Author

CAST



**CISQ Security**

**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. Security Violation Overview 4

2.1. CISQ 22 violations 4

2.2. ASCSM-CWE-22 - Path Traversal Improper Input Neutralization 5

2.3. ASCSM-CWE-78 – OS Command Injection Improper Input Neutralization 5

2.4. ASCSM-CWE-79 – Cross-site Scripting Improper Input Neutralization 5

2.5. ASCSM-CWE-89 – SQL Injection Improper Input Neutralization 6

2.6. ASCSM-CWE-99 – Name or Reference Resolution Improper Input Neutralization 6

2.7. ASCSM-CWE-120 – Buffer Copy without Checking Size of Input 6

2.8. ASCSM-CWE-252-resource– Unchecked Return Parameter Value of named Callable and Method Control Element with Read, Write, and Manage Access to Platform Resource 7

2.9. ASCSM-CWE-134 – Format String Improper Input Neutralization 7

2.10. ASCSM-CWE-134 – Format String Improper Input Neutralization 7

2.11. ASCSM-CWE-327 – Broken or Risky Cryptographic Algorithm Usage 8

2.12. ASCSM-CWE-396 – Declaration of Catch for Generic Exception 8

2.13. ASCSM-CWE-397 – Declaration of Throws for Generic Exception 8

2.14. ASCSM-CWE-434 – File Upload Improper Input Neutralization 9

2.15. ASCSM-CWE-456 – Storable and Member Data Element Missing Initialization 9

2.16. ASCSM-CWE-606 – Unchecked Input for Loop Condition 9

2.17. ASCSM-CWE-667 – Shared Resource Improper Locking 10

2.18. ASCSM-CWE-672 – Expired or Released Resource Usage 10

2.19. ASCSM-CWE-681 – Numeric Types Incorrect Conversion 10

2.20. ASCSM-CWE-706 – Name or Reference Resolution Improper Input Neutralization 11

2.21. ASCSM-CWE-772 – Missing Release of Resource after Effective Lifetime 11

2.22. ASCSM-CWE-789 – Uncontrolled Memory Allocation 11

2.23. ASCSM-CWE-798 – Hard-Coded Credentials Usage for Remote Authentication 12

2.24. ASCSM-CWE-835 – Loop with Unreachable Exit Condition (Infinite Loop) 12

3. Appendix 13

3.1. About CAST Software Intelligence 13

3.2. How CAST AIP Works 13

# 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 CISQ 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*

# Security Violation Overview

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

## CISQ 22 violations

List of CISQ rules 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 |

*Table 2: CISQ Top 22 Rules*

## ASCSM-CWE-22 - Path Traversal Improper Input Neutralization

List of ASCSM-CWE-22 violations 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 |

*Table 3: ASCSM-CWE-22* *violations*

## ASCSM-CWE-78 – OS Command Injection Improper Input Neutralization

List of ASCSM-CWE-78 violations 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 |

*Table 4: ASCSM-CWE-78* *violations*

## ASCSM-CWE-79 – Cross-site Scripting Improper Input Neutralization

List of ASCSM-CWE-79 violations 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 |

*Table 5: ASCSM-CWE-79* *violations*

## ASCSM-CWE-89 – SQL Injection Improper Input Neutralization

List of ASCSM-CWE-89 rules 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 |

*Table 6: ASCSM-CWE-89* *violations*

## ASCSM-CWE-99 – Name or Reference Resolution Improper Input Neutralization

List of ASCSM-CWE-99 rules 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 |

*Table 7: ASCSM-CWE-99* *violations*

## ASCSM-CWE-120 – Buffer Copy without Checking Size of Input

List of ASCSM-CWE-120 rules 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 |

*Table 8: ASCSM-CWE-120 violations*

## ASCSM-CWE-129 – Unchecked array index range

List of ASCSM-CWE-129 rules 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 |

*Table 9: ASCSM-CWE-129 violations*

## ASCSM-CWE-134 – Format String Improper Input Neutralization

List of ASCSM-CWE-134 rules 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 |

*Table 10: ASCSM-CWE-134 violations*

## ASCSM-CWE-252-resource– Unchecked Return Parameter Value of named Callable and Method Control Element with Read, Write, and Manage Access to Platform Resource

List of ASCSM-CWE-252-resource rules 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 |

*Table 11: ASCSM-CWE-252-resource violations*

## ASCSM-CWE-327 – Broken or Risky Cryptographic Algorithm Usage

List of ASCSM-CWE-327 rules 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 |

*Table 12: ASCSM-CWE-327 violations*

## ASCSM-CWE-396 – Declaration of Catch for Generic Exception

List of ASCSM-CWE-396 rules 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 |

*Table 13: ASCSM-CWE-396 violations*

## ASCSM-CWE-397 – Declaration of Throws for Generic Exception

List of ASCSM-CWE-397 rules 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 |

*Table 14: ASCSM-CWE-397 violations*

## ASCSM-CWE-434 – File Upload Improper Input Neutralization

List of ASCSM-CWE-434 rules 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 |

*Table 15: ASCSM-CWE-434 violations*

## ASCSM-CWE-456 – Storable and Member Data Element Missing Initialization

List of ASCSM-CWE-456 rules 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 |

*Table 16: ASCSM-CWE-456 violations*

## ASCSM-CWE-606 – Unchecked Input for Loop Condition

List of ASCSM-CWE-606 rules 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 |

*Table 17: ASCSM-CWE-606 violations*

## ASCSM-CWE-667 – Shared Resource Improper Locking

List of ASCSM-CWE-667 rules 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 |

*Table 18: ASCSM-CWE-667 violations*

## ASCSM-CWE-672 – Expired or Released Resource Usage

List of ASCSM-CWE-672 rules 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 |

*Table 19: ASCSM-CWE-672 violations*

## ASCSM-CWE-681 – Numeric Types Incorrect Conversion

List of ASCSM-CWE-681 rules 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 |

*Table 20: ASCSM-CWE-681 violations*

## ASCSM-CWE-772 – Missing Release of Resource after Effective Lifetime

List of ASCSM-CWE-772 rules 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 |

*Table 21: ASCSM-CWE-772 violations*

## ASCSM-CWE-789 – Uncontrolled Memory Allocation

List of ASCSM-CWE-789 rules 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 |

*Table 22: ASCSM-CWE-789 violations*

## ASCSM-CWE-798 – Hard-Coded Credentials Usage for Remote Authentication

List of ASCSM-CWE-798 rules 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 |

*Table 23: ASCSM-CWE-798 violations*

## ASCSM-CWE-835 – Loop with Unreachable Exit Condition (Infinite Loop)

List of ASCSM-CWE-835 rules 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 |

*Table 24: ASCSM-CWE-835 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.

