Faysal Aziz

PCI Risk Shield

OWASP-driven risk mitigation for PCI DSS v4.0.1.

FA-0345 · One day

Software Development · Cybersecurity

Introduction

One day course

Payment security is no longer just an audit exercise; weak applications, exposed APIs, vulnerable dependencies, poor access control, and payment-page script abuse can all become direct routes into cardholder data environments.

This 1-day course focuses on practical risk mitigation for PCI DSS v4.0.1 using current OWASP guidance, including OWASP Top 10:2025 and OWASP ASVS 5.0.0. PCI SSC confirms PCI DSS v4.0.1 is the active supported standard after PCI DSS v4.0 retirement, with the 31 March 2025 effective date for new requirements unchanged.

The course will be delivered by an instructor with over 30 years of industry experience, using real industry-demanded content instead of academic theory.

Learning outcomes

- Understand PCI DSS v4.0.1 risk mitigation expectations for applications, APIs, payment pages, and supporting systems
- Map OWASP Top 10:2025 risks to relevant PCI DSS controls
- Identify common application and payment security weaknesses before audit or breach exposure
- Apply secure coding, vulnerability management, WAF, logging, and testing controls
- Prepare practical evidence for PCI DSS validation discussions

Prerequisites

- Basic understanding of web applications and APIs
- Basic awareness of PCI DSS or payment environments
- Familiarity with application development, security, audit, or IT operations
- No advanced penetration testing experience required

Training outline

1. PCI DSS v4.0.1 Risk Mitigation Context

PCI DSS purpose and scope

1. Cardholder data environment
2. Account data protection
3. System components
4. Connected-to and security-impacting systems
5. Merchant and service provider responsibilities

PCI DSS v4.0.1 application security focus

1. Requirement 6 secure systems and software
2. Requirement 11 security testing
3. Requirement 12 targeted risk analysis
4. Payment page protection
5. Third-party service provider risk

Risk-based compliance approach

1. Threat identification
2. Vulnerability prioritization
3. Business impact considerations
4. Compensating control awareness
5. Customized approach awareness

2. OWASP Risk Model for PCI DSS

OWASP Top 10:2025 overview

1. Broken Access Control
2. Security Misconfiguration
3. Software Supply Chain Failures
4. Cryptographic Failures
5. Injection
6. Insecure Design
7. Authentication Failures
8. Software or Data Integrity Failures
9. Security Logging and Alerting Failures
10. Mishandling of Exceptional Conditions

OWASP ASVS 5.0 alignment

1. Security architecture
2. Authentication controls
3. Session management
4. Access control
5. Input validation
6. Cryptography
7. Error handling and logging
8. Data protection
9. API security
10. Configuration security

OWASP-to-PCI control mapping

1. Secure software development
2. Vulnerability discovery
3. Secure code review
4. Application security testing
5. Payment page script control
6. Logging and monitoring
7. Remediation evidence

3. Secure Software Development for PCI DSS

Secure SDLC foundations

1. Security requirements
2. Threat modeling
3. Secure design review
4. Secure coding standards
5. Developer security responsibilities

Secure coding risk areas

1. Authentication weaknesses
2. Authorization bypass
3. Injection flaws
4. Cross-site scripting
5. Insecure deserialization
6. Insecure file handling
7. Secrets exposure
8. Weak error handling

Code review and assurance

1. Manual secure code review
2. Peer review
3. SAST integration
4. Dependency review
5. Security defect tracking
6. Release approval controls

4. Application and API Risk Mitigation

Web application controls

1. Input validation
2. Output encoding
3. Secure session handling

4. CSRF protection
5. Secure headers
6. Rate limiting
7. Error handling

API security controls

1. API inventory
2. Strong authentication
3. Object-level authorization
4. Schema validation
5. Token protection
6. Excessive data exposure prevention
7. Abuse and automation controls

Authentication and access control

1. MFA considerations
2. Least privilege
3. Role-based access control
4. Privileged access control
5. Account lifecycle management
6. Session timeout and reauthentication

5. Vulnerability Management and Remediation

Vulnerability identification

1. Asset inventory
2. Software inventory
3. Dependency inventory
4. Vulnerability scanning
5. Application security testing
6. Threat intelligence inputs

Vulnerability ranking

1. Severity classification
2. Exploitability
3. Business impact
4. CDE exposure
5. Compensating control review

Remediation workflow

1. Critical vulnerability handling
2. Patch management
3. Secure configuration fixes
4. Code-level fixes
5. Retesting
6. Closure evidence

6. Public-Facing Web Application Protection

PCI DSS public-facing application expectations

1. Ongoing threat and vulnerability handling
2. Application vulnerability assessments
3. Web-based attack prevention
4. Automated technical solutions
5. WAF and WAAP positioning

WAF and WAAP controls

1. Detection mode
2. Prevention mode
3. Rule tuning
4. False positive handling
5. Virtual patching
6. Bot and abuse protection
7. Alert review

Security testing support

1. DAST
2. API security testing
3. Penetration testing
4. Authenticated scanning
5. Retesting after remediation
6. Evidence retention

7. Payment Page and E-Commerce Risk Mitigation

Payment page security

1. Hosted payment pages
2. Embedded payment forms
3. iFrames
4. Third-party scripts
5. Client-side attack surface

PCI DSS script management

1. Script inventory
2. Script authorization
3. Script integrity
4. Script justification
5. Change monitoring
6. Tamper detection

E-skimming prevention

1. Unauthorized script detection
2. Security-impacting HTTP headers
3. Content Security Policy
4. Subresource Integrity
5. Browser-side monitoring
6. Incident escalation

8. Logging, Monitoring and Incident Readiness

Security logging

1. Authentication events
2. Access control failures
3. Administrative activity
4. Application errors
5. WAF events
6. API abuse events

Monitoring and alerting

1. Alert prioritization
2. Attack pattern detection
3. Suspicious payment activity
4. Vulnerability exploitation attempts
5. Log review process

Incident readiness

1. Breach indicators
2. Containment process
3. Evidence preservation
4. Escalation workflow
5. Post-incident remediation

9. PCI DSS Evidence and Audit Preparation

Required documentation

1. Security policies
2. Secure coding standards
3. Risk assessments
4. Vulnerability reports
5. Remediation records
6. Test results

7. Change records

Evidence quality

1. Traceability
2. Ownership
3. Dates and approvals
4. Screenshots and exports
5. Retest confirmation
6. Exception handling

Common audit gaps

1. Incomplete asset scope
2. Missing software inventory
3. Weak remediation records
4. Untuned WAF controls
5. Poor script inventory
6. Inconsistent logging
7. Unsupported risk acceptance

Disclaimer

This course outline is provided as a general training guideline only. The trainer may amend, restructure, add, remove, or substitute topics, examples, sequence, depth, tools, or delivery emphasis at their professional discretion, without prior notice, to suit participant background, organizational needs, regulatory interpretation, classroom pace, and current industry developments.

© 2026 Faysal Aziz · Kuala Lumpur