作者

CAST

******

**OWASP 2017 TOP 10**

**总结报告**

应用名称 –

版本–

CAST AIP -

|  |
| --- |
|  |
|  |

Monday, xx July 2012

我的应用名称

版本号

CAST工具版本

# 目录

目录

1. 引言

1.1. 应用特征

2. 安全违规概述

2.1. OWASP -2017 前 10 大漏洞

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 – 越权访问

2.7. OWASP -2017 A6 – 安全配置错误

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 – 使用具有已知漏洞的组件

2.11. OWASP -2017 A10 – 日志记录和监控不足

3. 附录

3.1. 关于 CAST 软件智能

3.2. 关于 CAST 安全

# 引言

此评估旨在度量应用程序的安全健康状况，并确定当前安全问题的一些根源，以及识别未来可能出现的任何风险。此评估使用CAST应用智能平台(AIP)自动扫描应用程序的代码介质，以根据OWASP标准审查应用的架构、设计和代码。

CAST AIP采用业内推荐安全规则标准(OWASP、CWE、CISQ)，CAST具有数据流分析和系统级分析(从表示层到数据库层)的独特能力，可以提供最准确的安全性发现，避免大量误报。

## 应用特征

此评估仅限于应用系统的代码技术实现(前端表示层到数据库层)，不包括业务功能检查。

|  |  |
| --- | --- |
| 名称 | 值 |
| 千行代码 | 504 |
| 文件 | 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

本节概述了CAST AIP针对OWASP 2017标准进行的结构质量分析和测试中发现的最严重的安全漏洞。有关OWASP安全标准的详细信息参见 [这里](https://www.owasp.org/index.php/Top_10-2017_Top_10)。

## OWASP -2017 前 10 大 漏洞

OWASP的[前10大漏洞](https://www.owasp.org/index.php/Top_10-2017_Top_10)是主要用于识别应用系统中最严重的web应用程序安全风险。

本应用程序中所发现违反OWASP -2017规则的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| OWASP-2017 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| A1-注入 | 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 前10大 漏洞*

## OWASP -2017 A1 – 注入

这类规则主要发现的问题为：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，就会出现注入漏洞，如SQL、NoSQL、OS和LDAP注入。攻击者的恶意数据可以欺骗解释器执行非预期的命令或在没有适当授权的情况下访问数据。

本应用中发现违反A1-注入的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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 |

*表格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程序功能常常实现错误，允许攻击者破坏密码、密钥或会话令牌，或者利用其他实现漏洞来临时或永久地使用其他用户的身份。

本应用中发现的违反A2-失效的身份验证的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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- 失效身份验证的漏洞*

## OWASP -2017 A3 – 敏感数据暴露

许多web应用程序和API不能正确地保护敏感数据，比如金融、医疗和PII。攻击者可以窃取或修改这些弱保护的数据来进行信用卡欺诈、身份盗窃或其他犯罪。敏感数据可能会在没有额外保护的情况下受到破坏，比如休眠或传输过程中加密时，或者在与浏览器交换数据时缺乏特别的预防措施。

本应用中发现违反A3-敏感数据暴露的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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*

## OWASP -2017 A4 – XML外部实体 (XXE)

许多过时的或配置较差的XML处理器会使用XML文档中的外部实体引用。外部实体可以使用文件URI处理程序、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来公开内部文件。

本应用中发现违反A4-XML外部实体的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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 – 越权访问

许多较旧的或配置较差的XML处理器会评估XML文档中的外部实体引用。外部实体可以使用文件URI处理程序、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来公开内部文件。

本应用中发现违反A5-越权访问的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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 – 越权访问漏洞*

## OWASP -2017 A6 – 安全配置错误

安全配置错误是最常见的问题。这通常是不安全的默认配置、不完整或临时配置、开放云存储、配置错误的HTTP头和包含敏感信息的冗长错误消息所导致的结果。不仅所有操作系统、框架、库和应用程序都必须进行安全配置，而且必须及时修补/升级它们。

本应用中发现的违反A6-安全配置错误的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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- 安全错误配置漏洞*

## OWASP -2017 A7 – 跨站脚本 (XSS)

当应用程序在新web页面中包含不受信任的数据而没有进行适当的验证、转义或使用可以创建HTML或JavaScript的浏览器API使用用户提供的数据更新现有web页面时，就会出现XSS漏洞。XSS允许攻击者在受害者的浏览器中执行脚本，这些脚本可以劫持用户会话、破坏web站点或将用户重定向到恶意站点。

本应用中发现的违反A7-跨站脚本的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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

不安全的反序列化常常导致远程代码执行，即使反序列化漏洞不会导致远程代码执行，也可以使用它们执行攻击，包括重播攻击、注入攻击和特权升级攻击。

本应用中发现的违反A8-不安全的反序列化的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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 – 使用具有已知漏洞的组件

组件（如库、框架和其他软件模块)使用与应用程序相同的特权运行。如果一个脆弱的组件被利用，这样的攻击会导致严重的数据丢失或服务器接管。使用具有已知漏洞的组件的应用程序和api可能会破坏应用程序防御并启用各种攻击和影响。

本应用中发现的违反A9-使用具有已知漏洞组件的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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 – 使用已知漏洞组件的漏洞*

## OWASP -2017 A10 – 日志记录和监控不足

日志记录和监控不足，加上缺少或没有有效地集成事件响应，使得攻击者可以进一步攻击系统、维护持久性、转向更多系统，以及篡改、提取或销毁数据。大多数违约研究表明，检测违约的时间超过200天，通常由外部方检测，而不是内部流程或监控。

本应用中发现违反A10-日志记录和监控不足的问题列表。

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总漏洞 | 新增漏洞 | 已减少漏洞 |
| 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 12: A10 –日志记录和监控不足的漏洞*

# 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

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)。