作者

CAST



**NIST SP 800 53R4**

**总结报告**

应用名称 –

分析版本 –

CAST AIP -

|  |
| --- |
|  |
|  |

星期 , 年 月 日

我的应用名称

版本编号

我的CAST版本

# 目录

[目录 2](#_Toc12442441)

[1. 简介 3](#_Toc12442442)

[1.1. 应用特征 3](#_Toc12442443)

[2. NIST SP 800 53R4 发布概述 4](#_Toc12442444)

[NIST SP 800 53R4 整体概述 4](#_Toc12442445)

[2.1. NIST-SP-800-53R4-AC 5](#_Toc12442446)

[2.2. NIST-SP-800-53R4-AU 5](#_Toc12442447)

[2.3. NIST-SP-800-53R4-CA 6](#_Toc12442448)

[2.4. NIST-SP-800-53R4-CM 6](#_Toc12442449)

[2.5. NIST-SP-800-53R4-IA 7](#_Toc12442450)

[2.6. NIST-SP-800-53R4-SA 7](#_Toc12442451)

[2.7. NIST-SP-800-53R4-SC 8](#_Toc12442452)

[2.8. NIST-SP-800-53R4-SI 8](#_Toc12442453)

[3. 附件 9](#_Toc12442454)

[3.1. 关于CAST软件智能 9](#_Toc12442455)

[3.2. 工作原理 9](#_Toc12442456)

# 简介

此评估旨在确定应用的安全状况，并确定造成当前安全问题的根本原因以及未来应用退化的风险。该评估使用CAST应用智能平台（AIP）根据“NIST标准”自动扫描应用介质，审查架构、设计和代码。

CAST AIP采用的质量规则来自行业流行的通用标准（OWASP、CWE、CISQ、STIG、PCI、NIST）。CAST具有执行数据流和系统级分析（从表示层到数据库层）的独特能力，提供最准确的安全性发现，减少误报。

## 应用特征

此评估重点关注所述应用（用户界面到数据库）的技术实现，而不分析业务功能。

|  |  |
| --- | --- |
| **Name** | **Value** |
| kLoC | 504 |
| Files | 6,586 |
| Classes | 593 |
| SQL Art. | 0 |
| Tables | 119 |

*图1：应用技术特征 表1：应用规模特征*

# NIST SP 800 53R4 发布概述

本节内容总结了CAST 应用智能平台（CAST AIP）按照“联邦信息系统和组织的安全隐私管理措施——NIST特别版本800-53第4版（[官方来源](https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-4/archive/2013-04-30/documents/sp800-53-rev4-ipd.pdf)）”进行结构质量分析与测量所识别的最严重的安全漏洞。

## NIST SP 800 53R4 整体概述

NIST SP800 53R4标准下的CAST适用范围。

|  |  |  |  |
| --- | --- | --- | --- |
| NIST SP800 53R4 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| Requirement 1 | 0 | 0 | 0 |
| Requirement 2 | 0 | 0 | 0 |
| … | 0 | 0 | 0 |

*表2： NIST SP800 53R4 总结*

## NIST-SP-800-53R4-AC

关于该应用的“NIST-SP-800-53R4访问控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表3:NIST SP800 53R4 AC汇总*

## NIST-SP-800-53R4-AU

关于该应用的“NIST-SP-800-53R4审计和责任控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表4：NIST SP800 53R4 AU总结*

## NIST-SP-800-53R4-CA

关于该应用的“NIST-SP-800-53R4安全评估和授权控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表5：NIST SP800 53R4 CA总结*

## NIST-SP-800-53R4-CM

关于该应用的“NIST-SP-800-53R4配置管理控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表6： NIST SP800 53R4 CM总结*

## NIST-SP-800-53R4-IA

关于该应用的“NIST-SP-800-53R4身份与验证控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表7：NIST SP800 53R4 IA总结*

## NIST-SP-800-53R4-SA

关于该应用的“NIST-SP-800-53R4系统与服务获取控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表8：NIST SP800 53R4 SA总结*

## NIST-SP-800-53R4-SC

关于该应用的“NIST-SP-800-53R4系统与通信保护控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表9：NIST SP800 53R4 SC总结*

## NIST-SP-800-53R4-SI

关于该应用的“NIST-SP-800-53R4系统与信息完整性控制”调查结果列表。

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |
| Rule 6 | 0 | 0 | 0 |
| Rule 7 | 0 | 0 | 0 |
| Rule 8 | 0 | 0 | 0 |

*表10：NIST SP800 53R4 SI总结*

# 附件

## 关于CAST软件智能

软件智能通过系统分析数据库结构、软件框架和源代码，帮助团队更好地沟通、决策及驱动团队，保护企业和品牌，不断提高安全性和可靠性，更好地理解关键系统的复杂性。众多企业依靠CAST软件智能提高最终用户满意度，加快上市时间，防止业务中断并降低成本，克服现有障碍，成功应对创新挑战。

关于CAST软件智能更多相关信息，请访问<https://www.castsoftware.com/software-intelligence> 。

## 工作原理

CAST可连接至所有主要的SCM（源代码管理）系统，支持不同语言的源代码扫描分析。源代码作为元数据处理并存储在CAST知识库中——构成CAST AIP分析与生成信息的基础。CAST扫描分析整个应用——包括传统组件、应用定制包和各种现代分布式技术环境。来自第三方代码分析器的数据也可集成到CAST知识库中，并在AIP仪表盘中集中显示。

