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

1. Introduction

1.1. Application Characteristics

2. NIST SP 800 53R4 Release Overview

2.1. NIST SP 800 53R4 Summary

3. NIST SP 800 53R4 Findings Details

3.1. NIST-SP-800-53R4-AC

3.2. NIST-SP-800-53R4-AU

3.3. NIST-SP-800-53R4-CA

3.4. NIST-SP-800-53R4-CM

3.5. NIST-SP-800-53R4-IA

3.6. NIST-SP-800-53R4-SA

3.7. NIST-SP-800-53R4-SC

3.8. NIST-SP-800-53R4-SI

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 NIST 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*

# 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 Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4 ([Official Source](https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf))

## NIST SP 800 53R4 Summary

Findings summary based on 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 |

*Table 2: NIST SP800 53R4 standards summary*

# NIST SP 800 53R4 Findings Details

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

List of NIST-SP-800-53R4 Access Controls 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 3: NIST SP800 53R4 AC summary*

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

List of NIST-SP-800-53R4 Audit and Accountability Controls 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: NIST SP800 53R4 AU summary*

## 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 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: NIST SP800 53R4 CA summary*

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

List of NIST-SP-800-53R4 Configuration Management Controls 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: NIST SP800 53R4 CM summary*

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

List of NIST-SP-800-53R4 Identification and Authentication Controls 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: NIST SP800 53R4 IA summary*

## 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 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: NIST SP800 53R4 SA summary*

## 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 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: NIST SP800 53R4 SC summary*

## 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 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: NIST SP800 53R4 SI summary*

# 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).