Secure Web Application Development Course:

Developing Web Applications in Accordance with Industry Requirements

AppSec Consulting's Secure Web Application Development Course is designed to align web application development goals with IT security objectives. The purpose of the course is to help developers improve application delivery by increasing security awareness and meeting industry and regulatory compliance requirements such as PCI DSS. The course focuses on application development strategies and tactics that secure software at the source. Intended audience includes architects, designers, developers and IT risk managers and is delivered on-site over two days. This course is also available online.

Compliance with PCI Requirements

PCI DSS requires members, merchants and service providers develop all web applications based on secure coding guidelines such as the Open Web Application Security Project Guide (OWASP). This course provides prescriptive guidance in developing web applications in compliance with PCI-DSS.

Course Outline:

Security Principles Overview

- Defense in depth
- Positive security model
- Failing safely
- Least privilege
- Security by obscurity
- Keep security simple
- Intrusion detection
- Design and Coding best practices

Authentication

- Authentication overview
- Authentication controls
- Positive authentication
- Reauthentication (sensitive transactions)
- Referer checks
- "Remember me" feature
- Default accounts
- Allowed characters in usernames and passwords
- Password policies and storing passwords
- Proper logout
- Account expiry
- Design and Coding best practices

Authorization

- Authorization overview
- Principle of least privilege
- Controlling access to protected resources
- Reauthorization
- Separation of duties
- Design and Coding best practices

Session Management

- Sessions overview
- Securing session tokens/Session token predictability/Session fixation

- Session timeouts
- Proper session clearing procedures
- Design and Coding best practices

Input/Output Validation

- Validation overview
- Data validation strategies
- URL encoding
- HTML encoding
- Specific methods for preventing XSS, SQL Injection, parameter manipulation (URL/cookie/hidden fields)
- Design and Coding best practices

Configuration

- Application-level configuration
- Infrastructure-level configuration

Error Handling

- Detailed error messages
- Failing safe
- Debug aids
- Centralized error handling (external frameworks)
- Design and Coding best practices

Logging

- Log review procedures
- Logging standards
- Securing logs
- Design and Coding best practices

Cryptography

- Cryptographic algorithms
- Recommended strong algorithms
- Insecure/obsolete algorithms
- Recommended algorithms and key sizes
- Digital signatures
- Securing communications with HTTPS
- Key management
- Summary of best practices

Web Services Security

- Introduction to Web Services
- SOAP Overview
- SOAP Security Considerations
- REST Overview
- REST Security Considerations
- Summary of best practices

The modules are structured to give an overview of the topic, introduce the different types of attacks and then suggest design and coding solutions to prevent these attacks. The course covers the OWASP Top-10 vulnerabilities, in addition to others that AppSec Consulting security engineers have come across in real-life security engagements.

Online Course

The course is also available online as a self-paced learning course. With just a web browser and an internet connection, students can take the course from anywhere at their own pace. Course completion progress is tracked at the page level and a report is provided.

About AppSec Consulting:

We've been doing this for over 12 years, and our continuum of services is designed to fit just about everyone's security needs. Every service we provide comes with a level of experience and focused attention you won't find anywhere else. Our Security Testing team will help you identify the technical issues you should be thinking about, and our Strategic Advisory Services team will work with you to develop strategies for addressing them - that means assurance for you, your customers and your partners. And because we're independently owned, you'll find us completely agnostic regarding the solutions and vendors we recommend – this means you get the solution that fits your needs, not ours.

This can't wait, so give us a call at 408.224.1110 today.

You'll speak with an Information Security expert, not a sales person — we'll listen a lot, determine your needs, and provide clear, actionable recommendations. We look forward to seeing how we can help.

Information. Security. Handled.™

appsecconsulting.com | 408.224.1110