

作者

CAST



**CISQ 合规报告**

|  |
| --- |
|  |
|  |

日期：

**应用名称：**我的应用名称

**版本：** 版本编号

**CAST AIP：**我的CAST 版本

# 目录

1. 简介

1.1. 应用特征

2. CISQ 总结

2.1. CISQ 违规总结

3. CISQ安全性评估——CAST调查结果

4. CISQ可靠性评估——CAST调查结果

5. CISQ性能效率评估——CAST调查结果

6. CISQ可维护性评估——CAST调查结果

7. 附件

7.1. 关于CAST软件智能

7.2. 关于CISQ自动化质量特性评估

# 简介

本评估根据CISQ规则，了解指定应用的整体质量，并衡量应用的总体运行状况。本评估使用CAST应用智能平台（CAST AIP）对指定应用进行扫描，基于当前行业最佳实践以及可能影响性能的已知设计缺陷信息，对架构、设计和代码进行审查。

CAST AIP根据来自软件工程协会（SEI）、国际标准组织（ISO）、信息技术软件质量联盟（CISQ）、电气和电子工程师协会（IEEE）以及技术供应商行业的标准规范和测量方法，进行1200多项评估检查，分析识别应用具体缺陷，并采用评估指标，划分分析结果，客观量化应用的结构质量。

## 应用特征

本评估仅关注所述应用的技术实现（从数据库到用户界面），不分析业务功能。

|  |  |
| --- | --- |
| 名称 | 值 |
| kLoC | 504 |
| Files | 6,586 |
| Classes | 593 |
| SQL Art. | 0 |
| Tables | 119 |

*图 1: 应用技术特征 表1: 应用特征*

# CISQ 总结

本节概述CAST AIP在结构质量分析评估中，根据CISQ标准，识别的应用违反CISQ的具体漏洞。有关CISQ标准的详细信息，请参见[此处](http://it-cisq.org/standards/automated-quality-characteristic-measures)。

## CISQ 违规总结

CISQ标准下CAST识别的违规列表。

| 规则 | 总违规 | 新增违规 | 移除违规 |
| --- | --- | --- | --- |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表 2: CISQ 总结*

# CISQ安全性评估——CAST调查结果

安全性评估是为了了解应用保护信息和数据安全的程度，以便对相关人员及其他产品、系统提供与其权限类型/级别相匹配的数据访问等级（ISO 25010）。安全性评估识别不良编码和应用架构导致的潜在安全漏洞风险。软件保障社区（Software Assurance community）对安全问题进行了广泛的研究，安全问题被编入常见漏洞列表信息（CWE），发布于cwe.mitre.org。

基于CWE/系统网络安全协会发布的25个最危险的软件缺陷，CISQ自动源代码安全评估确定软件中最普遍、最常被利用的安全漏洞，其中22个软件缺陷可通过源代码分析被识别出来，构成CISQ度量的基础。这22个缺陷是未经授权的一方系统违规的最常见方式，这些未经授权的渗透将导致信息被盗、记录更改或其他形式的恶意行为，CISQ度量可以很好地预测应用遭受未经授权的渗透的难易程度。

CAST识别的CISQ安全违规列表

| CAST 规则 | 总违规 | 新增违规 | 移除违规 |
| --- | --- | --- | --- |
| 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 |

*表3: CISQ 安全违规*

# CISQ可靠性评估——CAST调查结果

可靠性评估是对潜在应用故障风险及应用在意外情况下的稳定性进行度量。根据ISO/IEC/IEEE 24765，可靠性是指一个系统、产品或组件在规定的条件下，在规定的时间段内执行规定功能的程度。可靠性评估的目的是防止或减少可能导致用户受到直接影响的应用宕机、中断、数据损坏和错误。

CISQ自动化源代码可靠性评估包括29个严重违反架构和编码实践的行为，这些行为会影响应用程序的可用性、容错性、可恢复性和数据完整性。CISQ可靠性评估基于软件中发现的违规次数生成质量分数，当除以软件的大小时，可将其转换为密度度量。

CAST识别的CISQ可靠性违规列表

| CAST 规则 | 总违规 | 新增违规 | 移除违规 |
| --- | --- | --- | --- |
| 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 |

*表4: CISQ 可靠性违规*

# CISQ性能效率评估——CAST调查结果

性能效率评估是对在规定条件下影响应用响应和资源使用的应用特性（ISO/IEC 25010）进行评估。性能效率影响客户满意度、员工生产力、应用可扩展性，还导致响应时间慢、处理/存储资源的使用效率低。应用的性能效率取决于每个组件的性能，也取决于每个组件对自身所参与的、组成事务的组件链的行为的影响。

CISQ性能效率自动源代码评估由15个严重违反响应时间、处理器使用和应用内存使用的行为组成。质量分数是根据源代码中发现的违规次数产生的，当除以软件大小时，可以用作密度度量。

CAST识别的CISQ效率性违规列表

| CAST 规则 | 总违规 | 新增违规 | 移除违规 |
| --- | --- | --- | --- |
| 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 |

*表5: CISQ 效率性违规*

# CISQ可维护性评估——CAST调查结果

CAST识别的CISQ可维护性违规列表

| CAST 规则 | 总违规 | 新增违规 | 移除违规 |
| --- | --- | --- | --- |
| 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 |

*表6: CISQ 可维护性违规*

# 附件

## 关于CAST软件智能

软件智能提供软件架构、端到端事务流、数据访问模式等方面的深刻洞察力，帮助提高IT团队工作效率。CAST软件智能已成功帮助数百家国际知名企业改善其最终用户满意度、加快其产品上市时间、防止业务中断并有效降低成本，使企业级客户能够克服技术障碍、成熟应对创新潮流。

了解更多CAST软件智能相关信息，请点击[此处](https://www.castsoftware.com/software-intelligence)。

## 关于CISQ质量特性自动评估

CISQ开发了质量特性自动评估方法，用以管理应用软件的结构质量。CISQ安全性、可靠性、性能效率和可维护性的自动化评估方法经对象管理组织OMG®认证，是全球通用的IT组织标准。

CISQ标准由编码规则发展而来，内容包括IT组织需避免的、由静态代码分析检测到的、严重违反良好架构和编码实践的违规行为。CISQ评估与质量相关的架构和编码违规数量，然后创建缺陷密度的评估指标。

|  |  |
| --- | --- |
| 安全性 | 基于通用缺陷列表（CWE）存储库的前25个安全漏洞，评估源代码关键安全违规 |
| 可靠性 | 评估软件可用性、容错性、可恢复性方面的关键违规 |
| [性能效率](http://it-cisq.org/standards/automated-quality-characteristic-measures/performance-efficiency/) | 评估软件对响应时间、处理器、内存及其他资源利用的关键违规 |
| 可维护性 | 评估应用的模块、架构遵从、可重复使用性、可分析性和可变更性方面的关键违规 |