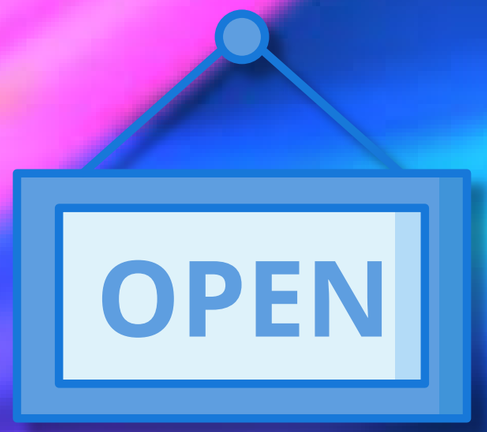
eLearning for Secure Application Development

Interactive

Self-paced

24/7/365



INDEX

Click on the page numbers to navigate directly to that page.

Application Security Fundamentals

100 Introduction to Application Security

OWASP Top 10; NIST 800-53 Rev 4 (SA, SI)

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 that an organization faces when addressing application security are discussed. Learn to produce and deploy secure applications cost-effectively. Common challenges that an organization faces when addressing application security are discussed.

Audience: *all staff, technical leaders, business leaders, web and mobile developers, non-web developers, security architects and specialists, testers, software architects*

102 Introduction to the Secure Development Lifecycle

NIST 800-53 Rev 4 (SA)

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

103 Introduction to Managing Application Security

NIST 800-53 Rev 4 (SA, SI)

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 and specialists, software architects*

104 Introduction to the OWAASP Top Ten

OWASP Top Ten

The OWASP Top Ten project represents a consensus from the application security community about what the most critical web application security flaws are at a given point in time. For each flaw, a description, example vulnerabilities, example attacks and guidance on how to avoid these is provided. In this module, we cover the latest release, the OWASP Top Ten 2017.

Audience: *managers and leaders, builders, breakers, defenders*

105 Introduction to Application Security Awareness

PCI 6; OWASP Top 10; NIST 800-53 Rev 4 (SA)

The OWASP Top Ten project represents a consensus from the application security community about what the most critical web application security flaws are at a given point in time. For each flaw, a description, example vulnerabilities, example attacks and guidance on how to avoid these is provided. In this module, we cover the latest release, the OWASP Top Ten 2017.

Audience*: technical leaders, business leaders, web and mobile developers, non-web developers, security architects and specialists, testers, software architects*

106 Common Components of an Application Security Program

PCI 6; OWASP Top 10; NIST 800-53 Rev 4 (SA, SI)

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

107 Security in the Application Development Lifecycle

PCI 6; OWASP Top 10; NIST 800-53 Rev 4 (SA, SI)

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

Application Security Knowledge Domains (ASKD) Series

ASKD Overview of ASKD Controls

PCI 6; OWASP Top 10

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

ASKD Authentication and Identity

PCI 6.5.10; OWASP Top 10 (A2); NIST 800-53 Rev 4 (IA)

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

ASKD Authorization and Access Control

PCI 6.5.8; OWASP Top 10 (A4, A7); NIST 800-53 Rev 4 (AC)

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

Audience: *web and mobile developers, non-web developers, security architects and specialists, testers, software architects*

ASKD Sensitive Data Protection

PCI 6.5.3; OWASP Top 10 (A6); NIST 800-53 Rev 4 (SA, SC, SI)

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

ASKD Session Management

PCI 6.5.10; OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC, SC)

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 and mobile developers, non-web developers, security architects and specialists, testers,software architects*

ASKD Validation and Encoding

PCI 6.5.1; OWASP Top 10 (A1, A3); NIST 800-53 Rev 4 (SI)

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: *Audience: web and mobile developers, non-web developers, security architects and specialists, testers, software architects*

ASKD Logging and Audit

PCI 6.5.5; OWASP Top 10 (A5); NIST 800-53 Rev 4 (AC, AU, RA, SI)

The Logging and Audit security control often gets 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 and mobile developers, non-web developers, security architects and specialists, testers, software architects v*

Compliance Series

601 PCI DSS for Application Security Professionals

PCI 6; OWASP Top 10

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 (PCI DSS, version 3.2, released in April 2016) and discuss the areas particularly relevant to application security.

Audience: *technical leaders, web and mobile developers, non-web developers, security architects and specialists, testers, software architect*

602 Introduction to General Data Protection Regulation (GDPR)

GDPR is the General Data Protection Regulation of the European Union. It is intended to synchronize laws between EU countries regarding data and its privacy, ownership, protection and the rights of citizens with respect to their data. We discuss which entities must comply with GDPR's requirements; what is considered protected data; and what the requirements are to protect data. In the most horrendous breach case, organizations can be levied with penalties of up to €20 million or 4% of annual worldwide revenue, whichever is greater.

Audience: *technical leaders, business leaders*

603 Introduction to GDPR for Application Security Professionals

Learners will understand what specific actions are required by application security professionals to assist with GDPR compliance; tasks required for data inventories; and application security activities needed for compliance activities. We discuss the Data Protection Impact Assessment (DPIA) and address how to complete accurate and thorough documentation. Cybersecurity practices that must be implemented by Data Controllers and Data Processors to achieve GDPR compliance are discussed.

Audience: *web and mobile developers, non-web developers, security architects and specialists, testers, software architects*

Implementing Application Security Programs

421 Application Security Risk Management

NIST 800-53 Rev 4 (SA, SI)

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 SDLC.

Audience*: technical leaders, business leaders, security architects and specialists, software architects*

450 Integrating Security into Waterfall Projects

NIST 800-53 Rev 4 (SA)

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 and specialists, software architects*

460 Session Management

PCI 6; OWASP Top 10; NIST 800-53 Rev 4 (SA, SI)

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: *NIST 800-53 Rev 4 (SA)*

Secure Testing and Verification

101 Introduction to Application Security Verification

NIST 800-53 Rev 4 (CA, RA, SA)

Application security verification is the process of confirming 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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

411 Effective Security Testing

OWASP Top 10; NIST 800-53 Rev 4 (CA, RA, SA)

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 and specialists, testers*

412 Effective Security Code Review

IST 800-53 Rev 4 (CA, RA, SA)

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 and specialists, testers*

413 Introduction to the OWASP Application Security Verification Standard (ASVS)

OWASP Top 10

The OWASP ASVS Project is an open application security standard for web applications and web services. The standard is used to design, build and test application security controls. It also provides lists of security requirements and tests that help to define, build, test and verify an application's security posture.

Audience*: web developers, security architects and specialists, testers*

420 Threat Modeling and Security Architecture Review

NIST 800-53 Rev 4 (CA, RA, SA)

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 and mobile developers, non-web developers, security architects and specialists, software architects*

Common Attacks and Vulnerabilities

180 Buffer Overflows

PCI 6.5.2; NIST 800-53 Rev 4 (SI)

Buffer Overflows, sometimes called Buffer Overruns, are one of the most common and dangerous software vulnerabilities. Verify whether 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 and mobile developers, non-web developers, security architects and specialists*

213 Preventing Cross-Site Scripting Attacks

PCI 6.5.7; OWASP Top 10 (A3); NIST 800-53 Rev 4 (SI)

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 and mobile developers, security architects and specialists*

226 Unsafe Redirects and Forwards

OWASP Top 10 (A10); NIST 800-53 Rev 4 (SI)

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 and mobile developers, security architects and specialists*

227 Clickjacking

OWASP Top 10 (A7); NIST 800-53 Rev 4 (SI)

Clickjacking refers to an attack that hijacks a victim's mouse clicks on a trusted website to do what the attacker wants rather than what the user intended. Understand how Clickjacking works and the risks that arise from such flaws, as well as how to test and defend against these vulnerabilities.

Audience: *web and mobile developers, security architects and specialists*

236 Preventing Forged Requests (CSRF)

PCI 6.5.9; OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC)

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 and mobile developers, security architects and specialists*

331 Understanding DOM-based XSS

OWASP Top 10 (A3); NIST 800-53 Rev 4 (SI)

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 and mobile developers, security architects and specialists, software architects*

332 Deserialization

In this module, we explore the advantages and risks of serialization and deserialization (the processes of converting objects to a transportable format and back). While this approach to storing or transmitting data is convenient, vulnerabilities can arise if not implemented carefully. Also addressed are the secure coding techniques that should be used to mitigate these vulnerabilities. Note: Java is used for the examples in this module, but the concepts involved apply to all programming languages that support this type of functionality.

Audience: *security architects and specialists*

333 SQL Injection: Understanding and mitigating attacks and vulnerabilities

PCI 6.5.1; OWASP Top Ten (A1); NIST 800-53 (Rev. 4) SI

SQL Injection is one of the leading application vulnerabilities associated with data breaches. In this module, we will take a deep dive to understand what the vulnerability is, what vulnerable code may look like in our applications and the leading techniques we can employ to mitigate against SQL Injection.

Audience: *ecurity architects and specialists*

Common Attacks and Vulnerabilities

334 XML External Entity (XXE) Injection: Understanding/Mitigating Attacks and Vulnerabilities

PCI 6.5.1; OWASP Top Ten (A1); NIST 800-53 (Rev. 4) SI

XML External Entity (XXE) is associated with a class of injection attacks that leverage the entity expansion features of XML parsers. These attacks are classified as a server-side request forgery. XXE attacks allow attackers to hijack the server-side process running the XML parser to steal data from your system or others, or even use your system as a base to attack others. This module introduces the XXE attack and how it is typically used against applications, as well as how to secure your applications against it.

Audience: *security architects and specialists*

335 Exploiting File Upload and Download Functionality

Many web applications perform little to no validation when it comes to file uploads and downloads. This functionality can be attacked to compromise an application and potentially its underlying infrastructure. In this module, we discuss fundamental techniques that can be used to defend against this type of attack.

Audience: *developers; testers*

336 Integer Overflow, Underflow and Wraparound

When an integer arithmetic operation has a result that's too big or too small, an overflow or underflow can occur. A wraparound and unexpected results can create significant security issues impacting data confidentiality, integrity and availability.

Audience: *developers; testers*

Secure Application Development

Input Validation

110 Input Validation

PCI 6.5.1; OWASP Top 10 (A1); NIST 800-53 Rev 4 (SI)

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 and mobile developers, non-web developers, security architects and specialists*

221 Input ValidationInput Validation Strategy

PCI 6.5.1; OWASP Top 10 (A1, A3); NIST 800-53 Rev 4 (SI)

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 and mobile developers, non-web developers, security architects and specialists, software architects*

212 Preventing Injection Attacks

PCI 6.5.1; OWASP Top 10 (A1); NIST 800-53 Rev 4 (SI)

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 and mobile developers, non-web developers, security architects and specialists, software architects*

214 Using Canonicalization and Encoding

OWASP Top 10 (A1); NIST 800-53 Rev 4 (SI)

This introduction to canonicalization and encoding covers why proper decoding and encoding are 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 and mobile developers, security architects and specialist*

215 Performing Secure File Uploads and Downloads

PCI 6.5.1; OWASP Top 10 (A4); NIST 800-53 Rev 4 (SI)

The complexities of implementing file uploads and downloads securely in a web application are addressed. Validating upload requests and 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 and mobile developers, security architects and specialists*

216 Preventing Header Injection

PCI 6.5.1; OWASP Top 10 (A1); NIST 800-53 Rev 4 (SI)

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 and mobile developers, security architects and specialistsv*

Secure Application Development

Access Control/Authorization

120 Access Control

PCI 6.5.8; OWASP Top 10 (A7); NIST 800-53 Rev 4 (AC)

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 and mobile developers, non-web developers, security architects and specialists*

221 Access Control Strategy

PCI 6.5.8; OWASP Top 10 (A7, A4); NIST 800-53 Rev 4 (AC)

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 and mobile developers, non-web developers, security architects and specialists, software architects*

222 Presentation Layer Access Control

PCI 6.5.8; OWASP Top 10 (A7); NIST 800-53 Rev 4 (AC)

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 and mobile developers, security architects and specialists*

223 223 URL-based Access Control

PCI 6.5.8; OWASP Top 10 (A7); NIST 800-53 Rev 4 (AC)

Learn effective strategies for URL-based access control. Understand common attacks and how to defend against them. Discover techniques to verify the strength of 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 and mobile developers, security architects and specialists*

224 Business Layer Access Control

PCI 6.5.8; OWASP Top 10 (A7); NIST 800-53 Rev 4 (AC)

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 and mobile developers, security architects and specialistscts*

225 Implementing Data Layer Access Control

PCI 6.5.8; OWASP Top 10 (A7, A4); NIST 800-53 Rev 4 (AC)

Learn to secure sensitive data stored by your application. Data access control is a security mechanism that establishes 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 and mobile developers, security architects and specialists*

Secure Application Development

Authentication

130 Authenticating Users

PCI 6.5.10; OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC, IA)

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 basic workings of web applications, including HTML and HTTP.

Audience: *web and mobile developers, non-web developers, security architects and specialists*

231 Authentication Strategy

PCI 6.5.10; OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC, IA)

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 and mobile developers, non-web developers, security architects and specialists, software architects*

232 Understanding HTTP Authentication Schemes

OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC, IA)

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 and mobile developers, security architects and specialists*

233 Secure Session Management

PCI 6.5.10; OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC, SC)

Session hijacking allows user sessions to be taken over by an attacker. Learn how to determine whether 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 and mobile developers, security architects and specialists*

234 Protecting Credentials

OWASP Top 10 (A2); NIST 800-53 Rev 4 (SC)

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

Audience: *web and mobile developers, non-web developers, security architects and specialistscts*

235 Managing Identity within an Application

OWASP Top 10 (A2); NIST 800-53 Rev 4 (AC)

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 and mobile developers, non-web developers, security architects and specialists*

Secure Application Development

Error Handling and Logging

140 Error Handling and Security Logging

PCI 6.5.5; OWASP Top 10 (A5); NIST 800-53 Rev 4 (AC, AU, SC, SI)

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 and mobile developers, security architects and specialists*

241 Handling Security Errors and Detecting Attacks

PCI 6.5.5; OWASP Top 10 (A5); NIST 800-53 Rev 4 (AC, AU, RA; SC, SI)

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 and mobile developers, non-web developers, security architects and specialists*

242 Effective Security Logging

PCI 6.5.5; OWASP Top 10 (A5); NIST 800-53 Rev 4 (AC, AU, SC, SI)

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. Establishing accountability and using logs for forensics are also discussed..

Audience: *web and mobile developers, non-web developers, security architects and specialistts*

Sensitive Data Protection

150 Protecting Sensitive Data

PCI 6.5.3; OWASP Top 10 (A6); NIST 800-53 Rev 4 (AC, SC)

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 and mobile developers, non-web developers, security architects and specialists*

251 Introduction to Cryptography

PCI 6.5.3; OWASP Top 10 (A6); NIST 800-53 Rev 4 (SC)

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 and mobile developers, non-web developers, security architects and specialists, testers, software architects*

252 Using Cryptography Securely

PCI 6.5.3; OWASP Top 10 (A6); NIST 800-53 Rev 4 (SC)

Understand cryptographic techniques to encrypt and hash data and 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 and mobile developers, non-web developers, security architects and specialists*

253 X.509 Certificates

OWASP Top 10 (A6); NIST 800-53 Rev 4 (SC)

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, how to install and properly protect certificates, and verify that your applications are using certificates correctly.

Audience: *web and mobile developers, security architects and specialists*

Secure Application Development

Secure Communications

160 Securing Communications

PCI 6.5.4; OWASP Top 10 (A5); NIST 800-53 Rev 4 (SC)

Security concerns related to transporting data across networks are discussed, considering both front-end interfaces and back-end 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 and mobile developers, security architects and specialists*

261 Using TLS

PCI 6.5.4; OWASP Top 10 (A5); NIST 800-53 Rev 4 (SC)

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 and mobile developers, security architects and specialistsialists*

262 Secure Cookie Use

OWASP Top 10 (A5); NIST 800-53 Rev 4 (AC, SC)

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 and mobile developers, security architects and specialists*

263 Using Services Securely

PCI 6.5.4; OWASP Top 10 (A5)

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 and mobile developers, security architects and specialists*

264 Using TLS in Java and .NET

PCI 6.5.4; OWASP Top 10 (A5); NIST 800-53 Rev 4 (SC)

Understand the relationship between server-side 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 serverside certificates and private keys in both Java and .NET.

Audience: *web and mobile developers, security architects and specialists*

Secure Application Development

Security Operations

170 Hardening Application Platforms and Frameworks

OWASP Top 10 (A5); NIST 800-53 Rev 4 (CM, SA)

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 and mobile developers, security architects and specialists*

273 Using Components Securely

OWASP Top 10 (A9); NIST 800-53 Rev 4 (CM, SA)

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

Audience: *web and mobile developers, non-web developers, security architects and specialists*

274 Guidelines for Hardening Application and Web Servers

Server hardening, the process of configuring settings after the base operating system and server hosting services have been installed on a machine, decreases the server's attack surface. Verifying that all components are hardened appropriately is a necessary step to build secure applications. In this module, we review server hardening techniques. While different combinations of operating systems and hosting services involve specific hardening methods and platform-specific requirements, the guidance in this course is generally applicable for all platforms.

Audience: *security architects and specialists s*

Web Services

291 Introduction to Web Services Security

NIST 800-53 Rev 4 (AC)

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 and mobile developers, security architects and specialists, testers, software architects*

251 Web Services Authentication and Authorization

PCI 6.5.8; OWASP Top 10 (A2, A4, A7); NIST 800-53 Rev 4 (AC)

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 contro

Audience: *web and mobile developers, security architects and specialists, testers, software architects*

Secure Application Development

Cloud Security

500 Introduction to Cloud Security

NIST 800-53 Rev 4 (AC, CM, SA)

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 and business leaders, web and mobile developers, security architects and specialists, testers, software architects*

501 Security Challenges in the Cloud

NIST 800-53 Rev 4 (AC, CM, SC)

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: *web and mobile developers, non-web developers, security architects and specialists*

502 Federation and Single Sign-On in the Cloud

NIST 800-53 Rev 4 (AC, CM, IA, SA)

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 and mobile developers, security architects and specialists, software architects*

503 Data Protection and Access Control in the Cloud

NIST 800-53 Rev 4 (AC, CM, SA, SC)

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 and mobile developers, security architects and specialists, software architects*

504 Encryption and Tokenization in the Cloud

OWASP Mobile Top 10; NIST 800-53 Rev 4 (AC, RA, SA, SC)

Learn to implement the security controls necessary to mitigate the top five critical security risks facing iOS applications. Mobileapplications 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 and mobile developers, security architects and specialists, testers, software architects*

505 Securing Software Development in the Cloud

NIST 800-53 Rev 4 (CM, SA, SC)

Organizations typically rely on 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 and mobile developers, security architects and specialists, software architects*

506 Legal, Regulatory and Common Pitfalls in the Cloud

NIST 800-53 Rev 4 (CM, SA)

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

Audience: *technical leaders, web and mobile developers, security architects and specialists*

Secure Application Development

Secure Mobile Application Development

311 Understanding Mobile Application Threats

OWASP Mobile Top 10; NIST 800-53 Rev 4 (RA, SC)

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 and business leaders, web and mobile developers, security architects and specialists, testers, software architects*

312 Mobile Application Security — Top 5 Risks

OWASP Mobile Top 10; NIST 800-53 Rev 4 (AC, RA, SC)

Mobile applications are different from their standard web counterparts, as their entire user interface is on the mobile device. This module will provide an understanding of the top five 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: *web and mobile developers, non-web developers, security architects and specialists*

313 Mobile Application Security for iOS

OWASP Mobile Top 10; NIST 800-53 Rev 4 (AC, RA, SA, SC)

Learn to implement the security controls necessary to mitigate the top five critical security risks facing iOS applications. Mobileapplications 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 and mobile developers, security architects and specialists, testers, software architects*

314 Mobile Application Security for Android

OWASP Mobile Top 10; NIST 800-53 Rev 4 (AC, RA, SA, SC)

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 and mobile developers, security architects and specialists, testers, software architectsv*

Introduction to Secure Coding (Java, .NET, C C++)

283 Introduction to Secure Coding in Java

NIST 800-53

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 and mobile developers, security architects and specialists*

284 Introduction to Secure Coding in .NET

NIST 800-53

Understand the risks associated with .NET applications, basic methods of secure coding and how to test applications. The module focuses 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 and mobile developers, security architects and specialists*

285 Introduction to Secure Coding in C and C++

NIST 800-53

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 — some methods and functions 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 and mobile developers, non-web developers, security architects and specialists*

DevSecOps

700 Introduction to DevSecOps

DevSecOps is the practice of developing and delivering secure software rapidly. Cybersecurity and the inclusive domains are brought in earlier in the development process by involving all needed parties, including security. Members of all domains contribute to the creative process. Continuous improvement takes place from the actionable feedback received.

Audience*: executives, managers, developers*