security <i>State Serialization Attacks and Mitigations</i>	1h
Protecting UI Routes with React Router <i>Secure Implementation of Client-side Routing</i>	1h
Auditing Third-Party React Libraries <i>Avoiding Vulnerable Third-Party React Libraries</i>	1h

LABS

Instructor-led Cooperative Code Remediation Labs <i>Fix code level vulnerabilities live with instructor guidance!</i>	4h
--	----



SECURE DESIGN & .NET CLASSES

Avi Douglan

Avi is a security architect and software developer, and has been involved in building secure products for close to 20 years. His research interests include efficient security engineering, usable security, and scaling enterprise security systems. As CTO of Bounce Security in Israel, Avi consults on software security to development teams of all sizes, and teaches them how to integrate security practices into their process. He is a leader of the OWASP Israel chapter, and created the AppSecIL security conference. He is also a community moderator on <https://security.StackExchange.com/>, and a volunteer high school tech teacher and mentor.

THREAT MODELING WORKSHOP | 2 DAYS, HANDS ON .NET SECURITY | 2 DAYS, HANDS ON

"Avi prepared a course for our architects at Amdocs on Threat Modeling. I must say, Avi is very pleasant to work with and has delivered high quality material. He conducted live training with a good rhythm, ease and fluency. He was very knowledgeable and provided practical examples on the topic at hand. The audience was very satisfied with the session and I am happy to recommend on Avi's services with much confidence."

NADAV ATTIAS

"I've been working with Avi for more than 3 years. As an experienced AppSec specialist, he brought high standards and high-quality work to our research group. Avi's keen eye for details and his clear vision of the big picture makes him a top-notch consultant while his deep technical knowledge with the ability to explain and simplify complex processes makes him a true mentor. I would recommend Avi anytime."

EREZ YALON

"Avi helped the school teachers in teaching networks, information security and operating systems courses, enriching the students with important topics. Additionally, Avi mentored the students in developing their final projects. His contribution to the learning process was significant and helped greatly to understand the material studied as well as the students' successes in the final projects. Avi made a good personal connection with the students, and created a positive and pleasant atmosphere."

SARA SHARON

THREAT MODELING WORKSHOP



Instructor: Avi Douglan

Course Length: 2 Days, Hands On

Skill Level: Intermediate

Student Requirements: Some familiarity with development of a modern web-based application. Some coding experience (any modern language) preferred but not required.

You've decided that your products require a higher level of security, and now you need to start introducing security into your software design process. Threat Modeling is one of the most effective security activities that can be performed for a software application.

Threat modeling is a structured methodology for security-based analysis of a complex system. This can help you identify and prioritize potential threats and attack vectors, and understand the appropriate countermeasures. This can also empower the product teams to contribute to their own security, as well as build customer confidence.

In this hands-on, collaborative working session, the attendees all actively take part in creating the models. Your architects will take turns with each activity, and have an open dialogue around the models to evoke insight and examine our assumptions.

The interactive Workshop will kickstart your security design efforts, teach your teams the skills required to build their own threat models for their products, and train them with tangible hands-on experience so that they are confident to continue the secure design work and grow the ongoing threat models as a basis.

Key Takeaways

After we're done, you'll have the foundation of a threat model for your software application, and your teams will have the ability to continue to build further on this initial model.

Attendees will have the skillset, knowledge, and practical experience to threat model their own applications. They will have done a full, but small-scale threat model process on their own features.

As an added benefit, you will receive the completed threat models for the features we already worked on during the sessions, documented and diagrammed. This will be an excellent starting point from which the architects can easily continue to build the threat model for the rest of their applications.

Target Audience

Product security teams, software architects, senior developers. Pentesters that want to expand.

Threat Modeling Process

Modeling Basics and Tools

Framework and Building Blocks

Decomposing the Application

STRIDE and Other Models

Identifying Threats

Rating Risks

Designing Countermeasures

Retrospective

Integrating with Agile

Full Process Exercise

.NET SECURITY



Instructor: Avi Douglan

Course Length: 2 Days, Hands On

Skill Level: Intermediate

Student Requirements: Familiarity C#, and experience developing web applications and services

Laptop Requirements: Visual Studio

The .NET Framework is an incredibly versatile software platform, and C# is very popular for building large enterprise systems and even lightweight startup websites. It has undergone substantial changes over the last few years, and is supported in a wide range of environments. This secure coding class is designed to teach anyone involved in software development - programmers, architects, QA, PM, or security professional – how to build and maintain secure web and web service software.

CORE MODULES

Introduction to Application Security	1/2 hr
<i>Broad Introduction to Application Security</i>	
Introduction to Security Goals and Threats	1/2 hr
<i>Application Security Terminology Definitions</i>	
HTTP Security Basics	1.5 hr
<i>HTTP Response/Request Headers, Verbs, Secure Transport Basics</i>	
CORS and HTML5 Considerations	1 hr
<i>LocalStorage, HTML5 Sinks, CORS</i>	
Security in ASP.NET MVC and Web API	1 hr
<i>REST Design, XML, XXE, JSON, API Access Control</i>	
JSON Web Tokens	1/2 hr
<i>JWT Security Challenges</i>	
SQL and other Injection	2.5 hr
<i>Parameterization, EF/LINQ, Database Config, Command/LDAP Injection</i>	
Cross Site Request Forgery	1.5 hr
<i>CSRF Defenses for multiple architecture types (stateless, API, etc)</i>	
File Upload and File IO Security	1 hr
<i>Multi-Step Secure File Upload Defense, File I/O Security Basics</i>	
Deserialization Security	1/2 hr
<i>Safe Deserialization Strategies</i>	
Input Validation Basics	1/2 hr
<i>Whitelist Validation, Safe Redirects</i>	

Continued on page 21

Continued from page 20

USER INTERFACE SECURITY

XSS Defense	2 hr
-------------	------

Client side web security

Content Security Policy	1 hr
-------------------------	------

Advanced Client side web security

Content Spoofing and HTML Hacking	1/2 hr
-----------------------------------	--------

HTML based client-side injection attacks

IDENTITY & ACCESS MANAGEMENT

Authentication Best Practices	1 hr
-------------------------------	------

Best practices of web authentication

Session Management Best Practices	1 hr
-----------------------------------	------

Best practices of web session management

Password Policies	1 hr
-------------------	------

What makes up a good password and how to enforce it

Secure Password Storage	1 hr
-------------------------	------

How to store user passwords for authentication securely

Access Control Design	1 hr
-----------------------	------

How to design modern multi-tenant access control

OAuth Security	2 hr
----------------	------

Introduction to the OAuth authorization protocol

OpenID Connect Security	1 hr
-------------------------	------

Introduction to the OpenID connect federation protocol

CRYPTOGRAPHY

Cryptography Fundamentals	2.5 hr
---------------------------	--------

Introduction to applied cryptography

Advanced Cryptography Usage	1 hr
-----------------------------	------

Key management and certificate management

HTTPS/TLS Best Practices	1 hr
--------------------------	------

Introduction to transport security

PROCESS

Secure SDLC and AppSec Management	1hr
-----------------------------------	-----

Processes around building secure software

DevOps Best Practices	1hr
-----------------------	-----

Introduction to DevOps and DevSecOps with a CD/CI focus

Introduction to Threat Modeling	1 hr
---------------------------------	------

Overview of secure design and threat modeling for developers

POSSIBLE ADDITIONAL TOPICS

3rd Party Libraries

Standards (Top10, ASVS, GDPR, etc.)

Differences to ASP.NET Core

Azure Platform and Services



Essential Kubernetes Security

Abhay Bhargav

Abhay Bhargav is the founder of we45, a focused application security company, and Chief Architect of *Orchestron*, a *DevOps First* application vulnerability correlation and management platform. He has created pioneering works in DevSecOps and AppSec automation including the world's first hands-on training program on DevSecOps.

Abhay is a speaker and a trainer at major industry events including DEF CON, BlackHat, OWASP AppSecUSA, EU and AppSec Cali. His trainings have been sold out at AppSecUSA, EU, AppSecDay Melbourne, CodeBlue (Japan), BlackHat USA, and SHACK. He is the author of two international publications *Secure Java: For Web Application Development* and *PCI Compliance: A Definitive Guide*.

ESSENTIAL KUBERNETES SECURITY | 2 DAYS, HANDS ON

"Very good and detailed exposition of what kubernetes is and how it works. Lengthy and detailed explanation of kubernetes concepts. Amazing labs' infrastructure and platform. Extensive lab exercises and very good communication and support."

"I really liked the engagement and the knowledgeable trainers, really helped open my eyes to how many security issues there can be with K8s."

"Easy to use, cook-book style labs. Holistic approach for such a complex area as Kubernetes is, however with deep detailed insight into security and real world use cases."

ESSENTIAL KUBERNETES SECURITY



Instructor: Abhay Bhargav

Course Length: 2 Days, Hands On

Skill Level: Intermediate

Student Requirements:

- Working knowledge of Linux command line
- Basic knowledge of programming language
- Working knowledge of Docker or any container run time
- Basic knowledge of Kubernetes useful but not mandatory

Key Takeaways:

- Practical and in-depth view of both attacking (red team) and defending Kubernetes clusters. Offers deep insight on Kubernetes security configuration, implementation, challenges and limitations.
- Covers unconventional areas of Kubernetes security in terms of security of service mesh implementations and open policy agent.
- Holistic coverage of defense techniques with detailed coverage of Kubernetes defense and vulnerability assessment.

Target Audience:

- AppSec engineers and professionals
- DevOps professionals
- Senior security managers overseeing cloud/DevSecOps initiatives
- Penetration testers
- Cloud engineers

Kubernetes has emerged as the leading container orchestration and management platform for on-prem and cloud environments. However, Kubernetes is a multi-headed beast with several minute and nuanced security configuration parameters. In addition, attackers take advantage of these insecurely configured and designed Kubernetes deployments and perform deep incursions into the organization's assets.

This training is a hard-core hands-on view of Kubernetes security from an attack and defense perspective. The course takes the participants through a journey where they start with setting up a Kubernetes cluster (simulating an on-prem Kubernetes) deployment, attack the cluster and learn, through multiple deep-dive examples and cookbooks on how they can effectively secure Kubernetes clusters.

The course is aimed at providing a view of attacking, auditing and defending Kubernetes clusters on-prem or on the cloud.

At the end of the training participants shall walk away with a comprehensive and practical view of Kubernetes security. We believe that they shall be equipped to address these and many other security concerns with Kubernetes within their own organizations, with a great deal of assurance.

MODULE LIST

Introduction to Kubernetes	2 hr
<ul style="list-style-type: none">• Role of Kubernetes in Container Orchestration• Kubernetes Architecture Deep-Dive• Exploring the Kubernetes Landscape• Deploying Services and Applications on Kubernetes Clusters	
Kubernetes – Red Team	5 hr
<ul style="list-style-type: none">• Kubernetes Threat Model and its Counterpoint in Security Practices• Attacking Kubernetes Clusters	
Kubernetes – Blue Team	8 hr
<ul style="list-style-type: none">• Kubernetes Authentication, Authorization and Admission Control• Kubernetes Secrets• Monitoring Kubernetes Clusters• Open Policy Agent (OPA) on Kubernetes Clusters• Container Runtimes and Impact on Kubernetes Security• Kubernetes Network Security• Kubernetes Vulnerability Assessment and Audit• Kubernetes Continuous Integration and Continuous deployment	



Advanced Mobile Security

Sven Schleier

Sven lives in sunny Singapore and is an application security expert and founder of S7ven Consulting. He has executed hundreds of penetration testing engagements and supported and guided software development projects for mobile and web applications during the whole SDLC. He is a core project leader and co-author of the *OWASP Mobile Security Testing Guide (MSTG)* and *OWASP Mobile Application Security Verification Standard (ASVS)*, and has created the *OWASP Mobile Hacking Playground*.

Sven has given talks and workshops worldwide to audiences, ranging from developers to penetration testers and students. Check him out on [Linked In](#).

iOS MOBILE SECURITY | 1 DAY, HANDS ON
ANDROID MOBILE SECURITY | 1 DAY, HANDS ON

"Sven is very well known in the security industry for his remarkable work done on the OWASP Mobile Security Testing Guide project. He is a hardcore technical leader who is passionate about security and knowledge sharing. I had the opportunity to work with him in many areas from pre-sales to project delivery and he has demonstrated his skills on client relationship management, people leadership and project management. It was a privilege working with him and given the opportunity it would be a pleasure working with him again. I highly recommend Sven to any organisation who wants to make a difference in their security culture!"

— SUMAN SOURAV

<https://www.linkedin.com/in/sumansourav/>

FEEDBACK FROM STUDENTS:

- High level of knowledge and willing to help the students, good job with the apps to test and the presentation.
- As a beginner in this field, I think the delivery was very good and helpful for me. The slides were easy to follow and to understand.
- The training was excellent although I don't have experience in Android or iOS apps it was a very good start for me.
- I like the pace and the instructor's patience to help everyone.
- Very hands on and practically useful skills. Take the theory and make it possible to put into practice!
- The training gave me a much better understanding of mobile security testing, and I now have a list of topics and tools to explore further. Thanks Sven for the training!

iOS SECURITY



Instructor: Sven Schleier

Course Length: 1 Day, Hands On

Lecture Skill Level: Intermediate

Student Requirements:

Basic knowledge about the iOS ecosystem and mobile coding practices

Laptop Requirements:

- macOS device that can run latest Xcode
- An iOS hardware device is **NOT** needed

This course teaches you how to identify security vulnerabilities in (your) iOS Apps. Sven is offering an end-to-end experience where students are given the opportunity to do static analysis of the source code and IPA and do dynamic analysis by executing and analysing the app during runtime. We exploit vulnerabilities, identify best practices and verify their effectiveness. Sven will share his experience and many small tips and tricks to attack and defend mobile apps.

An iOS hardware device is not needed by the participants. The iOS hands-on exercises of the training will instead be executed in a cloud-based virtualised environment that allows attendees to access a jailbroken iOS device during the training. One iOS instance will be provided for each participant.

After successful completion of this course, students will have a better understanding of how to implement an iOS app securely and also how to test for vulnerabilities. The course is based on the OWASP Mobile Security Testing Guide (MSTG), with Sven being one of the main authors. The OWASP MSTG is a comprehensive, open source guide for both iOS and Android and is the de-facto industry standard for Mobile Security.

Classes are custom built from the following learning modules. (Please note times are approximate.)

CORE MODULES

Introduction into mobile security. . . <i>... and it's differences to web application security</i>	.5hr
Overview of the iOS Platform <i>Security Architecture (Code Signing, Sandboxing etc.)</i>	.5 hr
Jailbreaking. . . <i>... and why an attacker doesn't need it to attack your app</i>	.5 hr
Secure Networking <i>Analysing all (non-)HTTP traffic and making it secure with App Transport Security (ATS)</i>	1 hr
Frida Crash Course <i>Understand how attackers use dynamic instrumentation to attack mobile apps</i>	1 hr
Introduction into SSL Pinning <i>Best practices for using and implementing SSL Pinning</i>	1 hr
Static Analysis <i>Automated static analysis of source code and 3rd party libraries</i>	1 hr
Biometric Authentication <i>Making Touch and Face ID bulletproof</i>	1 hr
Introduction into Reverse Engineering Attacks <i>Bypassing detection controls and best practices for implementing client-side security controls in general</i>	1.5 hr
Sensitive Data in Local Storage <i>Secure usage of the KeyChain and best practices for storing data</i>	1 hr
Stateless authentication in Mobile Apps <i>JSON Web Tokens (JWT) and it's security implications</i>	1 hr
Deep Links <i>Avoid business logic vulnerabilities</i>	1 hr
WebViews <i>Secure configuration and common attacks</i>	.5 hr
Capture The Flag (CTF) <i>Investigate an app with the newly learned skills and win a prize!</i>	1 hr

ANDROID SECURITY



Instructor: Sven Schleier

Course Length: 1 Day, Hands On

Lecture Skill Level: Intermediate

Student Requirements:

Basic knowledge about the Android ecosystem and mobile coding practices

Laptop Requirements:

- Any laptop with at least 8GB Ram, 50GB of free storage and full administrative access
- An Android hardware device is **NOT** needed

This course teaches you how to identify security vulnerabilities in (your) Android App(s). Sven is offering an end-to-end experience where students are given the opportunity to do static analysis of the source code and APK and do dynamic analysis by executing and analysing the app during runtime. We exploit vulnerabilities, identify best practices and verify their effectiveness. Sven will share his experience and many small tips and tricks to attack and defend mobile apps.

An Android hardware device is not needed by the participants. The Android hands-on exercises of the training will instead be executed in a cloud-based virtualised environment that allows attendees to access a rooted Android device during the training. One Android instance will be provided for each participant.

After successful completion of this course, students will have a better understanding of how to implement an Android app securely and also how to test for vulnerabilities. The course is based on the OWASP Mobile Security Testing Guide (MSTG), with Sven being one of the main authors. The OWASP MSTG is a comprehensive, open source guide for both iOS and Android and is the de-facto industry standard for Mobile Security.

Classes are custom built from the following learning modules. (Please note times are approximate.)

CORE MODULES

Introduction into mobile security... ... and it's differences to web application security	.5 hr
Overview of the Android Platform Security Architecture (Permission Model, Sandboxing etc.)	.5 hr
Rooting... ... and why an attacker doesn't need it to attack your app	.5 hr
Secure Networking Analyzing all (non-)HTTP traffic and making it secure	1 hr
Frida Crash Course Understand how attackers use dynamic instrumentation to attack mobile apps	1 hr
Introduction into SSL Pinning Best practices for using and implementing SSL Pinning	1 hr
Static Analysis Manual and automated static analysis of source code to identify a Deeplink vulnerability; analysis of 3rd party libraries	1.5 hr
Biometric Authentication Making it bulletproof	1 hr
Introduction into Reverse Engineering Attacks Bypassing detection controls and best practices for implementing client-side security controls in general	1 hr
Sensitive Data in Local Storage Secure usage of the KeyStore and best practices for storing data	1 hr
WebViews Secure configuration and common attacks	.5 hr
Capture The Flag (CTF) Investigate an app with the newly learned skills and win a prize!	1 hr

