

# PHP安全开发：从白帽角度做安全

中国婚博会PHP高级工程师 汤青松

# 分享内容

◆WEB安全现状

◆常见漏洞分析

◆如何提升安全

# 安全环境现状



# 一个17岁小朋友是怎么通过黑产月入8K+的？



汤清松

3月21日 13:37 来自 微博 weibo.com

昨天认识一个做黑产的小孩，17岁不读书天天在家下载各种APP,然后用FD抓包改包，月入8K+ 黑产门槛这么低吗？😱

阅读 9450 推广

📄 11

💬 3

👍 6










# QQ群黑产线报群

查找 找人 | 找群 | 找主播 | 找课程 | 找服务

漏洞 低价 线报

90后 TFBOYS 美食 旅游

返回 搜索: 漏洞 低价 线报 搜索不到我的群? 范围: 全国 默认 人数 活跃度

 <p><b>漏洞低价购物群</b> 64/200 行业交流 进群不要屏蔽消息本群经常更新最新<b>线报</b></p> <p>河北省承德市 +加群</p>	 <p><b>塔木 - 至尊线报群</b> 156/500 IT/互联网   低价商品   各类教程   ...</p> <p>山东省济南市 +加群</p>	 <p><b>石油线报D台</b> 9/200 IT/互联网   线报   游戏   活动 本群专注 &amp;nbsp;推 &amp;nbsp;话费 &amp;nbsp;流量 &amp;nbsp;低价免单商品 &amp;nbsp;漏洞活动。在本群，吾等一...</p> <p>河北省廊坊市 +加群</p>
 <p><b>【宋总】高质量线报V2</b> 586/2000 品牌,产品 每天更新各种<b>漏洞</b> <b>BUG</b> <b>低价</b> 商品! 定时更新有利 益破零项目! 不定时发放福利 置顶些群福利发放...</p> <p>+加群</p>	 <p><b>VZ线报网络平台业务</b> 34/1000 IT/互联网   APP   手机   手机软件 ... 大量手机APP软件都在群里, 请自动下载。废话不多 说, 交钱进群。自动转账10元给群主。。。。...</p> <p>江苏省徐州市 +付费加群</p>	 <p><b>小狼·禁言线报活动2群</b> 28/500 购物 这是一个全网活动<b>线报</b>群, 会每天不定时更新全网 商家活动, <b>低价</b>商品, 店家<b>BUG</b><b>漏洞</b>, 还有一些...</p> <p>广东省广州市 &gt;&gt; 进入 +加群</p>
 <p><b>非鱼线报群</b> 2/200</p>	 <p><b>淘宝京东漏洞优惠群</b> 1/2000</p>	 <p><b>淘宝低价商品发布群</b> 407/500</p>



port:3306 country:China 探索一下

搜索结果 全球视角

搜索类型

- 公网设备
- Web 服务

Year

2014	62239
2015	140026
2016	848984
2017	808837

Port

3306	1860086
------	---------

Country

CHINA	1860086
HANGZHOU	522291
BEIJING	407916
UNKNOWN	126176
GUANGZHOU	73104
KWUN HANG	59816
SHENZHEN	54180
SHANGHAI	46980
CENTRAL DIST...	46569
NANJING	40771
JINAN	39603

找到约 1,860,086 条结果 (0.057 秒).

58.60%

MySQL:4.0.20a-nt

China Shenzhen

五月 17, 2017

3306

MYSQL

58.84%

MySQL:5.5.53

China

五月 17, 2017

3306

MYSQL

58.50%

MySQL:5.7.3-m13

China Jinan

五月 17, 2017

3306

MYSQL

通过搜索国内IP的端口情况  
发现开放3306端口的服务器  
数量达到了180万之多



# WEB漏洞的特征

# WEB漏洞分类

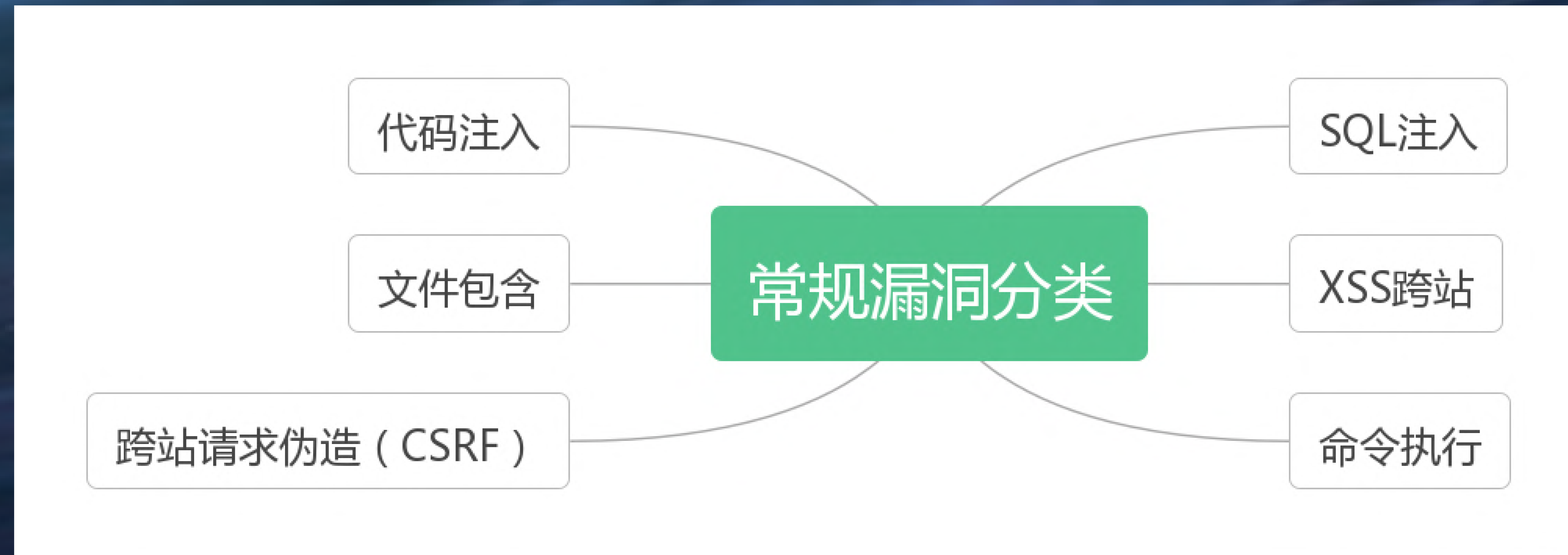
◆常规漏洞

◆逻辑漏洞

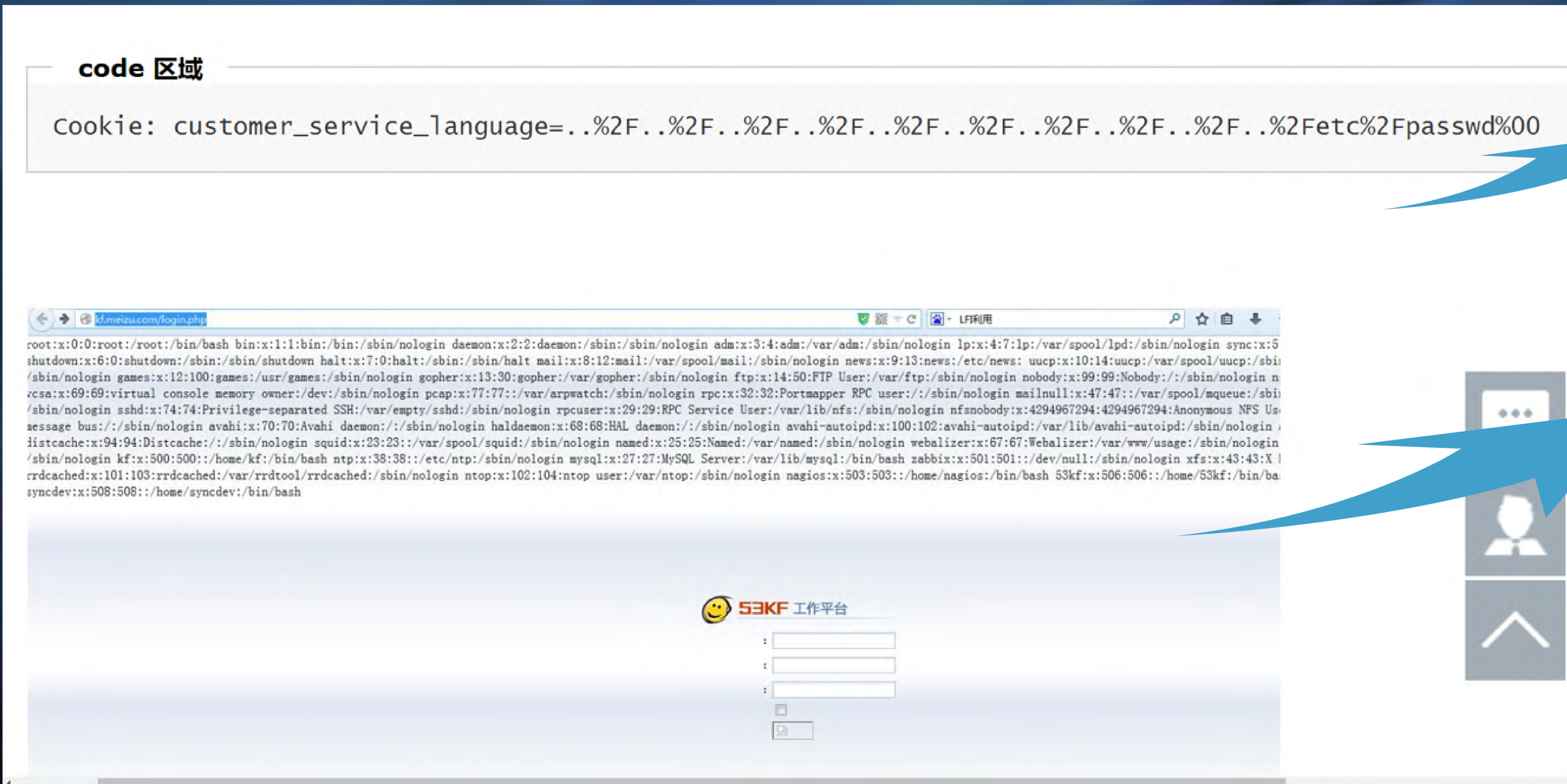
◆第三方通用漏洞



# 常规漏洞有哪些？



# PHP本地文件包含漏洞案例



code 区域

Cookie: customer\_service\_language=...%2F...%2F...%2F...%2F...%2F...%2F...%2F...%2F...%2Fetc%2Fpasswd%00

cookie加载的语言地址  
被用户所能控制,改成了 /etc/passwd

PHP支持代码混合  
文本文件内容会被直接输出



# PHP远程文件包含漏洞案例

Load URL

Execute  Enable Post data  Enable Referrer

**PHP Version 5.2.17** PHP Logo

<b>System</b>	Linux localhost 2.6.18-308.1.1.el5 #1 SMP Wed Mar 7 04:17:30 EST 2012 i686
<b>Build Date</b>	Aug 31 2011 17:05:36
<b>Configure Command</b>	<pre>./configure '--host=i686-redhat-linux-gnu' '--build=i686-redhat-linux-gnu' '--target=i386-redhat-linux' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/usr/com' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-curl' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--enable-wddx' '--with-kerberos' '--enable-ucd-snmp-hack' '--enable-shmop' '--enable-calendar' '--without-mime-magic' '--without-sqlite' '--with-libxml-dir=/usr' '--enable-xml' '--with-system-tdata' '--enable-force-cgi-redirect' '--enable-openssl' '--with-imagick' '--with'</pre>

参数P的参数用户可控制

改成了远程的文件,并且利用了apache的解析漏洞使jpg文件作为PHP文件执行

PHP支持代码混合后  
文本文件内容被直接输出



# 文件包含漏洞如何避免

◆open\_basedir 限制活动范围

◆过滤.(点) /(斜杠) \ (反斜杠)

◆禁止服务器远程文件包含

# PHP的代码注入案例

参数没有经过编码和过滤

直接写入了文件

```
1 <?php
2
3 function writeConfig($cAccount,$domain){
4
5     $path = dirname(__FILE__).'/../OpenPlatform/config/kdBind.php';
6
7     $info = '<?php $bindInfo = array("'" . $domain . "' => '" . $cAccount . "'); ?>';
8
9     file_put_contents($path,$info); ← 4
10
11 }
12
13 function getParam($name, $defaultValue = null) {
14
15     return isset($_GET[$name]) ? $_GET[$name] : (isset($_POST[$name]) ? $_POST[$name] : $defaultValue); ← 2
16
17 }
18
19 $cAccount = getParam('cAccount'); ← 1
20
21 $domain = getParam('domain');
22
23 writeConfig($cAccount,$domain); ← 3
```



# PHP的代码注入案例

```
_home_www_html_corpmgr_file_Placard_config_..._OpenPlatform_config_kdBind.php x
1  <?php $bindInfo = array(""=>"${@print(system('cat /etc/issue'))}"); ?>
```

www.wooyun.org

写入产生的代码文件





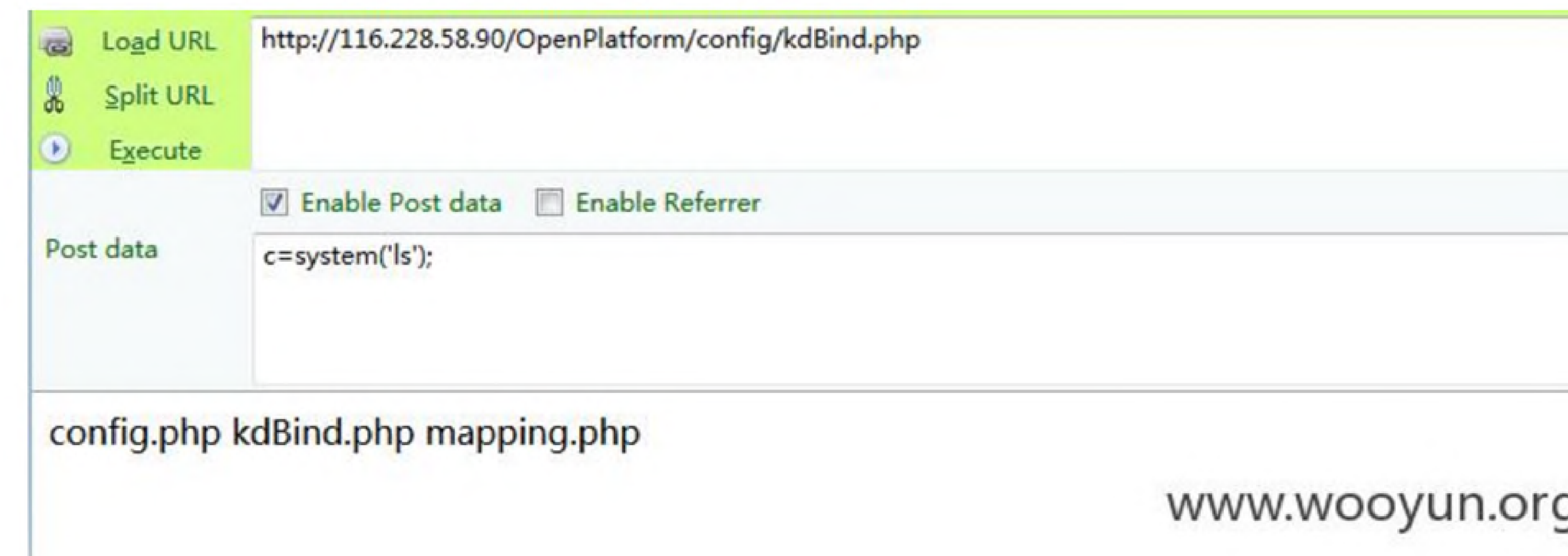
# PHP的代码注入案例

现在只要简单闭合构造完整的一句话就ok了。

一句话 : cAccount=")"?><?php @eval(\$\_POST['c']);?><?php("&domain= 闭合,一句话

phpinfo : cAccount=")"?><?php phpinfo();?><?php("&domain= 闭合,phpinfo()

提交后shell地址 : \*\*.\*\*.\*\*.\*/OpenPlatform/config/kdBind.php



# PHP代码注入漏洞如何防范

- ◆不要把参数直接存储成可以运行的代码
- ◆同时尽量不要使用eval执行接收的参数
- ◆一定要确保函数参数不能被用户所控制



# PHP安全开发扩展 Taint

```
<?php
$a = $_GET['a'];

$file_name = '/tmp' . $a;
$output    = "Welcome, {$a} !!!";
$var       = "output";
$sql       = "Select * from " . $a;
$sql       .= "ooxx";

echo $output;
//Warning: main(): Attempt to echo a string which might be tainted in xxx.php on line x

print $$var;
//Warning: main(): Attempt to print a string which might be tainted in xxx.php on line x

include($file_name);
//Warning: include() [function.include]: File path contains data that might be tainted in xxx.php on x

mysql_query($sql);
//Warning: mysql_query() [function.mysql-query]: First argument contains data that might be tainted in xxx.php on line x
?>
```

在一些关键函数或语句(echo, print, system, exec)

没有经过转义, 安全过滤处理, 就使用来自\$\_GET,

\$\_POST或者\$\_COOKIE的数据, Taint会提示Warning

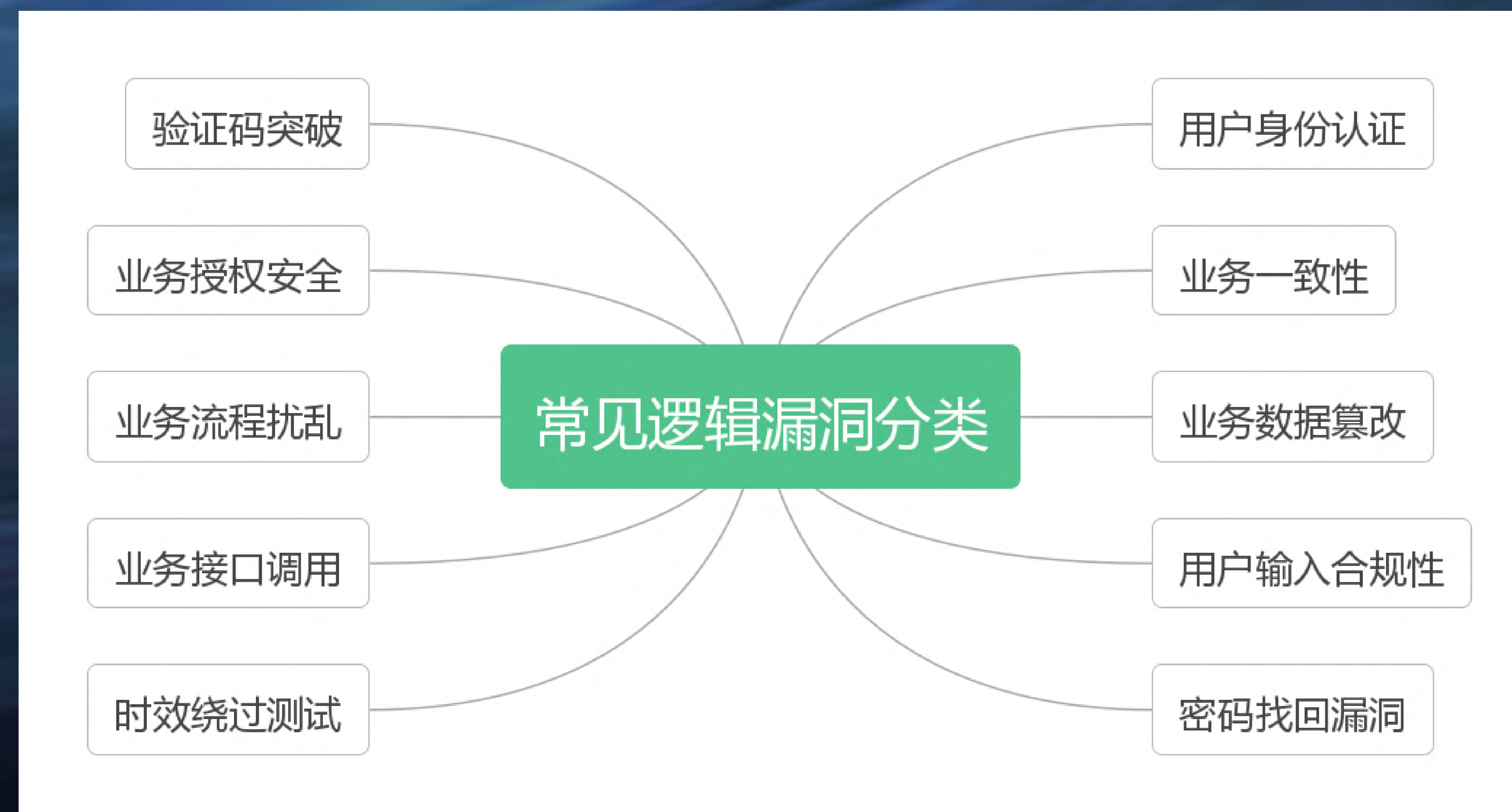


# 常规漏洞有哪些特点？

- ◆参数过滤不严谨
- ◆可以通过扫描器扫描出来
- ◆代码层面的BUG



# 业务逻辑漏洞有哪些？





# 平行越权漏洞案例

### 个人中心

1: [REDACTED]  
普通会员  
安全退出

### 交易管理

我的订单  
我的购物车

### 个人信息管理

个人资料  
修改密码  
收货地址  
第三方绑定管理

### 收货信息

订单号: 20150616142940  
下单时间: 2015/6/16 14:29:40  
订单状态: 取消  
会员用户名: 4579  
收货人: 谭  
发票抬头:  
手机: 186  
电话: 081  
地址: 四川省,攀枝花  
配送方式: 同城快递  
快递费用: ¥ 25.00  
票品应付总金额: ¥ 1305.00  
票品实付总金额: ¥ 1305.00  
备注:

### 订单详细

票务信息	价格	数量	小计
 TFBOYS FANS' TIME 2015/8/8 16:00 首都体育馆	¥ 1280.00	1	¥ 1280.00

票品总计: ¥1280.00  
+ 运费: ¥25.00

[返回](#)

张三能看到李四的订单信息

# 垂直越权漏洞案例

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

新闻管理 车商通

deale... /dealerback/initDealerNewsAction?did=82567

fujia  
上次登陆时间: 2015-08-21 浏览会员页 退出

新闻管理 >

51 全部新闻 47 优惠促销 0 新车到店 4 企业动态及保养

发布时间: 全部 新闻标题: 确定 新闻发布

新闻标题	新闻类别	浏览量	发布时间	操作
这款SUV满足你对浪漫七夕的所有想象	优惠促销	2301	2015-08-18 09:18	置顶 修改 删除
七夕带女朋友出去约会开SUV更配哟	优惠促销	65	2015-08-21 09:33	置顶 修改 删除
与道奇酷威一起打造完美七夕之旅	优惠促销	91	2015-08-20 09:13	置顶 修改 删除
传奇车型进口克莱斯勒300C音响的奥义	优惠促销	104	2015-08-19 09:09	置顶 修改 删除
陪你看流星雨Jeep大切诺基浪漫不缺席	优惠促销	91	2015-08-19 09:01	置顶 修改 删除
听说“小短假”与7座SUV更配哦	优惠促销	845	2015-08-16 08:46	置顶 修改 删除
大切西南行 开启非凡极致之旅	企业动态	1391	2015-08-11 08:55	置顶 修改 删除

www.wooyun.org

普通用户进入了管理后台



# 越权逻辑漏洞防范

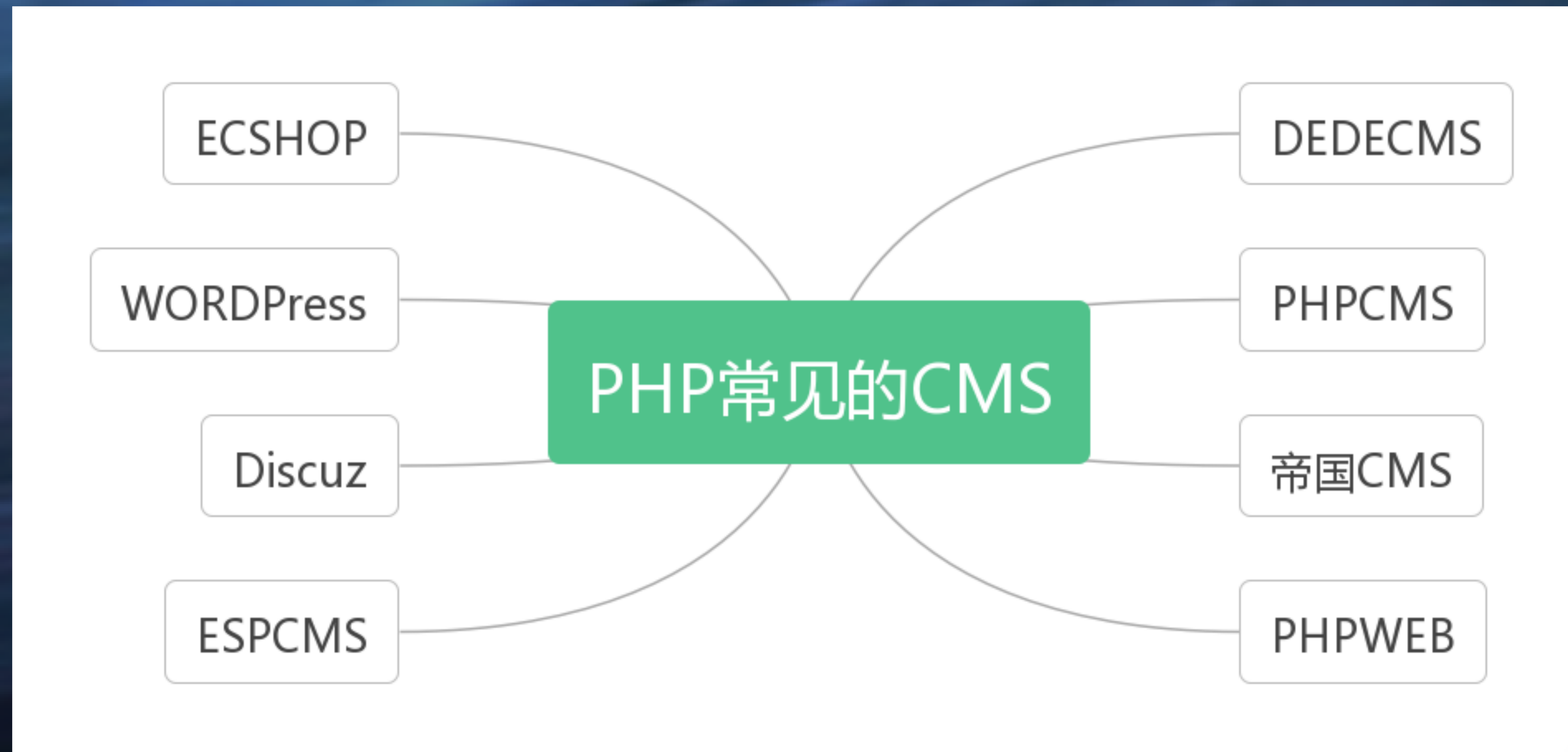
- ◆前台和后台的查询尽量不用同一个查询接口
- ◆尽量不要暴露出连续ID如订单号
- ◆越权不仅限于展示，修改数据也会出现

# 什么是逻辑漏洞?

- ◆设计业务逻辑上的缺陷
- ◆并非编码层面错误
- ◆人为主观的漏洞



# PHP中常见的开源系统有哪些？



# 第三方通用漏洞漏洞案例

The screenshot displays the browser's developer tools with the 'Headers' tab selected. The 'Cookie' header is expanded, showing a long string of cookies. A red circle highlights a specific cookie value: `1409911186f7544773106f4c06dcb4bf4; cntphlogintime=1409911186`. A red arrow points from this cookie value to a CAPTCHA input field on the page below, which contains the value '4uqz'. The CAPTCHA field is also circled in red. The browser's console shows a message: 'Resource interpreted as Script but transferred with MIME type text/html: "http://localhost/empirecms/e/member/login/loginjs.php?t=0.560035064853728".'

国内一个很知名的开源系统，审核代码时候发现  
图片验证码的值被简单MD5加密放在cookie中  
造成大批使用了此开源系统的网站受到此影响



DedeCMS

探索一下

搜索结果

找到约 372,350 条结果 (0.174 秒)。

搜索类型

公网设备

Web 服务

Webapp

DedeCMS 400366

20150618 126226

5.7.49 67373

5.7.32 21093

20160928 13791

5.7.22 10717

5.7.41 7317

5.7.46 6952

20150522 6100

5.7.40 5612

20100928 4934

phpMyAdmin 8398

WordPress 960

Discuz! 701

phpwind 233

Z-Blog 141

MetInfo 53

QiboCMS 44

鄂西... 潭... 方网站... 开发有限公司

ASP.NET DedeCMS 20150618

Microsoft IIS httpd 7.5

MICROSOFT IIS HTTPD

longta.com

China Wuhan

Windows

61.

五月 20, 2017

HTTP/1.1 200 OK  
Content-Type: text/html  
Last-Modified: Tue, 19 May 2017 00:55:32 GMT  
Accept-Ranges: bytes  
ETag: "5824f59d3ad0d21:0"  
Server: Microsoft-IIS/7.5  
X-Powered-By: ASP.NET  
Date: Sat, 20 May 2017 06:03:56 GMT  
Content-Length: 1972

www.大发888.com,大发888,大发888娱乐场,大发888娱乐场下载

DedeCMS 20150618

Nginx

lon

104.2

五月 20, 2017

PHP

NGINX

HTTP/1.1 200 OK  
Server: nginx  
Date: Fri, 19 May 2017 23:34:07 GMT  
Content-Type: text/html  
Last-Modified: Tue, 16 May 2017 02:25:29 GMT  
Transfer-Encoding: chunked  
Connection: keep-alive  
Vary: Accept-Encoding  
Content-Encoding: gzip

2015年爆出高危漏洞的版本依然未升级

很明显已被利用做黑产宣传

## 第三方通用漏洞有哪些特点？

- ◆采用第三方的代码：开源系统、编辑器等等
- ◆在张三网站发现漏洞，会在李四网站同样出现
- ◆漏洞影响范围更加的广泛



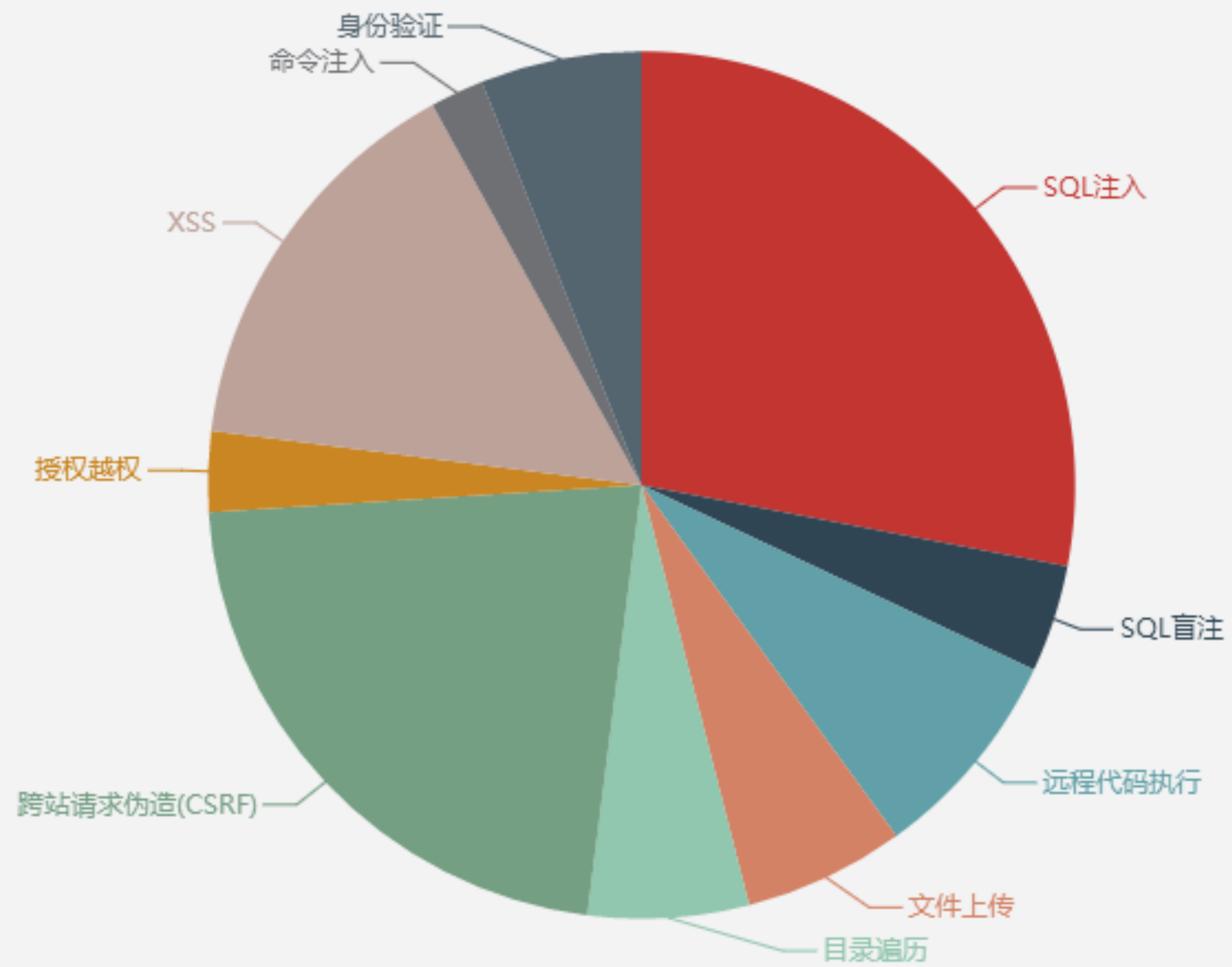
## 如何防范第三方通用漏洞？

- ◆溯源检查-- 代码版本是否存在已知的漏洞
- ◆版本更新-- 有安全补丁时候尽快完成升级
- ◆后台隐藏-- 尽量不使用默认管理后台地址

# 2016年度Web漏洞统计

Exploit-db 统计

- SQL注入
- SQL盲注
- 远程代码执行
- 文件上传
- 目录遍历
- 跨站请求伪造(CSRF)
- 授权越权
- XSS
- 命令注入
- 身份验证





# WEB漏洞分析总结

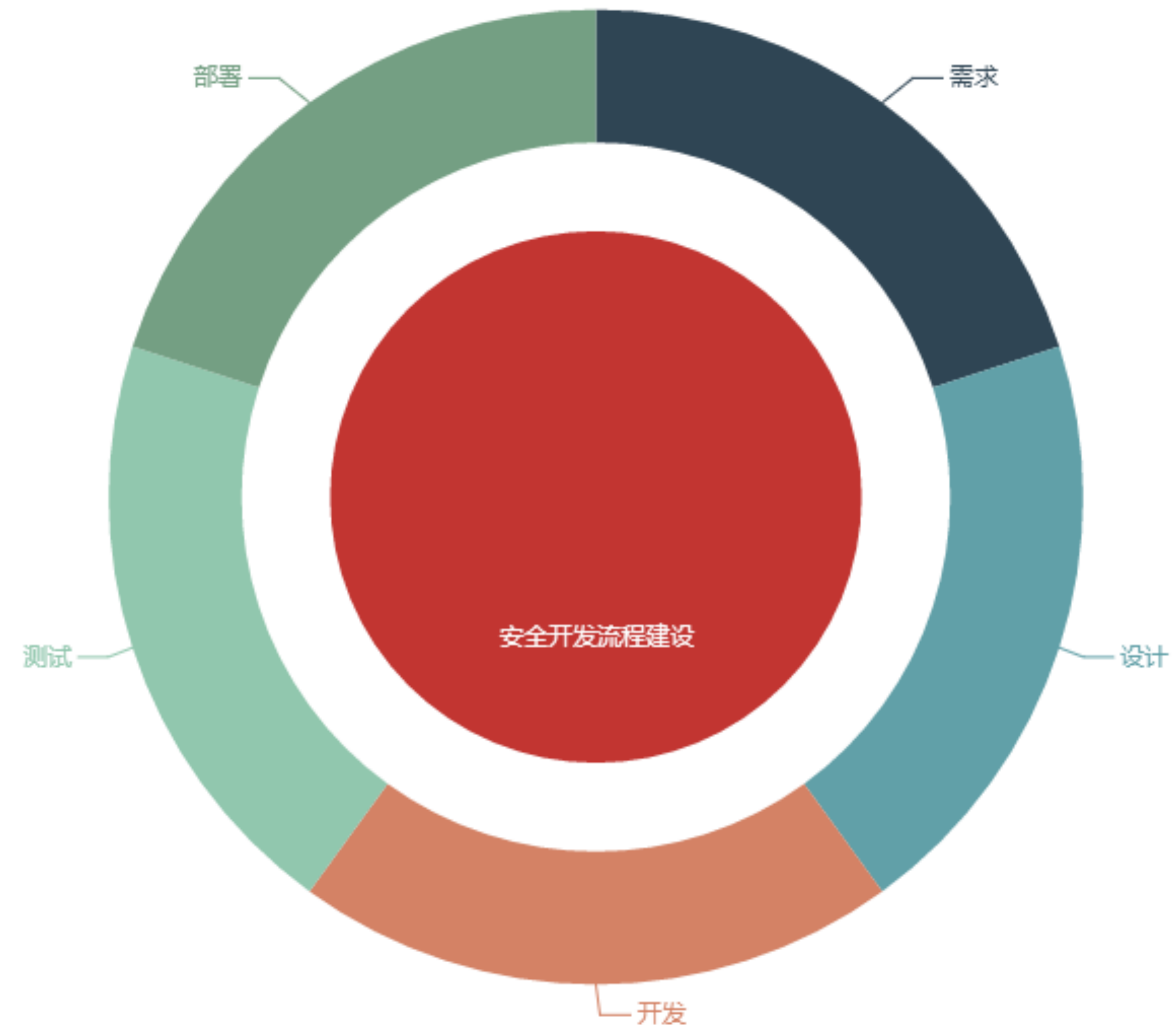
◆常规漏洞 -- 代码层面漏洞

◆逻辑漏洞 -- 人为主观漏洞

◆通用漏洞 -- 第三方代码造成的漏洞

提升WEB系统安全等级





那么多Web安全风险和漏洞，企业如何应对？

SDL安全开发生命周期



# SDL是什么?

- ◆安全开发生命周期 英文字母缩写 (Security Development Lifecycle)
- ◆最初来源于微软, 用于office、windows后 安全漏洞大大减少

# 为什么要用SDL?

## ◆提升Web应用的安全性

减少web应用的安全漏洞

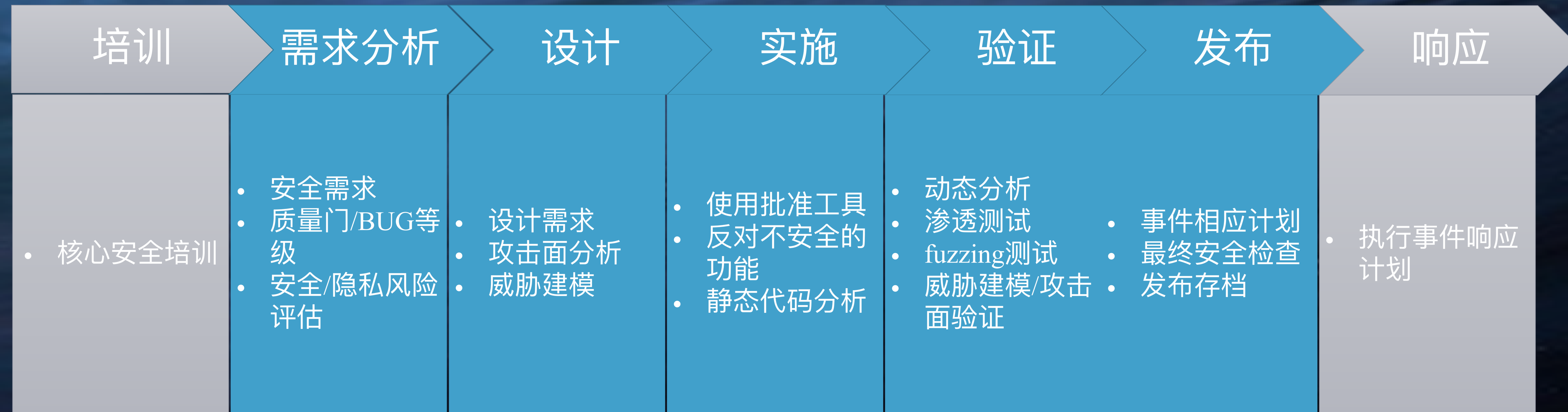
## ◆降低安全漏洞修复成本

美国国家标准与技术研究所估计，如果在项目发布后

再执行漏洞修复计划，修复成本相当于设计阶段修复的30倍



# 微软SDL流程框架图



# 规范Web应用开发流程

安全需求分析

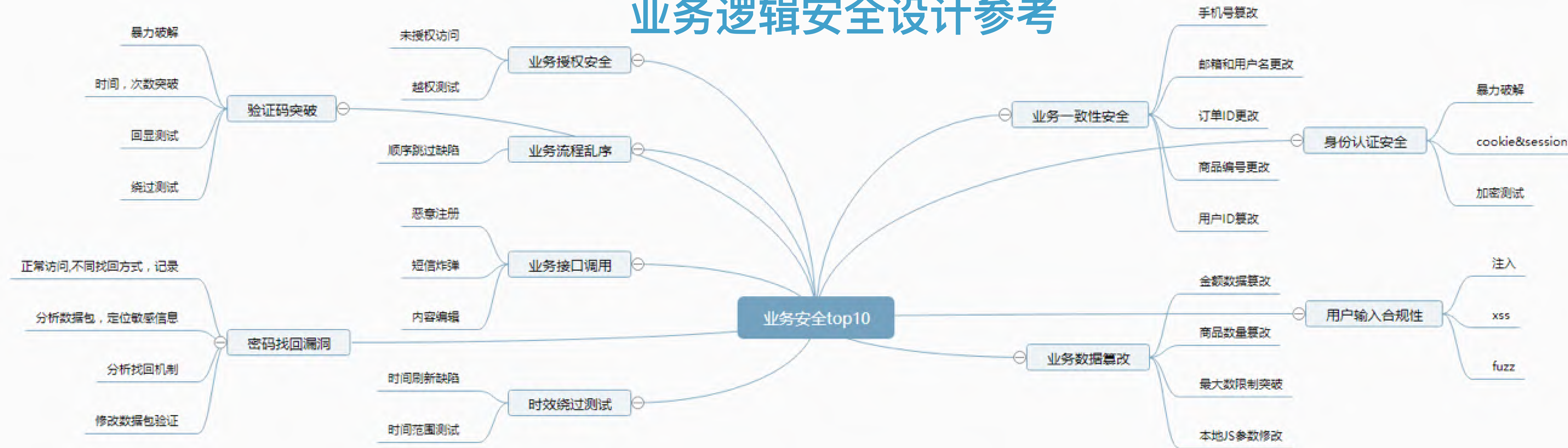
代码检测

安全测试

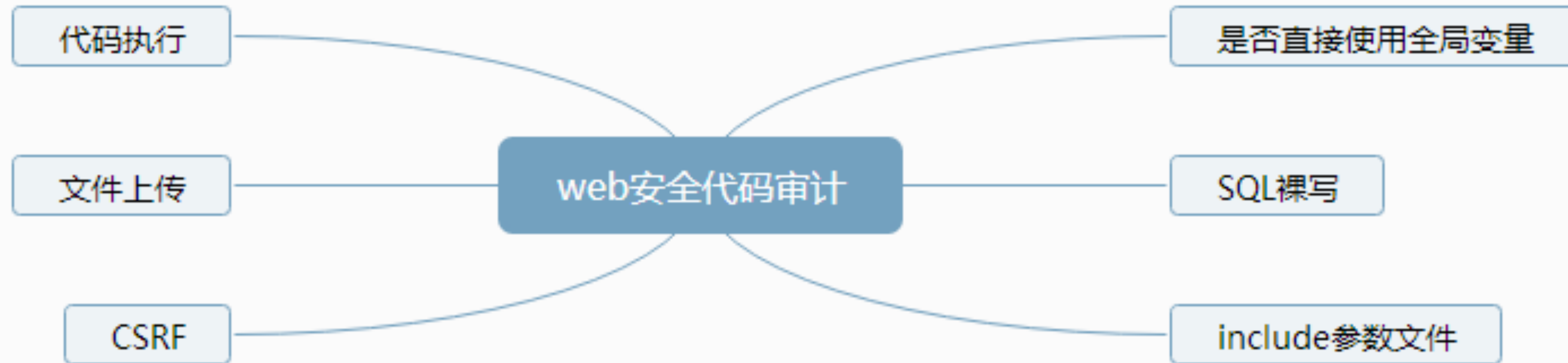
……



# 业务逻辑安全设计参考



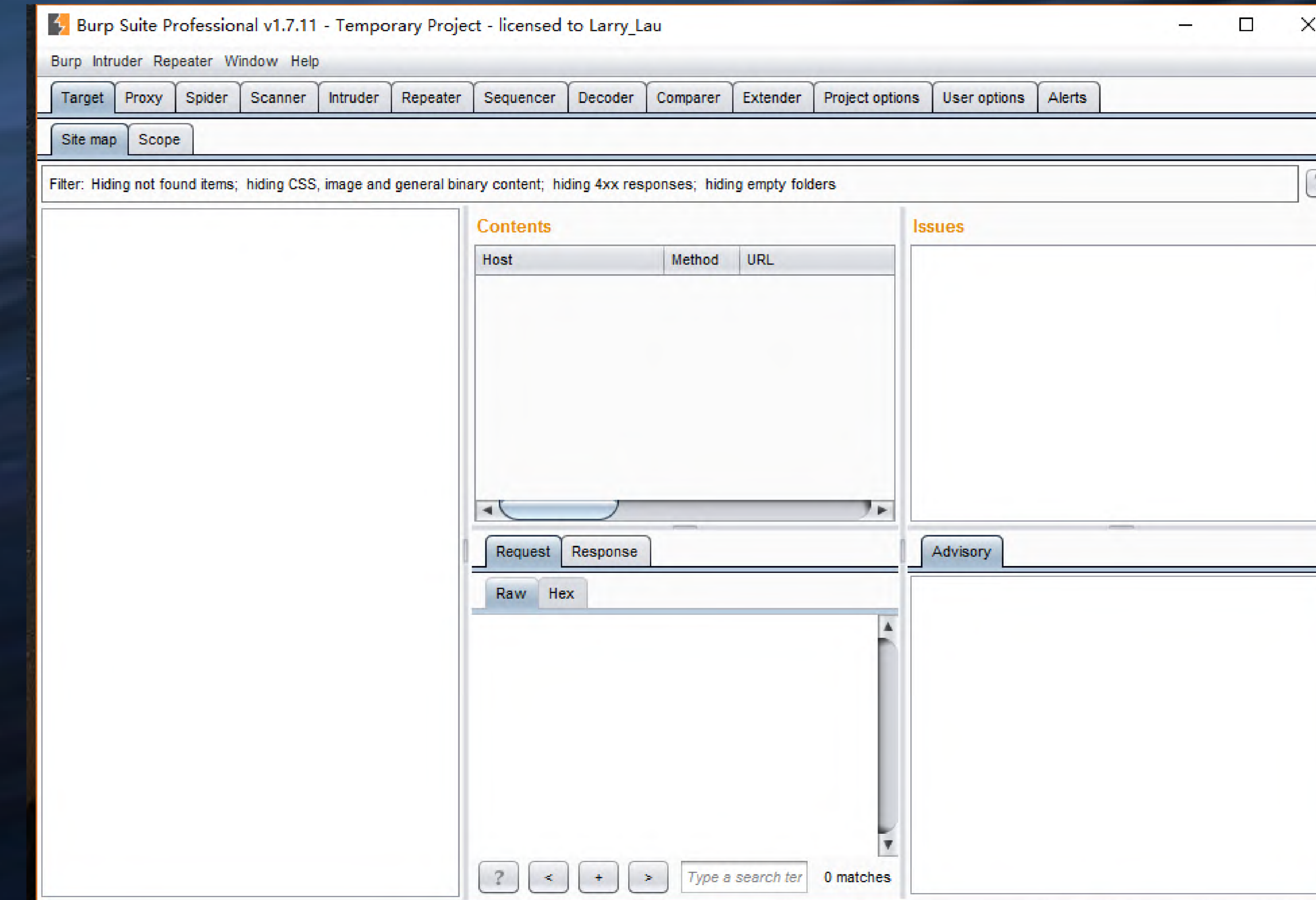
# 代码审计安全部分参考





# 安全测试工具burp suite

- ◆通过代理可以修改原始数据包
- ◆扫描器能自动的发现安全漏洞
- ◆爬虫能枚举应用的内容和功能



# 项目部署Web防火墙 ngx\_lua\_waf

- ✓ 用于过滤post, get, cookie方式常见的web攻击
- ✓ 防止sql注入, 本地包含, 部分溢出, fuzzing测试, XSS,SSRF等web攻击
- ✓ 防止svn/备份之类文件泄漏
- ✓ 防止压力测试类的攻击, 屏蔽常见的扫描黑客工具, 扫描器等异常的网络请求
- ✓ 屏蔽图片附件类目录PHP执行权限, 防止webshell上传



# WEB安全环境总结

- ◆安全是一个整体
- ◆不在于它强大的地方有多强大
- ◆而在于它薄弱的地方有多薄弱





WeChat: [songboy8888](#)

Email: [soupqingsong@foxmail.com](mailto:soupqingsong@foxmail.com)





# PHP

2017·北京  
全球开发者大会

