作者

CAST

******

**PCI DSS V3.1**

**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. PCI DSS V 3.1 总结

2.1 PCI DSS V 3.1 漏洞总结

3. PCI DSS – Requirement 1–CAST分析发现

4. PCI DSS – Requirement 2–CAST分析发现

5. PCI DSS – Requirement 3–CAST分析发现

6. PCI DSS – Requirement 4–CAST分析发现

7. PCI DSS – Requirement 5–CAST分析发现

8. PCI DSS – Requirement 6–CAST分析发现

9. PCI DSS – Requirement 7–CAST分析发现

10. PCI DSS – Requirement 8–CAST分析发现

11. PCI DSS – Requirement 10–CAST分析发现

12. 附录

12.1 关于CAST软件智能

12.2 关于CAST 安全性

12.3 PCI DSS V3.1 在CAST 方案中的适用性

# 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PCI标准审查架构、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, 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

本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。

|  |  |
| --- | --- |
| **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：应用规模特征*

# PCI DSS V 3.1 总结

本节概述了CAST AIP根据《支付卡行业（PCI）数据安全标准、要求及安全评估步骤V3.1》（PCI DSS V 3.1）在结构质量分析中发现的最严重的安全漏洞。

## PCI DSS V 3.1 漏洞总结

PCI DSS V 3.1 模块描述

|  |  |  |
| --- | --- | --- |
| **模块** | **Req#** | **描述** |
| 建立和维护安全的网络和系统 | **1**  **2** | 安装、维护防火墙配置以保护持卡人数据；  不要对系统密码和其他安全参数使用供应商提供的默认值。 |
| 保护持卡人数据 | **3**  **4** | 保护存储的持卡人数据；  加密持卡人数据在开放公共网络中的传输。 |
| 维护漏洞管理程序 | **5**  **6** | 保护所有系统免受恶意软件攻击，并定期更新防病毒软件或程序；  开发和维护安全系统和应用。 |
| 实施强有力的访问控制措施 | **7**  **8** | 按业务需要限制对持卡人数据的访问；  识别并验证对系统组件的访问。 |
| 定期监测和测试网络 | **10** | 对网络资源和持卡人数据的所有访问进行跟踪和监控 |

*表2: PCI DSS 模块描述*

基于PCI DSS V3.1 标准的CAST分析发现。

| PCI-DSS-V3.1 | 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3: PCI DSS 3.1 总结表*

# PCI DSS – Requirement 1–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 1

| 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 : PCI-DSS-V3.1-Req1* *漏洞*

# PCI DSS – Requirement 2–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 2

| 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 : PCI-DSS-V3.1-Req2* *漏洞*

# PCI DSS – Requirement 3–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 3

| 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 : PCI-DSS-V3.1-Req3* *漏洞*

# PCI DSS – Requirement 4–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 4

| 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 : PCI-DSS-V3.1-Req4* *漏洞*

# PCI DSS – Requirement 5–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 5

| 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 : PCI-DSS-V3.1-Req5* *漏洞*

# PCI DSS – Requirement 6–CAST分析发现

CAST识别漏洞列表—— PCI DSS V3.1 Requirement 6

| 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 : PCI-DSS-V3.1-Req6* *漏洞*

# PCI DSS – Requirement 7–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 7

| 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 : PCI-DSS-V3.1-Req7* *漏洞*

# PCI DSS – Requirement 8–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 8

| 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11 : PCI-DSS-V3.1-Req8* *漏洞*

# PCI DSS – Requirement 10–CAST分析发现

CAST识别漏洞列表——PCI DSS V3.1 Requirement 10

| 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12 : PCI-DSS-V3.1-Req-10* *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/)。

## 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, STIG。了解CAST安全性的更多信息，请点击[此处](https://www.castsoftware.com/products/security-dashboard) 。

## PCI DSS V3.1 在CAST 方案中的适用性

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