网站安全风水图

来自知道创宇的经验2011

钟晨鸣

www.knownsec.com
evilcos@gmail.com
微博：@evilcos

关于我

网名余弦，研究部总监@知道创宇

- 做这些事：
  - Web安全产品的核心技术研发
    - 网马监控、Web漏洞扫描器、WAF、数据中心等
  - Web/Web2.0安全研究
    - 我们自己的Web安全研究流程
- 让互联网更好更安全

目录

来自知道创宇的Web安全视角：

一. 网站安全**微观**研究

二. 网站安全**宏观**研究

最终目标：

掌握Web安全趋势，提供最切实际的解决方案！

一. 网站安全微观研究

你的网站风水好吗

基础架构层是否足够安全

网络做好隔离了吗？

服务器打补丁了吗？

不该开放的端口是不是开放了？

并且还存在弱口令？

不同的业务分离了吗？

子域分离了吗？

各模块之间、各层之间的权限配置好了吗？

你的网站风水好吗

Web应用层是否足够安全

基于的Web框架安全吗？

SQL查询都参数化了吗？

文件上传过滤好了吗？

调试与错误信息关了吗？

XSS肯定不存在了？

是不是忽略了CSRF？

风水

没安全意识的决策者很可怕

没安全意识的开发团队很可怕

没安全意识的运维团队很可怕

第一个决策

第一行代码

黑客如何拿下你的网站

单看Web应用层

可能直接拿下，服务端风险有：SQL注入、文件上传、文件包含、命令注入、各种信息泄露等，然后配合一些社会工程学方法

间接拿下，客户端风险有：XSS、CSRF、跨域漏洞等，然后再配合更多的社会工程学方法

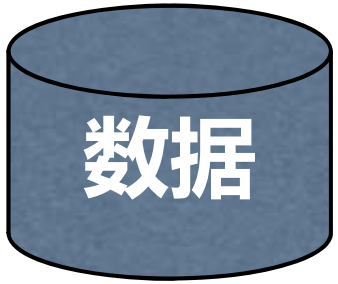
如果是仅拿下网站的一个用户权限？

只要有Web客户端风险足矣！

你的网站有什么价值

数据！各种数据！

- 地下产业链的核心需求就在这
- 这也是黑客们最感兴趣的一类



网站类型很多，我们做了归纳

数据

比如社交网站

- 真实身份库，好友关系库，虚拟货币……

比如电子商务类网站（包括那些团购）

- 客户数据、电子货币……

比如政府类网站

- 暗链SEO，定向挂马得到更多数据……

比如个人网站

- 暗链SEO，各种账号数据……

微观而全面

“微观”是指针对具体一个网站

从全面的角度来评估一个网站的安全风险与存在的各种漏洞，并提供一个针对性的完整解决方案

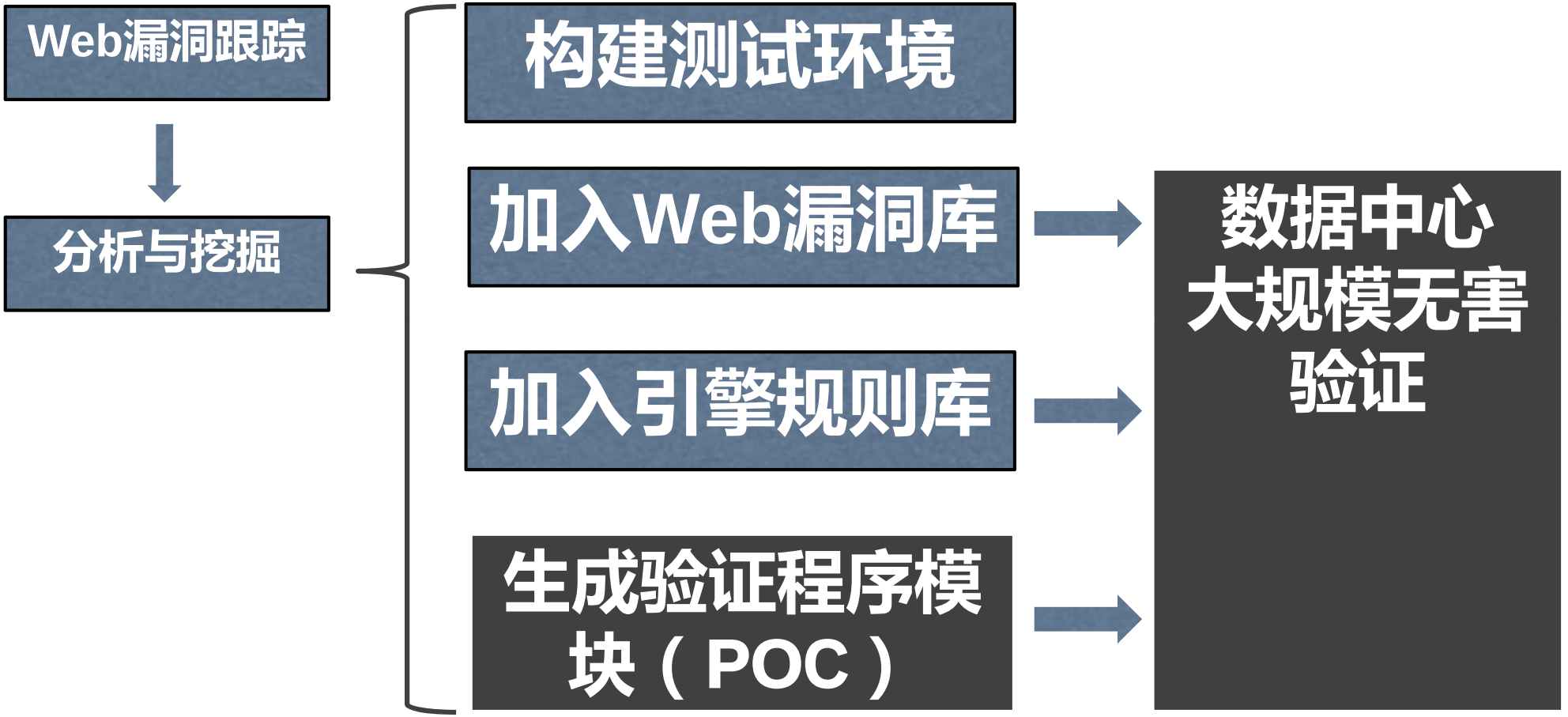
如何加快这个过程？

我们有WSL

WSL != 猥琐流

WSL == Web Security Loop

我们自己的Web安全研究流程


Web漏洞跟踪
分析与挖掘
构建测试环境
加入Web漏洞库
加入引擎规则库
生成验证程序模块（POC）
数据中心大规模无害验证

WSL重点

Web应用层安全

服务端风险、信息泄露、客户端风险等

基础架构层安全

网络、服务器、储存等

为什么需要WSL

有了这套完整的流程，我们能够

- 快速分析出漏洞根本原因
- 甚至更进一步挖掘出相关0day
- 我们能很好地演示该漏洞的危害
- 我们的**扫描器**能第一时间告警相关网站用户的漏洞风险
- 我们的**WAF**能更完美的阻止特定漏洞带来的威胁
- 我们能快速响应可能出现的Web安全事件
- 我们能在更宏观的层面知道这个漏洞影响范围

二. 网站安全宏观研究

数据中心

基于分布式爬虫系统

爬取全国600w多的网站，并不断增加新的入库

集群虚拟化部署

大数据量，数据存储可扩展

Web漏洞库：700多条高质量的漏洞

POC库，近100条高质量漏洞验证POC

为什么需要数据中心

- 互联网爆炸式增长，我们不想“迷茫”
- 基础信息的提供和数据挖掘，更好的把握互联网走向
- 宏观的了解WEB安全现状

指纹统计

服务器操作系统

window 2003 server/ubuntu 10.04 server...

Web容器的统计

Apache/Tomcat/IIS 6/IIS 7...

服务端语言的统计

php 5/php 4/asp...

CMS、论坛、Blog等Web应用

风险统计

有具体Web应用漏洞的网站

被挂马的网站

被挂暗链的网站

存在后门webshell的网站

按行业划分，哪些行业是“重灾区”

按区域划分，哪些省市是“重灾区”

…

一些趋势

被挂马网站呈下降趋势

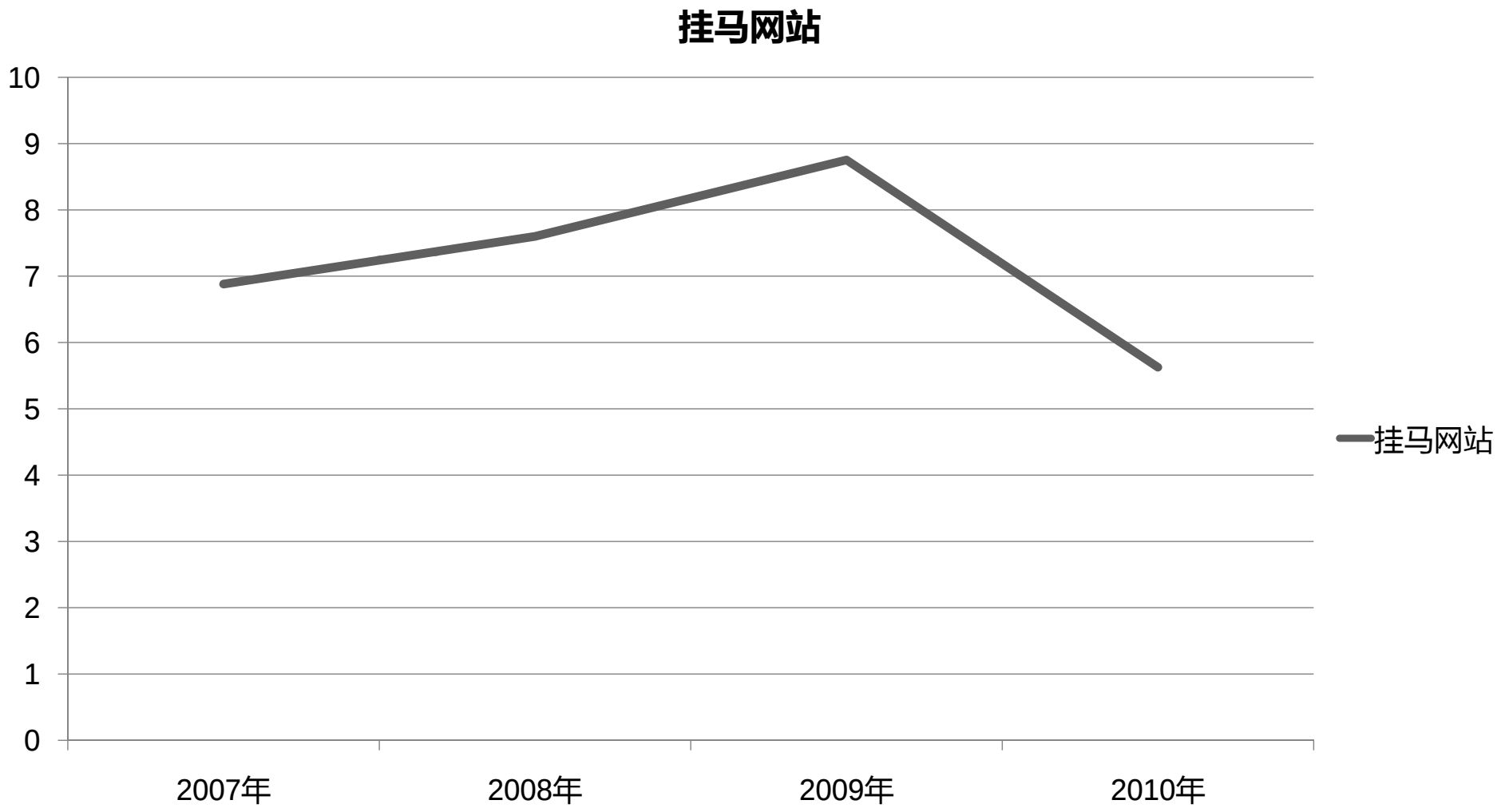
被挂暗链网站却呈现上升趋势

开源应用成为黑客首选

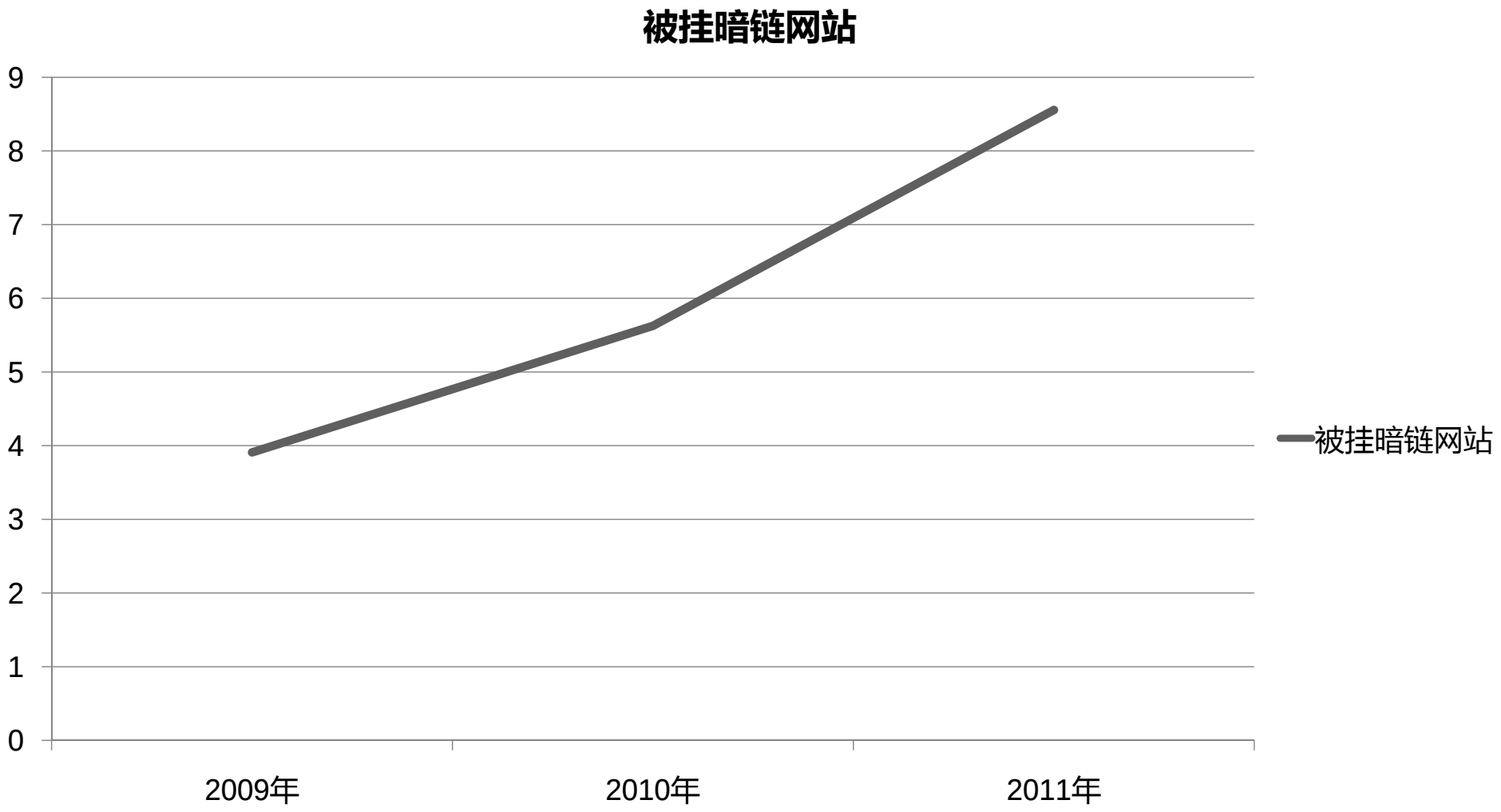
WEB2.0网站，XSS和CSRF的挖掘和利用，越来越被重视

……

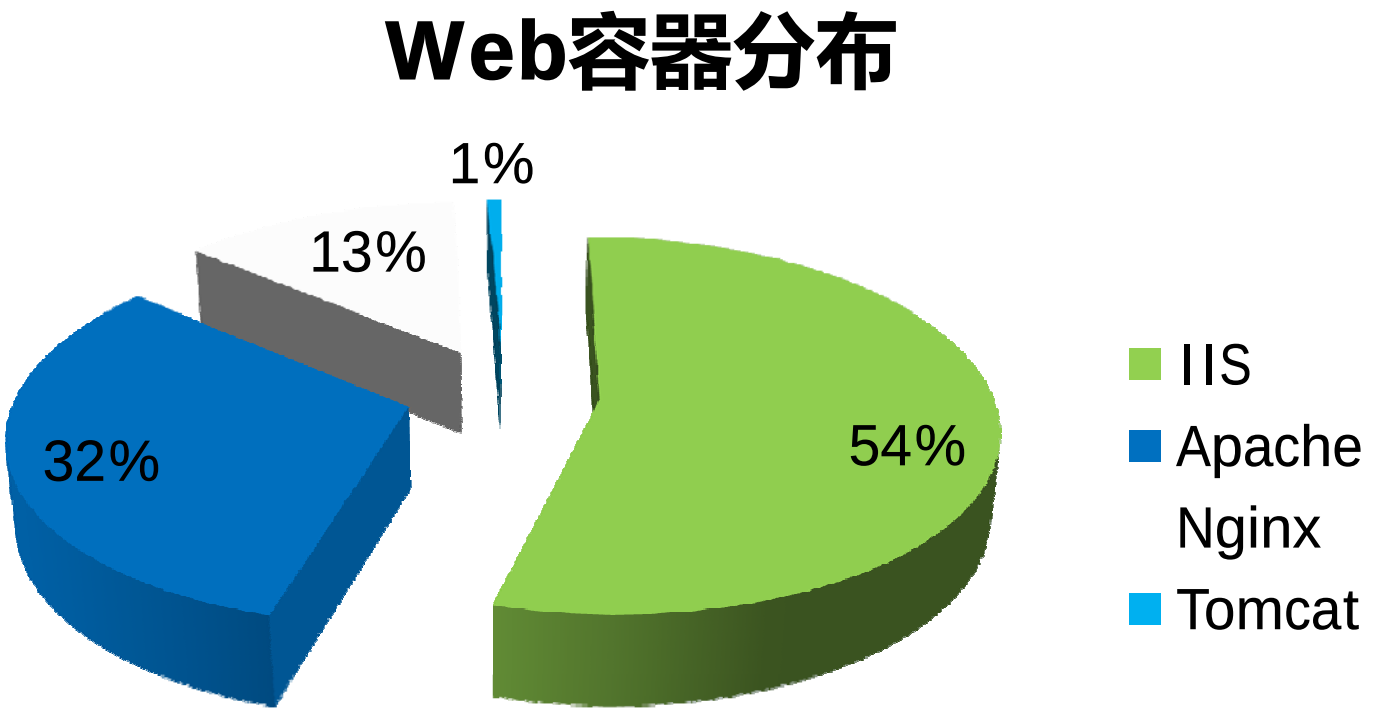
挂马网站



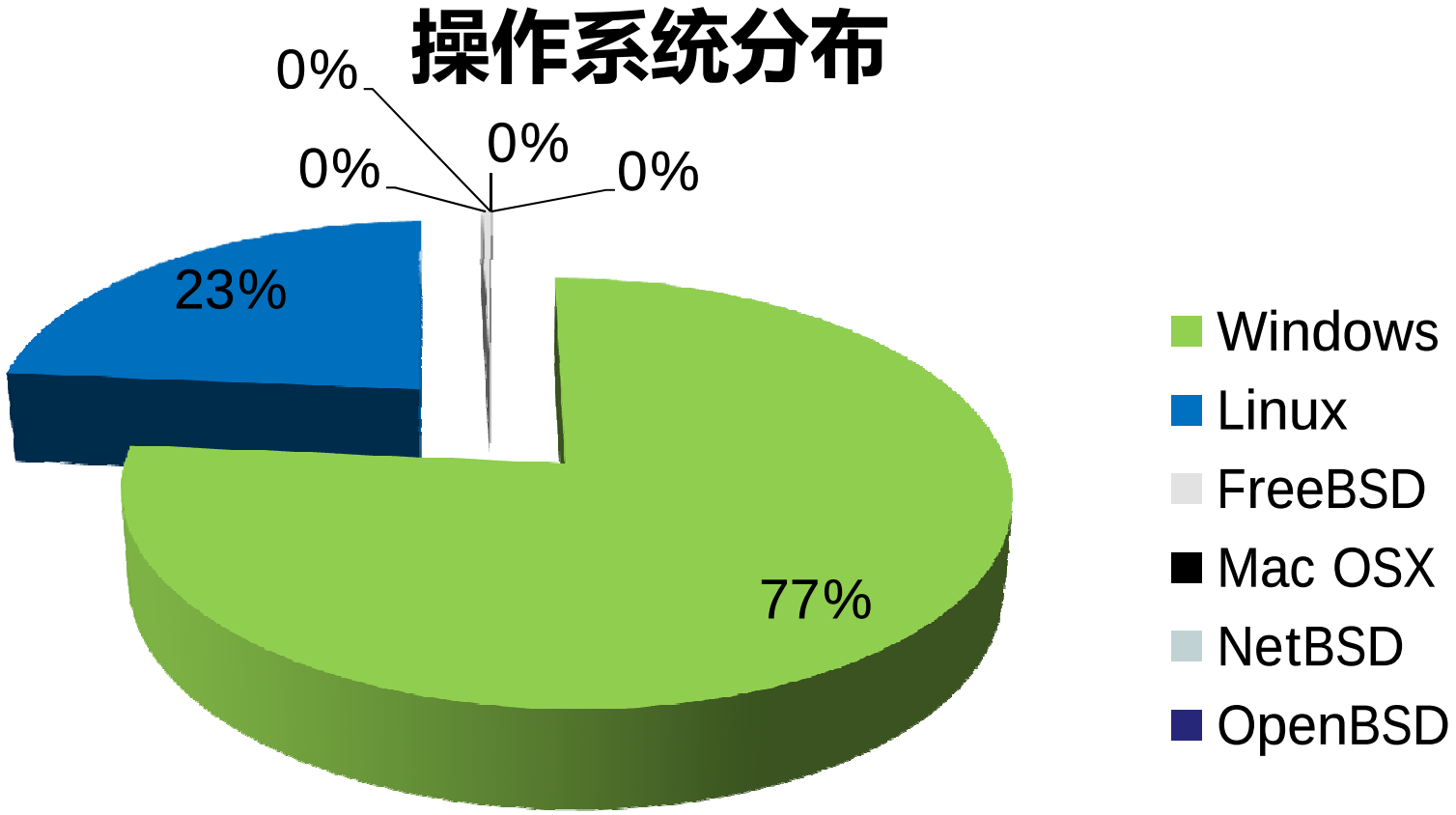
暗链网站



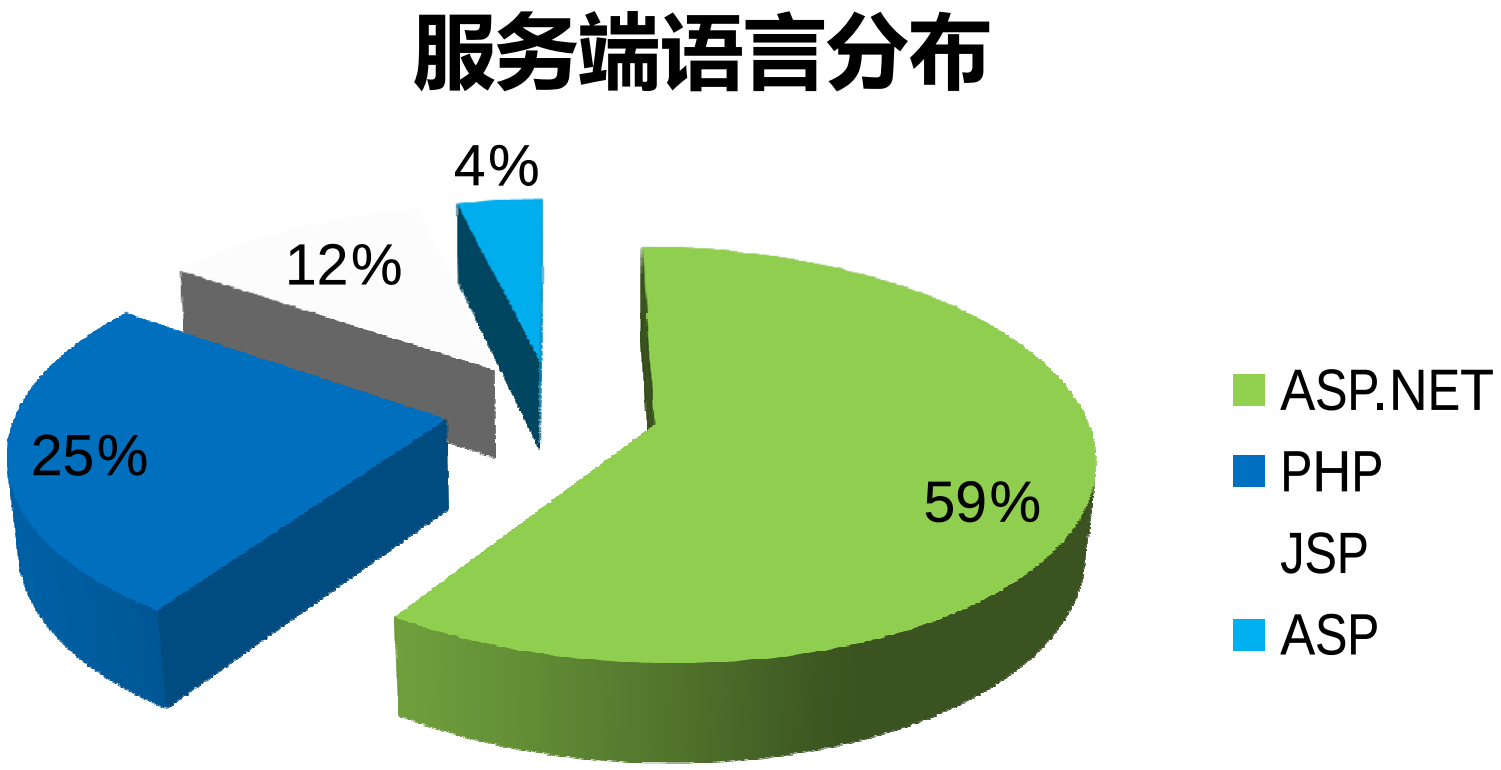
Web容器统计



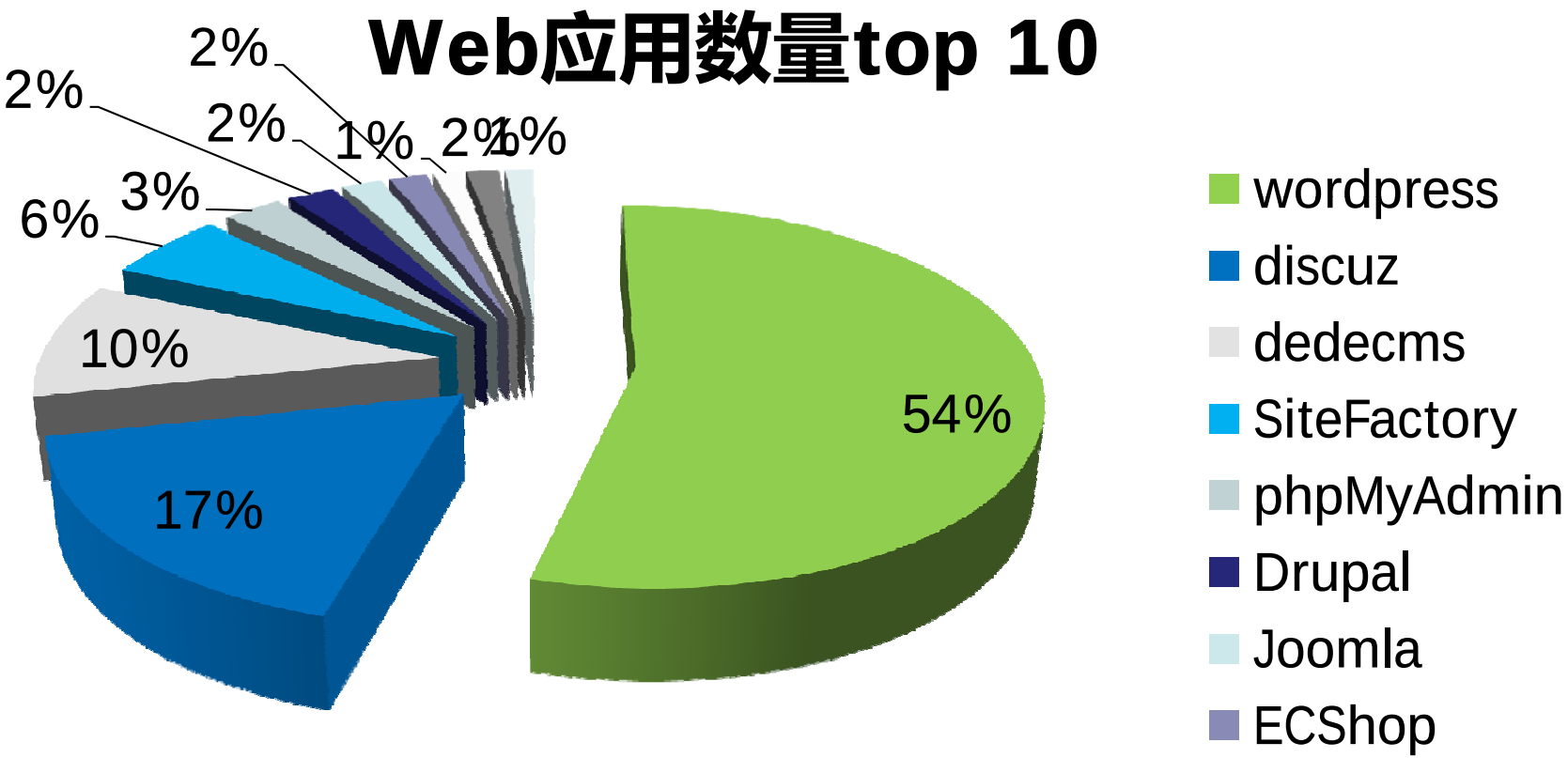
操作系统统计


操作系统分布
0%
0%
0%
0%
23%
77%
Windows
Linux
FreeBSD
Mac OSX
NetBSD
OpenBSD

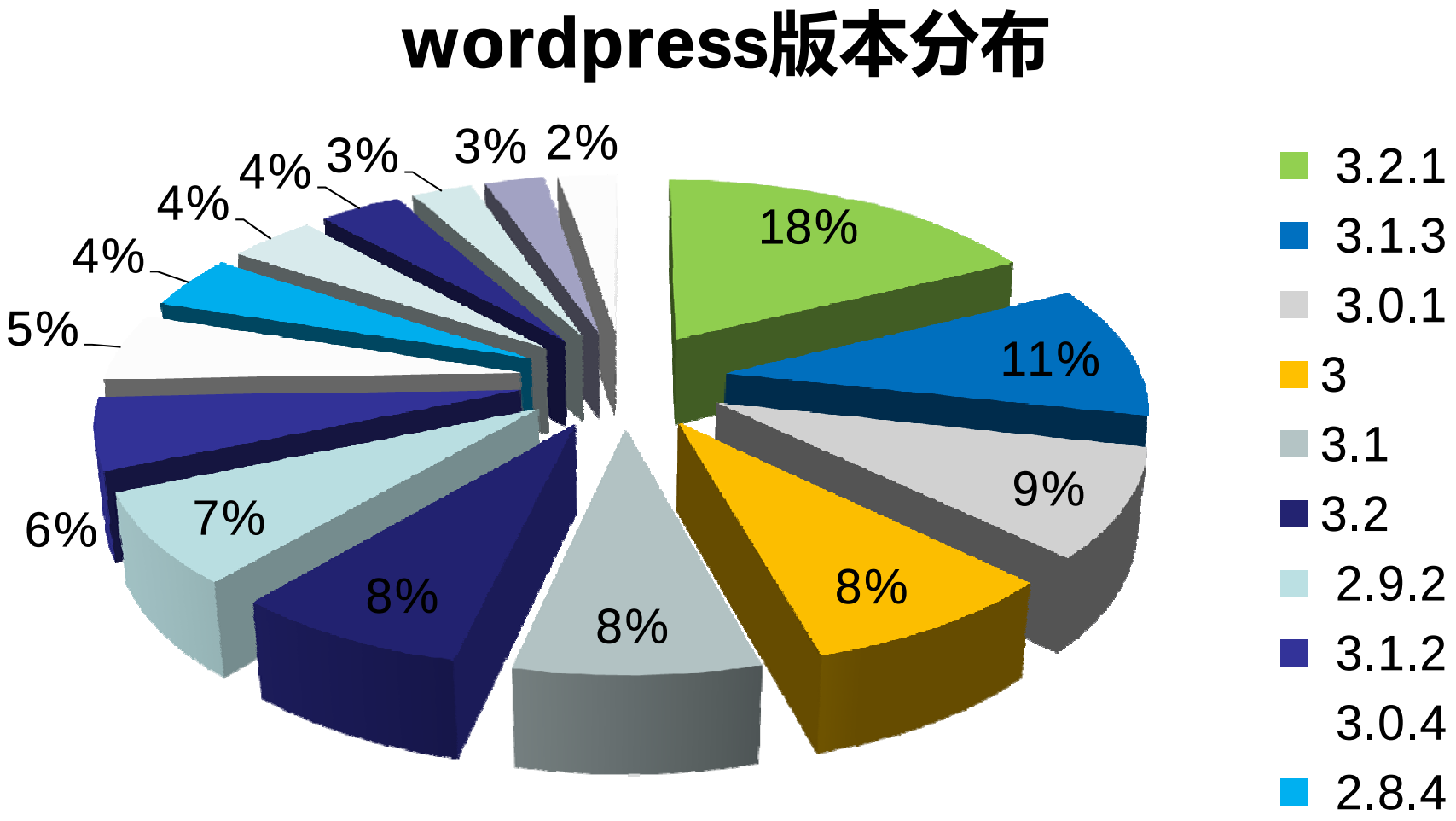
服务端语言统计



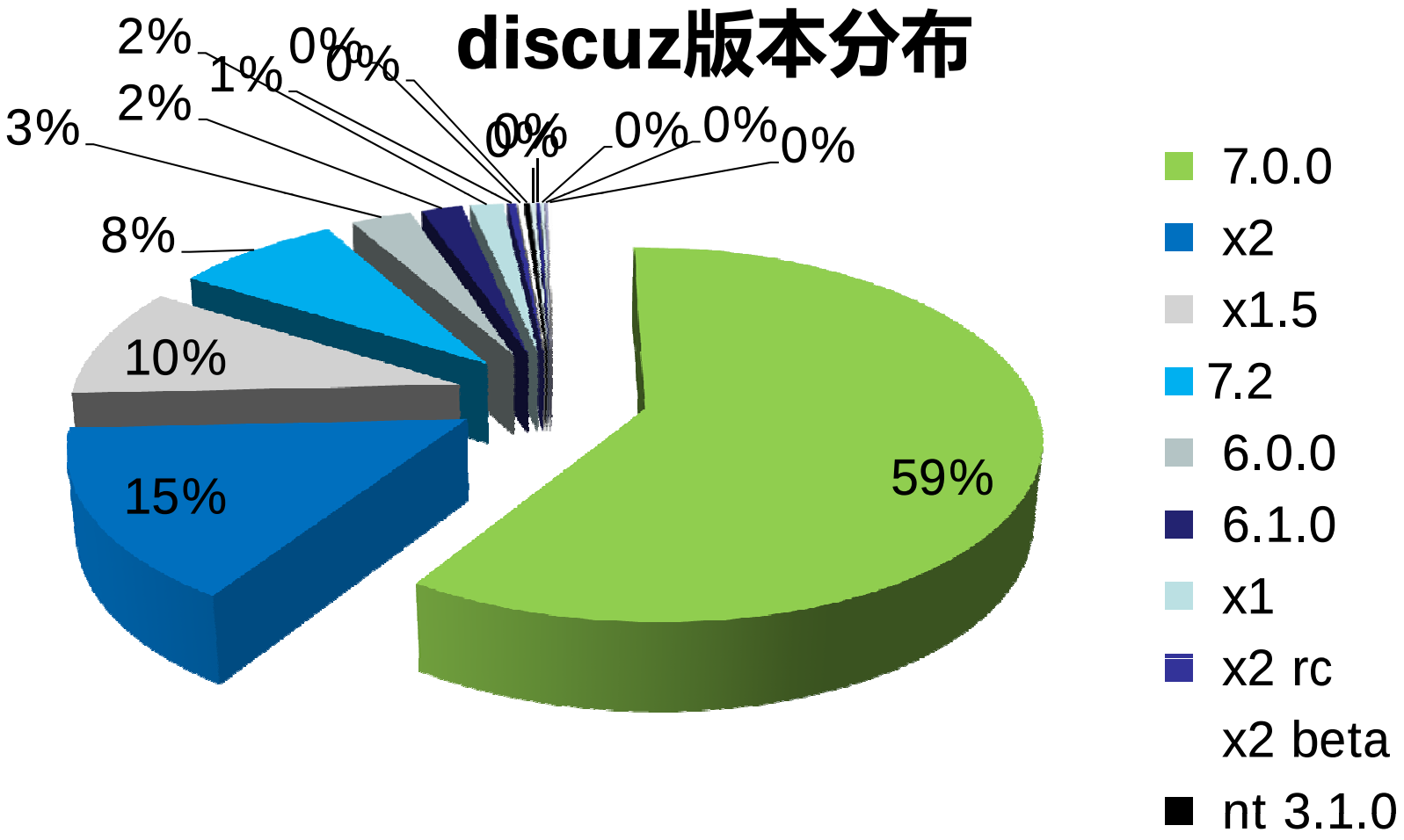
Web应用top 10


Web应用数量top 10
54%
17%
10%
6%
3%
2%
2%
2%
1%
1%
wordpress
discuz
dedecms
SiteFactory
phpMyAdmin
Drupal
Joomla
ECShop

wordpress top 15



discuz top 10



统计数据的意义

在宏观层面让我们知道网站的风险分布

利于我们做更精准的判断

利于我们给出更完美的解决方案

最后

感谢知道创宇研究部的几位热情可爱的白帽子！:) 你们知道我在说你们。

Q&A