公 开

# 2015 年第二季度开源软件源代码
# 安全漏洞分析报告

国家互联网应急中心

实验室

2015 年 7 月

# 目录

# 1 概述

近年来，随着软件技术飞速发展，开源软件已在全球范围内得到了广泛应用。数据显示，从 2012 年起，已有超过 80%的商业软件使用开源软件。开源软件的代码一旦存在安全问题，必将造成广泛、严重的影响。为了解当前开源软件的安全情况，实验室本季度对 30 款广泛使用的知名开源软件进行了源代码安全测试。结合漏洞扫描工具和人工审计的结果 ,形成了本漏洞分析报告。本次测试在代码层面共发现高危安全漏洞 3511 个。与上季度的结果相比，这些开源软件存在的安全问题依然严重。

# 2 被测开源软件

表 1 列出了本次被测的 30 个开源软件项目的概况，涵盖 java 和 php 这两种编程语言。这些软件项目都是国际、国内知名的，拥有广泛用户的软件项目的最新版本，其中不乏由知名软件公司开发的软件。由于这些软件大多具有巨大的用户群体，软件中的安全漏洞很可能会造成严重的后果。

表 1 被测开源软件项目概览

| 项目名称 | 版本号 | 主要编程语言 | 功能说明 | 代码行数(L) |
|---|---|---|---|---|
| AFinal | 0.5.1 | Java | Android的sqlite orm和ioc框架 | 6839 |
| Argo | 1.0.1 | Java | 58 同城的 web 框架 | 11704 |
| beetl | 2.2.0 | Java | java 模板引擎 | 29080 |
| Carbon Forum | 3.1.0 | PHP | 高性能 PHP 论坛 | 26452 |
| cynthia | 2.0.0 | Java | 问题管理/BUG 管理/任务管理/项目管理系统 | 74873 |
| dhroid | 1.0.0 | Java | Android 极速开发框架 | 10800 |
| druid | 1.0.12 | Java | Jdbc连接池、监控组件 | 193376 |

| | | | | |
|---|---|---|---|---|
| Dubbo | 2.5.4 | Java | 高性能优秀的服务框架 | 112768 |
| Fastjson | 1.2.6 | Java | Java 语言实现的 JSON 解析器和生成器 | 83801 |
| fastweixin | 1.2.1 | Java | 微信公众平台服务器 | 5956 |
| JFinal | 1.9 | Java | JAVA 极速 WEB+ORM 框架 | 12045 |
| JFinal Extensions | 3.1.3 | Java | 对 java 极速 web 框架 jfinal 的一个扩充 | 20293 |
| kaola | 4.0.0 | Java | JavaEE 企业级应用开发领域的平台工具 | 325561 |
| KJFrameForAndroid | 1.0.2 | Java | Android 应用开发框架 | 12115 |
| LaneWeChat | 1.5.1 | PHP | 微信 PHP 开发框架 | 1684 |
| MyQEE | 3.0.1 | PHP | PHP 框架 | 34940 |
| Nutz | 1.0.1 | Java | Java 应用框架 | 69379 |
| ONES | 1.2.1 | PHP | 开源企业管理软件 | 77394 |
| OSAdmin | 1.0.1 | PHP | PHP 开源管理后台 | 26780 |
| RoboBinding | 1.0.1 | Java | Android 数据绑定框架 | 22827 |
| S2jh | 1.0.0 | Java | 企业级 Web 应用的基础开发框架 | 184010 |
| snakerflow | 2.5.1 | Java | 开源工作流引擎 | 12604 |
| Spiderman | 1.2.1 | Java | Java 网络蜘蛛/网络爬虫 | 20912 |
| StartBBS | 1.3.0 | PHP | 轻量开源社区系统 | 33069 |
| ThinkCMF | 1.1.2 | PHP | 内容管理框架 | 150126 |
| ThinkOX | 1.0.1 | PHP | 基于 ThinkPHP 的轻量级 SNS 框架 | 171884 |
| ThinkPHP | 1.2.1 | PHP | 轻量级 PHP 开发框架 | 37086 |
| webmagic | 0.5.2 | Java | 无须配置、便于二次开发的爬虫框架 | 25400 |
| WindFramework | 1.1.2 | PHP | php 框架 | 12189 |
| 禅道 | 7.2 | PHP | 开源项目管理软件 | 86563 |

# 3 测试内容

## 3.1 安全漏洞种类

本次测试涵盖各类常见安全漏洞。根据安全漏洞形成的原因、被利用的可能性、造成的危害程度和解决的难度等因素进行综合考虑，可以将常见的安全漏洞分为八类：

1) 输入验证与表示（Input Validation and Representation）

   输入验证与表示问题通常是由特殊字符、编码和数字表示所引起的，这类问题的发生是由于对输入的信任所造成的。这些问题包括：缓冲区溢出、跨站脚本、SQL 注入、命令注入等。

2) API 误用（API Abuse)

   API 是调用者与被调用者之间的一个约定，大多数的 API 误用是由于调用者没有理解约定的目的所造成的。当使用 API 不当时，也会引发安全问题。

3) 安全特性（Security Features）

   该类别主要包含认证、访问控制、机密性、密码使用和特权管理等方面的漏洞。

4) 时间和状态（Time and State）

   分布式计算与时间和状态有关。线程和进程之间的交互及执行任务的时间顺序往往由共享的状态决定，如信号量、变量、文件系统等。与分布式计算相关的漏洞包括竞态条件、阻塞误用等。

5) 错误和异常处理缺陷（Errors）

   这类漏洞与错误和异常处理有关，最常见的一种漏洞是没有恰当的处理错误（或者没有处理错误）从而导致程序运行意外终止，另一种漏洞是产生的错误给潜在的攻击者提供了过多信息。

6) 代码质量问题（Code Quality）

低劣的代码质量会导致不可预测的行为。对于攻击者而言，低劣的代码使他们可以以意想不到的方式威胁系统。常见的该类别漏洞包括死代码、空指针解引用、资源泄漏等。

7) 封装和隐藏缺陷（Encapsulation）

合理的封装意味着区分校验过和未经检验的数据，区分不同用户的数据，或区分用户能看到和不能看到的数据等。常见的漏洞包括隐藏域、信息泄漏、跨站请求伪造等。

8) 代码运行环境的缺陷（Environment）

该类漏洞是源代码之外的问题，例如运行环境配置问题、敏感信息管理问题等，它们对产品的安全仍然是至关重要的。

前七类漏洞与源代码中的安全缺陷相关，它们可以成为恶意攻击的目标，一旦被利用会造成信息泄露、权限提升等严重后果。最后一类漏洞描述实际代码之外的安全问题，它们容易造成软件的运行异常、数据丢失等严重问题。

## 3.2 安全漏洞级别

我们将源代码的安全问题分为四种级别：极高危（Critical）、高危（High）、中等（Medium）和低（Low）。衡量级别的标准包括两个维度，可信程度（confidence）和严重程度（severity）。可信程度是指发现的问题是否准确的可能性，比如将每个strcpy()调用都标记成缓冲区溢出漏洞的可信程度很低。严重程度是指假设测试技术真实可信的情况下检出问题的严重性，比如缓冲区溢出（buffer overflow）通常是比空

指针引用（null pointer dereference）更严重的安全问题。将这两个因素综合起来可以准确的为安全问题划分级别，如图 1 所示。

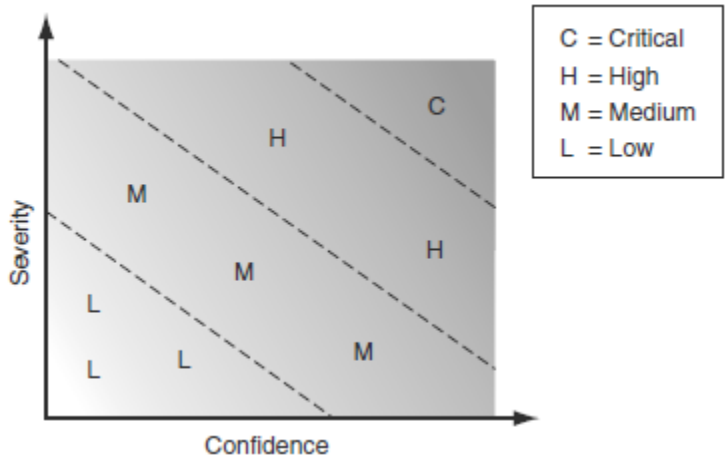



图 1 漏洞级别与严重程度、可信程度的关系

# 4 开源软件项目的安全漏洞情况

## 4.1 安全漏洞情况概览

由于极高危、高危级别的安全漏洞危害程度较高，更能反映出软件中迫切需要解决的安全问题，本部分仅讨论被测项目中的这两种级别的漏洞情况。表 2 展示了被测开源项目中存在的极高危以及高危安全漏洞的情况，图 2 用柱状图展示了该表中的各项分析结果。从中可以看出，大多数软件项目都存在不同程度的安全问题。这些项目中总计发现极高危漏洞 572 个，高危漏洞 2939 个。

依据此次代码测试结果，PHP 和 JAVA 依然是漏洞多发语言。安全问题最为突出的几款软件全部为 JAVA 语言开发。漏洞总数排名第一的是国内知名度最高的 JAVA 分布式框架 Dubbo（2.5.4 版本），包含漏洞高达 1119 个，其中极高危漏洞 121 个，高危漏洞 998 个，同时它也是漏洞密度（漏洞数量/代码行数）最高的软件，漏洞密度为

0.99%。而另一款 JAVA 开源软件 Druid 以总漏洞数 543 个在漏洞总数上排名第二，其中极高危漏洞 93 个，高危漏洞 450 个； 其漏洞密度为 0.28%，属于中等水平。漏洞总数排名第三的是 JavaEE 企业级应用开发领域的平台工具 Kaola ,包含漏洞 208 个，其中极高危漏洞 34 个 ,高危漏洞 174 个 ;但由于其代码量较大 ,漏洞密度仅为 0.06%，在本次被测软件中属于漏洞密度较低的一款。

PHP 语言中，开源框架系统 Carbon Forum 漏洞数为 170 个，极高危漏洞为 48 个，高危漏洞为 122 个，在本次测试的 PHP 开源软件中，漏洞总数排名第一；同时漏洞密度为 0.64%，在所有被测软件中属于较高水平。

根据本次测试结果，软件的漏洞数量与漏洞密度不一定正相关。例如，JAVA WEB 框架 JFinal 共包含漏洞 98 个，极高危漏洞数 2 个，在所有被测软件中漏洞数目居中，但由于其代码量不大 ,漏洞密度高达 0.81% ,仅低于漏洞密度排名第一的软件 Dubbo。

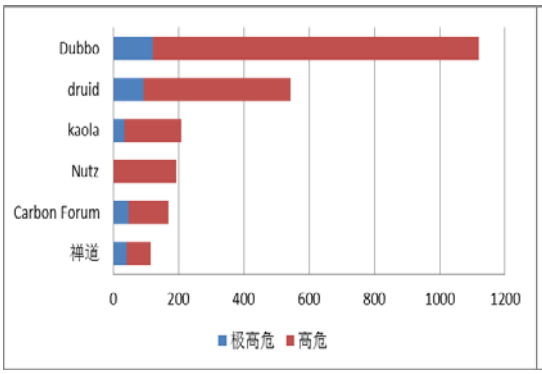
在本次测试中，安全情况最好的软件是 JAVA 爬虫软件 Spiderman，其中不包含任何极高危漏洞，高危漏洞数仅为 1，在所有被测软件中漏洞总数最少，且漏洞密度仅为 0.02%，低于其他任意一款被测软件。此外，AFinal、fastweixin、RoboBinding 这三款 JAVA 软件中没有检测出任何极高危漏洞，且总漏洞数小于 20，总体安全性也较好。

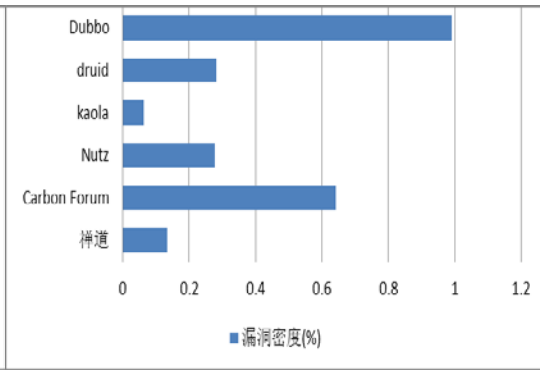
与上季度相比，这批开源软件系统的总体安全情况有明显改善，但安全问题依然比较严重。这项统计充分说明了这批项目的安全性情况，漏洞数量排名靠前的项目处于极其容易被攻击者利用的状态 ,实际使用者急需通过安装补丁或者更新版本的方式进行修复和升级。

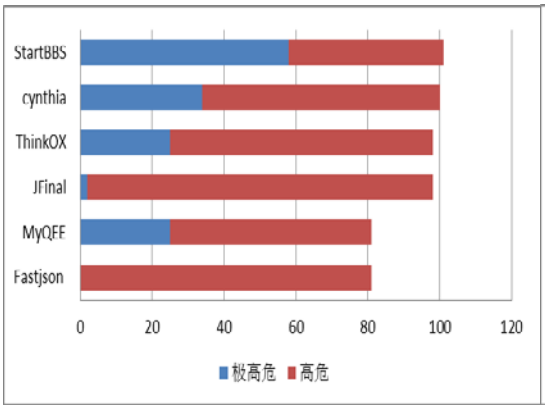
表 2. 开源软件项目中安全漏洞概览

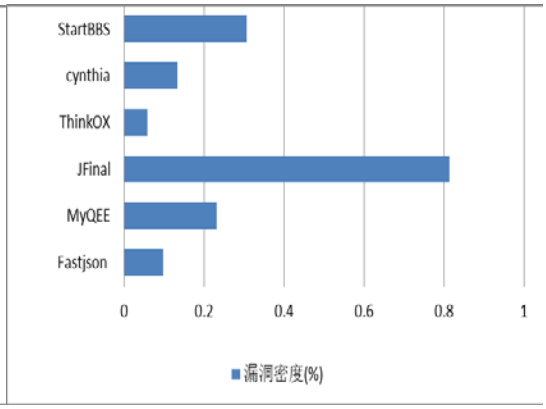
| 项目名称 | 极高危(C) | 高危(H) | 总和(H+C) | 漏洞密度%((H+C)/L) |
|---|---|---|---|---|
| AFinal | 0 | 6 | 6 | 0.087732125 |
| Argo | 0 | 21 | 21 | 0.179425837 |
| beetl | 0 | 21 | 21 | 0.07221458 |
| Carbon Forum | 48 | 122 | 170 | 0.642673522 |
| cynthia | 34 | 66 | 100 | 0.133559494 |
| dhroid | 0 | 71 | 71 | 0.657407407 |
| druid | 93 | 450 | 543 | 0.280800099 |
| Dubbo | 121 | 998 | 1119 | 0.992302781 |
| Fastjson | 0 | 81 | 81 | 0.096657558 |
| fastweixin | 0 | 9 | 9 | 0.151108126 |
| JFinal | 2 | 96 | 98 | 0.813615608 |
| JFinal Extensions | 2 | 20 | 22 | 0.108411768 |
| kaola | 34 | 174 | 208 | 0.063889717 |
| KJFrameForAndroid | 0 | 29 | 29 | 0.239372678 |
| LaneWeChat | 2 | 2 | 4 | 0.237529691 |
| MyQEE | 25 | 56 | 81 | 0.231825987 |
| Nutz | 2 | 191 | 193 | 0.278182159 |
| ONES | 34 | 27 | 61 | 0.078817479 |
| OSAdmin | 1 | 46 | 47 | 0.175504108 |
| RoboBinding | 0 | 18 | 18 | 0.078853989 |
| S2jh | 16 | 48 | 64 | 0.034780718 |
| snakerflow | 1 | 59 | 60 | 0.476039353 |
| Spiderman | 0 | 1 | 1 | 0.004781943 |
| StartBBS | 58 | 43 | 101 | 0.305421996 |

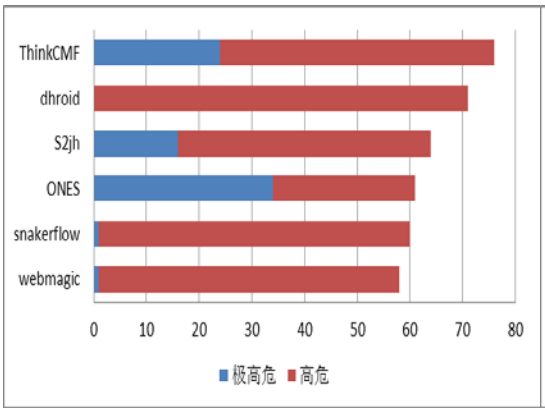
| | | | | |
|---|---|---|---|---|
| ThinkCMF | 24 | 52 | 76 | 0.050624142 |
| ThinkOX | 25 | 73 | 98 | 0.057015196 |
| ThinkPHP | 6 | 19 | 25 | 0.067410883 |
| webmagic | 1 | 57 | 58 | 0.228346457 |
| WindFramework | 3 | 8 | 11 | 0.090245303 |
| 禅道 | 40 | 75 | 115 | 0.132851218 |

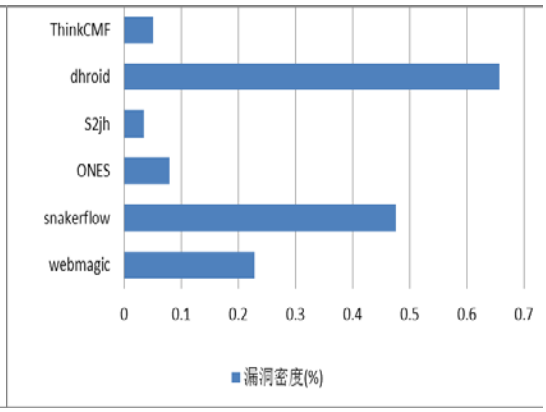


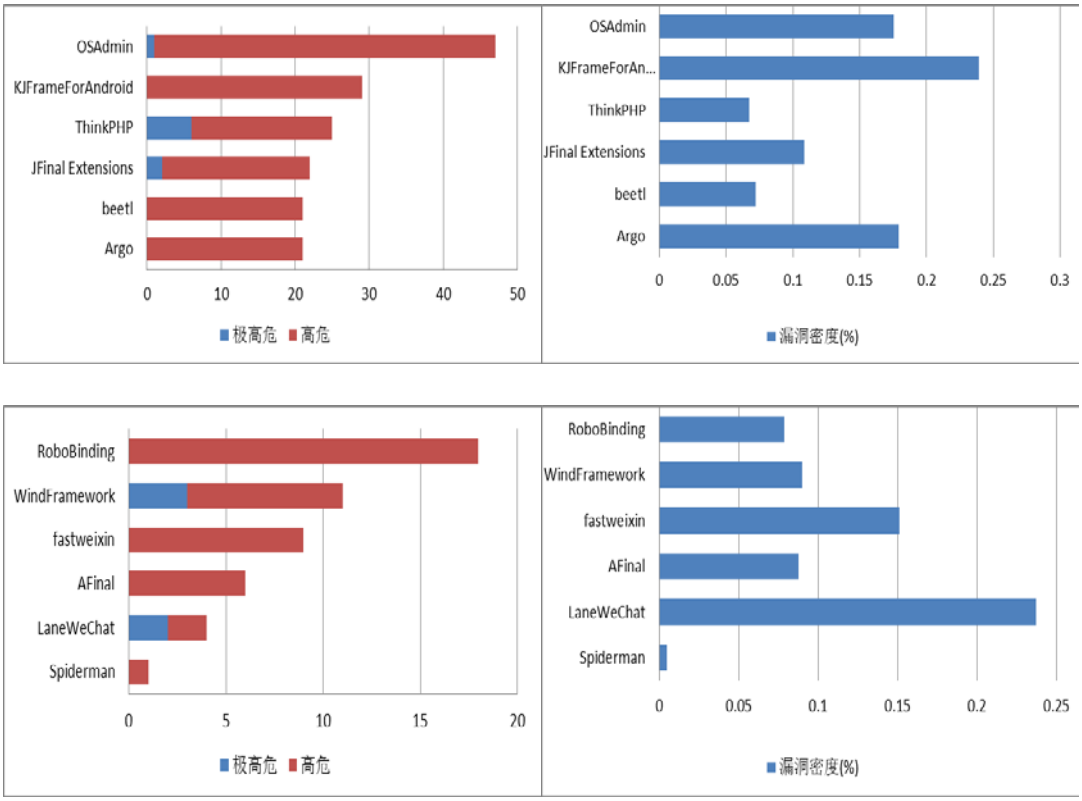



图 2 开源软件项目中安全漏洞分析图

## 4.2 高危安全漏洞分布情况

此次测试中发现的高危漏洞不仅数量众多，覆盖的种类也较为繁杂。图 3 展示了被测项目中高危以上级别漏洞大类的分布情况。数据表明，绝大多数漏洞为“安全特性”和“输入验证与表示”类漏洞。“安全特性”类漏洞可能导致加密算法被破解，进而导致用户隐私信息泄露等严重安全问题。“输入验证与表示”类型漏洞易被攻击者利用，通过绕过用户输入验证从而对 Web 应用系统进行攻击，产生较严重危害。此外，“代码质量问题”类漏洞也占据了较大比例，产生的主要原因是开发人员安全意识不足，此类漏洞会导致内存溢出、资源耗尽等安全隐患，严重情况下会导致系统运行异常、甚至系统崩溃。

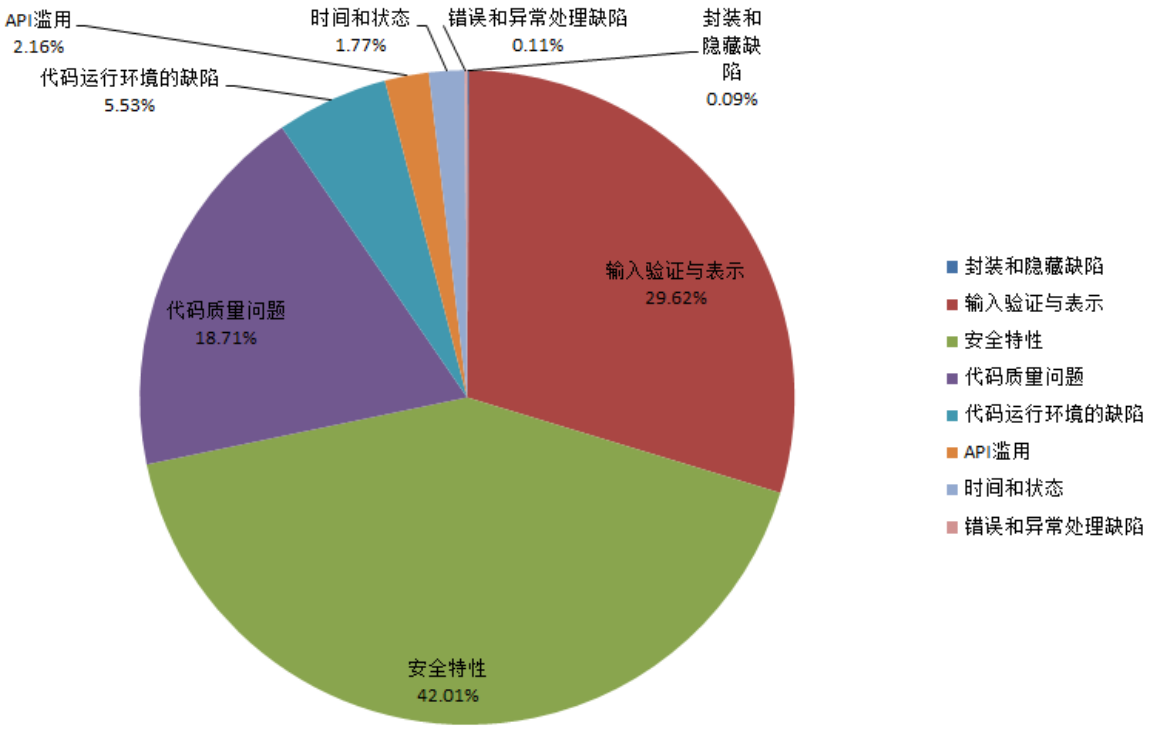



图 3 被测项目中的高危以上级别安全漏洞分布情况（按大类划分）

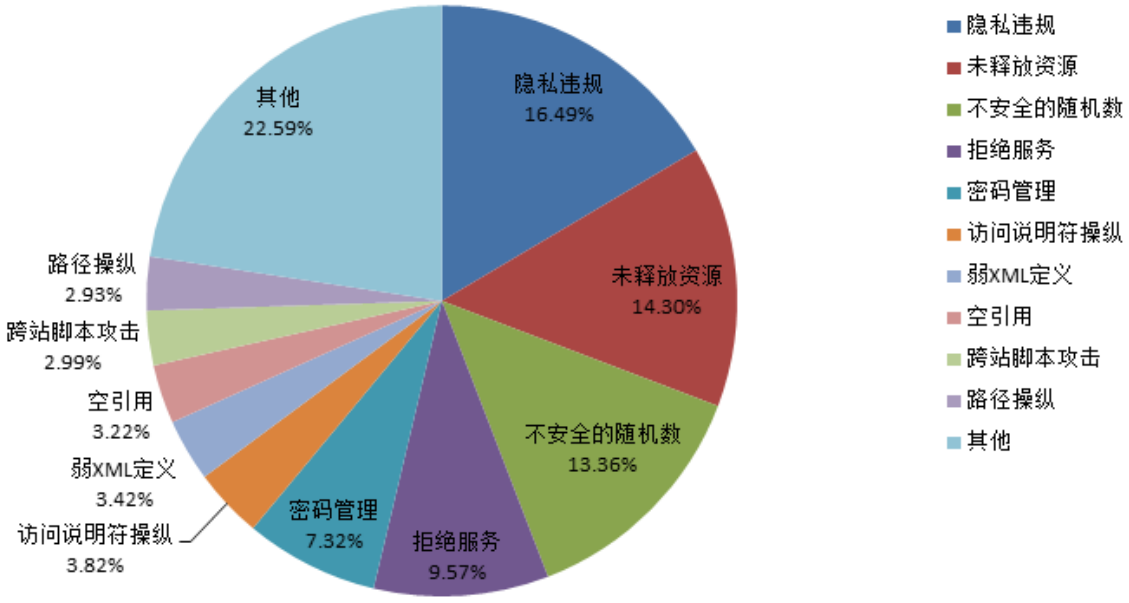



图 4 被测项目中的高危以上级别安全漏洞分布情况（按具体安全漏洞划分）

图 4 进一步展示了被测项目中的各种具体的高危以上级别安全漏洞的分布情况。在被测的 30 个项目中，出现次数超过 100 次的高危以上漏洞共有 10 种。可以看出，出现最多的前 5 种漏洞依次是：隐私违规(16.49%，579 个)、未释放资源（14.3%，502

个）、不安全的随机数（13.36%， 469 个）、拒绝服务（10%，336 个）和密码管理（7.32%，257 个）。下面对这 5 种漏洞进行简要说明，并给出防范建议。

1）隐私违规（属于安全特性缺陷）

危害：对机密信息（如客户密码或身份证号码）处理不当会危及用户的个人隐私。

防范：妥善处理隐私数据，禁止将其写入日志或文件等介质。

2）未释放资源（属于代码质量缺陷）

危害：当程序没有释放某个资源时，可能只会导致一般的软件可靠性问题，但如果攻击者能够故意触发资源泄漏，该攻击者就有可能通过耗尽资源池的方式发起拒绝服务攻击。

防范：每个资源的打开操作都要有对应的关闭操作。

3）不安全的随机数（属于安全特性缺陷）

危害：标准的伪随机数值生成器不能抵挡各种加密攻击。

防范：使用密码学的伪随机数生成器，使输出结果较难预测。

4）拒绝服务（属于输入验证与表示缺陷）

危害：攻击者可以造成程序崩溃或使合法用户无法正常使用。

防范：排除代码中只需要使用少量请求就可以使得攻击者让应用程序过载的漏洞。

5）密码管理（属于安全特性缺陷）

危害：程序中可能存在硬编码、弱加密等不安全的密码处理方式，容易导致密码泄露、口令被破解等安全问题。

防范：避免代码中存在硬编码，并使用安全的加密方式对密码进行加密处理，保存在数据库或配置文件中。

## 4.3 安全漏洞总体分布情况

本部分进一步展示被测项目中，所有级别安全漏洞的总体分布情况。图 5 展示了被测项目中所有级别安全漏洞大类的分布情况。数据表明，“错误和异常处理缺陷”、“封装和隐藏缺陷”以及“代码质量问题”相关的漏洞比例最高，这三类漏洞的产生主要是由于开发人员安全意识不强所导致的；这些漏洞虽然不易产生重大危害，但可能导致系统运行不稳定、系统重要信息泄露等安全隐患，一旦被攻击者利用也会造成严重后果。而“安全特性缺陷”和“输入验证与表示”相关漏洞比例也较高，这两大类漏洞往往危险级别较高，极易被攻击者利用且产生严重破坏，需要引起开发人员的高度重视。

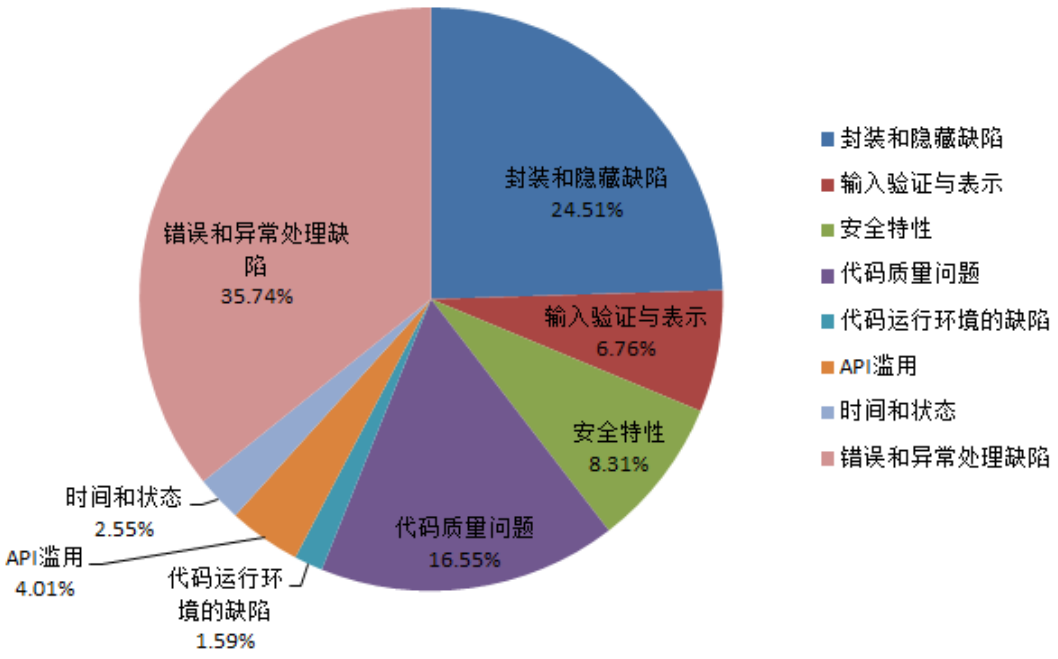



图 5 被测项目中的安全漏洞的分布情况（按大类划分）

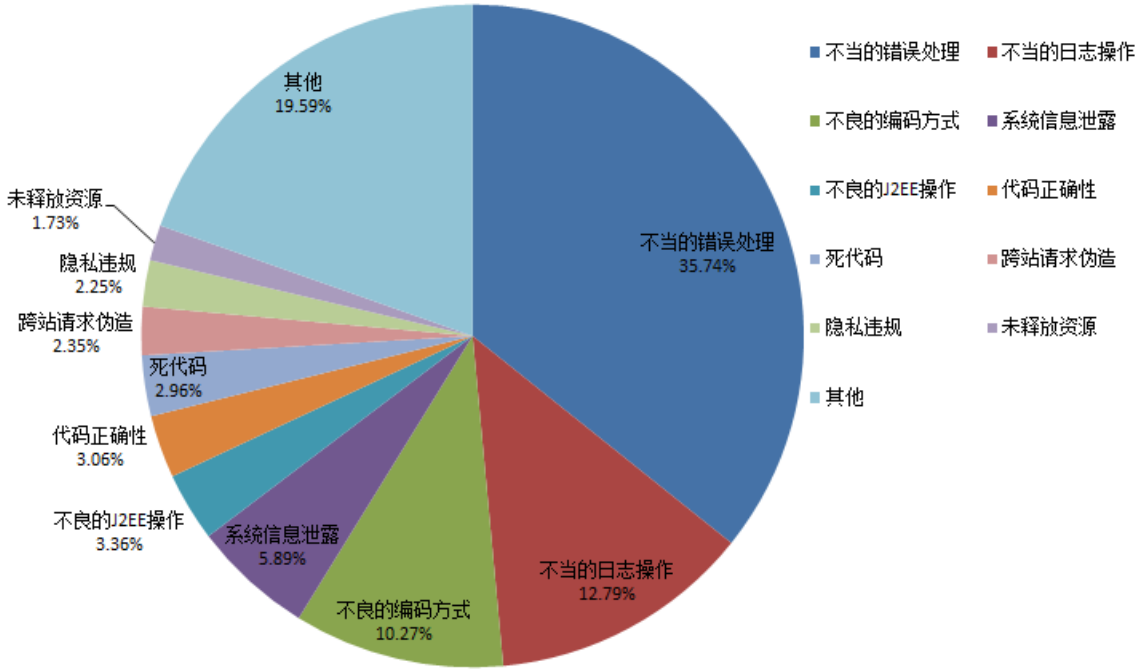



图 6 被测项目中的安全漏洞的分布情况（按具体安全漏洞划分）

图 6 进一步展示了被测项目中的各种具体的安全漏洞的分布情况。在被测的 30 个项目中，出现次数超过 500 次的漏洞共有 11 种。可以看出，出现最多的前 5 种漏洞依次是：不当的错误处理（35.74%，10349 个）、不当的日志操作（12.79%， 3703 个）、不良的编码方式（10.27%，2974 个）、系统信息泄露（5.89%，1706 个）和不良的 J2EE 操作（3.36%，974 个）。下面对这 5 种漏洞进行简要说明，并给出防范建议。

1）不当的错误处理（属于错误和异常处理缺陷）

危害：在异常处理上存在不当的操作方式，如抛出或捕获的异常种类过于笼统等，会导致调用者很难处理和修复发生的错误。

防范：使用安全的异常处理方式，针对特定的情况抛出合适的异常并捕获特定种类的异常。

2）不当的日志操作（属于封装和隐藏缺陷）

危害：系统没有使用专门的日志记录工具进行日志处理，导致难以监控程序的运行状况。

防范：使用专门的日志记录工具，方便随时监控程序的运行状况。

3）不良的编码方式（属于代码质量问题）

危害：代码中存在不好的编码方式（如变量赋值后并不使用，而变成死存储；一个代码块中不包含任何指令等），除了造成存储浪费以外，很可能是代码逻辑出现错误。

防范：检查代码编写是否存在错误；如果逻辑上不存在错误，建议删除冗余代码并修改代码样式，提高可维护性。

4）系统信息泄露（属于封装和隐藏缺陷）

危害：由于对系统敏感信息处理不当，会暴露系统数据或调试信息，这会帮助攻击者获悉系统脆弱点，从而进行攻击尝试。

防范：区分敏感和不敏感信息，对于敏感信息禁止输出。错误信息应由自定义页面输出，避免错误页面中包含系统信息。

5）不良的 J2EE 操作（属于 API 滥用缺陷）

危害：在进行 J2EE 开发时，如果没有使用 J2EE 推荐的方式进行开发，极易造成代码过度复杂并导致代码出错。

防范：使用 J2EE 推荐的方法进行通信等操作。

# 5 关于本报告的说明

一、本报告仅从代码角度进行漏洞分析。在实际系统中，由于软件实际部署环境、安全设备等的限制，部分漏洞可能无法通过渗透测试得到验证。

二、本报告中的漏洞仅适用于表 1 中列出的特定软件版本。当软件版本有任何更新、修改和优化时，本报告不再适用。