PCI Compliance Refresher for Developers - TT8161

Equip developers with the skills to meet PCI compliance requirements, stay current with updates, and maintain secure, compliant applications.

Duration: 1 Day
Skill Level: Intermediate
Available Format: ; Instructor-Led, Onsite In Person ; On Public Schedule

The **PCI Compliance Refresher for Developers** course is a streamlined, skills-focused program designed to help experienced developers stay compliant with PCI DSS standards. This course revisits essential compliance concepts while introducing updates to regulations and best practices. Through discussions, real-world examples, and light hands-on labs, participants will reinforce their secure coding knowledge, practice identifying and mitigating vulnerabilities, and ensure they remain up-to-date with compliance requirements. By the end of the day, developers will have refreshed their skills and gained the confidence to maintain PCI-compliant applications in evolving regulatory environments.

What You'll Learn

Overview

The **PCI Compliance Refresher for Developers** course is a streamlined, skills-focused program designed to help experienced developers stay compliant with PCI DSS standards. This course revisits essential compliance concepts while introducing updates to regulations and best practices. Through discussions, real-world examples, and light hands-on labs, participants will reinforce their secure coding knowledge, practice identifying and mitigating vulnerabilities, and ensure they remain up-to-date with compliance requirements. By the end of the day, developers will have refreshed their skills and gained the confidence to maintain PCI-compliant applications in evolving regulatory environments.

Objectives

This course combines engaging instructor-led presentations, demonstrations, and light hands-on labs to help you:

- **Refresh Your PCI DSS Knowledge.** Revisit the 12 PCI DSS requirements and their application in secure software development.
- **Enhance Secure Data Practices.** Reaffirm your ability to encrypt and securely handle sensitive payment card data.
- **Identify and Address Vulnerabilities.** Practice techniques to detect and fix vulnerabilities like SQL injection and insecure data storage.
- **Validate Applications for Compliance.** Strengthen your skills in reviewing, testing, and validating applications to meet PCI DSS standards.
- **Stay Current with Compliance Strategies.** Learn how to adapt to updates in PCI DSS and integrate compliance into modern development practices.

If your team requires different topics, additional skills, or a custom approach, our team will collaborate with you to tailor the course to your specific needs.

Audience

This refresher course is designed for experienced developers, including backend engineers, web developers, and data handlers, who already have a foundational understanding of PCI compliance. It's ideal for professionals who need to update their skills and stay compliant with PCI DSS while reinforcing secure coding practices.

Pre-Requisites

To ensure a smooth learning experience and maximize the benefits of attending this course, you should have the following prerequisite skills:

- **Working Knowledge of PCI DSS.** Familiarity with the basics of PCI DSS and its relevance to software development.
- **Experience with Secure Coding.** Prior experience implementing encryption, input validation, or secure data handling in applications.
- **Proficiency in Programming.** Strong coding skills in a programming language such as Java, Python, or C#.

Agenda

Please note that this list of topics is based on our standard course offering, evolved from typical industry uses and trends. We'll collaborate with you to tune this course and

level of coverage to target the skills you need most. Topics, agenda and labs are subject to change and may adjust during live delivery based on audience skill level, interests and participation.

1. **Introduction to PCI Compliance (Refresher)**
   - Review the purpose and importance of PCI DSS and its ongoing relevance to developers.

2. **Updates to PCI DSS Requirements**
   - Explore recent changes to PCI DSS regulations and their implications for secure application development.

3. **Lab 1: Updating Data Encryption Practices**
   - Apply updated encryption techniques to securely store payment card data in compliance with current standards.

4. **Reinforcing Secure Development Practices**
   - Refresh knowledge of secure coding practices and their integration into the development lifecycle.

5. **Lab 2: Testing and Fixing Code Vulnerabilities**
   - Identify vulnerabilities in a provided codebase and apply fixes to ensure compliance with PCI DSS requirements.

6. **Validating and Auditing Applications**
   - Review techniques and tools for validating compliance through code reviews, testing, and audits.

7. **Adapting to PCI DSS Updates**
   - Discuss strategies for staying compliant as PCI DSS evolves, including continuous monitoring and improvement.

8. **Wrap-Up and Q&A**
   - Review key concepts, discuss remaining questions, and provide resources for ongoing compliance support.

Related Courses

TT8120	Web Application Security Essentials: Understanding OWASP Risks and Fixes That Really Work

For More Information

Please contact us or call 844-475-4559 toll free for more information about our training services (instructor-led, self-paced or blended), coaching and mentoring services, public course enrollment or questions, partner programs, courseware licensing options and more.