Seebug 漏洞平台
2016 年度报告

2017.02.24

北京知道创宇信息技术有限公司

目录

一、概述

Seebug 原名 Sebug，最初于 2006 年上线，作为国内最早、最权威的漏洞库为广大用户提供了一个漏洞参考、分享与学习平台。

Seebug 以打造良好的漏洞生态圈为己任，经过十余年不断的完善与更新现已成长为国内知名安全厂商知道创宇旗下一个成熟、独具特色的漏洞社区。

2015 年，Seebug 在国际上首次提出“漏洞灵魂”概念，将每个漏洞视为鲜活的个体而非一段冷冰冰的介绍或代码，每次发现、披露、验证与利用均构成漏洞生命周期的重要节点，共同形成一个不断迭代的过程，为后续研究提供严谨、规范、有价值的参考。

此外，为了尊重白帽子的劳动成果、最大程度发挥社区优势，Seebug 还在第四届 KCon 黑客大会上推出百万奖励计划，使漏洞交易变得公开、透明。

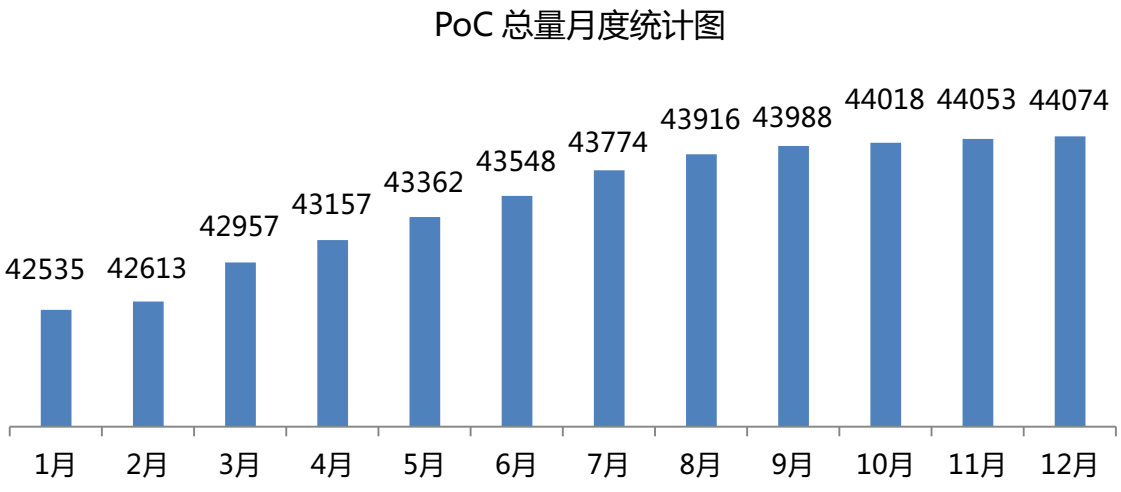
2016 年，Seebug 国际版正式上线，携手 ZoomEye、Pocsuite 共同亮相举世瞩目的黑帽大会，在国际舞台上一展风采。

二、漏洞详情等信息以及漏洞验证程序(PoC)收录状况

Seebug 统计结果显示，截至 2016 年 12 月 31 日，Seebug 共收录漏洞 51909 个(日常维护漏洞数量)，其中 2016 年新增漏洞 2350 个，占漏洞总数 4.5%。收录 PoC 数量 44074 个，其中 2016 年新增 1920 个，占 PoC 总数的 4.4%。从漏洞危险等级来看，2016 年新增高危漏洞 419 个，中危漏洞 1748 个，低危漏洞 183 个。从漏洞类型来看，2016 年 SQL 注入类漏洞所占比例高达 46%。

2.1 漏洞验证程序(PoC)数量统计分析

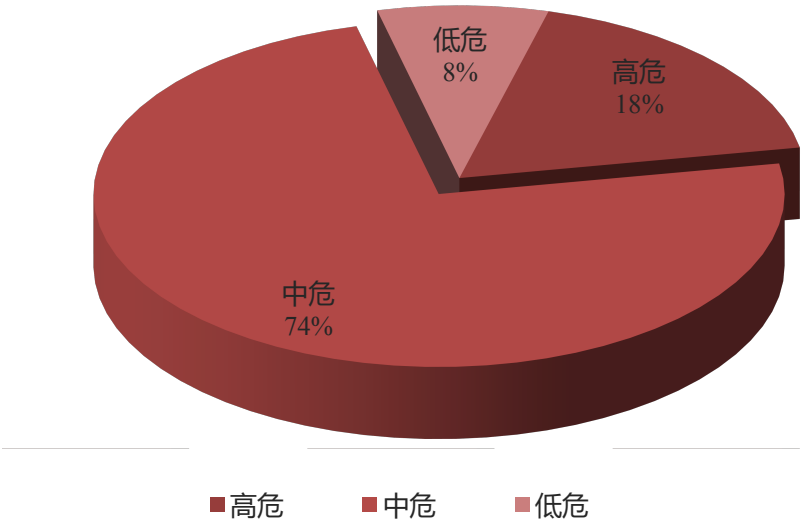
Seebug 统计结果显示，共收录 PoC 数量 44074 个。2016 年新增 1920 个，占 PoC 总数的 4.4%。由下图可见，上半年增长速度较快。



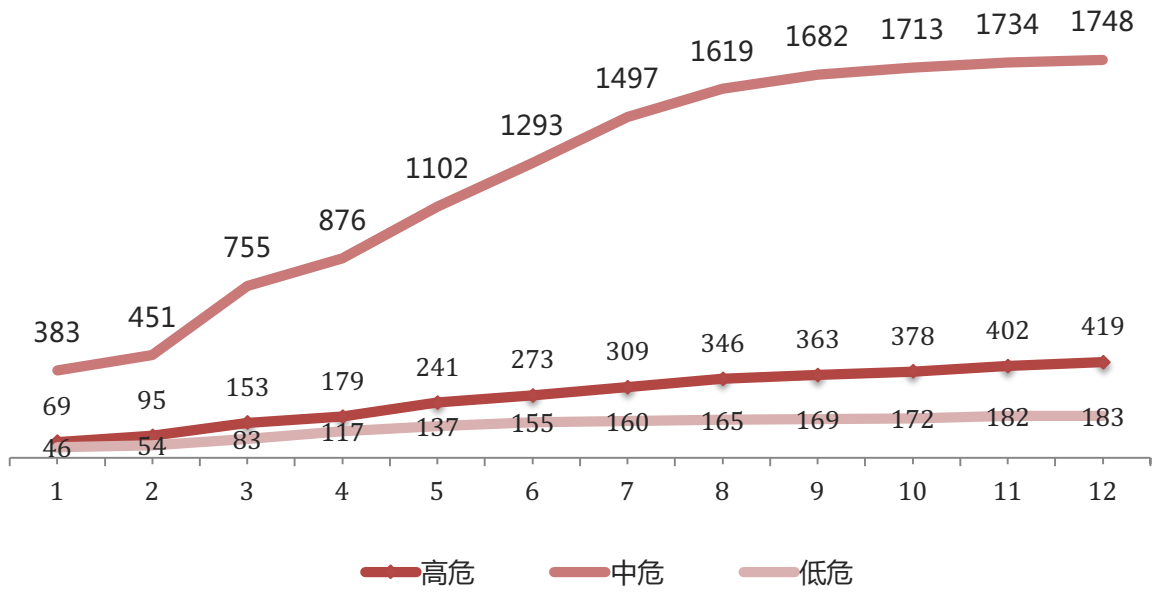
2.2 收录漏洞的危害等级分布统计分析

Seebug 根据漏洞的利用复杂程度、影响范围等将危害分为三个等级，即高危、中危、低危。2016 年新增漏洞危害等级分布如图所示，其中高危漏洞 419 个(占 18%)，中危漏洞 1748 个(占 74%)， 低危漏洞 183 个(占 8%)。高危漏洞中有我们熟知的 DirtyCOW 漏洞(CVE-2016-5195)、OpenSSH 远程代码执行漏洞（CVE-2016-10010）、Nginx 权限提升（CVE-2016-1247）、win32k 权限提升漏洞(CVE-2016-7255)等，多数为各大主流操作系统漏洞。

2016 年 Seebug 新增漏洞风险等级分布统计图



2016 年 Seebug 月度漏洞增长统计图

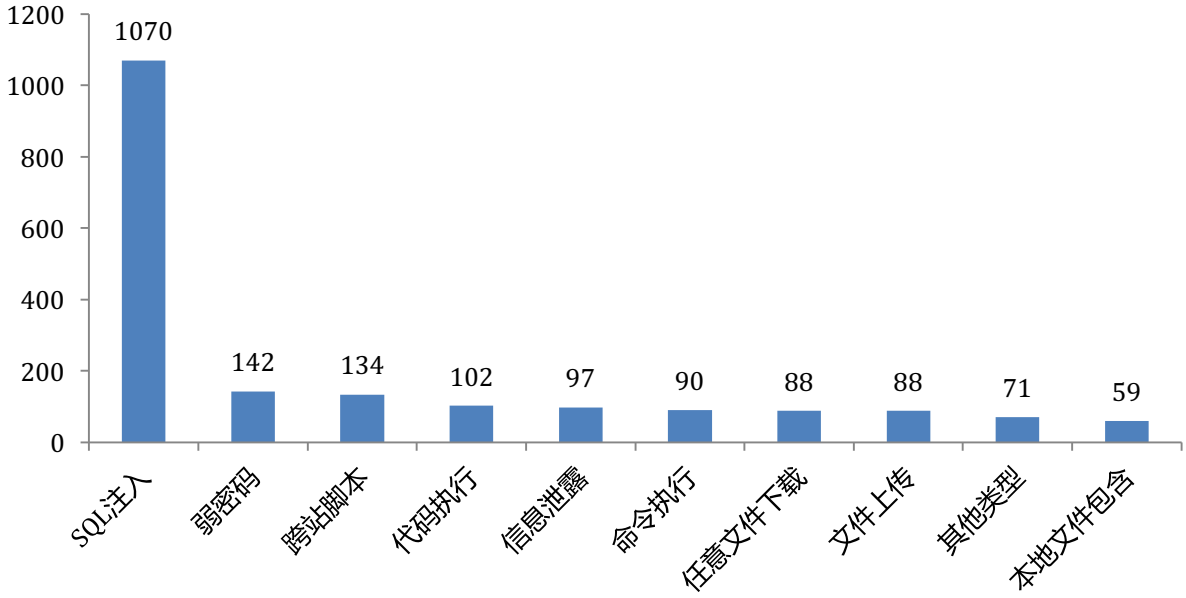


2.3 收录漏洞的类型分布统计分析

2016 年 Seebug 新增漏洞类型统计结果显示，SQL 注入漏洞最多，达 1070 个，占 2016 年新增漏洞的 46%。大多数网站中常见 SQL 注入漏洞，这是由于网站对用户 Web 表单输入或请求内容过滤不充分造成的。攻击者通过 SQL 注入很容易造成网站数据库的信息泄露。位居第三位的跨站脚本攻击也同样是对 Web 表单或页面请求过滤不充分造成的，攻击者利用存在反射性 XSS 的网站可以构造恶意链接引诱用户点击，从而获取到用户的登录 cookie。利用存在存储型 XSS 的网站(如留言板)，通过留言板留言将恶

意代码存储在服务器，当有用户点击嵌入恶意代码的页面也会被盗取 cookie。如今大部分浏览器如 Chrome、Safari、Firefox 等都有对 CSP 的支持、有 XSS-Audtior 防护，从而使跨站脚本攻击的漏洞数量逐渐减少很多，但这些防护并不能彻底防范跨站脚本攻击。

2016 年 Seeebug 收录漏洞类型 TOP10

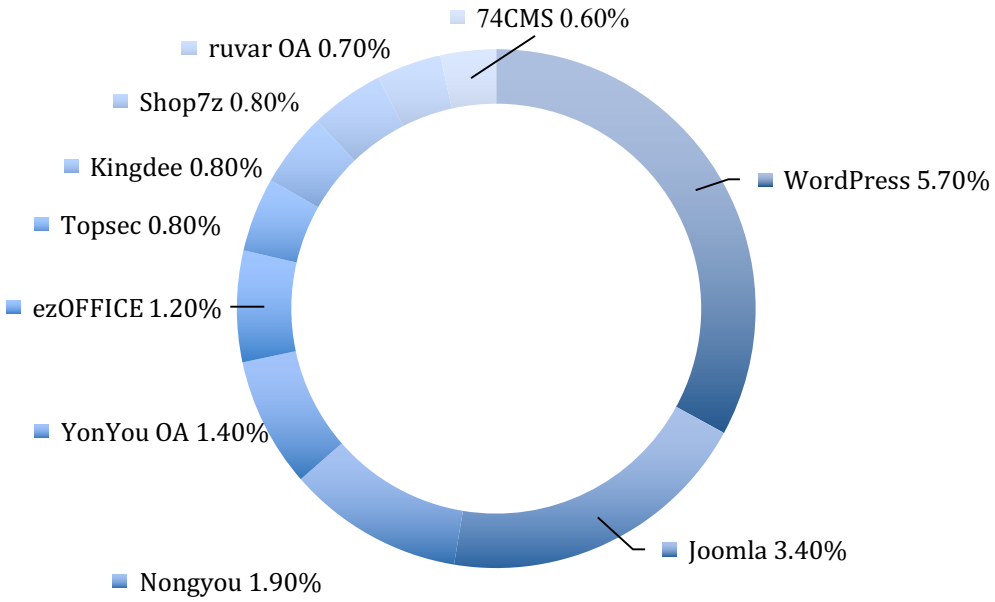


从上表中还可以看出弱密码和信息泄露漏洞也十分常见，通过后台统计发现，大部分是路由器、摄像头、工控设备的漏洞。随着科技的发展，智能设备的使用也越来越广泛，如何保证物联网安全越来越被安全研究人员所重视。

2.4 漏洞组件分布统计分析

Seebug 收录了可能受影响的组件 3946 个，通过对 2016 年 Seebug 新增漏洞受影响组件进行统计发现，WordPress 组件漏洞数量最多，共 133 个，占新增漏洞的 5.7%。另外可以从下图看出，Top10 组件全部为信息管理系统，可见像 WordPress、Joomla 这些管理系统依然是全球广大白帽子关注的重点 Web 应用。

受漏洞影响的 Top10 组件统计图



三、2016 年重大漏洞记录

3.1 Struts 2 远程代码执行漏洞(S2-032)

漏洞简介

Struts 2 是世界上最流行的 Java Web 服务器框架之一，2016 年 Seebug 共收录 Struts 2 组件漏洞 8 个，其中严重的有 2016 年 4 月爆出的 Struts2 远程代码执行漏洞(S2-032)，之后又曝出的(S2-033)、(S2-037)漏洞也都由于构造特殊的 Payload 绕过过滤触发 OGNL 表达式，从而造成任意代码执行。

漏洞影响

Apache Struts 2.3.18 ~ 2.3.28 版本(除 2.3.20.2 与 2.3.24.2 版本外)，在开启动态方法调用的情况下，构造特殊的 Payload 绕过过滤触发 OGNL 表达式，造成远程代码执行。

3.2 Dirty COW Linux 内核漏洞

漏洞简介

2016 年 10 月，Linux 公开了一个名为 Dirty COW 的内核漏洞 CVE-2016-5195，号称有史以来最严重的本地提权漏洞。Linux 内核的内存子系统在处理写时拷贝(Copy-on-Write)时存在条件竞争漏洞，可以使一个低权限用户修改只读内存映射文件，进而可能获取 root 权限。

漏洞影响

在 Linux 内核版本在大于等于 2.6.22 且小于 3.9 时都受该漏洞的影响。攻击者可以获取低权限的本地用户后，利用此漏洞获取其他只读内存映射的写权限，进一步获取 root 权限。

漏洞详情

在进行需要调用内核 get_user_pages()函数且 force 参数被置为 1 的写操作时（这里以对/proc/self/mem 进行写操作为例）漏洞触发流程大致如下：

- 第一次需要获取内存对应的页面，由于缺页会调用 faultin_page()，在调用过程中由于需要处理缺页错误执行了 do_cow_fault()调用，即 COW 方式的调页。
- 第二次回到 retry 执行时，依旧调用 faultin_page()函数，但是由于是写只读映射的内存所以会执行 COW 处理，在 COW 操作顺利完成返回到 faultin_page()函数中时，FOLL_WRITE 标志位被清掉(即去掉了 FOLL_WRITE 的权限要求)。
- 由于执行线程将让出 CPU，进程转而执行另一线程，带 MADV_DONTNEED 参数的 madvise()调用 unmap 清掉之前一直在处理的内存页，即对应的页表项(pte) 被清空了。
- 第三次回到 retry 执行时，又会与第一次做相同的操作，但不同的是调用 do_fault()函数进行调页时 FOLL_WRITE 标志位被清掉了，所以执行的是 do_read_fault()函数而非之前的 do_cow_fault()函数。

获取到 do_read_fault()调页后对应的页表项后，就可以实现对只读文件的写入操作，造成越权操作。

3.3 Nginx 权限提升漏洞(CVE-2016-1247)

漏洞简介

2016 年 11 月 15 日，国外安全研究员 Dawid Golunski 公开了一个新的 Nginx 漏洞 (CVE-2016-1247)，能够影响基于 Debian 系列的发行版，Nginx 作为目前主流的一个多用途服务器危害还是比较严重的，目前官方已对此漏洞进行了修复。

漏洞影响

Nginx 服务在创建 log 目录时使用了不安全的权限设置 ,可造成本地权限提升，恶意攻击者能够借此实现从 nginx/web 的用户权限 www-data 到 root 用户权限的提升。由于 Nginx 服务器广泛应用于 Linux 和 UNIX 系统，致使主流 GNU/Linux 发行版也都受到严重影响。

系统	受影响版本
Debian	Nginx < 1.6.2-5+deb8u3
Ubuntu 16.04 LTS	Nginx < 1.10.0-0ubuntu0.16.04.3
Ubuntu 14.04 LTS	Nginx < 1.4.6-1ubuntu3.6
Ubuntu 16.10	Nginx < 1.10.1-0ubuntu1.1

漏洞详情

在 Linux 系统下，我们可以通过编译一个含相同函数定义的 so 文件并借助/etc/ld.so.preload 文件来完成此操作，系统的 loader 代码中会检查是否存在/etc/ld.so.preload 文件，如果存在那么就会加载其中列出的所有 so 文件，它能够实现与 LD_PRELOAD 环境变量相同的功能且限制更少，以此来调用我们定义的函数而非原函数。此方法适用于用户空间的 so 文件劫持，类似于 Windows 下的 DLL 劫持技术。

由于 Nginx 在配置 log 文件时采用的是不安全权限设置，将 PoC 编译成 so 文件后，可以很容易将路径写入到/etc/ld.so.preload 文件中，这时候就可以实现对 geteuid()函数的 hook，进而实现 www-data 到 root 的权限提升。

3.4 Netgear R6400/R7000/R8000 - Command Injection 漏洞

漏洞简介

2016 年 12 月 7 日，NETGEAR R7000 路由器在 exploit-db 上被爆出存在远程命令执行漏洞，随着研究不断深入，R8000 和 R6400 这两款路由器也

被证实有同样的问题。2016 年 12 月 13 日，NETGEAR 官网上确认漏洞存在 ,对部分受影响的设备发出了 beta 版的固件补丁。2016 年 12 月 14 日，受影响的设备型号增加至 11 种。

漏洞影响

经过测试以下类型路由器均受到该漏洞影响： NETGEAR R6250 、NETGEAR R6400 、NETGEAR R6700 、NETGEAR R6900 、 NETGEAR R7000 NETGEAR R7100LG 、 NETGEAR R7300DST 、 NETGEAR R7900 、 NETGEAR R8000、 NETGEAR D6220 、 NETGEAR D6400。通过 ZoomEye 网络空间探测引擎得知，暴露在公网上的 R6400 类型设备大约 2177 个，R7000 大约有 14417 个，R8000 大约有 6588 个，可见影响之广。

漏洞详情

NETGEAR 的固件中的/usr/sbin/httpd 文件中的会检查请求报文中的 url 是否含有 cgi-bin，如果含有，则进行一系列分割操作，并且 cgi-bin 后面的值最终会被替换代码中/www/cgi-bin/%s > /tmp/cgi_results 部分的%s，并被 system()函数执行造成命令执行漏洞。

3.5 Mirai 及变种 Mirai

Mirai

Mirai 僵尸网络可以高效扫描 IoT 设备，感染采用出厂密码设置或弱密码加密的脆弱物联网设备，被感染后的设备还可以去扫描感染其他 IoT 设备，设备成为僵尸网络机器人后在黑客命令下发动高强度僵尸网络攻击。其中最严重的是，2016 年 10 月 21 日，美国域名服务商 Dyn 遭受大规模 DDos 攻击，造成包括 Twitter、Facebook 在内的多家美国网站无法被正确解析，进而造成了半个美国的网络瘫痪，其元凶就是 Mirai 僵尸网络。

变种 Mirai

Mirai 的逆向分析报告发布之后，变种 Mirai 也悄然而生。变种 Mirai 的感染方式已经不仅仅单纯扫描 23 和 2323 端口，可以通过一系列组件漏洞（例如 Eir's D1000 调制解调 7547 端口的任意执行命令）感染其他 IoT 设备。随着变种增多，Mirai 系列的僵尸网络势必会长期威胁网络空间安全。

四、Seebug 漏洞平台使用状况统计分析

Seebug 自 2015 年 7 月新版本上线以来，秉承赋予漏洞以灵魂的宗旨，征集悬赏收录各种通用型漏洞信息、详情以及 PoC。2015 年 11 月上线照妖镜功能，用于漏洞在线检测。2016 年 8 月开设了 Paper 专栏，分享包括 Web 安全、二进制等类型的学习文章。

4.1 2016 最受关注的 10 个漏洞

根据 Seebug 漏洞社区收录的漏洞详情页面访问量统计，2016 年人气漏洞 Top10 排名如下:

排名	漏洞名称
1	Redis 未授权访问
2	WebLogic “Java 反序列化”过程远程命令执行漏洞
3	Struts2 方法调用远程代码执行漏洞(S2-032)
4	JBoss “Java 反序列化”过程远程命令执行漏洞
5	Joomla 3.2.0 - 3.4.4 无限制 SQL 注入漏洞
6	ImageMagick 命令执行漏洞

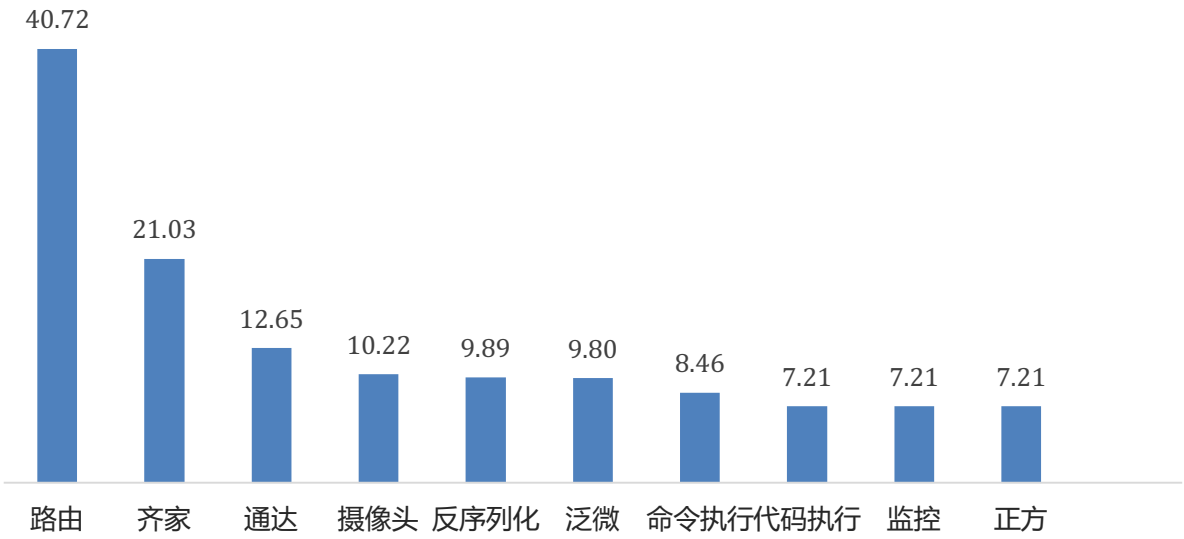
7	Linux 内核 2.6.22 < 3.9 权限提升漏洞 (Dirty COW)
8	WikkaWiki 1.3.2 Spam Logging PHP Injection
9	Memcached Server SASL 身份认证远程命令执行漏洞
10	Jenkins “Java 反序列化”过程远程命令执行漏洞

由点击量可以看出，很多古老的漏洞仍然受到广泛关注。Redis，Weblogoc，Struts，JBoss 等常用开发组件因为使用特别广泛，一旦爆发漏洞，就会产生巨大的危害。

4.2 搜索次数最高的十个漏洞关键词

2016 年度 Seebug 平台漏洞搜索关键词统计结果显示，路由器漏洞是大家关注的重点。其次，各种办公 OA 系统，命令执行，代码执行，反序列化漏洞等高危漏洞是社区用户关注的重点漏洞。这些漏洞轻则使服务器被攻陷，重则导致企业内网沦陷，重要商业机密数据被窃取。

TOP 10 关键词搜索量千分比



4.3 照妖镜：快速检测目标站点漏洞情况

自 2015 年 11 月上线以来，照妖镜共使用 82118 次，可在线检测漏洞 9 个。2016 年共使用 58564 次，在线检测漏洞新增 6 个：

- WordPress functions.php 主题文件后门漏洞
- Memcached 多个整数溢出漏洞 (CVE-2016-8704，CVE-2016-8705， CVE-2016-8706)
- Struts2 远程代码执行漏洞（S2-037）
- Struts2 远程代码执行漏洞（S2-033）

- WordPress 4.2.0-4.5.1 flashmediaelement.swf 反射型 XSS 漏洞，
- Struts2 方法调用远程代码执行漏洞(S2-032)

五、白帽子与奖励

5.1 百万现金 - Seebug 漏洞奖励计划

2016 年，是漏洞奖励计划的第二年，在发放完 2015 年的首批百万现金奖励之后，Seebug 漏洞社区团队再次投入二百万现金奖励。从前文可以看到，2016 这一年，Seebug 共收到白帽子提交漏洞/PoC/详情 4983 个。

漏洞现金奖励的门槛低，但是随着信息价值的提高，奖励也指数级的上涨。以下方式，都是可以获得奖励的途径：

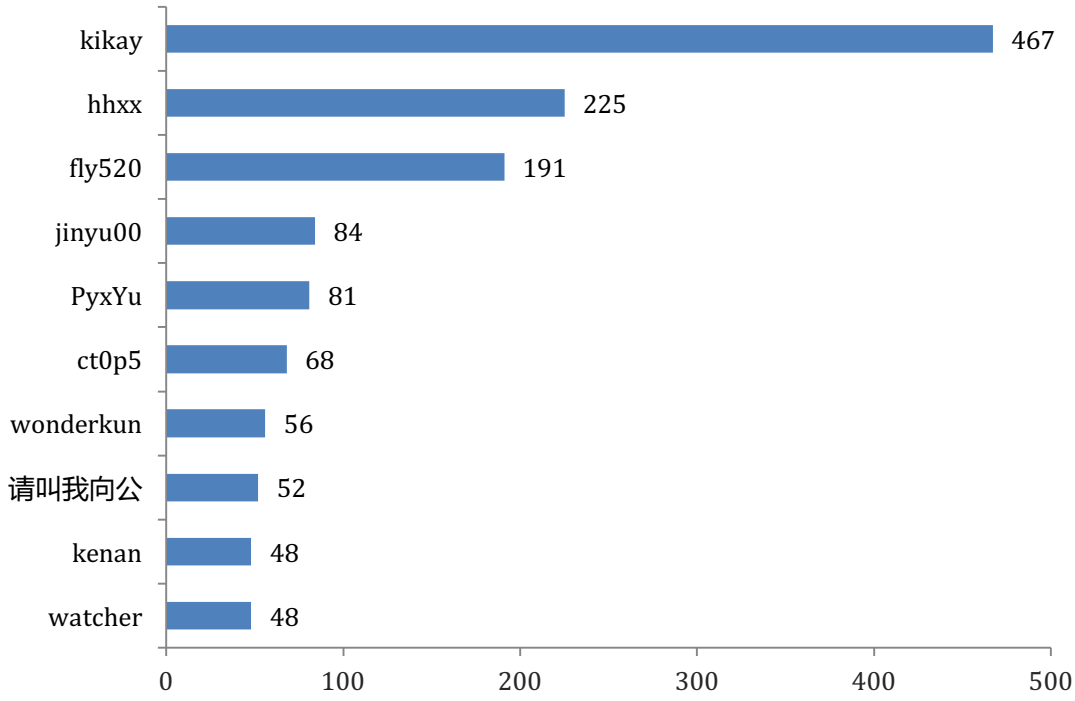
1. 补充完善 PoC/漏洞详情/漏洞修复方案等漏洞信息；
2. 提交受影响漏洞厂商相关数据；
3. 提交漏洞 ZoomEye Dork（ZoomEye 搜索关键词）；
4. 提交完善漏洞分类、组件相关信息；

5.2 Seebug 漏洞社区的核心白帽子

在 2016 年 8 月的 KCon 黑客大会上，Seebug 团队对 10 位核心白帽子进行了奖励，奖品包含证书以及纯银奖章等，希望他们能够再接再厉，提供更多的漏洞情报。

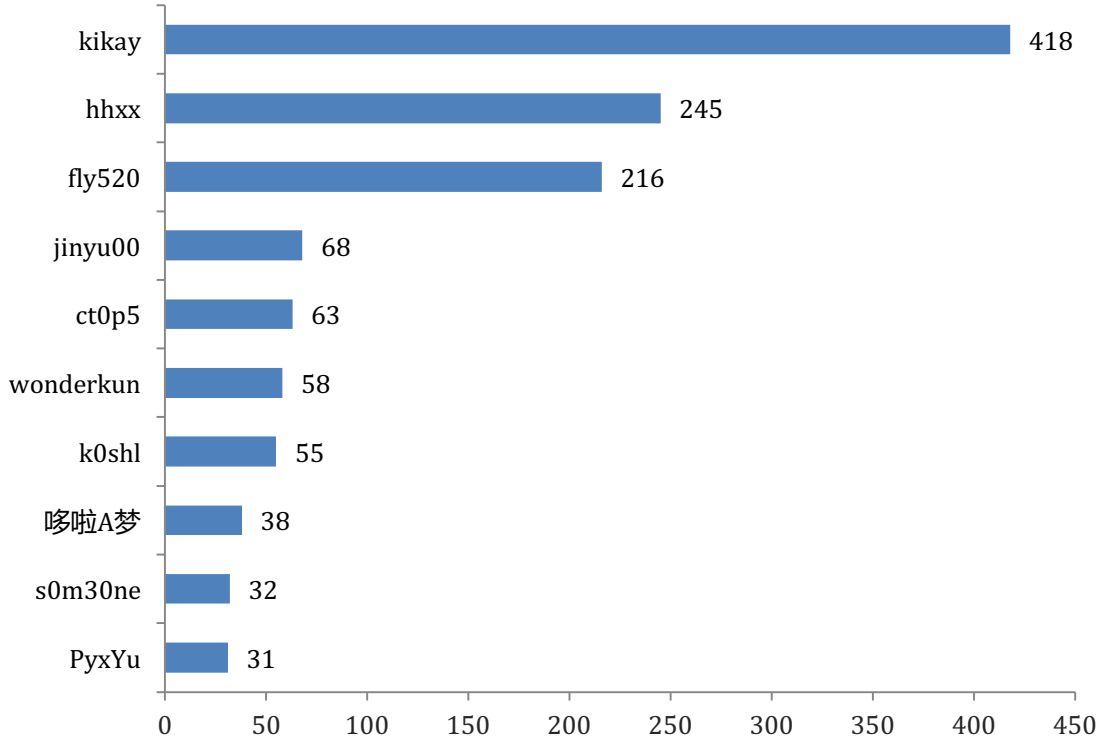
在 2016 年收录的 4983 个漏洞中，有以下十位白帽子提供了大量的漏洞资料，其中提交漏洞数最多的是 kikay，提交并被收录漏洞达到 467 个之多。

漏洞提交数量排名前十名的白帽子



Seebug 漏洞社区精华之处在于可以对已收录漏洞的 PoC 和详情进行补充，即便自己错过了第一提交时间，也仍然可以通过完善漏洞信息来获取 KB。

2016 年 Top 10 用户提交 PoC 数量排名见下图。



附录：Seebug 发展里程碑

2006 年 08 月 18 日- Bug Exp Search @BETA 版发布，以收集国内外网络安全缺陷与漏洞为主；

2006 年 10 月 25 日- Sebug 正式版发布，网站大改版，优化了部分代码并清除了若干安全隐患；

2008 年 08 月- Sebug Security Vulnerability DB 作为封面头条接受国内知名杂志《黑客手册》采访；

2009 年 03 月 - 添加 Paper 模块并收集国内外安全文档、测试文档以及历史漏洞 PoC；

2014 年 01 月- Sebug 移交知道创宇安全研究团队维护；

2015 年 07 月- Sebug 重新改版上线内测，提出赋予漏洞灵魂概念；

2015 年 08 月 - 知道创宇漏洞社区计划发布，Sebug 正式上线公测，面向白帽子悬赏百万漏洞贡献补贴

2015 年 11 月- Sebug 照妖镜功能上线；

2015 年 12 月- Sebug 新版上线，全新 VI 与整站风格，上线绵羊墙等功能；

2016 年 01 月 - Beebeeto 并入 Sebug，Sebug 品牌正式升级为 Seebug；

2016 年 1 月 29 日- Seebug 漏洞数量正式突破 5 万；

2016 年 03 月 28 日- Seebug 国际版上线；

2016 年 03 月 31 日- Seebug 与 ZoomEye、Pocsuite 共同亮相 Black Hat Asia；

2016 年 08 月 – Seebug Paper 专栏上线。