eLEARNING FOR SECURE APPLICATION DEVELOPMENT

Curriculum

Our Application Security eLearning program will help your team master the concepts they need – from increasing code security to meeting software assurance compliance standards – throughout the development lifecycle.

The self-paced modules are short and interactive with built-in learning quizzes, allowing busy professionals to learn at their own pace and master the material in manageable chunks. Contact us today to learn more.

TABLE OF CONTENTS

info@aspectsecurity.com 301-604-4882 www.aspectsecurity.com

info@aspectsecurity.com 301-604-4882 www.aspectsecurity.com

APPLICATION SECURITY FUNDAMENTALS

100 Introduction to Application Security

OWASP Top 10 *12:30 minutes*

Understand software application risks and see an outline of a practical application security program. Learn to produce and deploy secure applications cost-effectively. Common challenges an organization faces when addressing application security are discussed.

Audience: All Staff, Technical Leaders, Business Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

102 Introduction to the Secure Development Lifecycle

12:45 minutes

Approaches to integrate security into the software development lifecycle (SDLC) are discussed. Consider how to reduce your risk to an acceptable level, deploy applications securely and use standard security controls. Key foundations and activities that development teams can use during design and development to produce secure code are introduced. Topics include security architecture, standard controls, secure delivery and more.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

103 Introduction to Managing Application Security

24:30 minutes

Learn how your organization can take a balanced approach to integrating security into your application development lifecycle. Understand practical and cost-effective approaches for managing application security and the key security principles to consider when designing and acquiring your applications. Learn to build security into the software you produce early and often and examine how to balance the cost of application security against the risks your organization may face.

Audience: Technical Leaders, Business Leaders, Security Architects & Specialists, Software Architects

info@aspectsecurity.com 301-604-4882 www.aspectsecurity.com

ASPECT ADVISORY SERIES

AAS Introduction to Application Security Awareness

PCI 6, OWASP Top Ten *30:00 minutes*

We cut through the hype regarding application security. Get a real-world perspective on Application Security, learn about few recent breaches and understand what you can do to improve your organization's security posture.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS Common Components of an Application Security Program

PCI 6, OWASP Top Ten *30:00 minutes*

How do you develop an application security program for your organization? We explore what a functional application security program looks like and how you can start integrating it into your software development process – regardless of your development cycle's size and complexity. Learn how to assess your current software portfolio by using a risk-based assurance process and how to manage vulnerabilities as they are uncovered.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS Security in the Application Development Lifecycle

PCI 6, OWASP Top Ten *30:00 minutes*

We introduce specific key assurance activities needed for an organization to design, build and deploy secure applications. We highlight the benefits of these activities and show you how they fit into different project types and development approaches. Students will learn how to integrate security into your development lifecycle without creating a burden or a bottleneck.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

info@aspectsecurity.com 301-604-4882 www.aspectsecurity.com
ASPECT SECURITY
Application Security Experts

AAS Overview of ASKD Controls

PCI 6, OWASP Top Ten *30:00 minutes*

The Application Security Knowledge Domains function as key building blocks to Application Security and provide you with a framework for staying focused on what matters most regardless of whether you're acquiring or building an application. We show you how to apply these to your own applications and how you can extend them to your organization's specific technology stack.

Audience: Technical Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS ASKD - Authentication & Identity

PCI 6.5.10, OWASP Top Ten A2 *30:00 minutes*

This course examines the Authentication security control and its constituent parts. Students will review several common real-world Authentication scenarios to understand how the control works in applications and software. Then we look at Authentication from a security perspective, examining the common related issues and threats. Authentication as it relates to the concept of Identity is discussed.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS ASKD - Authorization and Access Control

PCI 6.5.8, OWASP Top Ten A4, A7 *30:00 minutes*

In this course, we review Authorization and Access Control, exploring the different components of the control as well as common faults and attacks. Policy Enforcement Points, Policy Decision Points and Access Control Policy logic are reviewed.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS ASKD - Sensitive Data Protection

PCI 6.5.3, OWASP Top Ten A6 *30:00 minutes*

Safeguarding important information from exposure to unauthorized parties is a key element of application security. In this course, we review the ASKD for Sensitive Data Protection. We examine the components needed to design and implement Sensitive Data Protection controls within a system. Common issues and threats are discussed.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS ASKD - Session Management

PCI 6.5.10, OWASP Top Ten A2 *30:00 minutes*

Session Management security issues are prevalent. Understanding the processes that regulate the communications between an entity (e.g., a user) and a relaying party (e.g., your application) is an important part of implementing the Session Management security control. Understanding when to start, refresh, and terminate a session is critical. This course covers the individual components of this security control as well as its related issues and threats.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS ASKD - Validation and Encoding

PCI 6.5.1, OWASP Top Ten A1, A3 *30:00 minutes*

Validation and Encoding controls are paramount to preventing Cross-Site Scripting, SQL Injection and a host of other attacks. This course identifies the key components needed to successfully design and implement Validation and Encoding controls. Common issues and threats related to the control are examined.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS ASKD - Logging and Audit

PCI 6.5.5, OWASP Top Ten A5 *30:00 minutes*

The Logging and Auditing security control often get overlooked when building a system, yet is critical to detecting and thwarting data breaches. This course examines the control's constituent parts and walks students through several common, real-world scenarios. Common issues and threats related to Logging and Audit controls are discussed.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

AAS PCI DSS for Application Security Professionals

PCI, OWASP Top Ten *30:00 minutes*

PCI DSS, also known as the Payment Card Industry Data Security Standard, is an international standard that governs the way merchants accept, process and protect credit card data within their systems. We provide an overview of the latest version of the standard (PCI DSS, version 3.2, released in April 2016) and discuss the areas particularly relevant to Application Security.

Audience: Technical Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

info@aspectsecurity.com 301-604-4882 www.aspectsecurity.com
ASPECT SECURITY
Application Security Experts

IMPLEMENTING APPLICATION SECURITY PROGRAMS

421 Application Security Risk Management

15:00 minutes

Learn to identify key application risk management standards to help stakeholders agree on the fundamentals. Understand how to identify and prioritize your application portfolio. Finally, produce compelling dashboards that make application security visible within your organization. To fully benefit from this module, you should have a basic understanding of Security Verification and the Software Development Lifecycle.

Audience: Technical Leaders, Business Leaders, Security Architects & Specialists, Software Architects

450 Integrating Security into Waterfall Projects

22:15 minutes

Explore methods of integrating security activities into a waterfall-style project. Understand how to integrate key security activities throughout the development lifecycle, from threat modeling to secure deployment and operation. Learn efficient approaches to reduce security risks to an acceptable level and build assurance evidence of an application's security posture. To fully benefit from this module, learners should have a working understanding of application security issues and software development processes.

Audience: Technical Leaders, Business Leaders, Security Architects & Specialists, Software Architects

460 Integrating Security into Agile Projects

19:50 minutes

The sprint structure of Agile projects makes them challenging for traditional approaches to application security, which track the stages in waterfall-style. Learn to integrate security into Agile projects by establishing Agile secure foundations, integrating security activities into sprints and developing job aids to expedite the process. Learners should have a working understanding of application security issues and Agile software methods.

Audience: Technical Leaders, Business Leaders, Security Architects & Specialists, Software Architects

SECURE TESTING & VERIFICATION

101 Introduction to Application Security Verification

12:00 minutes

Application security verification is the process of ensuring that an application (or group of applications) use appropriate security controls properly and do not contain vulnerabilities. Learn the benefits of a positive approach to application security verification. Understand the differences between security verification and penetration testing as well as the techniques and tools that can be incorporated into your process.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

411 Effective Security Testing

18:20 minutes

Learn a proven, repeatable process for scoping, structuring, executing and documenting an application security test. Understand how to plan the resources and access you need, identify testing targets, design your tests and report on the results. To benefit fully from this module, learners should understand common vulnerabilities and security verification methodologies.

Audience: Security Architects & Specialists, Testers

412 Effective Security Code Review

19:40 minutes

Understand the goals of an effective code review and how to plan a tailored code review strategy. Learn how tools complement manual processes. Hear strategies to effectively review large-scale enterprise applications. To get the most out of this module, students should also have completed prior modules on or have an advanced understanding of authentication strategy, enforcing access control and input validation.

Audience: Security Architects & Specialists, Testers

420 Threat Modeling and Security Architecture Review

17:30 minutes

Threat modeling and security architecture reviews effectively identify vulnerabilities throughout the software development lifecycle (SDLC). Learn a framework to organize security controls, threat agents, business functions and more to make security visible. Learners should have a high-level understanding of application security attack vectors and security verification processes.

Audience: Technical Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Software Architects

SECURE APPLICATION DEVELOPMENT

Introduction to Secure Coding

281 Introduction to Secure Coding for Rich Internet Applications

13:40 minutes

Understand the security threats to all stakeholders (server to client, client to server, client to client) in a Rich Internet Applications (RIA). Learn the guidelines for developing and deploying safer code for your applications. Learners should have a basic background in RIA technology and a foundational knowledge of application security.

Audience: Web & Mobile Developers, Security Architects & Specialists

282 Introduction to Secure Coding for AJAX Applications

16:00 minutes

Understand the challenges of securing AJAX-enabled web applications. In addition to securing the server using traditional web security techniques, the AJAX interface (which fields XML HTTP requests) must be protected. Learn how to minimize attack surfaces, control access to data and functions, protect against injection, and prevent forged requests. To benefit fully from this module, learners should be familiar with the basic workings of AJAX applications including XHR and HTTP.

Audience: Web & Mobile Developers, Security Architects & Specialists

283 Introduction to Secure Coding for Java

18:00 minutes

Secure Java applications by using a set of standard security controls to avoid the five most critical security vulnerabilities. Additionally, learn to test the security of these applications. To benefit fully from this module, learners should be familiar with the basic workings of web applications, including HTML and HTTP. Knowledge of Java web technology is also required.

Audience: Web & Mobile Developers, Security Architects & Specialists

284 Introduction to Secure Coding for .NET Applications

27:15 minutes

Understand the risks associated with .NET applications, basic methods of secure coding and how to test applications. The module will focus on the need for security controls, the five most critical security areas for .NET applications and how to verify an application's security. To benefit fully from this module, learners should be familiar with the basic workings of web applications, including HTML and HTTP. Knowledge of .NET web technology is also required.

Audience: Web & Mobile Developers, Security Architects & Specialists

285 Introduction to Secure Coding in C and C++

27:15 minutes

C++ consists of the Standard Library and the Standard Template Library which together provide a rich set of methods and functions to solve common programming tasks. As these libraries have evolved, there are now several methods and functions that perform the same task. What's important to know is that these libraries are prone to misuse – causing more security issues than others. This course provides guidance on common issues and security vulnerabilities in C and C++ so that you can develop software more securely.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

Input Validation

110 Input Validation

PCI 6.5.1; OWASP Top Ten A1 *16:00 minutes*

This module defines Input Validation, provides basics for verifying whether an application is vulnerable to Input Validation attacks and discusses common defense techniques. To benefit fully from this module, learners should be familiar with the basic workings of web applications including HTML and HTTP.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

180 Buffer Overflows

PCI 6.5.2 *41:50 minutes*

Buffer Overflows, sometimes called Buffer Overruns, are one of the most common and dangerous software vulnerabilities. Verify if an application is vulnerable to buffer overflow attacks and learn common techniques for defending against this category of attacks. To fully benefit from this module, students should have an advanced understanding of Input Validation as well as a basic understanding of programming languages that can suffer from buffer overflow vulnerabilities, primarily C and C++.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

211 Input Validation Strategy

PCI 6.5.1; OWASP Top Ten A1, A3 *30:40 minutes*

Get an overview of basic defenses against input manipulation and injection attacks. Strategies discussed include minimizing input to the application, validating incoming data and sanitizing outgoing data. A review of the common pitfalls of Input Validation will facilitate exploring new strategies. To benefit fully from the module, learners should be familiar with the basic workings of web applications, including HTML and HTTP.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Software Architects

212 Preventing Injection Attacks

PCI 6.5.1; OWASP Top Ten A1 *19:50 minutes*

Learners are introduced to injection flaws, common injection attacks and basic defenses against injection. We delve into key concepts including: interpreters, common injection vulnerability patterns, injection attacks and defenses, utilizing static commands and more. Basic knowledge of SQL, HTML, XML, and command line shells is helpful, but not required.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Software Architects

213 Preventing Cross-Site Scripting Attacks

PCI 6.5.7; OWASP Top Ten A3 *21:05 minutes*

This module details different types of Cross-Site Scripting (XSS) vulnerabilities and how they can be exploited. Discover how to find XSS flaws and evaluate their exploitability. Learn prevention strategies including how to properly escape output in different contexts in HTML.

Audience: Web & Mobile Developers, Security Architects & Specialists

214 Using Canonicalization and Encoding

OWASP Top Ten A1 *23:20 minutes*

This introduction to canonicalization and encoding covers why proper decoding and encoding is critical to performing effective Input Validation and identifying attacks. To benefit fully from this module, learners should be familiar with the basics of Input Validation and defending against injection attacks.

Audience: Web & Mobile Developers, Security Architects & Specialists

215 Performing Secure File Uploads and Downloads

PCI 6.5.1; OWASP Top Ten A4 *12:10 minutes*

The complexities of implementing file uploads and downloads securely in a web application are addressed. Validating upload requests, storing files carefully as well as testing file and upload features for vulnerabilities are covered. Learners should be familiar with HTTP and basic Input Validation techniques.

Audience: Web & Mobile Developers, Security Architects & Specialists

216 Preventing Header Injection

PCI 6.5.1; OWASP Top Ten A1 *18:00 minutes*

Challenges related to HTTP header injection and attack consequences are covered. Learn techniques to verify whether an application is vulnerable to header injection and how to defend against these attacks. To fully benefit from this module, learners should be familiar with HTTP and injection techniques.

Audience: Web & Mobile Developers, Security Architects & Specialists

331 Understanding DOM-Based XSS

OWASP Top Ten A3 *16:15 minutes*
Understand DOM-Based XSS, a specific type of Cross-Site Scripting (XSS) vulnerability. Learn how to recognize this vulnerability and prevent it from appearing in your code. For maximum understanding of this module, learners should be familiar with Reflected and Stored XSS.

Audience: Web & Mobile Developers, Security Architects & Specialists, Software Architects

Access Control/Authorization

120 Access Control

PCI 6.5.8; OWASP Top Ten A7 *15:30 minutes*
Understand how to limit the access of authenticated users to the resources and functions in your web application. Learn techniques to verify that an application is free from Access Control vulnerabilities along with attack defense methods. To benefit fully from this module, learners should understand the basics of authentication.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

221 Access Control Strategy

PCI 6.5.8; OWASP Top Ten A7, A4 *17:00 minutes*
Approaches for defining and enforcing Access Control policies are introduced. Core concepts are discussed and applied to typical web application architectures, including enforcing Access Control at the URL, business logic, data and presentation layers. Techniques for verifying application Access Control implementations are also discussed. To fully benefit from this module, learners should be familiar with the basics of Authentication.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Software Architects

222 Presentation Layer Access Control

PCI 6.5.8; OWASP Top Ten A7 *12:45 minutes*
Learn to identify potential vulnerabilities in the presentation layer. Understand how these vulnerabilities can affect the security of your application and how to defend against presentation layer attacks. Topics covered include forced browsing and direct object references. To fully benefit from this module, learners should be familiar with access control strategy.

Audience: Web & Mobile Developers, Security Architects & Specialists

223 URL-Based Access Control

PCI 6.5.8; OWASP Top Ten A7 *19:10 minutes*

Learn effective strategies for URL-based Access Control. Understand common attacks and how to defend against them. Discover techniques to verify the strength your application's URL-Based Access Control implementation. To fully benefit from this module, learners should be familiar with HTTP and access control strategy.

Audience: Web & Mobile Developers, Security Architects & Specialists

224 Business Layer Access Control

PCI 6.5.8; OWASP Top Ten A7 *17:40 minutes*

Learn techniques to enforce Access Control for business functions and how to verify business layer Access Control through testing and code review. Understand how the business layer can be exploited and how to implement protections in a simple, structured manner. To fully benefit from this module, learners should be familiar with Access Control strategy.

Audience: Web & Mobile Developers, Security Architects & Specialists

225 Implementing Data Layer Access Control

PCI 6.5.8; OWASP Top Ten A7, A4 *12:00 minutes*

Learn to secure sensitive data stored by your application. Data Access Control is a security mechanism that ensures that users are only allowed to access authorized data based on the user's identity, roles, and/or permissions. Common attacks on application data and strategies for defending against them are discussed. To get the most from this module, learners should be familiar with Access Control strategy.

Audience: Web & Mobile Developers, Security Architects & Specialists

226 Unsafe Redirects and Forwards

OWASP Top Ten A10 *17:45 minutes*

Learn how attackers exploit unsafe redirects and forwards. Understand how to eliminate these vulnerabilities by minimizing the use of untrusted data and validating all untrusted data used. Access Control concerns associated with performing server-side forwards are covered. To get the most from this module, learners should understand the basics of HTTP and Input Validation.

Audience: Web & Mobile Developers, Security Architects & Specialist

227 Clickjacking

OWASP Top Ten A7 *16:10 minutes*

Understand Clickjacking, a common attack where attackers frame pages from other sites to hijack a victim's mouse clicks on a trusted website to authorize invocation of a function of the attacker's choosing rather than the function the user intended to authorize. Learn the risks of Clickjacking flaws as well as how to test and defend against these vulnerabilities.

Audience: Web & Mobile Developers, Security Architects & Specialists

Authentication

130 Authenticating Users

PCI 6.5.10; OWASP Top Ten A2 *27:50 minutes*

User authentication is defined, common attacks and vulnerabilities are discussed, and strategies to defend against attacks and avoid vulnerabilities are provided. Credentials, cookies, sessions and user management are covered. To benefit fully from this module, learners should be familiar with the basics workings of web applications including HTML and HTTP.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialist

231 Authentication Strategy

PCI 6.5.10; OWASP Top Ten A2 *17:30 minutes*

Understand the techniques used by web applications to authenticate users and handle identity. Strengths and weaknesses associated with different authentication schemes are examined, recommendations to minimize authentication vulnerabilities are provided and techniques to verify authentication schemes are shown. To benefit fully from this module, learners should be familiar with the basic workings of web applications, HTTP and sessions.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Software Architects

232 Understanding HTTP Authentication Schemes

OWASP Top Ten A2 *18:50 minutes*

Understand how authentication and sessions work in HTTP as well as common attacks on authentication schemes – including brute force attacks, session hijacking and session fixation. Learn to avoid authentication and session attacks, as well as how to properly implement logout functions. To fully benefit from this module, learners should understand HTTP and sessions.

Audience: Web & Mobile Developers, Security Architects & Specialists

233 Secure Session Management

PCI 6.5.10; OWASP Top Ten A2 *16:50 minutes*

Session hijacking allows user sessions to be taken over by an attacker. Learn how to determine if applications are vulnerable to session management attacks and how to defend against them. To fully benefit from this module, learners should be familiar with HTTP and authentication strategy.

Audience: Web & Mobile Developers, Security Architects & Specialists

234 Protecting Credentials

OWASP Top Ten A2 *18:20 minutes*

Understand how to protect user, application and systems credentials, both in transit and in storage. This module will show how to build standards that will ensure protected credentials across all of your applications as well as how to verify that your applications are correctly protecting credentials.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

235 Managing Identity within an Application

OWASP Top Ten A2 *13:00 minutes*

Identity is one of the most critical areas in application security. This module will help you make architectural decisions about managing identity and avoid common pitfalls. To benefit fully from this module, learners should have a basic understanding of authentication strategy.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

236 Preventing Forged Requests (CSRF)

PCI 6.5.9; OWASP Top Ten A2 *14:15 minutes*

Cross-Site Request Forgery (CSRF) allows an attacker to trick a victim's browser into issuing requests to a vulnerable web application. Learn techniques to check applications for CSRF vulnerabilities and defend against attacks. To benefit fully from this module, learners should be familiar with the basic workings of web applications, including HTML and HTTP. They should also understand the basics of authentication and session management.

Audience: Web & Mobile Developers, Security Architects & Specialists

Error Handling & Logging

140 Error Handling and Security Logging

PCI 6.5.5; OWASP Top Ten A5 *14:00 minutes*

Learn about basic error handling patterns to prevent information leakage and Denial of Service (DoS) attacks. Proper logging techniques are described to ensure a complete security record. Understand how to implement simple intrusion detection techniques to make your applications more attack resistant.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

241 Handling Security Errors and Intrusion Detection

PCI 6.5.5; OWASP Top Ten A5 *11:20 minutes*

Learn to securely handle exceptions (including security exceptions) and how to avoid leaking implementation details to attackers. Understand how to establish a security exception hierarchy and a general error handling scheme, including strategies for generating safe error messages and detecting intrusions.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

242 Effective Security Logging

PCI 6.5.5; OWASP Top Ten A5 *15:30 minutes*

Effective security logging can help identify and triage attacks. Learn which events to log, what to capture for each event, how to detect security problems when reviewing logs and how to verify proper logging implementation. Ensuring accountability and using logs for forensics are also discussed.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

Sensitive Data Protection

150 Protecting Sensitive Data

PCI 6.5.3; OWASP Top Ten A6 *20:00 minutes*

Learn techniques for protecting particularly sensitive or regulated data, including credit card information, social security numbers and healthcare data. Understand how to verify that your applications protect the sensitive data that they process. The basics of key management, encryption algorithms, hashing and secure random number generation are covered.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

251 Introduction to Cryptography

PCI 6.5.3; OWASP Top Ten A6 *16:30 minutes*

Cryptography basics are presented including: the fundamentals of using keys and algorithms to securely encrypt data: key management; hashing; digital signatures; and random numbers. This course provides a foundation for Module 252, *Using Cryptography Securely*.

Audience: Technical Leaders, Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists, Testers, Software Architects

252 Using Cryptography Securely

OWASP Top Ten A6 *16:00 minutes*

Understand cryptographic techniques to encrypt and hash data as well as how to use proven cryptographic libraries securely. Identifying sensitive information, public key infrastructure (PKI) and common vulnerabilities related to cryptography are also discussed.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

253 X.509 Certificates

OWASP Top Ten A6 *25:50 minutes*

X.509 Certificates are the most common type of digital certificate. Learn their structure and key elements as well as common certificate formats. Understand the key and certificate lifecycle, install and properly protect certificates and verify that your applications are properly using certificates.

Audience: Web & Mobile Developers, Security Architects & Specialists

Secure Communications

160 Securing Communications

PCI 6.5.4; OWASP Top Ten A5 *24:10 minutes*

Security concerns related to transporting data across networks are discussed, considering both front-end interfaces and backend services. Learn basic security controls for these connections including TLS, Authentication, Access Control and data encryption. To benefit fully from this module, learners should be familiar with the basic workings of web applications including HTML and HTTP, as well as understand the basics of session management.

Audience: Web & Mobile Developers, Security Architects & Specialists

261 Using TLS

PCI 6.5.4; OWASP Top Ten A5 *18:40 minutes*

Learn to properly implement, test and verify TLS in an application to protect data in transit. Particular focus is given to the transitions between the secure and insecure components of an application. To benefit fully from this module, learners should be familiar with the basic workings of HTTP, cryptography and certificates.

Audience: Web & Mobile Developers, Security Architects & Specialists

262 Secure Cookie Use

OWASP Top Ten A5 *23:10 minutes*

Understand common attacks against cookies and how to defend against them. Learn techniques to secure cookies, including “Secure” and “HttpOnly” flags, session expiration times and encryption. To benefit fully from this module, learners should be familiar with the basic workings of web applications including HTML and HTTP.

Audience: Web & Mobile Developers, Security Architects & Specialists

263 Using Services Securely

PCI 6.5.4; OWASP Top Ten A5 *21:00 minutes*

Understand the risks and necessary controls to securely use services within an application. Core security areas to be considered with services are covered, including authentication and access control and input validation. Additionally, learn to securely transmit and store data via services and verify that service use is secure. Learners should have some background in security fundamentals.

Audience: Web & Mobile Developers, Security Architects & Specialists

264 Using TLS in Java and .Net

OWASP Top Ten A5 *23:00 minutes*

Understand the relationship between server and client side certificates and private keys. Get acquainted with commonly used, publicly available TLS libraries for Java and .NET and how to use them properly. Learn how to install and protect client and server side certificates and private keys in both Java and .NET.

Audience: Web & Mobile Developers, Security Architects & Specialists

Security Operations

170 Hardening Application Platforms and Frameworks

OWASP Top Ten A5 *28:00 minutes*

Get a high-level understanding of the techniques used to harden application platforms, including the application framework, application server, web server and host layers. Learners should be familiar with the basic workings of web applications, particularly in the deployment environment.

Audience: Web & Mobile Developers, Security Architects & Specialists

271 Hardening Web Servers

OWASP Top Ten A5, A9 *11:50 minutes*

Understand hardening concepts and learn how to determine what hardening changes to make to your web server and when to make them. Consider how to adapt to the requirements, risks and constraints of your situation with a prioritized, risk-management approach to hardening changes.

Audience: Security Architects & Specialists

272 Hardening Application Servers

OWASP Top Ten A5, A9 *9:20 minutes*

Learn what is required to harden a web application server including configuration options. This module focuses on what hardening changes to make to your application server, as well as how to adapt to the particular requirements, risks and constraints of your situation.

Audience: Security Architects & Specialists

273 Using Components Securely

OWASP Top Ten A9 *11:30 minutes*

The use of components during application development has surged. Minimize your security risks when using libraries and learn to identify components with known vulnerabilities. Understand how to develop a component inventory to use across applications and update components with known vulnerabilities.

Audience: Web & Mobile Developers, Non-Web Developers, Security Architects & Specialists

Web Services

291 Introduction to Web Services Security

17:45 minutes

Web services, common web service architectural styles and the security standards available to each style of web service are introduced. WSDL security issues are explained as well as recommended architectures for providing security services within a web service. To benefit fully from this module, learners should be familiar with web applications and web services including XML and HTTP. Basic authentication, access control and session management knowledge is also required.

Audience: Technical Leaders, Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

292 Web Services Authentication and Authorization

PCI 6.5.8; OWASP Top Ten A2, A4, A7 *20:25 minutes*

Understand the challenges of authenticating and authorizing web service requests. Web authentication models are discussed along with how to leverage WS-Security to include practically any type of authentication token. Learn how to use the same techniques for providing access control as in a typical web application. Additionally, understand how to use WS-Security to include authorization tokens, typically SAML assertions, in SOAP requests to provide access control.

Audience: Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

Secure Mobile Application Development

311 Understanding Mobile Application Threats

OWASP Mobile Top Ten *14:05 minutes*

Learn the threats to mobile computing and how to apply existing application security principles to the mobile environment. Explore vectors like location-based attacks, SMS, Bluetooth, contacts, photos, purchasing and calls. This module provides an introduction to managing the security of your mobile applications.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

312 Mobile Application Security – Top 5 Risks

OWASP Mobile Top Ten *15:45 minutes*

Mobile applications are different than their standard web counterparts, as their entire user interface is on the mobile device. This module will provide an understanding of the Top 5 categories of risks against mobile applications, as well as how to defend against, reduce or eliminate risks. Areas of focus include protecting sensitive data; server side controls; device authentication and authorization controls; session management; and cryptography.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

313 Mobile Application Security for iOS

OWASP Mobile Top Ten *36:20 minutes*

Learn to implement the security controls necessary to mitigate the top five critical security risks facing iOS applications. Mobile applications are subject to the same vulnerabilities as traditional web applications and have unique client-side concerns. Learners will understand iOS development and security models to deliver more secure native mobile applications.

Audience: Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

314 Mobile Application Security - Android

OWASP Mobile Top Ten *29:00 minutes*

Mitigate the top five critical security risks facing Android applications. Mobile applications are subject to the same vulnerabilities as traditional web applications and have unique client-side concerns. Learners will understand Android development and security models to deliver more secure native mobile applications.

Audience: Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

Cloud Security

500 Introduction to Cloud Security

19:25 minutes

Organizations are moving their applications and data out of traditional data center networks into the cloud. What does this mean for security? In this module, learners will explore the fundamentals of the cloud and how it differs from traditional data center environments. Also discussed are cloud service and deployment models.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

501 Security Challenges in the Cloud

30:02 minutes

Learn about the security challenges that are unique to the cloud. Get guidance on the fundamental security controls necessary to address these challenges. Specific vulnerabilities and topics discussed include nefarious use of the cloud; insecure interfaces and APIs; data leakage via shared resources; data loss; traffic hijacking; malicious insiders; and privacy.

Audience: Technical Leaders, Business Leaders, Web & Mobile Developers, Security Architects & Specialists, Testers, Software Architects

502 Federation and Single Sign-On in the Cloud

33:48 minutes

Authentication is the foundation of strong application security in the overall context of an application. Managing authentication in the cloud can be especially complicated. In this module you will learn about Federated Identity, Single Sign-On and the relationship between the two. Advance and Just-in-Time Provisioning will be discussed, along with common Single Sign-On implementations.

Audience: Technical Leaders, Web & Mobile Developers, Security Architects & Specialists, Software Architects

503 Data Protection and Access Control in the Cloud

34:35 minutes

In this module, cloud-specific data protection concerns and strategies are addressed. Learn data persistence strategies often employed by cloud vendors and the security concerns related to each. Understand how to separate business and administrative functionality to increase a system's security posture. Get practical strategies for evaluating the effectiveness of security controls in a multi-tenant environment and for controlling access to your cloud management APIs.

Audience: Technical Leaders, Web & Mobile Developers, Security Architects & Specialists, Software Architects

504 Encryption and Tokenization in the Cloud

35:18 minutes

Organizations typically rely on to two technical security controls, encryption and tokenization, to secure data-at-rest. Implementation of these controls is more complicated in the cloud than in a traditional data center environment. Learn the primary data-at-rest protections used in the cloud. Also discussed are the challenges of key management and the role tokenization plays in protecting data-at-rest. Finally, understand practical strategies to implement encryption and tokenization solutions.

Audience: Technical Leaders, Web & Mobile Developers, Security Architects & Specialists, Software Architects

505 Securing Software Development in the Cloud

22:40 minutes

Learn to secure source code repositories such as GitHub and how to examine and remove sensitive data from the repository's history as part of a migration. Understand how to use the cloud's dynamic nature to provision and de-provision test environments to reduce the likelihood of encountering false positives. We discuss the special testing considerations and how to automate security testing via unit and integration tests.

Audience: Technical Leaders, Web & Mobile Developers, Security Architects & Specialists

506 Legal, Regulatory and Common Pitfalls in the Cloud

27:05 minutes

As organizations move more of their infrastructure and application hosting to the cloud, it is vital to consider key provisions in contract negotiations with the cloud provider. A high-level understanding of common portions and limitations of cloud-provider contracts ensures an organization can address any residual risk and evaluate the efficacy of various cloud providers. We cover the regulations and high-level guarantees that should be part of any cloud-based business arrangement. Encryption, reporting, disaster recovery, downtime credits and cyber liability insurance are also discussed.

Audience: Technical Leaders, Web & Mobile Developers, Security Architects & Specialists