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

Table of Content 2

1. Introduction 3

1.1. Application Characteristics 3

2. Security Violation Overview 4

2.1. CWE Top 25 violations 4

2.2. CWE-22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') 5

2.3. CWE-78 – Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') 5

2.4. CWE-79 – Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') 5

2.5. CWE-89 – Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') 6

2.6. CWE-120 – Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') 6

2.7. CWE-131– Incorrect Calculation of Buffer Size 6

2.8. CWE-134 – Use of Externally-Controlled Format String 7

2.9. CWE-190 – Integer Overflow or Wraparound 7

2.10. CWE-250 – Execution with Unnecessary Privileges 7

2.11. CWE-306 – Missing Authentication for Critical Function 8

2.12. CWE-307 – Improper Restriction of Excessive Authentication Attempts 8

2.13. CWE-311 – Missing Encryption of Sensitive Data 8

2.14. CWE-327 – Use of a Broken or Risky Cryptographic Algorithm 9

2.15. CWE-352 – Cross-Site Request Forgery (CSRF) 9

2.16. CWE-434 – Unrestricted Upload of File with Dangerous Type 9

2.17. CWE-494 – Download of Code Without Integrity Check 10

2.18. CWE-601 – URL Redirection to Untrusted Site ('Open Redirect') 10

2.19. CWE-676 – Use of Potentially Dangerous Function 10

2.20. CWE-732– Incorrect Permission Assignment for Critical Resource 11

2.21. CWE-759 – Use of a One-Way Hash without a Salt 11

2.22. CWE-798 – Use of Hard-coded Credentials 11

2.23. CWE-807 – Reliance on Untrusted Inputs in a Security Decision 12

2.24. CWE-829 – Inclusion of Functionality from Untrusted Control Sphere 12

2.25. CWE-862 – Missing Authorization 12

2.26. CWE-863 – Incorrect Authorization 13

3. Appendix 14

3.1. About CAST Software Intelligence 14

3.2. How CAST AIP Works 14

# 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 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 CWE standard. Details about CWE Security Standard can be found at - https://cwe.mitre.org/data/definitions/900.html

## CWE Top 25 violations

List of CWE top 25 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: CWE Top 25 Rules*

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

List of 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: CWE-22* *violations*

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

List of 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: CWE-78* *violations*

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

List of 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: CWE-79* *violations*

## 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

|  |  |  |  |
| --- | --- | --- | --- |
| 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: CWE-89* *violations*

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

List of 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 7: CWE-120* *violations*

## CWE-131– Incorrect Calculation of Buffer Size

List of CWE-131 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: CWE-131 violations*

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

List of 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 9: CWE-134 violations*

## CWE-190 – Integer Overflow or Wraparound

List of CWE-190 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: CWE-190 violations*

## CWE-250 – Execution with Unnecessary Privileges

List of CWE-250 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: CWE-250 violations*

## CWE-306 – Missing Authentication for Critical Function

List of CWE-306 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: CWE-306 violations*

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

List of CWE-307 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: CWE-307 violations*

## CWE-311 – Missing Encryption of Sensitive Data

List of CWE-311 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: CWE-311 violations*

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

List of 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 15: CWE-327 violations*

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

List of CWE-352 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: CWE-352 violations*

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

List of 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 17: CWE-434 violations*

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

List of CWE-494 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: CWE-494 violations*

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

List of CWE-601 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: CWE-601 violations*

## CWE-676 – Use of Potentially Dangerous Function

List of CWE-676 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: CWE-676 violations*

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

List of CWE-732 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: CWE-732 violations*

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

List of CWE-759 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: CWE-759 violations*

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

List of 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: CWE-798 violations*

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

List of CWE-807 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: CWE-807 violations*

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

List of CWE-829 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 25: CWE-829 violations*

## CWE-862 – Missing Authorization

List of CWE-862 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 26: CWE-862 violations*

## CWE-863 – Incorrect Authorization

List of CWE-863 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 27: CWE-863 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.

