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

1. Introduction

1.1. Application Characteristics

2. Security Violation Overview

2.1. CISQ Security Vulnerabilities

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

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

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

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

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

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

2.8. ASCSM-CWE-129 – Unchecked array index range

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

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

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

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

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

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

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

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

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

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

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

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

2.21. ASCSM-CWE-789 – Uncontrolled Memory Allocation

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

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

3. Appendix

3.1. About CAST Software Intelligence

3.2. 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 CISQ Security standards.

CAST AIP adapts the quality rules from best-in-class industry standards (OWASP, CWE, CISQ). 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*

# Security Violation 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 CISQ standard. Details about CISQ Security Standard can be found [here](http://it-cisq.org/standards/automated-quality-characteristic-measures/security/).

## CISQ Security Vulnerabilities

List of CISQ rules that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| 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 Top 22 Rules*

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

List of ASCSM-CWE-22 Vulnerabilities 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 |

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

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

List of ASCSM-CWE-78 Vulnerabilities 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 |

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

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

List of ASCSM-CWE-79 Vulnerabilities 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 |

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

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

List of ASCSM-CWE-89 rules 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 |

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

## 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 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 7: ASCSM-CWE-99* *Vulnerabilities*

## 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 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 8: ASCSM-CWE-120 Vulnerabilities*

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

List of ASCSM-CWE-129 rules 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 |

*Table 9: ASCSM-CWE-129 Vulnerabilities*

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

List of ASCSM-CWE-134 rules 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 |

*Table 10: ASCSM-CWE-134 Vulnerabilities*

## 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 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 11: ASCSM-CWE-252-resource Vulnerabilities*

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

List of ASCSM-CWE-327 rules 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 |

*Table 12: ASCSM-CWE-327 Vulnerabilities*

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

List of ASCSM-CWE-396 rules 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 |

*Table 13: ASCSM-CWE-396 Vulnerabilities*

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

List of ASCSM-CWE-397 rules 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 |

*Table 14: ASCSM-CWE-397 Vulnerabilities*

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

List of ASCSM-CWE-434 rules 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 |

*Table 15: ASCSM-CWE-434 Vulnerabilities*

## 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 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 16: ASCSM-CWE-456 Vulnerabilities*

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

List of ASCSM-CWE-606 rules 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 |

*Table 17: ASCSM-CWE-606 Vulnerabilities*

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

List of ASCSM-CWE-667 rules 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 |

*Table 18: ASCSM-CWE-667 Vulnerabilities*

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

List of ASCSM-CWE-672 rules 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 |

*Table 19: ASCSM-CWE-672 Vulnerabilities*

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

List of ASCSM-CWE-681 rules 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 |

*Table 20: ASCSM-CWE-681 Vulnerabilities*

## 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 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 21: ASCSM-CWE-772 Vulnerabilities*

## ASCSM-CWE-789 – Uncontrolled Memory Allocation

List of ASCSM-CWE-789 rules 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 |

*Table 22: ASCSM-CWE-789 Vulnerabilities*

## 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 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 23: ASCSM-CWE-798 Vulnerabilities*

## 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 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 24: ASCSM-CWE-835 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/software-intelligence) 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, and OWASP.

To find out more about CAST Security, [click here](https://www.castsoftware.com/use-cases/application-security).