



GOPS 2016  
Shanghai



# 全球运维大会

2016

重新定义运维

上海站

会议时间： 9月23日-9月24日

会议地点： 上海·雅悦新天地大酒店

主办单位：



指导单位：



# 微信公众号的自动化安全监控

刘瑞恺 平安科技银河实验室



# 目录



1

背景与起因

2

公众号开发101

3

常见安全问题

4

自动化监控

5

结语

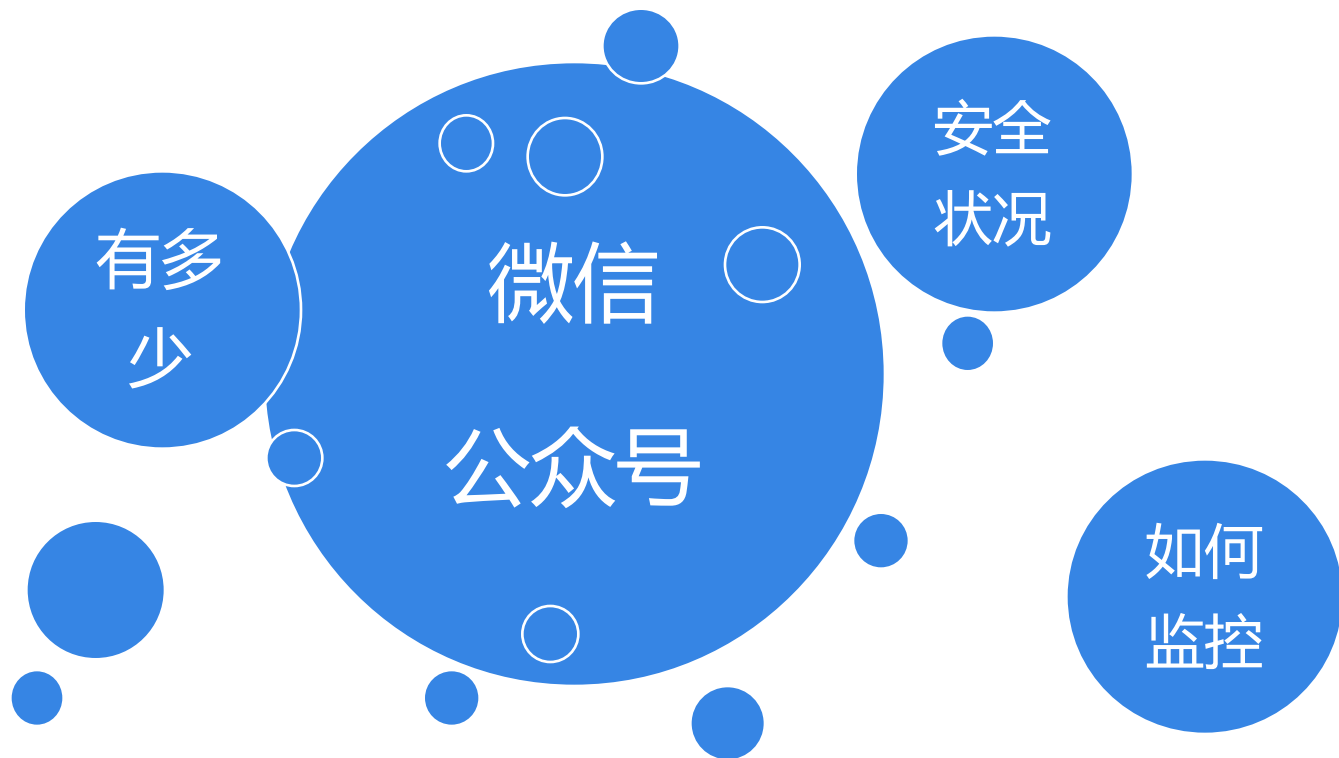


# whoami

- 平安科技 银河实验室
- 安全研究员
- Android应用安全



# 一批漏洞引发的思考



# 初探

- 数量众多
  - 不同业务
  - 不同地区
- 情况复杂
  - 外包
  - 建站平台



# 目录

1 背景与起因

➔ 2 公众号开发101

3 常见安全问题

4 自动化监控

5 结语



# 自定义菜单

- 直接访问外部网页
- 发送消息
  - 文本
  - 图文



# 文本消息

- `<a>` 标签
- 直接点击



# 图文消息

- 设置原文链接
- 正文中点击“阅读原文”



# 可能存在的外部链接



自定义菜单项跳转

安,很高兴为您服务。  
如您持有我行信用卡请点击这  
里验证身份,即可使用以下功  
能:  
1.快速查账单,额度,积分  
2.微信免费消费,还款提醒  
3.微信免费账单

文本消息包含地址

猛戳【[阅读原文](#)】进入

[阅读原文](#) 阅读 100

图文消息的原文链接



# 目录

1 背景与起因

2 公众号开发101

➔ 3 常见安全问题

4 自动化监控

5 结语



# 常见安全问题成因

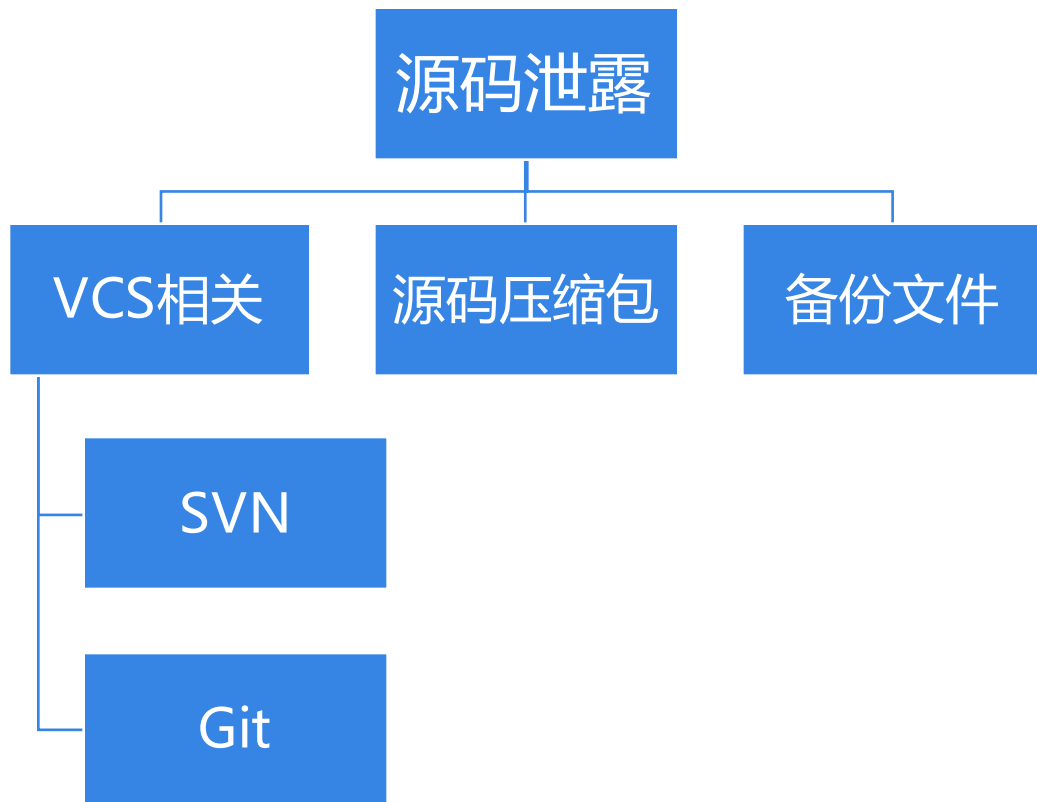


# 开发

- SQL注入
- 越权
- 逻辑漏洞
- XSS



# 发布



# 源码泄露导致控制公众号

- 源码压缩包
- 数据库连接密码
- 后台登陆



# 案例1

```
INSERT INTO `p_admin` (`id`, `groupid`, `username`, `realname`, `password`,  
(1, 1, 'admin', '贺', '2e4121', '014', 1436152259, '  
(2, 2, 'f', '风', '4db335', 'd5a', 1436233253,
```



# 案例1



The screenshot displays a web application's administrative interface. At the top, a browser address bar shows the URL `/index.php?r=admin/index/index`. Below this is a navigation bar with four buttons: "管理首页" (Management Home), "结构管理" (Structure Management), "内容管理" (Content Management), and "拓展应用" (Extension Applications). The left sidebar contains a menu with "全局设置" (Global Settings) and "后台登陆管理" (Backend Login Management). Under "全局设置", there are links for "网站设置" (Website Settings), "后台功能" (Backend Functions), "网站缓存" (Website Cache), and "前台模板" (Frontend Templates). Under "后台登陆管理", there is a link for "管理员管理" (Administrator Management). The main content area is titled "当前位置: 【环境信息】" (Current Location: [Environment Information]). It lists the following system details: "服务器域名/IP地址: www. (219. .75)", "服务器操作系统: Windows (内核版本: W !E8)", "服务器解译引擎: Apache/2.2.22 (Win32) PHP/5.4.6", "PHP版本: 5.4.6", "MySQL数据库: ✓", and "允许使用URL打开文件(allow\_url\_fopen): ✓".

管理首页 结构管理 内容管理 拓展应用

全局设置

- 网站设置
- 后台功能
- 网站缓存
- 前台模板

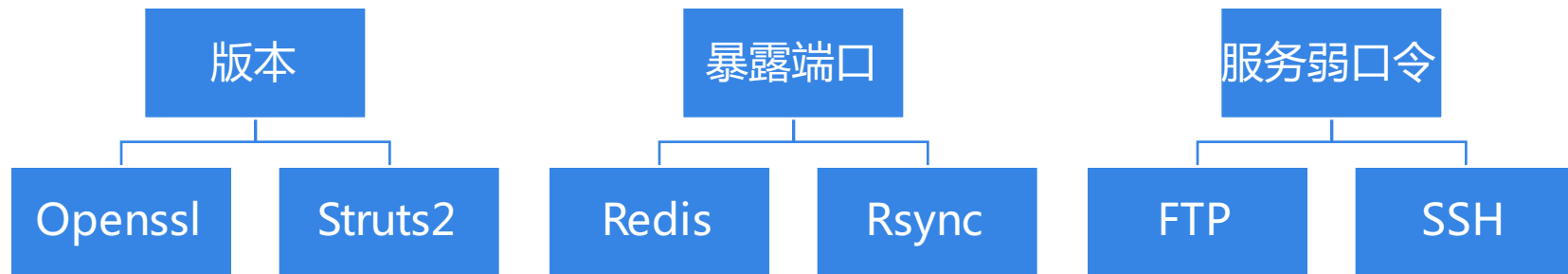
后台登陆管理

- 管理员管理

当前位置: 【环境信息】

|                                          |        |      |
|------------------------------------------|--------|------|
| 服务器域名/IP地址: www.:                        | i(219. | .75) |
| 服务器操作系统: Windows (内核版本: W                | !E8)   |      |
| 服务器解译引擎: Apache/2.2.22 (Win32) PHP/5.4.6 |        |      |
| PHP版本: 5.4.6                             |        |      |
| MySQL数据库: ✓                              |        |      |
| 允许使用URL打开文件(allow_url_fopen): ✓          |        |      |

# 运维



# Redis暴露导致控制公众号

- 暴露Redis
- 使用EasyWeChat公众号框架
- 从Redis获取access\_token



## 案例2

```
43. [redacted] 30:6379> keys *  
1) "xlivrdlogp"  
2) "laravel:easywechat.common.access_token.wx42" [redacted] 55"  
3) "laravel:overtrue.wechat.jsapi_ticket.wx42" [redacted] 55"  
4) "yqmxbysqrf"  
5) "dwyangohma"
```



## 案例2

“access\_token是公众号的全局唯一票据，公众号调用各接口时都需使用access\_token。开发者需要进行妥善保存。”

——微信公众平台开发者文档



## 案例2



# 危害



# 钓鱼好去处



# 目录

1 背景与起因

2 公众号开发101

3 常见安全问题

➔ 4 自动化监控

5 结语



# 基本思路



# 主要问题

- 整理目标公众号
- 采集公众号外部链接
- 自动化（约350公众号）



# 确定目标

关键词  
搜索



账号主  
体过滤



# 采集外部链接



自定义菜单项跳转

安,很高兴为您服务。  
如您持有我行信用卡请点击这里验证身份,即可使用以下功能:

- 1.快速查账单,额度,积分
- 2.微信免费消费,还款提醒
- 3.微信免费账单

文本消息包含地址

猛戳【[阅读原文](#)】进入

[阅读原文](#) 阅读 100

图文消息的原文链接



# 自动化

- 接口？
- 搜狗？
  - 爬虫/反爬虫
  - 只包含群发图文消息
- 对微信进行Hook

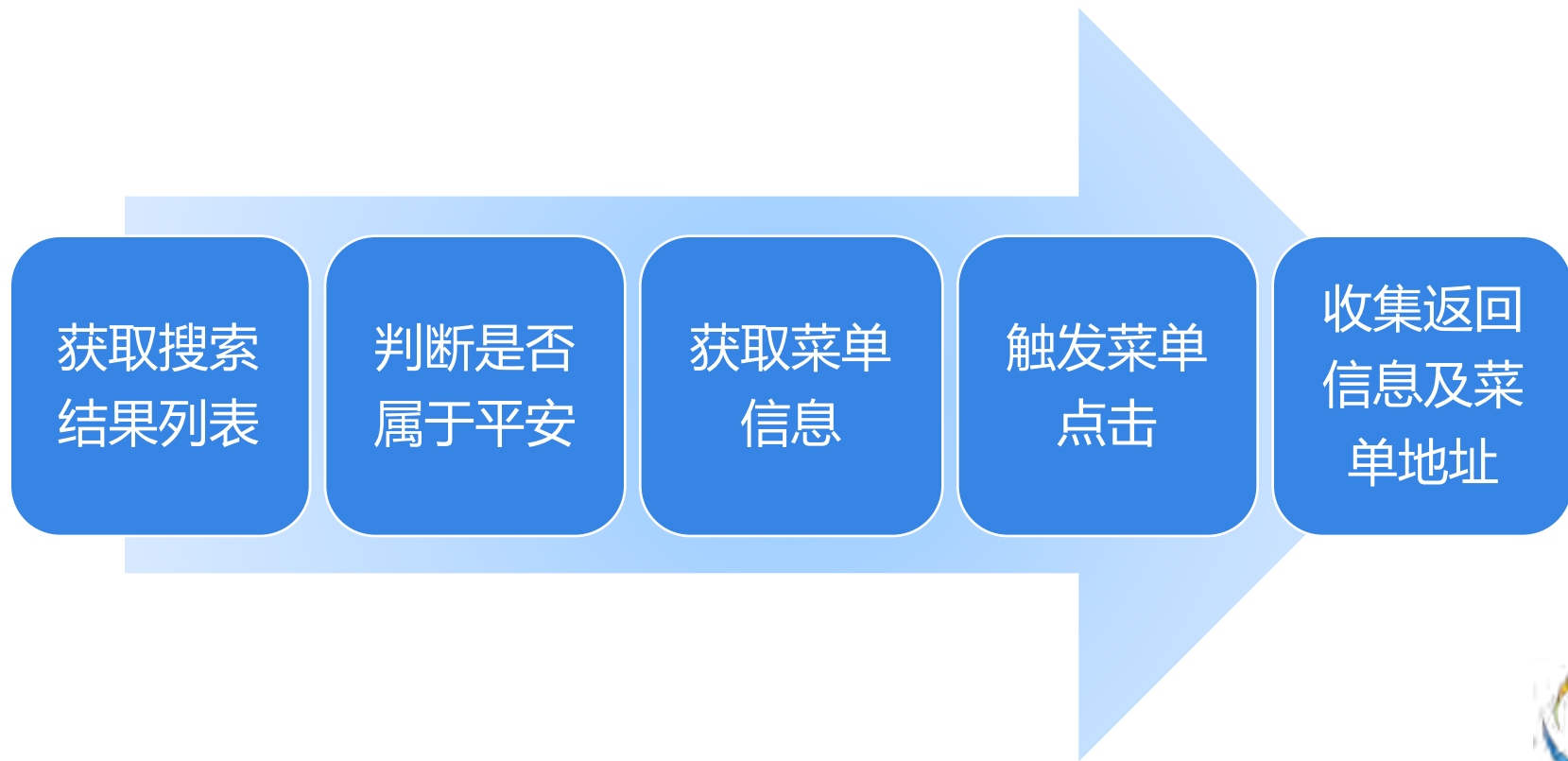


# Hook

- 动态修改运行时代码
- 辅助功能/获取关键数据
- 微信抢红包插件
- Xposed框架



# 具体实现



## 菜单信息示例截图

名称：平安人寿  
微信号：pars95511  
介绍：聪明的投保人都来这！(づー 3ー)づ我们为您提供以下服务：  
①新客户：热销产品介绍、保险需求分析、在线预约产品专家一对一业务办理；  
②公共功能：公司资讯、免费门店WiFi、人工坐席  
地区：CN, Guangdong, Shenzhen  
组织机构：中国平安人寿保险股份有限公司(已认证)  
认证详情页面：[http://mp.weixin.qq.com/mp/getverifyinfo?\\_\\_biz=MjM5NjYwNjUyMg==#wechat\\_webview\\_type=1&wechat\\_redirect](http://mp.weixin.qq.com/mp/getverifyinfo?__biz=MjM5NjYwNjUyMg==#wechat_webview_type=1&wechat_redirect)  
服务电话：95511  
图标地址：<http://wx.qlogo.cn/mmhead/Q3auHgzwzM7wYXpyZQ52ygWQ0LBjPeVG0ibwf5hYZplqW8Can31BDug/0>  
查看历史消息：[http://mp.weixin.qq.com/mp/getmasssendmsg?\\_\\_biz=MjM5NjYwNjUyMg==#wechat\\_webview\\_type=1&wechat\\_redirect](http://mp.weixin.qq.com/mp/getmasssendmsg?__biz=MjM5NjYwNjUyMg==#wechat_webview_type=1&wechat_redirect)  
一级按钮：微信门店 <http://m.pingan.com/c3/life/weixinfuwu.html>  
一级按钮：热销产品  
二级按钮：热销产品·预约咨询 "[https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect\\_uri=https%3A%2F%2Fm.pingan.com%2Fc3%2Flife%2Fweixin%2Fxiaochanpin.shtml%26weappNo%3DPARS95511\\_01&response\\_type=code&scope=snsapi\\_base](https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect_uri=https%3A%2F%2Fm.pingan.com%2Fc3%2Flife%2Fweixin%2Fxiaochanpin.shtml%26weappNo%3DPARS95511_01&response_type=code&scope=snsapi_base)"  
二级按钮：保险需求分析 ""  
一级按钮：更多  
二级按钮：免费上网 "<http://www.wx.gzfengchuan.com/login.html> "  
二级按钮：投诉与建议 ""  
二级按钮：我的客户经理 "[https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect\\_uri=https%3A%2F%2Fwww.pingan.com.cn%2Flife\\_insurance%2Fandroid%2Ftemplates%2Fmanager\\_index.html%3Ffrom%3Dweixin%26weappNo%3DPARS95511\\_01&response\\_type=code&scope=snsapi\\_base](https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect_uri=https%3A%2F%2Fwww.pingan.com.cn%2Flife_insurance%2Fandroid%2Ftemplates%2Fmanager_index.html%3Ffrom%3Dweixin%26weappNo%3DPARS95511_01&response_type=code&scope=snsapi_base)"  
二级按钮：代理人专区 "[https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect\\_uri=https%3A%2F%2Fsales.pa18.com%2Fwechat.sxBindStatus.loginFree%3Ffrom%3Dweixin%26weappNo%3DPARS95511\\_01&response\\_type=code&scope=snsapi\\_base](https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect_uri=https%3A%2F%2Fsales.pa18.com%2Fwechat.sxBindStatus.loginFree%3Ffrom%3Dweixin%26weappNo%3DPARS95511_01&response_type=code&scope=snsapi_base)"  
=====



# 一些细节

- 对抗模拟器检测
  - Xprivacy
- 网址白名单
  - .qq.com, .baidu.com, ...
- OAuth
  - 注入JavaScript代码模拟点击



# 目录

1 背景与起因

2 公众号开发101

3 常见安全问题

4 自动化监控

➔ 5 结语



# 采集

- 约350个公众号
- 1500+ URL
- 1小时
- 扩展性？



# 万里长征第一步

- 端口暴露
- 服务弱口令
- 代码泄露
- 存在安全问题的组件
- SQL注入？越权？逻辑漏洞？



# 扫描器





# Thanks

高效运维社区  
开放运维联盟

**荣誉出品**





## 想第一时间看到高效运维公众号的好文章么？

请打开高效运维公众号，点击右上角小人，并如右侧所示设置即可：



# GOPS2016 全球运维大会更多精彩

## GOPS2016 全球运维大会·北京站

2016年12月16日-17日  
北京国际会议中心

