GIC ENGINEERING CONSULTANTS

Supply Chain & AI Threat Intelligence Platform

PCI DSS 4.0 Compliance Gap Assessment

Application: demo-struts-app v1.0.0
Report Date: March 22, 2026
Framework: PCI DSS 4.0

DEMO ENVIRONMENT — GIC ENGINEERING CONSULTANTS INTERNAL USE

Generated by SCIP v1.0.0 — www.gicengineeringconsultants.com

Executive Summary

This report presents the PCI DSS 4.0 compliance gap assessment for **demo-struts-app**, generated by the GIC Supply Chain & AI Threat Intelligence Platform (SCIP). The assessment correlates Software Bill of Materials (SBOM) components against known vulnerability databases and maps findings to PCI DSS 4.0 requirements.

20	286	52	55%
Portfolio Risk Score (0–100, lower is better)	Total CVEs Identified	Critical Vulnerabilities	PCI DSS 4.0 Coverage

Vulnerability Severity Distribution

Severity	Count	Percentage
CRITICAL	52	18.2%
HIGH	128	44.8%
MODERATE	96	33.6%
LOW	10	3.5%
Total	**286**	**100%**

Top 3 Remediation Priorities

#	Action	Justification	Severity
1	Upgrade Apache Log4j from 2.14.1 to 2.17.1+	CVE-2021-44228 (Log4Shell) — CVSS 10.0, CISA KEV, Known Ransomware	CRITICAL
2	Upgrade Apache Struts from 2.5.30 to 6.x	Multiple RCE vulnerabilities including CVE-2017-5638 (Equifax breach vector)	CRITICAL
3	Upgrade Spring Framework from 5.3.15 to 6.x	CVE-2022-22965 (Spring4Shell) — CVSS 9.8	CRITICAL

PCI DSS 4.0 — Control-by-Control Assessment

11 of 20 PCI DSS 4.0 controls (55%) are assessable via software supply chain data. Each control shows its current status based on live SCIP correlation.

6.3.2 Maintain inventory of bespoke/custom and third-party software components — ■ PASS

Req 6 — Develop and Maintain Secure Systems

Evidence: SCIP maintains a complete SBOM inventory with 18 tracked components for demo-struts-app. All components include name, version, PURL identifier, and license. Inventory updated on each SBOM ingestion.

6.3.3 All software components protected from known vulnerabilities — ■ GAP

Req 6 — Develop and Maintain Secure Systems

Evidence: 286 known vulnerabilities identified across 16 of 18 components, including 52 CRITICAL. Key findings: Log4j 2.14.1 (CVE-2021-44228, CISA KEV), Struts 2.5.30 (multiple RCE), Spring 5.3.15 (CVE-2022-22965). Immediate remediation required.

6.4.1 Public-facing web applications protected against attacks — ■ GAP

Req 6 — Develop and Maintain Secure Systems

Evidence: Application contains components with known RCE vulnerabilities. Struts 2.5.30 and Spring 5.3.15 are public-facing framework components with actively exploited CVEs.

6.4.2 Automated solution detects and prevents web-based attacks — ■ PASS

Req 6 — Develop and Maintain Secure Systems

Evidence: SCIP provides automated detection via OSV vulnerability correlation (268K PURL mappings), CISA KEV monitoring (57K entries), EPSS scoring (210K entries), and 10 MITRE ATLAS detection rules.

8.3.6 Passwords meet minimum complexity requirements — ■ GAP

Req 8 — Identify Users and Authenticate Access

Evidence: Password complexity is an organizational policy control outside the scope of SBOM-based assessment. Requires separate QSA evaluation.

10.2.1 Audit logs capture individual user access to cardholder data — ■ PASS

Req 10 — Log and Monitor All Access

Evidence: SCIP integrates with Splunk audit logging. All SBOM ingestion, license validation, and compliance assessment actions are logged with timestamps and user context.

10.7.1	Failures of critical security controls detected and responded to promptly	■ **PASS**

Req 10 — Log and Monitor All Access

Evidence: SCIP includes 10 MITRE ATLAS detection rules plus OSV-based vulnerability alerting. Critical discoveries trigger immediate risk score recalculation.

11.3.1	Internal vulnerability scans performed quarterly	■ **PASS**

Req 11 — Test Security of Systems and Networks

Evidence: SCIP performs continuous vulnerability correlation against OSV database (updated daily for paid tier). 286 CVEs identified. Portfolio risk score: 20. Exceeds quarterly requirement.

11.3.2	External vulnerability scans performed quarterly	■ **PASS**

Req 11 — Test Security of Systems and Networks

Evidence: SCIP correlates SBOM components against external vulnerability databases (OSV, CISA KEV, EPSS). Provides continuous external vulnerability awareness.

12.3.3	Hardware/software technologies reviewed annually	■ **PASS**

Req 12 — Support Information Security with Policies

Evidence: SCIP maintains continuous SBOM inventory with version tracking. Component technologies reviewed on every ingestion.

12.3.4	Technologies reviewed to ensure continued security fix support	■ **PASS**

Req 12 — Support Information Security with Policies

Evidence: SCIP tracks component versions and correlates against known vulnerabilities. 16 of 18 components have active CVEs flagged for version upgrades.

Appendix: SBOM Component Inventory

Component	Version	Group	Max Severity
struts2-core	2.5.30	org.apache.struts	CRITICAL
log4j-core	2.14.1	org.apache.logging.log4j	CRITICAL
spring-core	5.3.15	org.springframework	CRITICAL
spring-webmvc	5.3.15	org.springframework	HIGH
jackson-databind	2.13.0	com.fasterxml.jackson.core	HIGH
tomcat-embed-core	9.0.55	org.apache.tomcat.embed	HIGH
netty-codec-http	4.1.70.Final	io.netty	HIGH
commons-collections	3.2.1	org.apache.commons	HIGH
snakeyaml	1.30	org.yaml	HIGH
hibernate-core	5.6.5.Final	org.hibernate	MODERATE
bcprov-jdk15on	1.69	org.bouncycastle	MODERATE
logback-classic	1.2.11	ch.qos.logback	MODERATE
httpclient	4.5.13	org.apache.httpcomponents	MODERATE
jackson-core	2.13.0	com.fasterxml.jackson.core	MODERATE
commons-io	2.11.0	commons-io	MODERATE
guava	31.1-jre	com.google.guava	LOW
slf4j-api	1.7.36	org.slf4j	—
commons-lang3	3.12.0	org.apache.commons	—