
MANICODE
SECURE CODING EDUCATION

MANICODE
SECURE CODING EDUCATION

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 DEVLOPMENT: 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 *Client side web security*	2 hr
Content Security Policy *Advanced Client side web security*	1 hr
Content Spoofing and HTML Hacking *HTML based client-side injection attacks*	.5 hr
Angular and AngularJS Security *Coding Angular applications securely*	.5 hr
React Security *Coding React applications securely*	.5 hr
Vue.js Security *Coding Vue.js applications securely*	.5 hr

IDENTITY & ACCESS MANAGEMENT

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

PROCESS

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

Continued on page 5

Continued from page 4

CORE MODULES

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

CRYPTO MODULES

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

STANDARDS

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

ADDITIONAL TOPICS

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

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

SECURING REACT APPLICATIONS

Instructor: Dr. Philippe De Ryck

Course Length: 1-3 Days

Skill Level: Intermediate-Expert

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, and finding reliable security advice is hard. This course provides React developers with the answers to all their security questions.

With a mix of lectures, demos, quizzes, and hands-on labs, participants discover best practices for building secure React applications. We investigate how to use and configure security mechanisms available in modern browsers. We explore how React handles security, along with common mistakes that circumvent these protections. Additionally, we discuss scenarios that address common questions, including secure data storage in the browser and the use of OAuth 2.0 and OpenID Connect.

This course offers practical and immediately applicable security advice for React architects and developers. Throughout the course, Philippe is available to answer any questions, including concrete scenarios applying to your own applications.

The course consists of 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 participants to gain hands-on experience with offensive and defensive technologies..

CONTENT

The Security Model of React Applications *Understanding the power and limitations of React security*	1 hr
Essential XSS Attacks and Defenses in React *Secure coding techniques to avoid pitfalls with React's XSS defenses*	1.5 hr
Mitigating Advanced XSS Attacks in React Applications *Finding and fixing advanced XSS problems in React applications*	1.5 hr
Defending React Applications with Content Security Policy *Concrete guidelines on using CSP in React applications*	1.5 hr
Content Security Policy Beyond XSS *Use cases for CSP as an effective defense-in-depth mechanism*	1hr
Securing Isomorphic and Server-side Rendered React *Overview of security concerns with server-side rendering*	1 hr
Securing Tokens in Single Page Applications *Security patterns to enhance token security in the browser*	1 hr
OAuth 2.0 and OpenID Connect Best Practices for SPAs *Overview of the technologies, security challenges and current best practices*	1.5 hr
Circumventing OAuth 2.0 security *Identifying and abusing weaknesses in the OAuth 2.0 security model for SPAs*	1 hr
Securing OAuth 2.0 with the Backend-For-Frontend Pattern *In-depth look at securing OAuth 2.0 with the BFF pattern*	1 hr
Offensive and Defense Hands-on Labs *Guided labs exploiting and solving application vulnerabilities*	4 hr

SECURING ANGULAR APPLICATIONS

Instructor: Dr. Philippe De Ryck

Course Length: 1-3 Days

Skill Level: Intermediate-Expert

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

Laptop Requirements: Any computer with a browser

ANGULAR

Angular applications disrupt the traditional web security landscape, and finding reliable security advice is hard. This course provides Angular developers with the answers to all their security questions.

With a mix of lectures, demos, quizzes, and hands-on labs, participants discover best practices for building secure Angular applications. We investigate how to use and configure security mechanisms available in modern browsers. We explore how Angular handles security out-of-the-box, along with common mistakes that circumvent these protections. Additionally, we discuss scenarios that address common questions, including secure data storage in the browser and the use of OAuth 2.0 and OpenID Connect.

This course offers practical and immediately applicable security advice for Angular architects and developers. Throughout the course, Philippe is available to answer any questions, including concrete scenarios applying to your own applications.

The course consists of 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 participants to gain hands-on experience with offensive and defensive technologies.

CONTENT

The Security Model of Angular Applications *Understanding the power and limitations of Angular security*	1 hr
Essential XSS Attacks and Defenses in Angular *Secure coding techniques to leverage Angular's built-in defenses*	1 hr
Advanced XSS Attacks and Defenses *Avoiding XSS pitfalls in Angular and using Trusted Types as a defense*	1 hr
Defending Angular applications with Content Security Policy *Concrete guidelines on using CSP in Angular applications*	1.5 hr
Content Security Policy beyond XSS *Use cases for CSP as a effective defense-in-depth mechanism*	1 hr
Securing Server-side Rendered Angular Pages *Overview of security concerns with server-side rendering*	.5 hr
Securing Tokens in Single Page Applications *Security patterns to enhance token security in the browser*	1 hr
OAuth 2.0 and OpenID Connect Best Practices for SPAs *Overview of the technologies, security challenges and current best practices*	1.5 hr
Circumventing OAuth 2.0 security *Identifying and abusing weaknesses in the OAuth 2.0 security model for SPAs*	1 hr
Securing OAuth 2.0 with the Backend-for-Frontend Pattern *In-depth look at securing OAuth 2.0 with the BFF pattern*	1 hr
Offensive and Defense Hands-on Labs *Guided labs exploiting and solving application vulnerabilities*	4 hr

WEB APPLICATION SECURITY FUNDAMENTALS

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

SECURING MODERN REST APIS IN NODEJS / SPRING BOOT

Instructor: Dr. Philippe De Ryck

Course Length: 1-2 Days + Hands-onLabs

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

KUBERNETES, DEVOPS & CLOUD SECURITY CLASSES

jimmy mesta

Jimmy Mesta is an application security leader that has been involved in Information Security for nearly 10 years. He is the chapter leader of OWASP Santa Barbara and co-organizer of the AppSec California security conference. Jimmy has spent time on both the offense and defense side of the industry and is constantly working towards building modern, developer-friendly security solutions. Jimmy's core focus has been in application and cloud security with an emphasis on secure architecture, automated testing, developer training and defensive techniques.

KUBERNETES SECURITY TRAINING OUTLINE | 1 OR 2 DAYS
DEVOPS PIPELINE TRAINING OUTLINE | HALF-DAY
INTRODUCTION TO CLOUD SECURITY: AZURE OR AWS | 1 DAY

"As Redspin's most senior and experienced web app pentester, Jimmy was frequently called on to break apps of all shapes and sizes, and as one of the most articulate members of the team, Jimmy always did a great job explaining specific findings and recommendations to clients."

ERIC ROGERS

"Over the nearly-three years that I had the pleasure of working with Jimmy, his positive attitude and technical skills constantly impressed me. As he grew professionally and moved up in our organization, his great attitude and ability to acquire new and relevant skills were a constant inspiration to his team."

DAVID SHAW

KUBERNETES SECURITY TRAINING OUTLINE

Instructor: Jimmy Mesta

Course Length: 1 or 2 Days

Skill Level: Intermediate

Laptop Requirements: Modern Web Browser and a steady internet connection

The Cloud as we know it is changing. Containers have taken the center stage as the preferred method of developing and deploying software into production. As security practitioners, we must adapt to the latest technologies or be left in the dust. This course will focus on the ins and outs of building a modern cloud infrastructure capable of taking containers from a developer's laptop to production, in a secure manner. This course will help attendees of all backgrounds gain a practical understanding of containers as well as Kubernetes and help teams responsible for Kubernetes make sane security decisions when moving towards container-based deployments.

Some of the principals and techniques covered in this course will include:

- DevSecOps Overview and Intro to Modern Infrastructure Security Topics
- Introduction to Containers
- Hardening Containers end-to-end
- Introduction to Kubernetes Components and Core Concepts
- Kubernetes Attack Surface
- Kubernetes Network Policies
- Securing a Cluster Using a Service Mesh
- Role-Based Access Control (RBAC)
- Storing Secrets in Kubernetes
- Building DevSecOps Pipelines in Kubernetes
- Data Security and Encryption
- Logging, Monitoring and Alerting
- Hands-on Kubernetes Attack and Defense Live Demonstration

**Heavier on container security if needed (Half-day focus)*

DEVOPS PIPELINE TRAINING OUTLINE

Instructor: Jimmy Mesta

Course Length: Half-Day

Skill Level: Intermediate

Pipelines are an integral piece in moving towards DevOps workflows but can present challenges for security teams in both defending pipelines from attacks as well as utilizing pipelines to secure applications and infrastructure. This course will dive into both sides of the equation. We will clear up common terminology used in modern pipeline infrastructure and then explore ways to make use of pipelines to discover vulnerabilities early and often. Then, we will threat model modern pipeline implementations and learn how to harden the pipeline itself from developer laptop to production.

Some of the principals and techniques covered in this course will include:

- CI/CD Overview
- Lab Setup
- Artifact Management and Supply Chain Security
- Production Security Considerations
- Auditing Pipelines

INTRODUCTION TO CLOUD SECURITY: AZURE OR AWS

Instructor: Jimmy Mesta

Course Length: 1 Day

Skill Level: Intermediate

Laptop Requirements: Modern Web Browser and a steady internet connection

The cloud is here to stay. As development and software delivery moves rapidly towards cloud infrastructure it is imperative we are equipped to address the challenges of security and compliance. Learn common cloud terminology and how to navigate the vast array of security controls that need to be considered when moving to a cloud provider. By the end of this class, you should understand how to address the common security challenges presented when running your software in cloud infrastructure.

Some of the principals and techniques covered in this course will include:

- Introduction to Cloud Security:
  How the Cloud is Changing the Software Security Landscape
- Infrastructure Security: Building a Secure Cloud-Native Infrastructure
- Lab: Setup
- Lab: Security Testing in CI/CD Pipelines
- Data Security in the Cloud:
  Demystifying Keys, Secrets, and Encryption in the Cloud
- Lab: Data Storage
- Serverless and Container Security:
  Securing Modern Software Deployment and Delivery Mechanisms
- Lab: Container and Kubernetes Security
- Monitoring and Alerting:
  Logging and Anomaly Detection in Modern Cloud Environments
- Q&A

SECURE DESIGN & .NET CLASSES

Avi Douglen

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 Douglen

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 Douglen

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

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

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. . . *. . . and it's differences to web application security*	.5hr
Overview of the iOS Platform *Security Architecture (Code Signing, Sandboxing etc.)*	.5 hr
Jailbreaking. . . *. . . and why an attacker doesn't need it to attack your app*	.5 hr
Secure Networking *Analysing all (non-)HTTP traffic and making it secure with App Transport Security (ATS)*	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 *Automated static analysis of source code and 3rd party libraries*	1 hr
Biometric Authentication *Making Touch and Face ID bulletproof*	1 hr
Introduction into Reverse Engineering Attacks *Bypassing detection controls and best practices for implementing client-side security controls in general*	1.5 hr
Sensitive Data in Local Storage *Secure usage of the KeyChain and best practices for storing data*	1 hr
Stateless authentication in Mobile Apps *JSON Web Tokens (JWT) and it's security implications*	1 hr
Deep Links *Avoid business logic vulnerabilities*	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

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

CISO & RESILIENCE CLASSES

Yiannis Pavlosoglou

Yiannis is a cybersecurity executive and founder of KIBERNA, a company specialising in data driven security for managing your cyber risks. With over 20 years of experience in Information Security, he has applied NIST, CERT RMM, and numerous ISO and BSI standards while helping businesses protect their digital assets. Coming from a technical background, he holds a PhD in designing routing protocols, has spent more than 5 years as a professional penetration tester and has committed over 10,000 lines of code for OWASP and others to the public domain. He has successfully held the position of CISO in two countries and is currently volunteering as an elected Board of Directors Member for (ISC)2 where he was elected in 2019 to oversee the CEO for a 3-year tenure. For more information, visit *https://www.linkedin.com/in/yiannisp/*.

THE MINDSET OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) | 1-2 DAY, HANDS ON

CYBER RESILIENCE | 1-1 1/2 DAYS, LECTURE

"If you want real advice on how to be a better CISO, this course is for you"

— CISO, UNDISCLOSED COMPANY IN ENERGY

"Yiannis actually breaks down in layman's terms what it takes to practice Identify, Protect, Detect, Respond and Recover" and be good at it!

– HEAD OF INFORMATION SECURITY

"This course teaches you why cyber resilience is not just a buzz phrase of two words cobbled together, but the most likely next evolution of our industry"

– OPERATIONAL RISK MANAGER

THE MINDSET OF THE CHIEF INFORMATION SECURITY OFFICER (CISO)

Instructor: Yiannis Pavlosoglou

Course Length: 1-2 Days, Hands On

Lecture Skill Level: Intermediate

Student Requirements:
Familiarity with the role and responsibilities of Head of Information Security, Information Security Officer, or Chief Information Security Officer.

Laptop Requirements:
Any laptop that can run a web browser and has Office applications for Word, Excel, and PowerPoint, or equivalent.

This class is designed for those entering, having recently being appointed to, or considering a future career in being a CISO. Key goal for participants is to become effective in their role. The fundamental contradiction we will tackle in this course is that the principles of confidentiality, integrity and availability often do not agree with the rule of business. This is especially true for organisations that are appointing a head of information security for the first time. As no two businesses have the same information security needs, this class is custom build from the following learning modules (times provided below are approximate).

BEFORE TAKING ON THE ROLE

Your reporting line *Why who you report into is important and common reporting line models*	1 hr
Your budget *Researching your potential future employer and what they spend in information security*	1 hr
Your team *Who else works there will determine your capability*	1 hr

YOUR FIRST 100 DAYS

Identify *Your assets*	1 hr
Identify *Your third parties*	1 hr
Protect *Controls you can trust vs Controls you need to change*	1 hr
Detect *Enterprise Logging & Monitoring*	1 hr
Respond *Your first incident – what you need to prepare*	1 hr
Recover *Never waste a good crisis*	1 hr

GOVERNANCE

Popular Frameworks	1 hr
C-Suite Buy-in	1 hr
Committee Structure	1 hr

Continued on page 27

Continued from page 26

CYBER BUSINESS AS USUAL (BAU)

Pennies for the Organisation	1 hr
Pennies for the Team	1 hr
Return on Security Investment (ROSI)	1 hr

CYBER CHANGE AS USUAL (CAU)

Don't fall behind on your controls	1 hr
Establish change governance	1 hr
Return on Security Investment (ROSI)	1 hr

CYBER RISK MANAGEMENT

Committee Structure	1 hr
Cyber Risk Appetite	1 hr
Your team	1 hr

AWARENESS & CULTURE

Your presence each week, each month, each quarter	1 hr
Managing feedback from phishing and other processes	1 hr
Driving behaviors	1 hr

3RD PARTY PROVIDERS

Your cloud providers	1 hr
Security requirements	1 hr
Driving the security industry forward	1 hr

STRATEGY

Your horizons	1 hr
Business Model Canvas	1 hr

SERVICES & PROCESSES

Building your Service Catalog	1 hr
Building the processes that support your services	1 hr
Managing your service posture	1 hr

YOUR TRANSITION

Planning for your Exit	1 hr
Order you Must Leave Behind	1 hr
Handovers	1 hr

YOUR TEAM

Offering Technical & Non-Technical Career Paths	1 hr
Managing your Managers	1 hr
Open door policy and contact with the wider team	1 hr

CYBER RESILIENCE

Instructor: Yiannis Pavlosoglou

Course Length: 1-1 1/2 Days, Lecture

Lecture Skill Level: Intermediate

Laptop Requirements:
Any laptop that can run a web browser and has Office applications for Word, Excel, and PowerPoint, or equivalent.

When you complete this class, you will have a firm understanding of Operational Resilience and Cyber Resilience. This class is for anyone who wants to help their organisation withstand disruptions and adopt their processes during stress or uncertainty. Common fallacy among information security professionals is that resilience is the job of another team, and we should be only concerned about the availability of systems. Looking at recent ransomware attacks, think again, cyber resilience is the key to prevent, adapt, recover and learn from such disruptions.

OPERATIONAL RESILIENCE

Your Organization's Mission and Business Services	1 hr
Understanding and Setting Disruption Service Thresholds	1 hr
Planning for Disruption Scenarios	1 hr

UNDERSTANDING IMPACT TOLERANCE

Service disruption definition	1 hr
Threshold of service tolerances	1 hr
Processes underpinning services	1 hr

UNDERSTANDING CYBER RESILIENCE

Withstanding an Information Security Event	1 hr
Absorbing an Information Security Event	1 hr
Recovering from an Information Security Event	1 hr

RESILIENT THREAT MANAGEMENT

Cyber Threats using the Diamond Adversary Model	1 hr
Layer 8 Hacking	1 hr
Recovering from an Information Security Event	1 hr

MANICODE
SECURE CODING EDUCATION

POB 676, Anahola, HI 96703 | (808) 652-3805 | jim@manicode.com | https://manicode.com

090721