作者

CAST

******

**OWASP 2017 TOP 10**

**合规总结报告**

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. 安全违规简介

2.1. OWASP -2017 Top 10 漏洞

2.2. OWASP -2017 A1 – 注入

2.3. OWASP -2017 A2 – 失效的身份验证

2.4. OWASP -2017 A3 – 敏感数据暴露

2.5. OWASP -2017 A4 – XML 外部实体 (XXE)

2.6. OWASP -2017 A5 – 失效的访问控制

2.7. OWASP -2017 A6 – 安全性错误配置

2.8. OWASP -2017 A7 – 跨站脚本 (XSS)

2.9. OWASP -2017 A8 – 不安全的反序列化

2.10. OWASP -2017 A9 – 使用带已知漏洞的组件

2.11. OWASP -2017 A10 – 日志记录&监视不足

3. 附录

3.1. 关于CAST软件智能

3.2. 关于CAST安全性

# 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OWASP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）。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 | 数值 |
| 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*

# 安全违规简介

本节内容总结了CAST 应用智能平台（CAST AIP）基于“OWASP 2017标准”进行结构质量分析所识别的关键安全漏洞。点击[此处](https://www.owasp.org/index.php/Top_10-2017_Top_10)了解更多OWASP安全标准的细节。

## OWASP -2017 Top 10 漏洞

[OWASP Top 10](https://www.owasp.org/index.php/Top_10-2017_Top_10)专注于识别组织中最严重的web应用安全风险。

在本应用中发现的基于OWASP -2017 规则的漏洞列表：

|  |  |  |  |
| --- | --- | --- | --- |
| OWASP-2017 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| A1-Injection | 0 | 0 | 0 |
| A3-2017 | 0 | 0 | 0 |
| A6-2017 | 0 | 0 | 0 |
| A7-2017 | 0 | 0 | 0 |
| A… | 0 | 0 | 0 |

*表2: OWASP 2017 Top 10 规则*

## OWASP -2017 A1 – 注入

这类规则主要处理以下问题：当不受信任的数据作为命令或查询的一部分发送到解释器时，会出现注入缺陷（如SQL、OS和LDAP注入）。攻击者的恶意数据可以诱使解释器在未经适当授权的情况下执行非计划的命令或访问数据。

A1列表-在本应用中发现的注入漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表3: A1 – 注入漏洞*

## OWASP -2017 A2 – 失效的身份验证

与身份验证和会话管理相关的应用功能未正确实现，使得攻击者能够危害密码、密钥或会话令牌安全，或利用其它实施缺陷来临时或永久性获得其他用户的身份。

A2列表-在本应用中发现的失效的身份验证漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表4: A2- 失效的身份验证漏洞*

## OWASP -2017 A3 – 敏感数据暴露

许多web应用无法正确保护敏感数据，如金融、医疗和个人身份验证凭据。攻击者可以窃取或修改这些保护力度较弱的数据，以进行信用卡欺诈、身份盗窃或其他犯罪。敏感数据需要额外的保护，例如在静止或传输时的加密，以及与浏览器交换时的特殊预防措施。

A3列表 – 在本应用中发现的敏感数据暴露漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表5: A3- 敏感数据暴露漏洞*

## OWASP -2017 A4 – XML 外部实体 (XXE)

许多旧的或配置不良的XML处理器使用XML文档来评估外部实体引用。外部实体可被用于使用文件URI处理器打开内部文件、内部文件共享、内部端口扫描、远程代码执行和拒绝服务攻击等。

A4列表—在本应用中发现的XML外部实体漏洞列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表6: A4 – XML 外部实体漏洞*

## OWASP -2017 A5 – 失效的访问控制

通过身份验证的用户被允许执行的操作的未被适当限制。攻击者可利用这些漏洞访问未经授权的功能和/或数据，例如访问其他用户的帐户、查看敏感文件、修改其他用户的数据、更改访问权限等。

A5列表—在本应用中发现的失效的访问控制漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表7: A5 – 失效的访问控制漏洞*

## OWASP -2017 A6 – 安全性错误配置

安全性错误配置是最常见的问题。这通常是由于不安全的默认配置、不完整或特殊配置、开放的云存储、配置错误的HTTP头部信息和包含敏感信息的详细错误消息造成的。不仅需要安全地配置所有操作系统、框架、库和应用程序，而且必须及时对它们进行修补/升级。

A6列表-在本应用中发现的安全性错误配置漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表8: A6- 安全性错误配置漏洞*

## OWASP -2017 A7 – 跨站脚本 (XSS)

应用在一个新的网页中包含不可信的数据（不经正确验证或溢出），或通过一个可创建HTML或JavaScript的浏览器API使用用户提供的数据来更新现有的网页，将导致XSS缺陷发生。XSS使攻击者能在受害者浏览器中执行脚本，这些脚本劫持用户会话、破坏网站或将用户重定向到恶意网站。

A7列表-在此应用中发现的跨站脚本漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表9: A7- 跨站脚本漏洞*

## OWASP -2017 A8 – 不安全的反序列化

不安全的反序列化通常会导致远程代码执行。即使反序列化缺陷不会导致远程代码执行，它们也可被用于执行攻击，包括重播攻击、注入攻击和权限提升攻击。

A8列表 – 在此应用中发现的不安全的反序列化漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表10: A8- 不安全的反序列化漏洞*

## OWASP -2017 A9 – 使用带已知漏洞的组件

组件（如库、框架和其他软件模块）以与应用相同的权限运行。如果使用易受攻击的组件，可能会因攻击导致严重的数据丢失或服务器接管。使用具有已知漏洞组件的应用和API可能会破坏应用防御，导致各种攻击和影响。

A9列表-在此应用中发现的带已知漏洞组件的漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表10: A9 – 使用带已知漏洞的组件*

## OWASP -2017 A10 – 日志记录&监视不足

日志记录和监视不足，加上与事件响应的集成丢失或无效，使得攻击者能够进一步地、持续地攻击系统，并且面向更多系统实施攻击，篡改、提取或销毁数据。大多数违约研究表明，违约被发现的时间超过200天，通常是由外部方而不是内部流程或监控部门发现的。

A10列表-在此应用中发现的日志记录&监视不足漏洞

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 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 |

*表11: A10 –* *日志记录&监视不足漏洞*

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