

[作者] CAST

**应用名称：**我的应用名称

**版本：** 版本编号

**CAST AIP：**我的CAST 版本

CWE 前25大规则

总结报告

# 目录

目录

1. 引言

1.1. 应用特征

2. 安全违规概述

2.1. 漏洞违反 “CWE 前25大规则”

2.2. CWE-22 - 对受限目录路径名的限制不正确 ('Path Traversal'')

2.3. CWE-78 – 操作系统命令中特殊元素的中和不适当 ('OS Command Injection')

2.4. CWE-79 – 网页生成过程中输入的中和不适当 ('Cross-site Scripting')

2.5. CWE-89 – 在SQL命令中使用的特殊元素的不当中和 ('SQL Injection')

2.6. CWE-120 – 不检查输入大小的缓冲区副本('Classic Buffer Overflow')

2.7. CWE-131– 缓冲区大小计算错误

2.8. CWE-134 – 使用外部控制的格式字符串

2.9. CWE-190 – 整数溢出或环绕

2.10. CWE-250 – 不必要的特权执行

2.11. CWE-306 – 缺少关键功能的身份验证

2.12. CWE-307 – 对过度身份验证尝试的不当限制

2.13. CWE-311 – 缺少敏感数据的加密

2.14. CWE-327 – 使用破坏的或有风险的密码算法

2.15. CWE-352 – 跨站请求伪造(CSRF)

2.16. CWE-434 –危险类型的文件上载不受限制

2.17. CWE-494 – 未进行完整性检查的代码下载

2.18. CWE-601 – URL重定向到不受信任的站点 ('Open Redirect')

2.19. CWE-676 – 使用潜在危险功能

2.20. CWE-732– 关键资源的权限分配不正确

2.21. CWE-759 –使用不带Salt的单向散列

2.22. CWE-798 – 使用硬编码凭证

2.23. CWE-807 – 在安全决策中依赖不可信的输入

2.24. CWE-829 – 包含来自不受信任的控制范围的功能

2.25. CWE-862 – 缺少授权

2.26. CWE-863 – 不正确授权

3. 附录

3.1. 关于CAST软件智能

3.2. 关于CAST安全性

# 引言

此评估旨在评估确定应用安全状况，了解引起当前应用安全风险的根本原因，并识别应用未来可能面临的所有风险。此评估使用CAST应用智能平台（CAST AIP）对应用进行自动扫描，根据“CWE 前25大规则”标准来审查架构、设计和代码。

CAST AIP采用的质量规则来自一流行业标准（OWASP、CWE、CISQ）。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，提供最精确的安全性发现，减少误报率。

## 应用特征

此评估仅限于所述应用的代码技术实现（从数据库到用户界面），不包括功能检查。

|  |  |
| --- | --- |
| **名称** | **值** |
| 千行代码 | 504 |
| 文件数 | 6,586 |
| 类 | 593 |
| SQL 工件 | 0 |
| 数据库表 | 119 |

*图1: 应用技术特征 表1: 应用特征*

# 安全违规概述

本节概述CAST AIP系统结构质量的分析测量发现的最严重的安全漏洞，这些安全漏洞违反了“CWE 前25大规则”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)。

## 漏洞违反 “CWE 前25大规则”

该应用 “CWE 前25大规则”的漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CWE 前25大规则 | 总漏洞 | 添加漏洞 | 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 前25大规则*

## CWE-22 - 对受限目录路径名的限制不正确 ('Path Traversal'')

该应用CWE-22漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表3: CWE-22* 漏洞

## CWE-78 – 操作系统命令中特殊元素的中和不适当 ('OS Command Injection')

该应用CWE-78漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表4: CWE-78* 漏洞

## CWE-79 – 网页生成过程中输入的中和不适当 ('Cross-site Scripting')

该应用CWE-79漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表5: CWE-79* 漏洞

## CWE-89 – 在SQL命令中使用的特殊元素的不当中和 ('SQL Injection')

该应用CWE-89漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表6: CWE-89* 漏洞

## CWE-120 – 不检查输入大小的缓冲区副本('Classic Buffer Overflow')

该应用CWE-120漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表7: CWE-120* 漏洞

## CWE-131– 缓冲区大小计算错误

该应用CWE-131漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表8: CWE-131 漏洞*

## CWE-134 – 使用外部控制的格式字符串

该应用CWE-134 规则列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表9: CWE-134 漏洞*

## CWE-190 – 整数溢出或环绕

该应用CWE-190 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表10: CWE-190 漏洞*

## CWE-250 – 不必要的特权执行

该应用CWE-250漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表11: CWE-250 漏洞*

## CWE-306 – 缺少关键功能的身份验证

该应用CWE-306 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表12: CWE-306 漏洞*

## CWE-307 – 对过度身份验证尝试的不当限制

该应用CWE-307漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表13: CWE-307 漏洞*

## CWE-311 – 缺少敏感数据的加密

该应用CWE-311 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表14: CWE-311 漏洞*

## CWE-327 – 使用具有破坏性的或有风险的密码算法

该应用CWE-327 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表15: CWE-327 漏洞*

## CWE-352 – 跨站请求伪造(CSRF)

该应用CWE-352 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表16: CWE-352 漏洞*

## CWE-434 –危险类型的文件上载不受限制

该应用CWE-434 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表17: CWE-434 漏洞*

## CWE-494 – 未进行完整性检查的代码下载

该应用CWE-494 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表18: CWE-494 漏洞*

## CWE-601 – URL重定向到不受信任的站点 ('Open Redirect')

该应用CWE-601 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表19: CWE-601 漏洞*

## CWE-676 – 使用潜在危险功能

该应用 CWE-676 漏洞。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表20: CWE-676 漏洞*

## CWE-732– 关键资源的权限分配不正确

该应用CWE-732 漏洞。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表21: CWE-732 漏洞*

## CWE-759 –使用不带Salt的单向散列

该应用CWE-759 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表22: CWE-759 漏洞*

## CWE-798 – 使用硬编码凭证

该应用CWE-798 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表23: CWE-798 漏洞*

## CWE-807 – 在安全决策中依赖不可信的输入

该应用CWE-807 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表24: CWE-807 漏洞*

## CWE-829 – 包含来自不受信任的控制范围的功能

该应用CWE-829 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表25: CWE-829 漏洞*

## CWE-862 – 缺少授权

该应用CWE-862 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表26: CWE-862 漏洞*

## CWE-863 – 不正确授权

该应用CWE-863 漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST规则 | 总漏洞 | 添加漏洞 | 移除漏洞 |
| 规则1 | 0 | 0 | 0 |
| 规则2 | 0 | 0 | 0 |
| 规则3 | 0 | 0 | 0 |
| 规则4 | 0 | 0 | 0 |
| 规则5 | 0 | 0 | 0 |

*表27: CWE-863 漏洞*

# 附录

## 关于CAST软件智能

软件智能为IT人员提供软件架构、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。迄今， 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

IT人员需要采取主动的、智能的手段来积极应对网络风险、保障应用程序安全。在开发开始前，CAST软件智能就提供关于安全战略盲点的洞察力。凭借其独特的数据流和系统级分析能力，CAST提供了最准确的安全发现，减少大量误报。CAST安全规则来自行业最佳标准（CISQ、CWE和OWASP）。

了解更多CAST安全性相关信息，请点击[此处](https://www.castsoftware.com/use-cases/application-security)。