作者

CAST

******

**PCI DSS V3.1**

**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](#_Toc12442726)

[1. 简介 3](#_Toc12442727)

[1.1. 应用特征 3](#_Toc12442728)

[2. PCI DSS V 3.1发布概述 4](#_Toc12442729)

[PCI DSS V 3.1 整体概述 4](#_Toc12442730)

[2.1. PCI DSS – Requirement 1 5](#_Toc12442731)

[2.2. PCI DSS – Requirement 2 5](#_Toc12442732)

[2.3. PCI DSS – Requirement 3 6](#_Toc12442733)

[2.4. PCI DSS – Requirement 4 6](#_Toc12442734)

[2.5. PCI DSS – Requirement 5 7](#_Toc12442735)

[2.6. PCI DSS – Requirement 6 7](#_Toc12442736)

[2.7. PCI DSS – Requirement 7 8](#_Toc12442737)

[2.8. PCI DSS – Requirement 8 8](#_Toc12442738)

[2.9. PCI DSS – Requirement 10 9](#_Toc12442739)

[3. 附件 10](#_Toc12442740)

[3.1. 关于CAST软件智能 10](#_Toc12442741)

[3.2. 工作原理 10](#_Toc12442742)

# 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。此评估使用CAST应用智能平台（AIP）根据“PCI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*

# PCI DSS V 3.1发布概述

本节总结了CAST 应用智能平台（CAST AIP） “根据银行卡行业（PCI）数据安全标准、要求和安全评估程序v3.1”进行结构质量分析和测量所识别的最严重的安全漏洞。

## PCI DSS V 3.1 整体概述

PCI DSS V3.1标准下的CAST适用范围。

|  |  |  |
| --- | --- | --- |
| **模块** | **Req#** | **描述** |
| 搭建并维护安全网络与系统 | **1**  **2** | 安装并维护防火墙配置以保护持卡人数据；  对于系统密码和其他安全参数，不要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；  对于通过开放公共网络的持卡人数据进行加密传输； |
| 维护漏洞管理程序 | **5**  **6** | 保护所有系统免受恶意软件的侵害，并定期更新防病毒软件或程序；  开发并维护安全系统和应用； |
| 实施有力的访问控制措施 | **7**  **8** | 根据业务需要限制对持卡人数据的访问；  识别和验证对系统组件的访问； |
| 定期监测和测试网络 | **10** | 跟踪与监控对网络资源和持卡人数据的所有访问。 |

*表2：PCI DSS模块描述*

|  |  |  |  |
| --- | --- | --- | --- |
| PCI-DSS-V3.1 | Total Vulnerabilities | Added Vulnerabilities | Removed Vulnerabilities |
| 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

关于该应用的“PCI DSS V3.1 Requirement 1”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：PCI-DSS-V3.1-Req1违规*

## PCI DSS – Requirement 2

关于该应用的“PCI DSS V3.1 Requirement 2”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：PCI-DSS-V3.1-Req2违规*

## PCI DSS – Requirement 3

关于该应用的“PCI DSS V3.1 Requirement 3”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：PCI-DSS-V3.1-Req3* *违规*

## PCI DSS – Requirement 4

关于该应用的“PCI DSS V3.1 Requirement 4”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：PCI-DSS-V3.1-Req4* *违规*

## PCI DSS – Requirement 5

关于该应用的“PCI DSS V3.1 Requirement 5”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：PCI-DSS-V3.1-Req5 违规*

## PCI DSS – Requirement 6

关于该应用的“PCI DSS V3.1 Requirement 6”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：PCI-DSS-V3.1-Req6* *违规*

## PCI DSS – Requirement 7

关于该应用的“PCI DSS V3.1 Requirement 7”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：PCI-DSS-V3.1-Req7违规*

## PCI DSS – Requirement 8

关于该应用的“DSS V3.1 Requirement 8”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11：PCI-DSS-V3.1-Req8违规*

## PCI DSS – Requirement 10

关于该应用的“PCI DSS V3.1 Requirement 10”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12：PCI-DSS-V3.1-Req-10违规*

# 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。