作者

CAST

******

**OWASP 2013 TOP 10**

**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 -2013 Top 10 漏洞

2.2. OWASP -2013 A1 – 注入

2.3. OWASP -2013 A2 – 失效的身份验证和会话管理

2.4. OWASP -2013 A3 – 跨站脚本

2.5. OWASP -2013 A4 – 不安全的直接对象引用

2.6. OWASP -2013 A5 – 安全性错误配置

2.7. OWASP -2013 A6 – 敏感数据暴露

2.8. OWASP -2013 A7 –功能级访问控制缺失

2.9. OWASP -2013 A8 – 伪造跨站请求

2.10. OWASP -2013 A9 – 使用带有已知漏洞的组件

2.11. OWASP -2013 A10 – 未经验证的重定向和转发

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。

|  |  |
| --- | --- |
| 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*

# 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 2013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_2013-Top_10)了解更多OWASP安全标准的细节。

## OWASP -2013 Top 10 漏洞

[OWASP 2013 Top 10](https://www.owasp.org/index.php/Top_10_2013-Top_10) 漏洞是有关于web应用安全风险的关键漏洞。

在本应用中发现的基于OWASP -2013 规则的漏洞列表：

|  |  |  |  |
| --- | --- | --- | --- |
| OWASP-2013 | 总漏洞 | 新增漏洞 | 移除漏洞 |
| A1 | 0 | 0 | 0 |
| A2 | 0 | 0 | 0 |
| A3 | 0 | 0 | 0 |
| A4 | 0 | 0 | 0 |
| … | 0 | 0 | 0 |

*表2: OWASP 2013 Top 10 规则*

## OWASP -2013 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 -2013 A2 – 失效的身份验证&会话管理

与身份验证和会话管理相关的应用功能通常未能正确实现，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&会话管理漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| 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&会话管理漏洞*

## OWASP -2013 A3 – 跨站脚本

每当应用获取不受信任的数据并将其发送到web浏览器而没有进行适当的验证或溢出时，就会出现XSS缺陷。XSS允许攻击者在受害浏览器中执行脚本，这些脚本可以劫持用户会话、破坏网站或将用户重定向到恶意网站。

A3列表-在本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5: A3- 跨站脚本漏洞*

## OWASP -2013 A4 – 不安全的直接对象引用

当开发人员公开对内部实现对象（如文件、目录或数据库键）的引用时，会发生直接对象引用。没有访问控制检查或其他保护措施，攻击者可以操纵这些引用来访问未经授权的数据。

A4列表-在本应用中发现的不安全的直接对象引用漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| 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6: A4- 不安全的直接对象引用漏洞*

## OWASP -2013 A5 – 安全性错误配置

良好的安全性要求为应用、框架、应用服务器、web服务器、数据库服务器以及平台进行安全配置的定义和部署。默认设置通常是不安全的，所以应该定义、实现和维护安全设置。此外，软件应保持更新为最新版本。

A5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7: A5- 安全配置错误漏洞*

## OWASP -2013 A6 – 敏感数据暴露

许多web应用无法正确保护敏感数据，如信用卡、税务ID和身份验证凭据。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。

A6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8: A6 – 敏感数据暴露漏洞*

## OWASP -2013 A7 –功能级访问控制缺失

大多数web应用在使该功能在UI中可见之前验证功能级的访问权限。但是，当访问每个功能时，应用需要在服务器上执行相同的访问控制检查。如果请求未经验证，攻击者将能够伪造请求，在未经适当授权的情况下访问功能。

A7列表 –在本应用中发现的功能级访问控制缺失漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| CAST 规则 | 总违规 | 新增违规 | 移除违规 |
| 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 – 功能及访问控制缺失漏洞*

## OWASP -2013 A8 – 伪造跨站请求

CSRF攻击迫使已登录的受害者浏览器向易被攻击的web应用发送伪造的HTTP请求，包括受害者的会话cookie和其他自动包含的身份验证信息。攻击者迫使受害者浏览器生成请求，这一请求被易受攻击的应用认为是合法请求。

A8列表 –在本应用中发现的跨站请求伪造漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| 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 – 跨站请求伪造漏洞*

## OWASP -2013 A9 – 使用带有已知漏洞的组件

组件，如库、框架和其他软件模块，几乎总是以完全权限运行。如果使用易受攻击的组件，可能会导致严重的数据丢失或服务器接管。应用中带已知漏洞的组件可能会破坏应用防御，并导致一系列可能的攻击和影响。

A9列表 – 在本应用中发现的使用带已知漏洞的组件漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| 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: A9 – 使用带已知漏洞的组件*

## OWASP -2013 A10 – 未经验证的重定向和转发

Web应用程序经常将用户重定向和转发到其他页面和网站，并使用不受信任的数据来确定目标页面。未经正确的验证，攻击者可以将受害者重定向到网络钓鱼或恶意软件站点，或使用转发访问未经授权的页面。

A10 列表–在本应用中发现的使用未经验证的重定向与转发漏洞：

|  |  |  |  |
| --- | --- | --- | --- |
| 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12: A10 – 未经验证的重定向与转发漏洞*

# 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)。