作者

CAST

******

**CISQ 安全性**

**合规报告**

应用名称– 我的应用名称

版本 – 版本编号

CAST AIP – 我的CAST版本

|  |
| --- |
|  |
|  |

日期：

# 目录

1. 简介

1.1. 应用特征

2. CISQ 安全性

2.1. CISQ 安全漏洞总结

3. CISQ安全相关的CAST分析结果

4. 附件

4.1. 关于CAST软件智能

4.2. 关于CAST安全性

# 简介

本评估的目的是了解应用的安全状况，确定导致当前安全问题的根本原因，以及将来降级的任何风险。本评估使用CAST应用智能平台（CAST AIP）自动扫描应用，根据CISQ标准审查架构、设计和代码。

CAST AIP采用权威行业标准（OWASP、CWE、CISQ、STIG、PCI、NIST）的质量规则。CAST具有独特的数据流分析和系统级分析（从表示层到数据库层）能力，提供准确的安全发现，减少误报。

## 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 安全性

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个最危险的软件错误，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，其中有22个软件错误可通过源代码分析被识别出来，构成CISQ度量的基础。这22个错误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。

本节概述了CAST AIP根据CISQ标准进行的结构质量分析和测量中发现的最严重安全漏洞。有关CISQ安全标准的详细信息请点击[此处](http://it-cisq.org/standards/automated-quality-characteristic-measures/security/)。

## CISQ 安全漏洞总结

CISQ安全标准下CAST的调查结果。

| CISQ-安全性规则 | 总违规 | 添加违规 | 移除违规 |
| --- | --- | --- | --- |
| ASCSM-CWE-22 | 0 | 0 | 0 |
| ASCSM-CWE-78 | 0 | 0 | 0 |
| ASCSM-CWE-79 | 0 | 0 | 0 |
| ASCSM-CWE-89 | 0 | 0 | 0 |
| ASCSM-CWE-… | 0 | 0 | 0 |

*表2: CISQ 安全性总结列表*

# CISQ安全相关的CAST分析结果

CISQ安全相关的CAST分析结果列表

| 规则 | 总违规 | 添加违规 | 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 安全漏洞*

# 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CAST安全性

应对网络风险，保障应用安全，需采取主动的、智能的方法。CAST 软件智能帮助团队在开始开发前深入探索发现应用的架构安全盲点。凭借其独特的数据流分析和系统级别分析能力，CAST提供最准确的安全发现，减少安全误报。CAST安全规则来自一流的行业标准——CISQ、CWE、OWASP、PCI-DSS、NIST和STIG。了解CAST安全性的更多信息，请点击[此处](https://www.castsoftware.com/products/security-dashboard)。