Author

CAST

******

**PCI DSS 4**

**Compliance Report**

Application Name –

Version –

CAST AIP -

|  |
| --- |
|  |
|  |

Monday, xx July 2012

My Application Name

Version Number

My CAST Version

# Table of Content

Table of Content

1. Introduction

1.1. Application Characteristics

2. PCI DSS Summary

2.1. PCI DSS Vulnerabilities Summary

3. CAST Findings for PCI DSS – Requirement 6

4. CAST Findings for PCI DSS – Requirement 1

5. CAST Findings for PCI DSS – Requirement 2

6. CAST Findings for PCI DSS – Requirement 3

7. CAST Findings for PCI DSS – Requirement 4

8. CAST Findings for PCI DSS – Requirement 8

9. Appendix

9.1. About CAST Software Intelligence

9.2. About CAST Security

# Introduction

This assessment is an effort to determine the security health of the application and identify some of the root causes of current Security concerns, as well as any risks of future degradation. This assessment uses the CAST Application Intelligence Platform (AIP) to automatically scan the implementation of these applications to review the architecture, design, and code against PCI standards.

CAST AIP adapts the quality rules from best-in-class industry standards (OWASP, CWE, CISQ, STIG, PCI, NIST). With its unique ability to perform dataflow and system-level analysis (From Presentation layer to Database layer), CAST provides the most accurate security findings, reducing a lot of false positives.

## Application Characteristics

This assessment is focused solely on the technical implementation of the said application (user interface to database), with no investigation of the functionality.

|  |  |
| --- | --- |
| **Name** | **Value** |
| kLoC | 504 |
| Files | 6,586 |
| Classes | 593 |
| SQL Art. | 0 |
| Tables | 119 |

*Fig 1: Application Technology characteristics Table 1: Application characteristics*

# PCI DSS Summary

This section provides a summary of the most severe security vulnerability identified in the structural quality analysis and measurement by CAST AIP against the Payment Card Industry ([PCI](https://www.pcisecuritystandards.org/)) Data Security Standard, Requirements and Security Assessment Procedures.

## PCI DSS Vulnerabilities Summary

PCI DSS Modules available in CAST Solution:

|  |  |  |
| --- | --- | --- |
| **Module** | **Req#** | **Descriptions** |
| Maintain a Vulnerability Management Program | **PCI-DSS4-Requirement-6.2.4**  **PCI-DSS4-Requirement-6.3.2** | Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities  An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management |
| Build and Maintain a Secure Network and Systems | **PCI-DSS4-Requirement-1.4.5**  **PCI-DSS4-Requirement-2.2.2**  **PCI-DSS4-Requirement-2.2.6** | The disclosure of internal IP addresses and routing information is limited to only authorized parties.  Vendor default accounts are managed  System security parameters are configured to prevent misuse |
| Protect Cardholder Data | **PCI-DSS4-Requirement-3.6.1**  **PCI-DSS4-Requirement-4.2.1** | Procedures are defined and implemented to protect cryptographic keys  Strong cryptography and security protocols are implemented |
| Implement Strong Access Control Measures | **PCI-DSS4-Requirement-8.3.2** | Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. |

Findings summary for CAST under PCI DSS Standards.

| PCI-DSS-V4 | Total | Added | Removed |
| --- | --- | --- | --- |
| Requirement 1 | 0 | 0 | 0 |
| Requirement 2 | 0 | 0 | 0 |
| … | 0 | 0 | 0 |

# CAST Findings for PCI DSS – Requirement 6

List of CAST vulnerabilities for PCI DSS Requirement 6.

| Rules | Total | Added | Removed |
| --- | --- | --- | --- |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

# CAST Findings for PCI DSS – Requirement 1

List of CAST vulnerabilities for PCI DSS Requirement 1.

| Rules | Total | Added | Removed |
| --- | --- | --- | --- |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

# CAST Findings for PCI DSS – Requirement 2

List of CAST vulnerabilities for PCI DSS Requirement 2.

| Rules | Total | Added | Removed |
| --- | --- | --- | --- |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

# CAST Findings for PCI DSS – Requirement 3

List of CAST vulnerabilities for PCI DSS Requirement 3.

| Rules | Total | Added | Removed |
| --- | --- | --- | --- |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

# CAST Findings for PCI DSS – Requirement 4

List of CAST vulnerabilities for PCI DSS Requirement 4.

| Rules | Total | Added | Removed |
| --- | --- | --- | --- |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

# CAST Findings for PCI DSS – Requirement 8

List of CAST vulnerabilities for PCI DSS Requirement 8.

| Rules | Total | Added | Removed |
| --- | --- | --- | --- |
| Rule 1 | 0 | 0 | 0 |
| Rule 2 | 0 | 0 | 0 |
| Rule 3 | 0 | 0 | 0 |
| Rule 4 | 0 | 0 | 0 |
| Rule 5 | 0 | 0 | 0 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

# Appendix

## About CAST Software Intelligence

Software Intelligence creates understanding into software architecture, end to end transaction flows, data access patterns and more, helping teams work confidently and faster. Hundreds of companies rely on CAST Software Intelligence to improve end-user satisfaction and time-to-market, prevent business disruption and reduce cost, enabling them to move past today’s obstacles and to tackle the next wave of innovation.

[Click here](https://www.castsoftware.com) for more information about CAST Software Intelligence.

## About CAST Security

Cyber risk and application security require a proactive and intelligence-driven approach. CAST Software Intelligence shifts insight into security strategy blind spots before development starts. With its unique ability to do dataflow and system-level analysis, CAST provides the most accurate security findings, reducing a lot of false positives. CAST Security rules are adapted from best-in-class industry standards – CISQ, CWE, OWASP, PCI-DSS, NIST, and STIG. To find out more about CAST Security, [click here](https://www.castsoftware.com/products/security-dashboard).