Author

CAST



**NIST SP 800 53R4**

**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. NIST SP 800 53R4 release Overview 4

NIST SP 800 53R4 High Level Overview 4

2.1. NIST-SP-800-53R4-AC 5

2.2. NIST-SP-800-53R4-AU 5

2.3. NIST-SP-800-53R4-CA 6

2.4. NIST-SP-800-53R4-CM 6

2.5. NIST-SP-800-53R4-IA 7

2.6. NIST-SP-800-53R4-SA 7

2.7. NIST-SP-800-53R4-SC 8

2.8. NIST-SP-800-53R4-SI 8

3. Appendix 9

3.1. About CAST Software Intelligence 9

3.2. How CAST AIP Works 9

# 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*

# NIST SP 800 53R4 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

## NIST SP 800 53R4 High Level Overview

Applicable coverage for CAST under NIST SP800 53R4 Standards.

|  |  |  |  |
| --- | --- | --- | --- |
| NIST SP800 53R4 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| Requirement 1 | 0 | 0 | 0 |
| Requirement 2 | 0 | 0 | 0 |
| … | 0 | 0 | 0 |

## NIST-SP-800-53R4-AC

List of NIST-SP-800-53R4 Access Controls that 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 |

## NIST-SP-800-53R4-AU

List of NIST-SP-800-53R4 Audit and Accountability Controls that 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 |

## NIST-SP-800-53R4-CA

List of NIST-SP-800-53R4 Security Assessment and Authorization Controls that 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 |

## NIST-SP-800-53R4-CM

List of NIST-SP-800-53R4 Configuration Management Controls that 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 |

## NIST-SP-800-53R4-IA

List of NIST-SP-800-53R4 Identification and Authentication Controls that 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 |

## NIST-SP-800-53R4-SA

List of NIST-SP-800-53R4 System and Service Acquisitions Controls that 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 |

## NIST-SP-800-53R4-SC

List of NIST-SP-800-53R4 System and Communication Protection Controls that 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 |

## NIST-SP-800-53R4-SI

List of NIST-SP-800-53R4 System and Information Integrity Controls that 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 |

# 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.

