Author

CAST



**PCI DSS V3.1**

**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

1. Introduction

1.1. Application Characteristics

2. PCI DSS V 3.1 Release Overview

2.1. PCI DSS V 3.1 Summary

3. PCI DSS V 3.1 Findings Details

3.1. PCI DSS – Requirement 1

3.2. PCI DSS – Requirement 2

3.3. PCI DSS – Requirement 3

3.4. PCI DSS – Requirement 4

3.5. PCI DSS – Requirement 5

3.6. PCI DSS – Requirement 6

3.7. PCI DSS – Requirement 7

3.8. PCI DSS – Requirement 8

3.9. PCI DSS – Requirement 10

4. Appendix

4.1. About CAST Software Intelligence

4.2. 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 STIG 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 V 3.1 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 V3.1

## PCI DSS V 3.1 Summary

PCI DSS V 3.1 Modules descriptions.

|  |  |  |
| --- | --- | --- |
| **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** | Restrict access to cardholder data by business need to know  Identify and authenticate access to system components |
| Regularly Monitor and Test Networks | **10** | Track and monitor all access to network resources and cardholder data |

*Table 2: PCI DSS Module Description*

Findings summary for CAST under PCI DSS V3.1 Standards.

|  |  |  |  |
| --- | --- | --- | --- |
| PCI-DSS-V3.1 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| Requirement 1 | 0 | 0 | 0 |
| Requirement 2 | 0 | 0 | 0 |
| … | 0 | 0 | 0 |

*Table 3: PCI DSS 3.1 Summary Table*

# PCI DSS V 3.1 Findings Details

## PCI DSS – Requirement 1

List of PCI DSS V3.1 Requirement 1 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req1* *vulnerabilities*

## PCI DSS – Requirement 2

List of PCI DSS V3.1 Requirement 2 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req2* *vulnerabilities*

## PCI DSS – Requirement 3

List of PCI DSS V3.1 Requirement 3 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req3* *vulnerabilities*

## PCI DSS – Requirement 4

List of PCI DSS V3.1 Requirement 4 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req4* *vulnerabilities*

## PCI DSS – Requirement 5

List of PCI DSS V3.1 Requirement 5 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req5* *vulnerabilities*

## PCI DSS – Requirement 6

List of PCI DSS V3.1 Requirement 6 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req6* *vulnerabilities*

## PCI DSS – Requirement 7

List of PCI DSS V3.1 Requirement 7 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req7* *vulnerabilities*

## PCI DSS – Requirement 8

List of PCI DSS V3.1 Requirement 8 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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-V3.1-Req8* *vulnerabilities*

## PCI DSS – Requirement 10

List of PCI DSS V3.1 Requirement 10 that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| Rules | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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 12 : PCI-DSS-V3.1-Req-10* *vulnerabilities*

# 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).