Author

CAST



**NIST SP 800 53R4**

**合规报告**

应用名称 – 我的应用名称

分析版本 – 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. NIST SP 800 53R4 总结

2.1 NIST SP 800 53R4 漏洞总结

3. NIST-SP-800-53R4-AC ——CAST分析发现

4. NIST-SP-800-53R4-AU —— CAST分析发现

5. NIST-SP-800-53R4-CA——CAST分析发现

6. NIST-SP-800-53R4-CM——CAST分析发现

7. NIST-SP-800-53R4-IA——CAST分析发现

8. NIST-SP-800-53R4-SA——CAST分析发现

9. NIST-SP-800-53R4-SC——CAST分析发现

10. NIST-SP-800-53R4-SI——CAST分析发现

11. 附录

11.1 关于CAST软件智能

11.2 关于CAST安全性

11.3 NIST SP 800 53R4 在CAST 解决方案中的适用性

# 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，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，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 总结

本节内容总结了CAST 应用智能平台（CAST AIP）基于“安全隐私管理措施——NIST特别版本800-53第4版”进行结构质量分析所识别的关键安全漏洞。

## NIST SP 800 53R4 漏洞总结

对应NIST SP800 53R4 标准，CAST 分析总结

| NIST SP800 53R4 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| --- | --- | --- | --- |
| Requirement 1 | 0 | 0 | 0 |
| Requirement 2 | 0 | 0 | 0 |
| … | 0 | 0 | 0 |

*表2: NIST SP800 53R4 标准总结*

# NIST-SP-800-53R4-AC ——CAST分析发现

NIST-SP-800-53R4 接口控制——CAST识别的漏洞列表

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

*表3: NIST SP800 53R4 AC 总结*

# NIST-SP-800-53R4-AU —— CAST分析发现

NIST-SP-800-53R4 审计与责任管理——CAST识别的漏洞列表

| 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 |
| 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——CAST分析发现

NIST-SP-800-53R4 安全评估与权限控制——CAST识别的漏洞列表

| 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 |
| 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——CAST分析发现

NIST-SP-800-53R4 配置管理控制——CAST识别的漏洞列表

| 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 |
| 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——CAST分析发现

NIST-SP-800-53R4 身份识别与权限控制——CAST识别的漏洞列表

| 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 |
| 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——CAST分析发现

NIST-SP-800-53R4 系统与服务采集控制——CAST识别的漏洞列表

| 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 |
| 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——CAST分析发现

NIST-SP-800-53R4 系统与交流保护控制——CAST识别的漏洞列表

| 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 |
| 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——CAST分析发现

NIST-SP-800-53R4系统与信息完整性控制——CAST识别的漏洞列表

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

*表10: NIST SP800 53R4 SI 总结*

# 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)。

## NIST SP 800 53R4 在CAST 解决方案中的适用性

| 标准 | 描述 | 适用性 |
| --- | --- | --- |
| Cat1 | 0 | 0 |
| Cat2 | 0 | 0 |
| Cat3 | 0 | 0 |