SALT

Payment Card Industry Data Security Standard (PCI DSS) v4.0: Safeguarding Cardholder Data

PCI DSS v4.0 is a crucial framework for organizations handling cardholder data, highlighting the essential role of API security in payment processing. It requires businesses to integrate security throughout the API lifecycle, from development to maintenance. The standard stresses proactive measures to protect sensitive data, as APIs are often targeted for their access to vital payment information. Notably, section 6.2.4 underscores the need to secure the application's business logic, addressing threats from attacks that exploit API functionalities to bypass security measures. This focus on business logic protection reflects the evolving cyber threat landscape, where attackers misuse legitimate API operations for malicious purposes.

Secure Development Lifecycle (SDLC):

- "Security by design" principles integrated into API development.
- Secure coding practices to prevent common vulnerabilities like SQL injection and cross-site scripting (XSS).

Access Control:

- Implementation of multi-factor authentication (MFA) to verify user identities.
- Role-based access control (RBAC) to limit user privileges based on job functions.
- Strong authentication protocols like OAuth 2.0 to secure API endpoints.

Vulnerability Management:

- Regular vulnerability scanning and penetration testing of APIs.
- Prompt patching of identified vulnerabilities.
- Continuous monitoring of API traffic for suspicious activity.

Section 6.2.4 Emphasis:

- Protection against attacks that exploit business logic flaws.
- Mitigation of risks related to API manipulation and unintended functionality usage.
- Addressing threats such as cross-site scripting (XSS) and cross-site request forgery (CSRF).

Why It Matters: PCI DSS compliance safeguards customer trust and protects businesses from financial, reputational, and legal damage caused by data breaches. Secure APIs are essential for protecting the payment ecosystem and ensuring business continuity. PCI DSS v4.0 explicitly acknowledges the critical role of APIs in payment processing environments. APIs handling cardholder data must be securely developed, configured, and monitored to prevent breaches and maintain trust.

API Security Requirements:

- Secure Development: Implement OWASP API Security best practices to prevent attacks like injection and cross-site scripting.
- Access Controls: Enforce OAuth 2.0, MFA, and role-based access for API authentication.
- Regular Testing: Conduct API security reviews and vulnerability assessments to detect misconfigurations and threats.

Relevant Sections Referencing APIs:

- Requirement 2.2.7: Ensure that security features are implemented securely, including APIs, to prevent misuse.
- Requirement 6.2.3: Applications and APIs are developed securely to protect against known attacks.
- Requirement 6.2.4: Address common coding vulnerabilities in software-development processes, including those applicable to APIs.
- Requirement 6.3.2: Public-facing applications and APIs are reviewed for security vulnerabilities.

How Salt Security Helps: Salt Security offers a complete API discovery solution that allows you to locate all APIs that manage cardholder data, including shadow and zombie APIs. It automates vulnerability assessments to find security weaknesses, especially those related to business logic. Additionally, Salt Security's threat protection features can detect and stop attacks like credential stuffing and API abuse, which are common ways that cardholder data is breached. Its posture governance features help to maintain secure configurations and provide continuous monitoring to ensure ongoing PCI DSS compliance. Learn more about API Security and Compliance in our **White-paper.**