Author

CAST



**CISQ Security**

**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. CISQ Security

2.1. CISQ Security Vulnerabilities Summary

3. CAST Findings for CISQ Security

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*

# CISQ Security

Security assesses the degree to which an application protects information and data so that persons or other products or systems have the degree of data access appropriate to their types and levels of authorization (ISO 25010). Security measures the risk of potential security breaches due to poor coding and architectural practices. Security problems have been studied extensively by the Software Assurance community and have been codified in the Common Weakness Enumeration (CWE) at [cwe.mitre.org](http://it-cisq.org/standards/automated-quality-characteristic-measures/security/cwe.mitre.org).

The CISQ Automated Source Code Security Measure draws from the [CWE/SANS Institute Top 25 Most Dangerous Software Errors](http://cwe.mitre.org/top25/#Listing) and identifies the most widespread and frequently exploited security weaknesses in software. Twenty-two of these weaknesses are detectable through analyzing the source code and form the basis of the CISQ measure. These 22 weaknesses constitute the most frequent ways unauthorized parties breach a system. Thus, the CISQ measure is a good predictor of how easily an application can suffer unauthorized penetration that results in stolen information, altered records, or other forms of malicious behavior.

This section provide a summary of the most severe security vulnerability identified in the structural quality analysis and mesurement by CAST AIP against the CISQ standard. Details about CISQ Security Standard can be found [here](http://it-cisq.org/standards/automated-quality-characteristic-measures/security/).

## CISQ Security Vulnerabilities Summary

Findings summary for CAST under CISQ Security Standards.

| CISQ-Security | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| --- | --- | --- | --- |
| ASCSM-CWE-22 | 0 | 0 | 0 |
| ASCSM-CWE-78 | 0 | 0 | 0 |
| ASCSM-CWE-79 | 0 | 0 | 0 |
| ASCSM-CWE-89 | 0 | 0 | 0 |
| ASCSM-CWE-… | 0 | 0 | 0 |

*Table 2: CISQ Security summary table*

# CAST Findings for CISQ Security

List of CAST findings related to CISQ Security.

| 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 |

*Table 3: CISQ Security* *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).