Author

CAST

 **OWASP TOP 10 2017**

Application Name –

Version –

CAST AIP -

|  |
| --- |
|  |
|  |

Monday, xx July 2012

My Application Name

Version Number

My CAST Version

# Summary

1. Summary 2

2. Introduction 3

2.1. Application Characteristics 3

2.2. Application Health(Security) 4

3. Security Violation Overview 5

3.1. OWASP -2013 Top 10 violations 5

3.2. OWASP -2017 Top 10 violations 6

4. Security Violation Details 7

4.1. OWASP -2013 Top 10 Violation Details 7

4.2. OWASP -2017 Top 10 Violation Details 15

5. Appendix 22

5.1. CAST Application Intelligence Platform 22

# Introduction

This assessment is an effort to determine the security health of Wembley 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 current industry best practices and known design flaws that may impact security posture. 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 Wembley 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 Fig 1: Application characteristics*

## Application Health (Security)

CAST AIP provides architects and engineers the ability to examine and drill down on critical application characteristics and attributes. The primary application health factor that is addressed in this assessment is Security, but a complete assessment can also be availed that provides some insight into: Robustness, Performance Efficiency, Transferability, and Changeability. (For detailed definitions of these attributes, see page 11 in the Appendix.)

|  |  |
| --- | --- |
| Quality Characteristics | Wembley |
| Security Score | 2.59 |
| Critical Violation | 528 |
| -Per File | 0.08 |
| -per KLOC | 1.04 |
| Complex Objects | 44 |
| -with violations | 38 |

*Table 3: Summary of application Security Health*

# 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 OWASP standard.

## OWASP -2017 Top 10 violations

List of OWASP -2017 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 4: OWASP 2017 Top 10 Rules*

## OWASP -2017 A1 - Injection

List of 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 |

## OWASP -2017 A3 – Sensitive Data Exposure

List of 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 |

## OWASP -2017 A6 – Security MisConfiguration

List of 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 |

## OWASP -2017 A7 – Cross-Site Scripting (XSS)

List of 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 |

## OWASP -2017 A8 – Insecure Deserialization

List of 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 |

## OWASP -2017 A9 – Using Components with known Vulnerabilities

List of 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 |

# Security Violation Details

## OWASP -2017 Top 10 Violation Details

|  |
| --- |
| Object name |
| Violation #1 |
| …. |

# Appendix

## CAST Application Intelligence Platform

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.

