
XDef 2013
第二届
全国网络与信息安全防护峰会
对话·交流·合作

勒紧你的裤腰带

“库带计划”那些事

@赵武360

关于我

- 360网站安全部门负责人
  - 360网站安全检测 webscan.360.cn
  - 360网站卫士 wangzhan.360.cn
  - 库带计划 loudong.360.cn
- Pangolin、JSky作者
- @赵武360

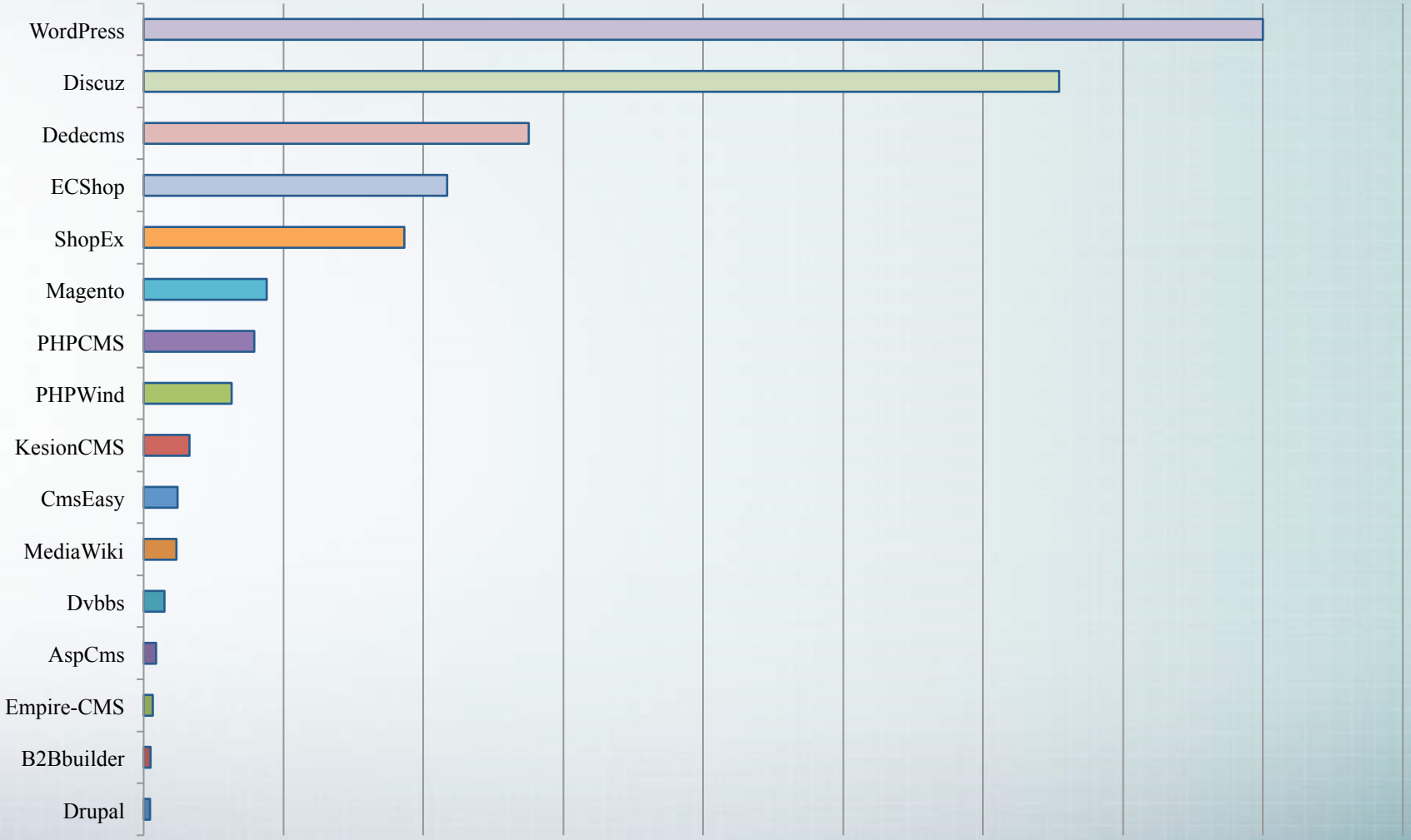
大纲

- 我是如何让老周掏出几百万的
- 库带计划运营背后的故事
- 案例展示
- 未来计划

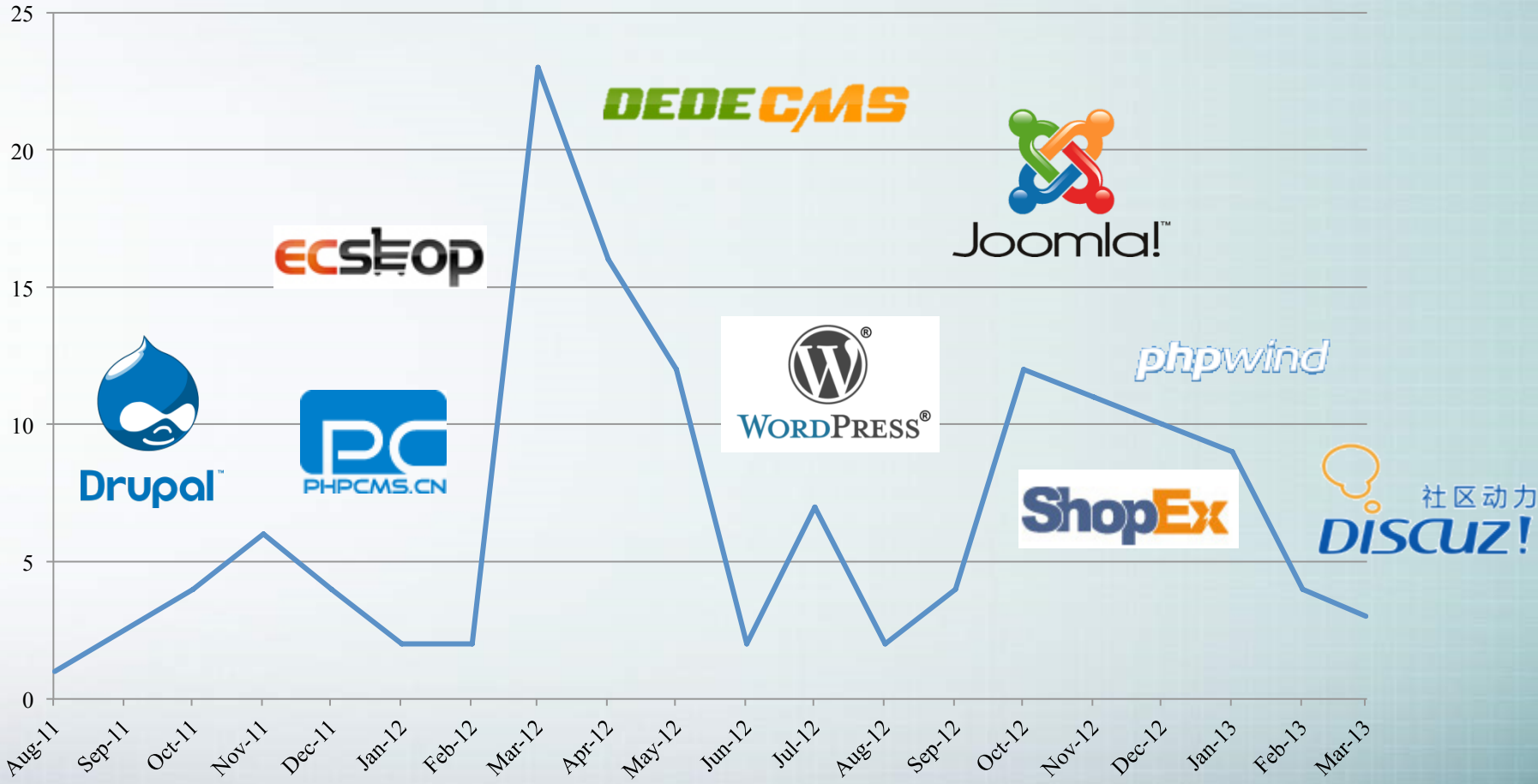
54%

基于开源系统搭建网站
(webscan)

第三方应用程序流行度排名



2012年102个漏洞



第三方厂商不会付费

安全，从来不是主业

没有财务预算或者不愿意

0day满天飞

漏洞用于黑产会比通知厂商
更有经济价值


NO MORE BUGS
NO FREE BUGS

ZDI

MS13-021

鸣谢

Microsoft 感谢下列人员或组织与我们一起致力于保护客户的利益：

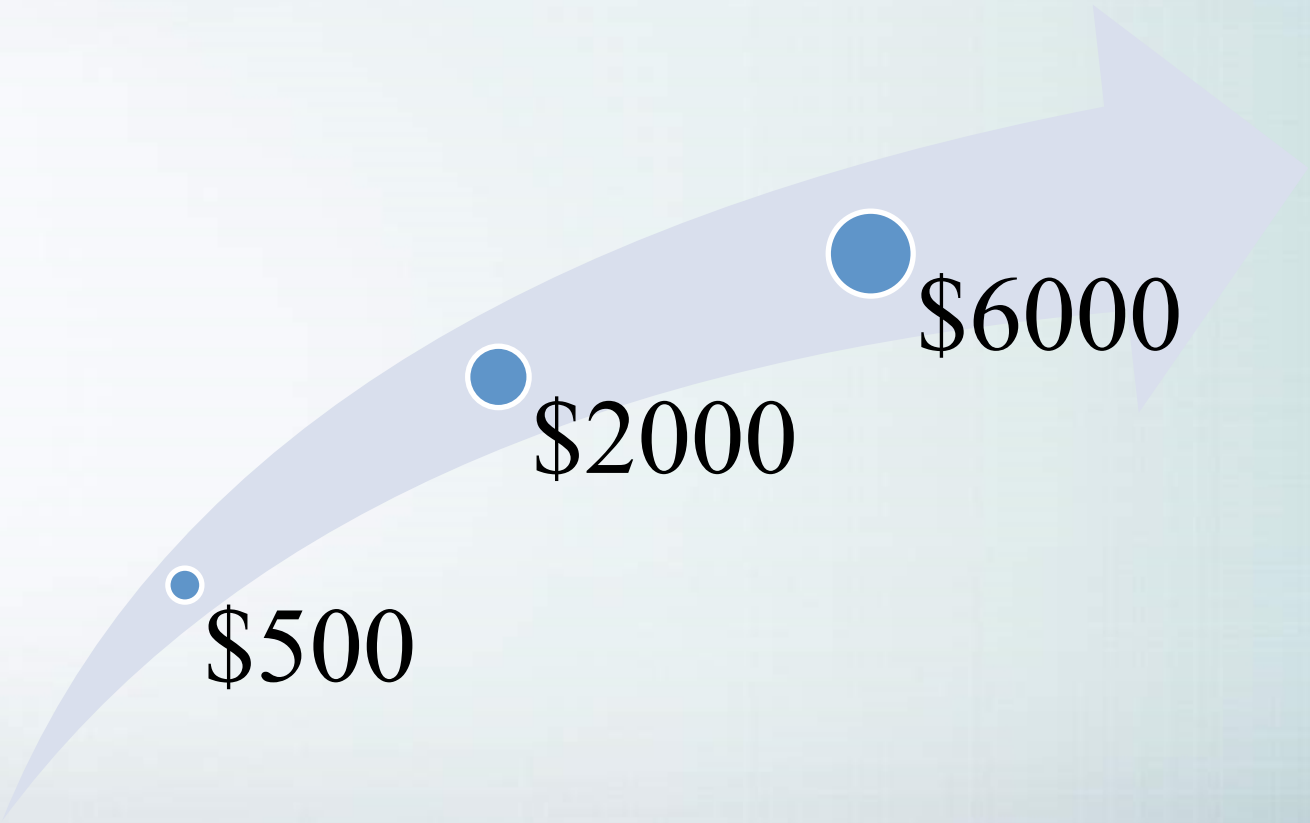
- TELUS Security Labs 的 Arseniy Akuney 报告了 Internet Explorer OnResize 释放后使用漏洞 (CVE-2013-0087)
- 一名匿名研究人员与 HP's Zero Day Initiative 合作报告了 Internet Explorer saveHistory 释放后使用漏洞 (CVE-2013-0088)
- 一名匿名研究人员与 HP's Zero Day Initiative 合作报告了 Internet Explorer CMarkupBehaviorContext 释放后使用漏洞 (CVE-2013-0089)
- Harmony Security 的 Stephen Fewer 与HP's Zero Day Initiative 合作报告了 Internet Explorer CCaret 释放后使用漏洞 (CVE-2013-0090)
- SkyLined 与 HP's Zero Day Initiative 合作报告了 Internet Explorer CCaret 释放后使用漏洞 (CVE-2013-0090)
- Yenteasy Security Research 的 Jose A Vazquez 与 Exodus Intelligence 合作报告了 Internet Explorer CElement 释放后使用漏洞 (CVE-2013-0091)
- Aniway.Aniway@gmail.com 与 HP's Zero Day Initiative 合作报告了 Internet Explorer GetMarkupPtr 释放后使用漏洞 (CVE-2013-0092)
- Aniway.Aniway@gmail.com 与 HP's Zero Day Initiative 合作报告了 Internet Explorer onBeforeCopy 释放后使用漏洞 (CVE-2013-0093)
- Simon Zuckerbraun 与 HP's Zero Day Initiative 合作报告了 Internet Explorer removeChild 释放后使用漏洞 (CVE-2013-0094)
- Venustech ADLab 的 Gen Chen 与我们一起努力处理了 Internet Explorer CTreeNode 释放后使用漏洞 (CVE-2013-1288)
- Qihoo 360 Security Center 与我们一起处理了 Internet Explorer CTreeNode 释放后使用漏洞 (CVE-2013-1288)

ZDI-13-054	CVE: CVE-2012-5205	Published: 2013-03-22
HP Intelligent Management Center DownloadReportSourceServlet Information Disclosure Vulnerability		
ZDI-13-053	CVE: CVE-2012-5204	Published: 2013-03-22
HP Intelligent Management Center IctDownloadServlet Information Disclosure Vulnerability		
ZDI-13-052	CVE: CVE-2012-5203	Published: 2013-03-22
HP Intelligent Management Center ReportImgServlet Information Disclosure Vulnerability		
ZDI-13-051	CVE: CVE-2012-5202	Published: 2013-03-22
HP Intelligent Management Center FaultDownloadServlet Information Disclosure Vulnerability		
ZDI-13-050	CVE: CVE-2012-5201	Published: 2013-03-22
HP Intelligent Management Center mibFileUpload Servlet Remote Code Execution Vulnerability		
ZDI-13-049	CVE: CVE-2013-1080	Published: 2013-03-22
Novell ZENworks Control Center File Upload Remote Code Execution Vulnerability		
ZDI-13-048	CVE: CVE-2013-1079	Published: 2013-03-22
Novell ZENWorks AdminStudio ISProxy ActiveX Remote Code Execution Vulnerability		
ZDI-13-047	CVE: CVE-2013-0094	Published: 2013-03-22
Microsoft Internet Explorer removeChild Use-After-Free Remote Code Execution Vulnerability		
ZDI-13-046	CVE: CVE-2013-0093	Published: 2013-03-22
Microsoft Internet Explorer onBeforeCopy Use-After-Free Remote Code Execution Vulnerability		

ZDI漏洞收录数量


ZDI漏洞收录数量
400
350
300
250
200
150
100
50
0
2005 2006 2007 2008 2009 2010 2011 2012
数量

0day平均漏洞价格



漏洞越少，价格越高

攻击目标转移，APT

Packetstorm

Current Bounty List

Reference	Description	Current Value	Date Added
APSB13-09	Adobe Flash Player Code Execution	$7,000.00	2013-03-21
APSB13-07	Adobe Acrobat Code Execution	$3,500.00	2013-03-21
MS13-027	Microsoft Kernel Privilege Escalation	$1,750.00	2013-03-21
MS13-026	Microsoft Outlook Mail Client Information Disclosure	$1,250.00	2013-03-21
MS13-023	Microsoft Visio Bug Viewer Remote Code Execution	$ 650.00	2013-03-21
MS13-022	Microsoft Silverlight Client Side Code Execution	$7,000.00	2013-03-21
MS13-021	Microsoft Internet Explorer Multiple Issues	$1,250.00+	2013-03-21
MS13-020	Microsoft OLE Automation Remote Code Execution	$3,500.00	2013-02-16
MS13-011	Microsoft Media Decompression Remote Code Execution	$3,500.00	2013-02-16
MS13-010	Microsoft Internet Explorer VML Remote Code Execution	$7,000.00	2013-02-16

All amounts are in US dollars.

Reward amounts

Rewards for qualifying bugs range from $100 to $20,000. The following table outlines the usual rewards for the anticipated classes of bugs:

	accounts.google.com	Other highly sensitive services [1]	Normal Google applications	Non-integrated acquisitions and other lower priority sites [2]
Remote code execution	$20,000	$20,000	$20,000	$1,337 - $5,000
SQL injection or equivalent	$10,000	$10,000	$10,000	$5,000
Significant authentication bypass or information leak	$10,000	$5,000	$1,337	$500
Typical XSS	$3,133.7	$1,337	$500	$100
XSRF, XSSI and other common web flaws	$500 - $3,133.7 (depending on impact)	$500 - $1,337 (depending on impact)	$500	$100

Google & Facebook

Rewards

- Our minimum reward is **$500 USD**
- There is **no maximum reward:** each bug is awarded a bounty based on its severity and creativity
- Only 1 bounty per security bug will be awarded

国内趋势

- 乌云（之前没有付费）
- 腾讯
- 360
- 网易
- 京东

谁来为漏洞买单

建立一个付费的第三方漏洞收录平台

库带计划：第三方漏洞收录

- 哪些第三方
  - WordPress、Discuz、ShopEX、ECShop、DedeCMS、PHPCMS、PHPWind、CmsEasy、AspCMS、FooSunCMS、Drupal、KingCMS、MediaWiKi、EmpireCMS、QiBoCMS、EspCMS……
- 使命：价值收益，改善安全研究人员的环境
- 黑客：站在十字路口的孤独者

流程

通知厂商修复

上报国家漏洞库

安全公司加入防护产品

安全公司加入扫描产品

奖励计划（波动)

漏洞厂商	漏洞等级	价格区间
重点厂商	高危	1000~10000
重点厂商	中危	300~1000
重点厂商	低危	0~300
其他厂商	高危	200~1000
其他厂商	中危	100~200
其他厂商	低危	0~100

国内第一家付费奖励计划

- 与现有“网络军火商”的区别（vupen）？
  - 免费提供给厂商
- 为什么只收第三方开源建站系统的漏洞？
  - 刑法修正案与白帽子产业链的悖论
- 靠什么盈利？
  - 没想过……为什么要盈利？

整体情况介绍

- 收录超过**700**个0day
- 影响超过**1,500,000**家网站
- 奖励金额超过**600,000**元

绝不让真正的雷锋吃亏

- 与国内现有一些厂商的安全响应中心的关系
  - 欢迎黑客给各大厂商直接报问题
    - 黑客与周鸿祎的故事
    - 某厂商从列表直接联系白帽子发奖励

- 如何解决漏洞被利用的问题
  - 永不对公众公开
    - 保护白帽子

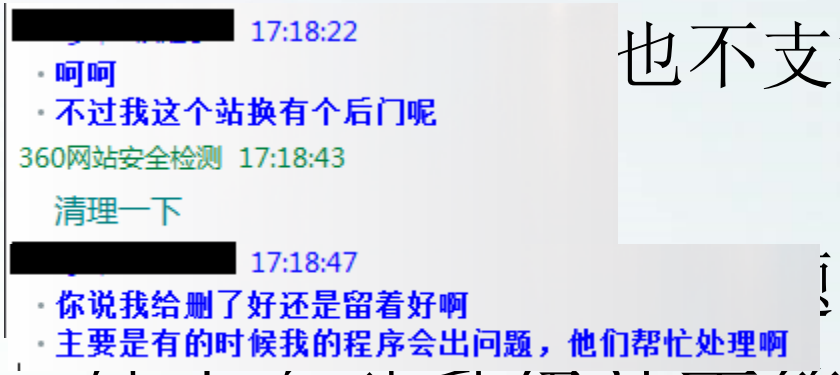
- 万元户计划背后的故事
  - Ecshop、shopex
  - 重金之下必有勇夫

中国网站生态链的一些问题

- 开源厂商安全不重视、响应不及时
  - 免费版有漏洞也不支持
- 技术能力有限
  - 修复补丁多次出问题
- 缺少自动升级补丁策略
  - 很大一批网站在官方出补丁的几个月后，漏洞依然存在
- 网站方的态度？？？

中国网站生态链的一些问题

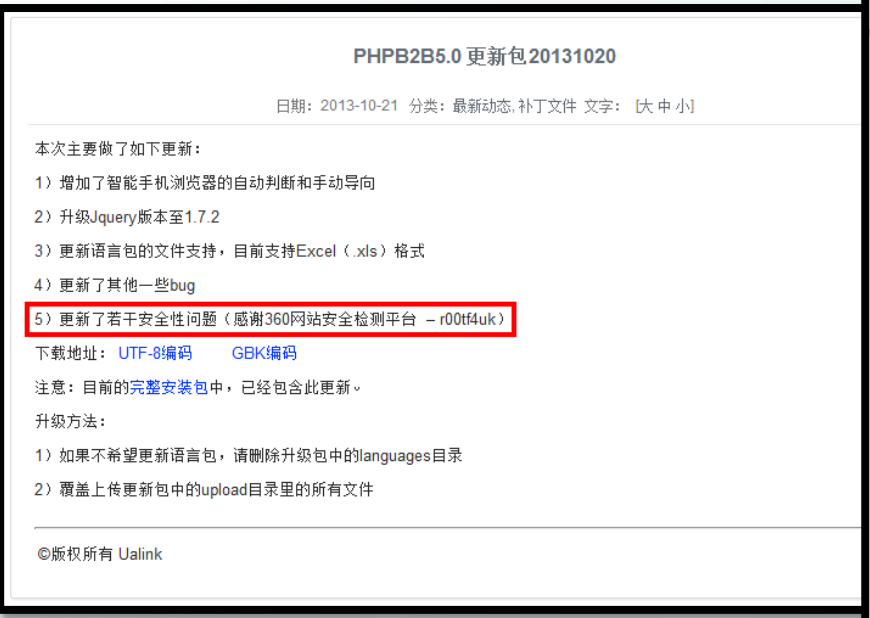
- 开源厂商安全不重视、
- 缺少自动升级补丁策略
  - 很大一批网站在官方出
    依然存在
- 网站方的态度？？？

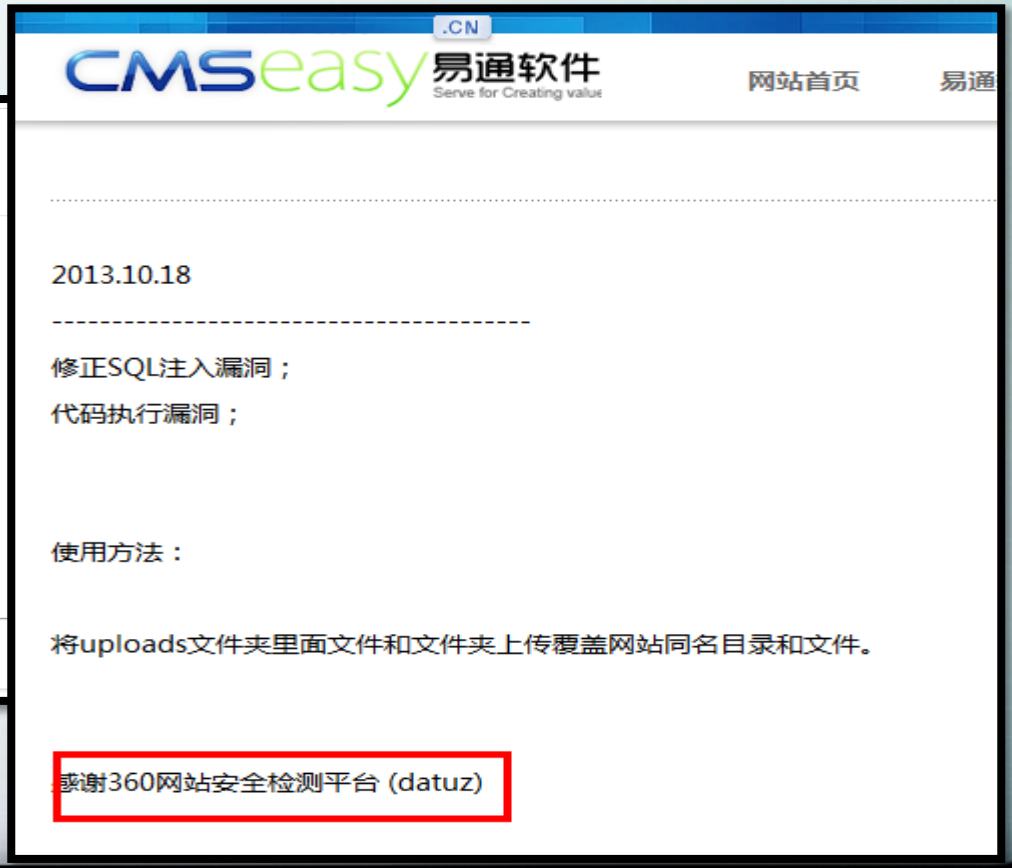


也不支持

产出

- 360 DedeCMS安全补丁包
  - 超过12个0day，个个致命





产出

- 360 DedeCMS安

修复问题：
1.修复表前缀不是sdb_的时候产生报错

2.修复部分过滤不严谨产生的二次注入问题

[补丁] 20130907|Modoer 安全补丁|Modoer

发表于 2013-9-7 14:14:51 | 只看该作者 | 倒序浏览

SQL注入漏洞，高危，请及时修复。

主题和会员卡用户行为过滤不严造成的SQL注入漏洞

感谢360网站安全检测平台(r00tf4uk)

修正如下：

如果发现已被入侵的话。请删除/do/c.php
然后再参考默认程序修改一下data/mysql_config.php为

感谢360网站安全检测平台（datuz）

[程　序] PHPCMS V9.4.2 正式版及升级补丁， 更新时间：2013年09月1

发表于 2013-8-28 14:03:19 | 只看该作者 | 倒序浏览

完整版下载地址：
GBK版本：http://download.phpcms.cn/v9/9.4/phpcms_v9.4.2_GBK.zip
UTF-8版本：http://download.phpcms.cn/v9/9.4/phpcms_v9.4.2_UTF8.zip

1、请先对原有文件进行备份。
2、上传upload中的文件到网站根目录，覆盖原有文件。
3、登录后台-更新缓存

版本V9.4.2 功能变更及bug修正说明：
1、修复投稿编辑器处提交**代码，管理员可触发事件，导致漏洞产生。
2、修复视频添加接口SQL注入bug
3、修复：会员投稿转向链接处 SQL注入问题
4、修复视频添加接口SQL注入bug
5、修复：投稿处 缩略图xss bug
6、修复漏洞：地图xss漏洞 7、PHPCMSV9 继续SQL注入
以上信息由（360网站安全检测平台）提供信息支持！
8、附件上传，未验证用户是否登录。 修复**格式文件上传BUG
9、修复分页无法保持的bug
10、修复投稿后，正文显示问题

感谢以下安全平台提供信息反馈：

互联网思维的安全

- 广泛的用户群
- 快速响应
- 不那么功利 ；）

演示一：xxx系统0day

- shopex 前台GETSHELL（http://loudong.360.cn/vul/info/id/1000）

演示二：IIS5 0day

- 感谢Yuange提供

未来计划

- 目标：让安全研究人员买得起房

- 谢谢

- 请搜索“库带计划”，或直接访问
  - http://loudong.360.cn