Author

CAST



**PCI DSS V3.2.1**

**Summary Report**

Application Name –

Version –

CAST AIP -

|  |
| --- |
|  |
|  |

Monday, xx July 2012

My Application Name

Version Number

My CAST Version

# Table of Content

Table of Content 2

1. Introduction 3

1.1. Application Characteristics 3

2. PCI DSS V 3.2.1 release Overview 4

PCI DSS V 3.2.1 High Level Overview 4

2.1. PCI DSS – Requirement 1 5

2.2. PCI DSS – Requirement 2 5

2.3. PCI DSS – Requirement 3 6

2.4. PCI DSS – Requirement 4 6

2.5. PCI DSS – Requirement 5 7

2.6. PCI DSS – Requirement 6 7

2.7. PCI DSS – Requirement 7 8

2.8. PCI DSS – Requirement 8 8

2.9. PCI DSS – Requirement 9 9

2.10. PCI DSS – Requirement 10 9

2.11. PCI DSS – Requirement 11 10

2.12. PCI DSS – Requirement 12 10

3. Appendix 11

3.1. About CAST Software Intelligence 11

3.2. How CAST AIP Works 11

# 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 CWE standards. CAST AIP applies over 1200 engineering checks based on standards and measurements developed by the Software Engineering Institute (SEI), International Standards Organization (ISO), Consortium for IT Software Quality (CISQ), the Institute of Electrical and Electronics Engineers (IEEE), Department of Homeland Security (DHS), US Computer Emergency Response Team (CERT), the National Institute of Standards and Technology (NIST), MITRE, Open Web Application Security Project (OWASP) and the technology provider industry. The resulting analysis identifies specific flaws in the software and aggregates this information into metrics to objectively quantify the structural quality of the application.

## 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 V 3.2.1 release Overview

This section provide a summary of the most severe security vulnerability identified in the structural quality analysis and mesurement by CAST AIP against the Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures V3.2.1

## PCI DSS V 3.2.1 High Level Overview

Applicable coverage for CAST under PCI DSS V3.2.1 Standards.

|  |  |  |
| --- | --- | --- |
| **Module** | **Req#** | **Descriptions** |
| **Build and Maintain a Secure Network and Systems** | **1**  **2** | Install and maintain a firewall configuration to protect cardholder data  Do not use vendor-supplied defaults for system passwords and other security parameters |
| **Protect Cardholder Data** | **3**  **4** | Protect stored cardholder data  Encrypt transmission of cardholder data across open, public networks |
| **Maintain a Vulnerability Management Program** | **5**  **6** | Protect all systems against malware and regularly update anti-virus software or programs  Develop and maintain secure systems and applications |
| **Implement Strong Access Control Measures** | **7**  **8**  **9** | Restrict access to cardholder data by business need to know  Identify and authenticate access to system components  Restrict physical access to cardholder data |
| **Regularly Monitor and Test Networks** | **10**  **11** | Track and monitor all access to network resources and cardholder data  Regularly test security systems and processes |
| **Maintain an Information Security Policy** | **12** | Maintain a policy that addresses information security for all personnel |

*Table 2: PCI DSS Table*

## PCI DSS – Requirement 1

List of PCI DSS V321 Requirement 1 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 3: PCI-DSS-V3.2.1-Req1* *violations*

## PCI DSS – Requirement 2

List of PCI DSS V321 Requirement 2 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 4: PCI-DSS-V3.2.1-Req1* *violations*

## PCI DSS – Requirement 3

List of PCI DSS V321 Requirement 3 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 5: PCI-DSS-V3.2.1-Req3* *violations*

## PCI DSS – Requirement 4

List of PCI DSS V321 Requirement 4 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 6: PCI-DSS-V3.2.1-Req4* *violations*

## PCI DSS – Requirement 5

List of PCI DSS V321 Requirement 5 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 7: PCI-DSS-V3.2.1-Req5* *violations*

## PCI DSS – Requirement 6

List of PCI DSS V321 Requirement 6 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 8: PCI-DSS-V3.2.1-Req6* *violations*

## PCI DSS – Requirement 7

List of PCI DSS V321 Requirement 7 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 9: PCI-DSS-V3.2.1-Req7* *violations*

## PCI DSS – Requirement 8

List of PCI DSS V321 Requirement 8 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 10: PCI-DSS-V3.2.1-Req8* *violations*

## PCI DSS – Requirement 9

List of PCI DSS V321 Requirement 9 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 11: PCI-DSS-V3.2.1-Req-9* *violations*

## PCI DSS – Requirement 10

List of PCI DSS V321 Requirement 10 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 13: PCI-DSS-V3.2.1-Req-10* *violations*

## PCI DSS – Requirement 11

List of PCI DSS V321 Requirement 11 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 3: PCI-DSS-V3.2.1-Req-11* *violations*

## PCI DSS – Requirement 12

List of PCI DSS V321 Requirement 12 had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Violations | Added Violations | Removed Violations |
| 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 |

*Table 3: PCI-DSS-V3.2.1-Req-12* *violations*

# 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.

For more information on CAST Software Intelligence, visit - <https://www.castsoftware.com/software-intelligence>

## How CAST AIP Works

CAST connects into all major SCM systems or can take source code in whatever format it is maintained in the organization. Source code is then processed and stored in the CAST Knowledge Base as metadata, which forms the basis for the analysis and information provided by CAST AIP. CAST looks at the entire application—including legacy components, packaged app customizations, and all modern distributed technology environments. Data from third party code analyzers can be integrated into the CAST Knowledge Base and displayed in AIP dashboards.

