公 开

2014 年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 1 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技术。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，实验室对三大类共计 30 款广泛使用的知名开源软件进行了源代码测试。结合漏洞扫描技术和人工审计分析，发现现有开源软件存在数量众多的安全问题。本次测试在代码安全层面共发现漏洞 39275 余个，其中极易被攻击者利用的高危漏洞占比非常高，超过了总数的 30%。

2 被测开源软件

本次测试软件项目包括三大类：国内十大优秀开源项目、十大开源建站软件和十大 Java 项目。表 1 列出了本次被测的 30 个开源软件项目的概况，这些软件都是国际、国内知名的拥有广泛用户的软件项目的最新版本，而且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。例如，Discuz!已拥有 14 年以上的应用历史和 200 多万网站用户案例，是全球成熟度最高、覆盖率最大的论坛软件系统之一。

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
ansj_seg	1.1	Java	中文分词器
DWZJUI	1.4.5	JavaScript	富客户端框架
JEECG	3.3.2	Java	微云快速开发平台
zTree	3.5.15	JavaScript	JQuery Tree 插件
ThinkPHP	3.2	PHP	PHP 开发框架

ueditor	1.3.6	JavaScript	富文本 web 编辑器
APDPlat	2.0	Java	应用级产品开发平台
ZenTao(禅道)	5.2.1	PHP	项目管理软件
Webbuilder	6.8	Java	Web 应用开发运行平台
FineUI	3.3.3	ASP.NET	网站控件库
DEDECMS(织梦)	5.7 SP1	PHP	内容管理系统
Discuz!	X3.1	PHP	社区论坛软件
ECShop	2.7.3	PHP	电子商务平台软件
EmpireCMS(帝国)	7.0	PHP	网站管理系统
ESPCMS(易思)	5.8.14.	PHP	企业网站管理系统
PHP168(齐博)	V7.0	PHP	网站管理系统
Phpcms	9.5.2	PHP	网站管理系统
Phpwind	9.0	PHP	社区论坛建站程序
SHLCMS(深喉咙)	4.2.0	PHP	网站管理系统
Wordpress	3.8.1	Java	博客内容管理系统
JSoup	1.7.3	Java	HTML 解析器
SLF4J	1.7.6	Java	Java 日志组件
Sonar	4.2-M14	Java	代码质量管理平台
SpringData-neo4j	2.3.4	Java	基于 Spring 框架构建应用的数据访问计数构建框架
SpringData-Hadoop	2.0.0		
Twitter_Storm	0.9.0.1	Java	实时数据处理平台
CruiseControl	2.8.4	Java	持续构建程序
Druid	1.0.12	Java	JDBC组件
Fastjson	1.2.3	Java	JSON 解析器和生成器
JFinal	1.9	Java	极速 WEB+ORM 框架

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。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，本报告只讨论开源项目中的这两种级别的漏洞情况。

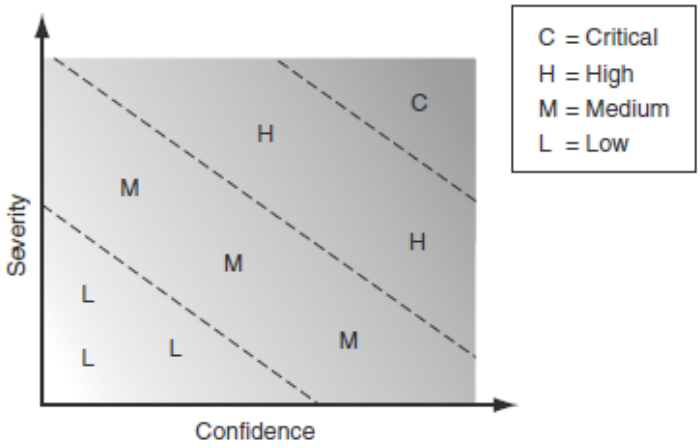

图 1 漏洞级别与严重程度、可信程度的关系

4 开源软件项目的安全漏洞情况

4.1 安全漏洞情况概览

图 2 展示了被测开源项目中存在的极高危害以及高度危害的安全漏洞的情况 纵坐标为项目名称，横坐标表示漏洞数目。由于不同项目之间漏洞总数差别较大，我们将这

些项目分为两部分展示，图（a）为漏洞总数前 5 的软件，图（b）为其他软件。

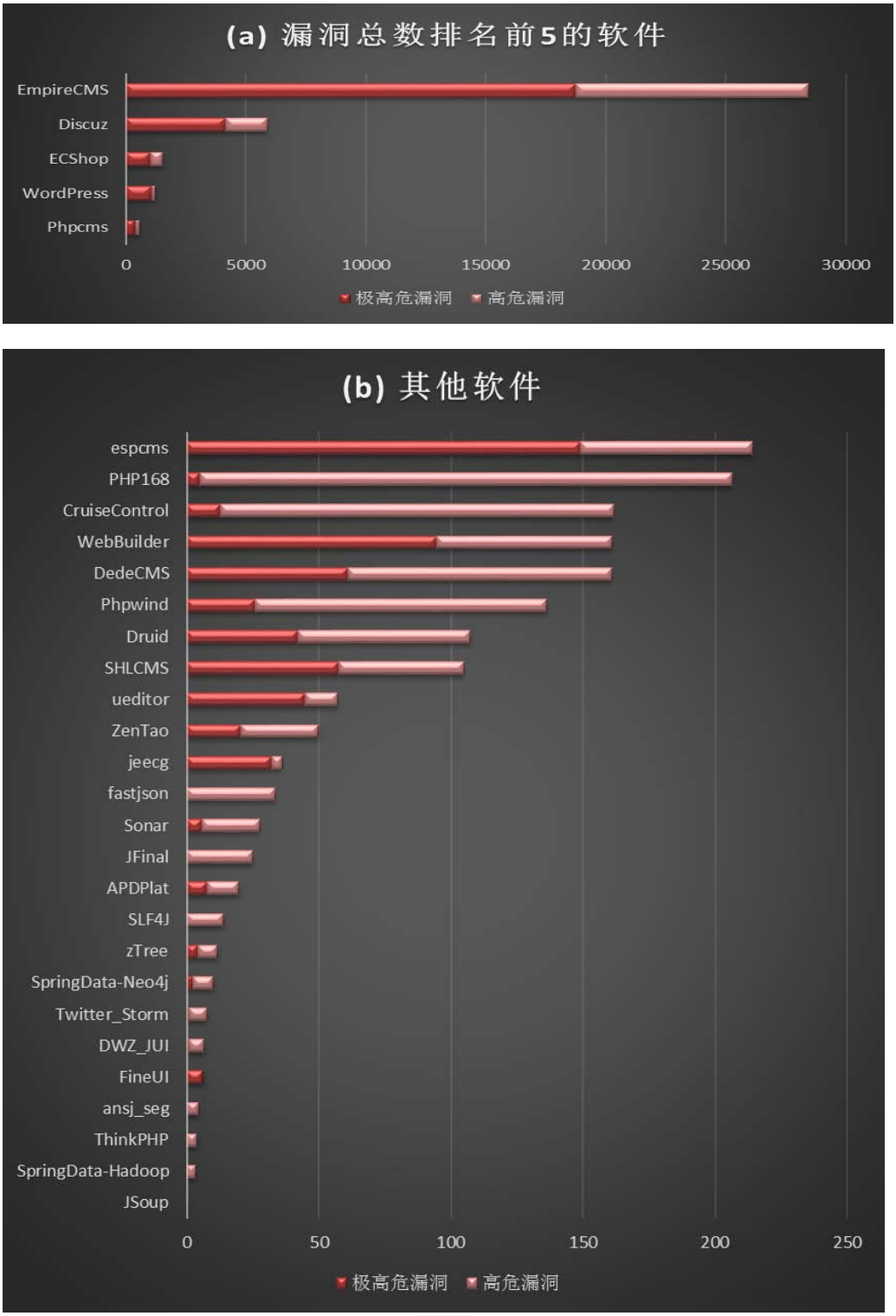

图 2. 开源软件项目中安全漏洞概览

从图中可以看出，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 25932 个，高危漏洞 13343 个，平均有极高危害漏洞 864 个，高度危害

漏洞 444 个，甚至有超过 10%的项目（EmpireCMS、Discuz、ECShop 和 Wordpress）漏洞总数超过了 1000 个。漏洞数量最多的软件项目是 EmpireCMS，该项目总共存在漏洞 28463 个，第 2 名 Discuz 漏洞总数的约 7 倍。第 2 名 Discuz 项目的漏洞数量也非常多，存在极高危漏洞 4143 个，高危漏洞 1754 个，是第 3 名 ECShop 的接近 3 倍。第 3 名 ECShop 也不容乐观，存在极高危漏洞 1022 个，高危漏洞 533 个。这项统计充分说明了这批项目的安全性情况，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。

4.2 安全漏洞总体分布情况

此次测试中发现的漏洞不仅数量众多，覆盖的种类也较为繁杂，如图 3 所示。

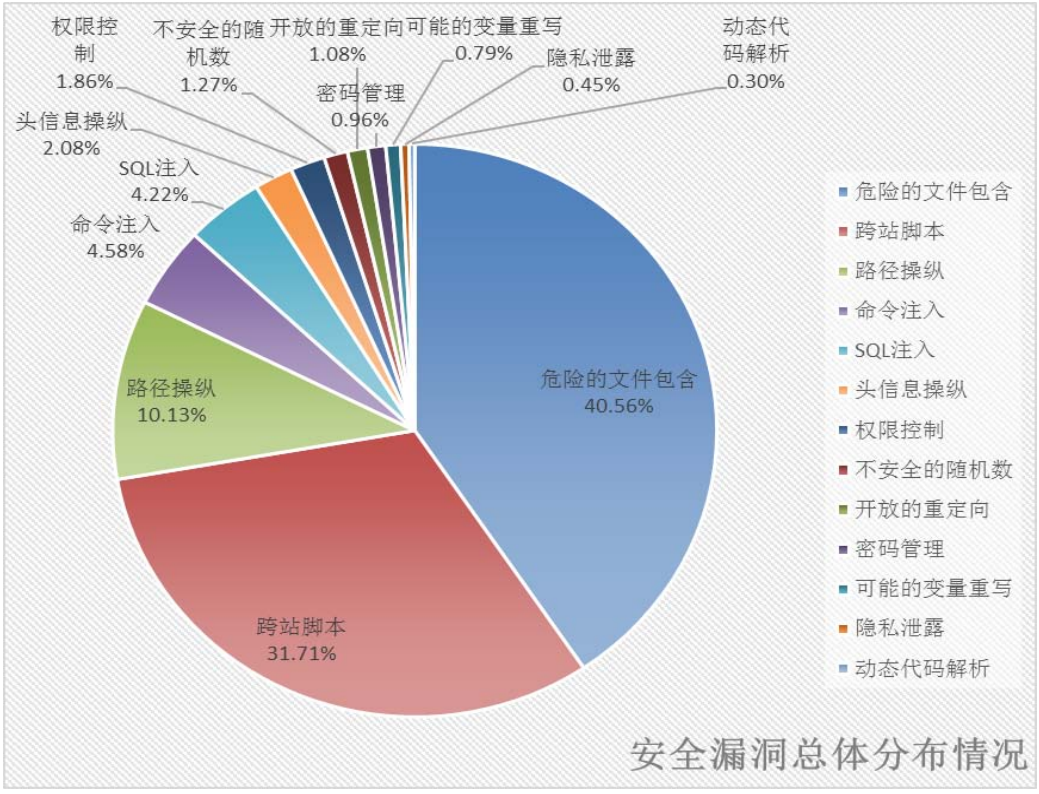

图 3 被测项目中的安全漏洞的总体分布情况

在被测的 30 个项目中，共出现安全漏洞 20 种。图 3 展示了在极高危和高危漏洞中，不同种类的漏洞数量分布情况。可以看出，出现最多的前 5 种漏洞依次是：危险文

件包含(40.56%，16068 个)、跨站脚本（31.71%，12564 个）、路径操纵（10.13%，4041 个）、命令注入（4.58%，1815 个）和 SQL 注入（4.22%，1673 个）。这 5 种漏洞都是输入验证与表示类型的安全漏洞，这也符合当前存在大量的绕过用户输入验证从而对 Web 应用系统进行攻击的现实情况。下面对这 5 种漏洞进行简要说明，并给出防范建议。

1）危险文件包含（属于输入验证与表示类漏洞）

危害：如果允许未经验证的用户输入控制动态包含在 JSP 中的文件，会导致恶意代码的执行。

防范：避免用户控制包含在 JSP 中的文件路径及文件名。

2）跨站脚本（属于输入验证与表示类漏洞）

危害：向一个 Web 浏览器发送未经验证的数据会导致该浏览器执行恶意代码。

防范：对浏览器执行的字符串严格校验或编码，确保恶意代码不会被浏览器执行。

3）路径操纵（属于输入验证与表示类漏洞）

危害：允许用户输入访问文件系统的路径，可以使攻击者访问或修改保护的系统资源。

防范：验证用户输入，禁止用户访问敏感系统资源。

4）命令注入（属于输入验证与表示类漏洞）

危害：执行不可信赖资源中的命令，或在不可信赖的环境中执行命令，都会导致程序以攻击者的名义执行恶意命令。

防范：禁止程序执行用户可控的命令。

5 ）SQL 注入（ 属于输入验证与表示类漏洞 ）

危害：通过不可信来源的输入构建动态 SQL 指令，攻击者就能够修改指令的含义或者执行任意 SQL 命令。

防范：采用参数化查询方式进行 SQL 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。