Author

CAST



**CWE 2011 Top 25**

**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. CWE Top 25 Vulnerabilities

2.2. CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

2.3. CWE-78 – Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

2.4. CWE-79 – Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

2.5. CWE-89 – Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

2.6. CWE-120 – Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

2.7. CWE-131– Incorrect Calculation of Buffer Size

2.8. CWE-134 – Use of Externally-Controlled Format String

2.9. CWE-190 – Integer Overflow or Wraparound

2.10. CWE-250 – Execution with Unnecessary Privileges

2.11. CWE-306 – Missing Authentication for Critical Function

2.12. CWE-307 – Improper Restriction of Excessive Authentication Attempts

2.13. CWE-311 – Missing Encryption of Sensitive Data

2.14. CWE-327 – Use of a Broken or Risky Cryptographic Algorithm

2.15. CWE-352 – Cross-Site Request Forgery (CSRF)

2.16. CWE-434 – Unrestricted Upload of File with Dangerous Type

2.17. CWE-494 – Download of Code Without Integrity Check

2.18. CWE-601 – URL Redirection to Untrusted Site ('Open Redirect')

2.19. CWE-676 – Use of Potentially Dangerous Function

2.20. CWE-732– Incorrect Permission Assignment for Critical Resource

2.21. CWE-759 – Use of a One-Way Hash without a Salt

2.22. CWE-798 – Use of Hard-coded Credentials

2.23. CWE-807 – Reliance on Untrusted Inputs in a Security Decision

2.24. CWE-829 – Inclusion of Functionality from Untrusted Control Sphere

2.25. CWE-862 – Missing Authorization

2.26. CWE-863 – Incorrect Authorization

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 CWE Top 25 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 CWE Top 25 standard. Details about CWE Security Standard can be found [here](https://cwe.mitre.org/data/definitions/900.html).

## CWE Top 25 Vulnerabilities

List of CWE top 25 rules that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| CWE-2011-Top25 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| CWE-22 | 0 | 0 | 0 |
| CWE-78 | 0 | 0 | 0 |
| CWE-79 | 0 | 0 | 0 |
| CWE-89 | 0 | 0 | 0 |
| CWE-… | 0 | 0 | 0 |

*Table 2: CWE Top 25 Rules*

## CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

List of CWE - 22 Vulnerabilities that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-22* *Vulnerabilities*

## CWE-78 – Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

List of CWE-78 Vulnerabilities that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-78* *Vulnerabilities*

## CWE-79 – Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

List of CWE-79 Vulnerabilities that had any findings in this application.

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-79* *Vulnerabilities*

## CWE-89 – Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

List of CWE-89 rules that had any findings in this application

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-89* *Vulnerabilities*

## CWE-120 – Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

List of CWE-120 rules that had any findings in this application

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-120* *Vulnerabilities*

## CWE-131– Incorrect Calculation of Buffer Size

List of CWE-131 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-131 Vulnerabilities*

## CWE-134 – Use of Externally-Controlled Format String

List of CWE-134 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-134 Vulnerabilities*

## CWE-190 – Integer Overflow or Wraparound

List of CWE-190 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-190 Vulnerabilities*

## CWE-250 – Execution with Unnecessary Privileges

List of CWE-250 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-250 Vulnerabilities*

## CWE-306 – Missing Authentication for Critical Function

List of CWE-306 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-306 Vulnerabilities*

## CWE-307 – Improper Restriction of Excessive Authentication Attempts

List of CWE-307 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-307 Vulnerabilities*

## CWE-311 – Missing Encryption of Sensitive Data

List of CWE-311 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-311 Vulnerabilities*

## CWE-327 – Use of a Broken or Risky Cryptographic Algorithm

List of CWE-327 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-327 Vulnerabilities*

## CWE-352 – Cross-Site Request Forgery (CSRF)

List of CWE-352 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-352 Vulnerabilities*

## CWE-434 – Unrestricted Upload of File with Dangerous Type

List of CWE-434 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-434 Vulnerabilities*

## CWE-494 – Download of Code Without Integrity Check

List of CWE-494 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-494 Vulnerabilities*

## CWE-601 – URL Redirection to Untrusted Site ('Open Redirect')

List of CWE-601 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-601 Vulnerabilities*

## CWE-676 – Use of Potentially Dangerous Function

List of CWE-676 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-676 Vulnerabilities*

## CWE-732– Incorrect Permission Assignment for Critical Resource

List of CWE-732 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-732 Vulnerabilities*

## CWE-759 – Use of a One-Way Hash without a Salt

List of CWE-759 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-759 Vulnerabilities*

## CWE-798 – Use of Hard-coded Credentials

List of CWE-798 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-798 Vulnerabilities*

## CWE-807 – Reliance on Untrusted Inputs in a Security Decision

List of CWE-807 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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: CWE-807 Vulnerabilities*

## CWE-829 – Inclusion of Functionality from Untrusted Control Sphere

List of CWE-829 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 25: CWE-829 Vulnerabilities*

## CWE-862 – Missing Authorization

List of CWE-862 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 26: CWE-862 Vulnerabilities*

## CWE-863 – Incorrect Authorization

List of CWE-863 rules that had any findings in this application -

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 27: CWE-863 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).