Author

CAST



**CWE (2011) Top 25**

**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. CWE (2011) Top 25 总结

2.1. CWE (2011) Top 25 违规发现

3. CWE (2011) Top 25 —— CAST分析结果

4. 附录

4.1. 关于CAST软件智能

4.2. 关于CAST安全性

# 简介

本评估旨在评估确定应用安全健康状况，了解导致当前应用安全风险的根本原因，并识别应用之后可能面临的风险。评估使用CAST应用智能平台（CAST AIP）对应用进行自动扫描，根据“CWE Top 25软件错误”来审查架构、设计和代码。

CAST AIP采用的质量规则来自权威行业标准（OWASP, CWE, CISQ, STIG, PCI, NIST）。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

本评估仅关注指定应用的技术实现（从数据库到用户界面），不分析业务功能。

|  |  |
| --- | --- |
| **Name** | **Value** |
| 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*

# CWE (2011) Top 25 总结

本节概述CAST AIP进行系统结构质量分析发现的关键安全漏洞，这些安全漏洞违反了“CWE 25种最危险的软件错误”标准。有关CWE安全标准的详细信息请点击[此处](https://cwe.mitre.org/data/definitions/900.html)。

## CWE (2011) Top 25 漏洞总结

对应CWE-2011-Top25标准，CAST分析结果总结

| CWE Top25软件错误 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| CWE-22 | 0 | 0 | 0 |
| CWE-78 | 0 | 0 | 0 |
| CWE-79 | 0 | 0 | 0 |
| CWE-89 | 0 | 0 | 0 |
| CWE-… | 0 | 0 | 0 |

*表2: CWE 25种最危险的软件错误*

# CWE (2011) Top 25 —— CAST分析结果

基于CWE (2011) Top 25，CAST识别漏洞列表

| CAST 规则 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| 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: CWE-2011-Top25* *漏洞*

# 附录

## 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)。