

Author

CAST

**Application Security & Development  
Security Technical Implement Guide**

**STIG Ver 4 Release 8**

**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. STIG Ver 4 Release 8 Summary

2.1. STIG Ver 4 Release 8 Summary for ASD

3. STIG Ver 4 Release 8 CAT I Findings Summary

4. STIG Ver 4 Release 8 CAT II Findings Summary

5. STIG Ver 4 Release 8 CAT III Findings Summary

6. Appendix

6.1. About CAST Software Intelligence

6.2. 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*

# STIG Ver 4 Release 8 Summary

This section provide a summary of the most severe security vulnerability identified in the structural quality analysis and mesurement by CAST AIP against the Application Security and Development (ASD) Security Technical Implementation Guide overview

Agency (DISA) “develops and maintains control correlation identifiers (CCIs), security requirements guide (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures

STIG Distribution and Reference: Parties within the DoD and Federal Government’s computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. For more details click on [STIG](http://iase.disa.mil/).

## STIG Ver 4 Release 8 Summary for ASD

**Vulnerability Severity Category Code Definitions**

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified is assigned a Severity Category Code of CAT I, II, or III.

CAT I: Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.

CAT II: Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.

CAT III: Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

**Findings summary for CAST under ASD STIG V4R8.**

| STIG V4R8 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| --- | --- | --- | --- |
| Cat1 | 0 | 0 | 0 |
| Cat2 | 0 | 0 | 0 |
| Cat3 | 0 | 0 | 0 |

*Table 2: STIG V4R8 summary*

**Findings summary for CAST under ASD STIG V4R8 with sub-standards.**

| STIG V4R8 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| --- | --- | --- | --- |
| Cat1 | 0 | 0 | 0 |
| Cat2 | 0 | 0 | 0 |
| Cat3 | 0 | 0 | 0 |

*Table 3: STIG V4R8 Overview*

# STIG Ver 4 Release 8 CAT I Findings Summary

List of STIG CAT I violations 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: STIG V4R8 CAT1 summary*

# STIG Ver 4 Release 8 CAT II Findings Summary

List of STIG CAT II violations 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: STIG V4R8 CAT2 summary*

# STIG Ver 4 Release 8 CAT III Findings Summary

List of STIG CAT III violations 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: STIG V4R8 CAT3 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).