2019 CATALOG
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

JAVASCRIPT WEB SECURITY CLASSES | RON PERRIS, INSTRUCTOR 8
Securing Express Applications 9
Securing React Applications 10

MOBILE, DEVOPS & PENTESTING CLASSES | JIMMY MESTA, INSTRUCTOR 11
Web Application Penetration Testing Fundamentals 13
iOS Attack & Defense 14
ANDROID Attack & Defense 15

ADVANCED WEB SECURITY CLASSES | PHILIPPE DE RYCK, INSTRUCTOR 16
PragmaticWeb Security 17

SECURE DESIGN & .NET CLASSES | AVI DOUGLEN, INSTRUCTOR 19
Threat Modeling Workshop 20
.NET Security 21
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 an 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.

“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
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.

Classes 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 OpenID connect federation protocol
  - 1 hr

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

Continued on page 5
### CORE MODULES

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

### CRYPTO MODULES

<table>
<thead>
<tr>
<th>Module</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptography Fundamentals</td>
<td>2 hr</td>
</tr>
<tr>
<td>Introduction to applied cryptography</td>
<td></td>
</tr>
<tr>
<td>HTTPS/TLS Best Practices</td>
<td>1 hr</td>
</tr>
<tr>
<td>Introduction to transport security</td>
<td></td>
</tr>
</tbody>
</table>

### STANDARDS

<table>
<thead>
<tr>
<th>Standard</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>OWASP Top Ten 2017</td>
<td>1 hr</td>
</tr>
<tr>
<td>Top Ten Web Security Risks</td>
<td></td>
</tr>
<tr>
<td>OWASP ASVS 4.0</td>
<td>1 hr</td>
</tr>
<tr>
<td>Comprehensive Secure Coding Standard</td>
<td></td>
</tr>
<tr>
<td>GDPR</td>
<td>1 hr</td>
</tr>
<tr>
<td>European Data Privacy Law</td>
<td></td>
</tr>
</tbody>
</table>

### ADDITIONAL TOPICS

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

<table>
<thead>
<tr>
<th>Module</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure SDLC and AppSec Management</td>
<td>2 hr</td>
</tr>
<tr>
<td>Introduction to Threat Modeling</td>
<td>1 hr</td>
</tr>
<tr>
<td>OWASP Top Ten 2017</td>
<td>1 hr</td>
</tr>
<tr>
<td>OWASP ASVS 3.1</td>
<td>1 hr</td>
</tr>
<tr>
<td>3rd Party Library Security Management</td>
<td>.5 hr</td>
</tr>
<tr>
<td>Legal and Contract Issues</td>
<td>.5 hr</td>
</tr>
<tr>
<td>DevOps Best Practices</td>
<td>1 hr</td>
</tr>
<tr>
<td>GDPR, PCI and other Compliance Issues</td>
<td>1 hr</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Module</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Spoofing and HTML Hacking</td>
<td>1 hr</td>
</tr>
<tr>
<td>XSS Defense</td>
<td>2 hr</td>
</tr>
<tr>
<td>Content Security Policy</td>
<td>1 hr</td>
</tr>
<tr>
<td>Angular.JS Security</td>
<td>1 hr</td>
</tr>
<tr>
<td>React.JS Security</td>
<td>1 hr</td>
</tr>
<tr>
<td>XSS Labs</td>
<td>2 hr</td>
</tr>
</tbody>
</table>
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 knowledgable 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

“There combine in depth understanding of security with broad technical knowledge and an intimate understanding of business divers 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

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

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

**LABS**
- Instructor-led Cooperative Code Remediation Labs
  - Fix code level vulnerabilities live with instructor guidance!
- Hacking the OWASP Top 10
  - Live hacking with Cross Site Scripting, SQL Injection and the rest

**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**
  - 1h
- **Overview of the Key Techniques for Building Security In Defensive Browser Executed JavaScript**
  - 1h
- **Avoiding Common Attacks with Secure Coding Patterns**
  - 1h
- **XSS Defense in React**
  - 1h
  - Powers and Limits of React’s XSS Built-in Defense
- **Content Spoofing and React Component Injection**
  - 1h
  - Avoiding Injection Attackers
- **Isomorphic and Server-side Rendered React**
  - 1h
  - Security Concerns when Rendering Server-side

### ADDITIONAL TOPICS

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

### LABS

- **Instructor-led Cooperative Code Remediation Labs**
  - 4h
  - Fix code level vulnerabilities live with instructor guidance!
"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

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.

MOBILE, DEVOPS & PENTESTING CLASSES

DEFENDING MODERN DEVOPS ENVIRONMENTS: A HANDS-ON APPROACH | 2 DAYS, HANDS ON
WEB APPLICATION PENETRATION TESTING FUNDAMENTALS | 2 DAYS, HANDS ON
IOS ATTACK & DEFENSE | 1 DAY, HANDS ON
ANDROID ATTACK & DEFENSE | 1 DAY, HANDS ON
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 technical course is geared towards defenders and focuses on the ins and outs as well as the security “gotchas” around building a modern cloud infrastructure capable of taking containers from a developer’s laptop to production Kubernetes clusters.

The hands-on portion of the course will rely heavily on Kubernetes for the deployment and orchestration of Docker containers. Each student will be provided with a production-ready Kubernetes cluster hosted in Google Container Engine (GKE).

All of the principles and tools covered can easily be applied to other cloud providers (AWS, Azure) as well as alternative container orchestration systems (Mesos Marathon, ECS).

KEY TAKEAWAYS
At the completion of this two-day course, students will have an operational, version controlled, deployment pipeline capable of shipping a container to a Kubernetes cluster while performing a number of automated security checks.

Attendees will go home with a deeper understanding of Kubernetes internals and the security blind spots that exist today.

Students will also be exposed to tools and methodologies to efficiently mitigate attacks against Kubernetes infrastructure.

TARGET AUDIENCE
This course is built for a wide variety of skill-sets and interests:

- Developers
- System Administrators
- Offensive Security Testers
- Defensive Security Engineers
- Anyone who is at an organization that is moving towards containers and Kubernetes

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

- DevSecOps Overview
- Cloud Infrastructure Security
- Docker Security Considerations
- Introduction to Kubernetes
- Kubernetes Attack Surface
- Identity and Access Management using RBAC
- Access Control via Network Policies
- Securing a Cluster Using a Service Mesh
- Storing Secrets in Kubernetes
- Building Pipelines in Kubernetes
- Data Security and Encryption
- Logging, Monitoring and Alerting
The Web Application Penetration Testing Fundamentals course is built to arm developers with the skills needed to identify and remediate common web application vulnerabilities. We will kick off the class with an introduction to web application penetration testing methodologies and get acquainted with popular tools used for manual and automated analysis.

The course will be structured around instructor-led labs and utilize intentionally vulnerable web applications to gain hands-on experience attacking web applications.

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

- Anatomy of HTTP Requests
- Reconnaissance and Enumeration
- Application Mapping
- Manual Vulnerability Discovery
- Common Web Application Vulnerabilities (OWASP Top Ten)
- Automated Tooling
- Reporting and Remediation

Instructor: Jimmy Mesta

Course Length: 2 Days, Hands On

Skill Level: Intermediate

Student Requirements: Students enrolled in this course should have a basic understanding of web application vulnerabilities and familiarity with the OWASP Top Ten. An understanding of web application architecture, intercepting HTTP requests, as well as intercepting proxies is an added bonus but not necessary to participate in this class.

Laptop Requirements: Local administrator on laptop preferred (or ability to disable all security software). Minimum 2GB of ram.
The iOS Attack & Defense course covers the latest secure development practices for iOS mobile applications as well as key security features in the iOS ecosystem. This course provides developers with the tools needed to write secure code as well as identify and analyze existing iOS applications for security vulnerabilities.

We will incorporate a combination of lecture and hands-on training utilizing a number of progressive labs.

By the end of the course, attendees will have the tools necessary to perform a basic security audit of an iOS mobile application as well as a fundamental understanding of how to build secure iOS applications.

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

- Introduction to Mobile Application Security Concepts
- iOS Architecture Overview
- Common iOS Application Vulnerabilities
- Setting up an iOS Security Lab
- Analyzing and Exploiting iOS Applications

Instructor: Jimmy Mesta

Course Length: 1 Day, Hands On

Skill Level: Intermediate

Student Requirements: Attendees of this course should have basic familiarity of iOS operating systems as well as knowledge of mobile application terminology. Students should also be comfortable running command-line tools and reading source code.
The Android Attack & Defense course covers the latest secure development practices for Android mobile applications as well as key security features in the Android ecosystem. This course provides developers with the tools needed to write secure code as well as identify and analyze existing mobile applications for security vulnerabilities.

We will incorporate a combination of lecture and hands-on training utilizing a number of progressive labs. By the end of the course, attendees will have the tools necessary to perform a basic security audit of an Android mobile application as well as a fundamental understanding of how to build secure Android applications.

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

- Introduction to Mobile Application Security Concepts
- Android Architecture Overview
- Common Android Application Vulnerabilities
- Setting up a Mobile Security Lab
- Analyzing and Exploiting Android Applications

Instructor: Jimmy Mesta

Course Length: 1 Day, Hands On

Skill Level: Intermediate

Student Requirements: Attendees of this course should have basic familiarity of Android operating systems as well as knowledge of mobile application terminology. Students should also be comfortable running command-line tools and reading source code.
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

“The course consists of high-quality course material. Philippe’s lectures cover the theory in a clear an concise manner. The practical labs in between provide a useful way to get practical experience. We have learned a ton of new security practices, which we will immediately adopt within our development team. The course is highly recommended.”

MATTIAS VANHOUTTE

“Philippe explains very thoroughly, yet in a very interesting and clear fashion how elementary it is for the malicious users to exploit a vulnerability. Obviously and most importantly, countermeasures are presented to help us engineers fix the problems systematically and protect our valuable software systems. The seminars switch between a top-down solid theory behind the security problems and their solutions and hands-on sessions to demonstrate those problems and try the countermeasures in practice.”

ARAM HOVSEPYAN
Building secure applications is more critical than ever. Unfortunately, distributing a couple of cheat sheets among developers does not get you very far. The key to building more secure software is knowledge. Knowledge of the current security landscape. Knowledge of relevant threats and their corresponding mitigation techniques.

This course helps developers grasp the full security picture. Not only do they yield direct results, but they also gear up developers to recognize security issues in future scenarios.

The lab sessions are based on a custom-built training application. This way, participants can try out attacks and defenses in a realistic setting. The traditional training application consists of a servlet-based backend and a JSP-based frontend. The web pages use HTML5 and JavaScript.

Participants are not expected to write chunks of code on the spot. All labs are prepared up front. Security features can be enabled and disabled through configuration files. In all cases, sample solutions are provided.

The training course is custom built from the modules listed below. A training day consists of approximately 6 hours of classes (lectures and labs). During the labs and the breaks, there is plenty of time to answer detailed questions or discuss individual scenarios.

### CORE SECURITY

<table>
<thead>
<tr>
<th>Module</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Security Model of the Web</td>
<td>1 hr</td>
</tr>
<tr>
<td>Browser security mechanisms, security principles, dependencies</td>
<td></td>
</tr>
<tr>
<td>The Basics of HTTP Security</td>
<td>1 hr</td>
</tr>
<tr>
<td>HTTP headers, input validation, authorization</td>
<td></td>
</tr>
<tr>
<td>Server-Side Injection Vulnerabilities</td>
<td>1 hr</td>
</tr>
<tr>
<td>SQL injection, Command injection, other types of injection</td>
<td></td>
</tr>
<tr>
<td>The Impact of HTTPS on an Application</td>
<td>1 hr</td>
</tr>
<tr>
<td>HTTPS basics, mixed content, SSL Stripping, HSTS</td>
<td></td>
</tr>
<tr>
<td>The Modern TLS Certificate Ecosystem</td>
<td>1 hr</td>
</tr>
<tr>
<td>Certificate weaknesses, certificate transparency, public key pinning</td>
<td></td>
</tr>
</tbody>
</table>

### API SECURITY

<table>
<thead>
<tr>
<th>Module</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common API Security Pitfalls</td>
<td>1 hr</td>
</tr>
<tr>
<td>Overview of common mistakes</td>
<td></td>
</tr>
<tr>
<td>JSON Web Tokens (JWT)</td>
<td>1 hr</td>
</tr>
<tr>
<td>JWT basics, signatures, encryption, key management</td>
<td></td>
</tr>
<tr>
<td>REST APIs, Sessions and Security</td>
<td>1 hr</td>
</tr>
<tr>
<td>Cookies, Authorization header, tokens</td>
<td></td>
</tr>
<tr>
<td>Cross-Origin Resource Sharing (CORS)</td>
<td>1 hr</td>
</tr>
<tr>
<td>Cross-origin communication, pitfalls, common mistakes</td>
<td></td>
</tr>
<tr>
<td>Introduction to OAuth 2.0 &amp; OpenID Connect</td>
<td>1-1.5 hr</td>
</tr>
<tr>
<td>The difference between OAuth 2.0 / OIDC, their purpose</td>
<td></td>
</tr>
<tr>
<td>Advanced OAuth 2.0 / OIDC Topics</td>
<td>1-2 hr</td>
</tr>
<tr>
<td>Using it as a client, using it in an API, scopes, permissions</td>
<td></td>
</tr>
</tbody>
</table>

Continued on page 15
# HTML / JAVASCRIPT SECURITY

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-Site Scripting (XSS)</td>
<td>1 hr</td>
</tr>
<tr>
<td>The cause of XSS, reflected/stored XSS, DOM-based XSS</td>
<td></td>
</tr>
<tr>
<td>Advanced Client-Side Injection Attacks</td>
<td>1 hr</td>
</tr>
<tr>
<td>XSS in Angular / React, template injection, script gadgets</td>
<td></td>
</tr>
<tr>
<td>Content Security Policy (CSP)</td>
<td>1 hr</td>
</tr>
<tr>
<td>Using CSP against XSS, CSP level 1 – 2 – 3</td>
<td></td>
</tr>
<tr>
<td>Advanced CSP Concepts</td>
<td>1 hr</td>
</tr>
<tr>
<td>HTTPS basics, mixed content, SSL Stripping, HSTS</td>
<td></td>
</tr>
<tr>
<td>HTML5 Sandbox and SRI</td>
<td>1 hr</td>
</tr>
<tr>
<td>Use cases, sandboxing, subresource integrity</td>
<td></td>
</tr>
</tbody>
</table>

# AUTHENTICATION / AUTHORIZATION

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Best Practices</td>
<td>1 hr</td>
</tr>
<tr>
<td>Password policies, account enumeration, brute force attacks</td>
<td></td>
</tr>
<tr>
<td>Secure Password Storage</td>
<td>1 hr</td>
</tr>
<tr>
<td>Data breaches, cracking passwords, secure password storage</td>
<td></td>
</tr>
<tr>
<td>Multi-Factor Authentication</td>
<td>1 hr</td>
</tr>
<tr>
<td>MFA, SMS-based, token-based, hardware-based</td>
<td></td>
</tr>
<tr>
<td>Implementing Secure Sessions</td>
<td>1 hr</td>
</tr>
<tr>
<td>Cookie weaknesses, cookie flags, cookie prefixes, CSRF</td>
<td></td>
</tr>
</tbody>
</table>

# LABS

<table>
<thead>
<tr>
<th>Course</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free-form tournament-style hacking labs</td>
<td>1-4 hrs</td>
</tr>
<tr>
<td>Guided labs on a training application</td>
<td>2-12 hrs</td>
</tr>
<tr>
<td>Complement lectures with custom labs to improve retention</td>
<td></td>
</tr>
</tbody>
</table>
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.

SECURE DESIGN & .NET CLASSES

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

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

Continued on page 21
Continued from page 20

**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
  - 1/2 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
- **Password Policies**
  - What makes up a good password and how to enforce it
  - 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 OpenID connect federation protocol
  - 1 hr

**CRYPTOGRAPHY**

- **Cryptography Fundamentals**
  - Introduction to applied cryptography
  - 2.5 hr
- **Advanced Cryptography Usage**
  - Key management and certificate management
  - 1 hr
- **HTTPS/TLS Best Practices**
  - Introduction to transport security
  - 1 hr

**PROCESS**

- **Secure SDLC and AppSec Management**
  - Processes around building secure software
  - 1 hr
- **DevOps Best Practices**
  - Introduction to DevOps and DevSecOps with a CD/CI focus
  - 1 hr
- **Introduction to Threat Modeling**
  - Overview of secure design and threat modeling for developers
  - 1 hr

**POSSIBLE ADDITIONAL TOPICS**

- **3rd Party Libraries**
- **Standards (Top10, ASVS, GDPR, etc.)**
- **Differences to ASP.NET Core**
- **Azure Platform and Services**