



点融秋季安全沙龙

微信公众号的自动化安全监控

平安科技银河实验室 刘瑞恺



目录

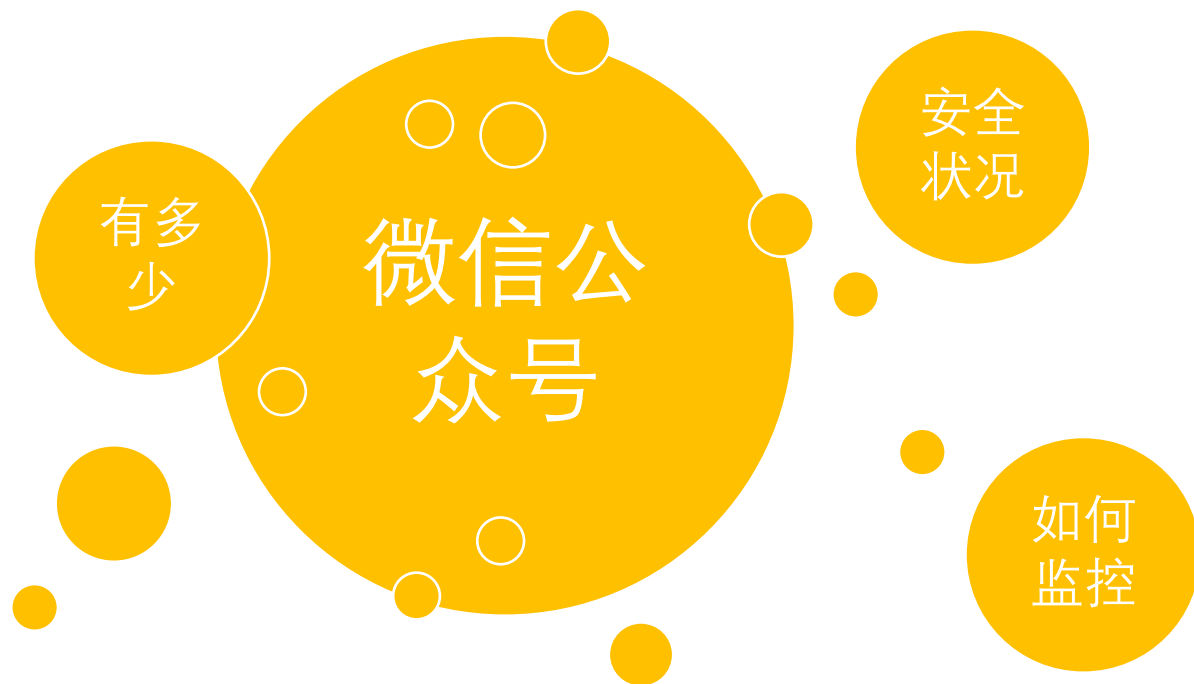
- 简介
- 公众号包含的链接
- 常见安全问题
- 自动化监控
- 总结

简介

whoami

- 平安科技银河实验室
- 安全研究员
- Android应用安全
- 逆向，密码学，CTF

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

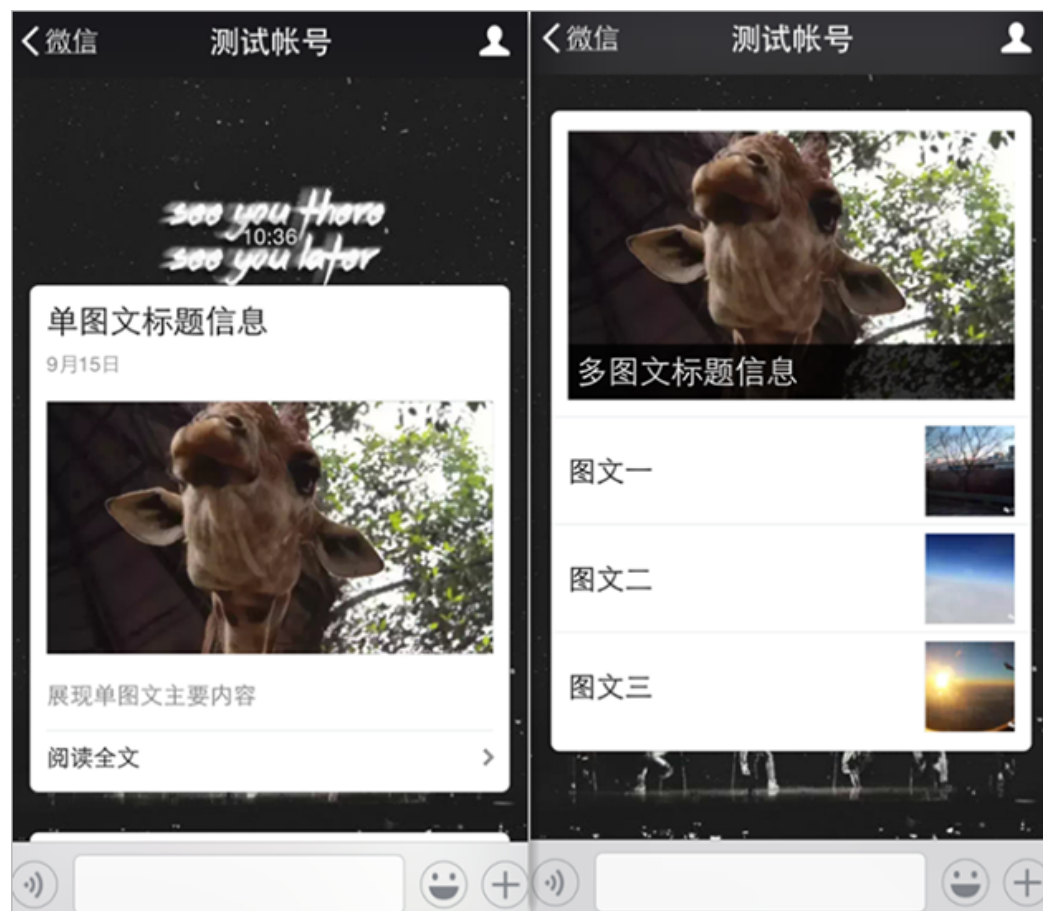
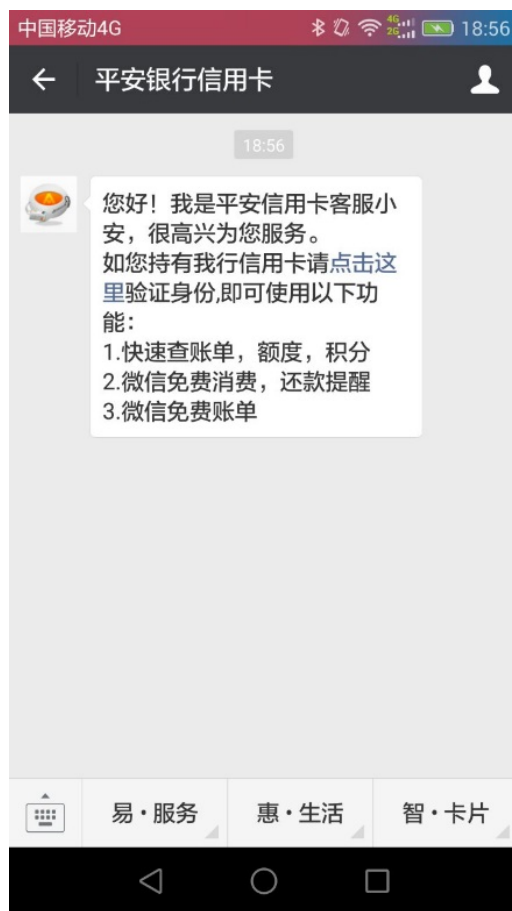
公众号包含的链接

自定义菜单

- 直接访问外部网页
- 回复消息
 - 文本
 - 图文



回复消息



外部链接来源



自定义菜单项

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

文本消息包含链接

猛戳【[阅读原文](#)】进入

[阅读原文](#) 阅读 100

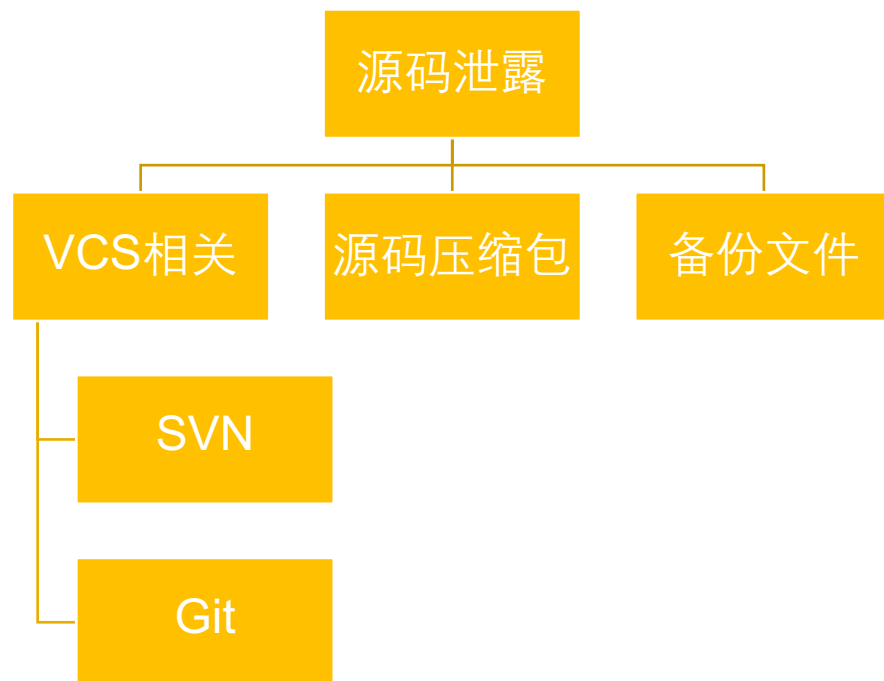
图文消息的原文链接

常见安全问题

开发

- SQL注入
- 越权
- 逻辑漏洞
- XSS

发布



源码泄露导致公众号被控制

- 源码压缩包
- 数据库连接密码
- 后台登陆

案例1

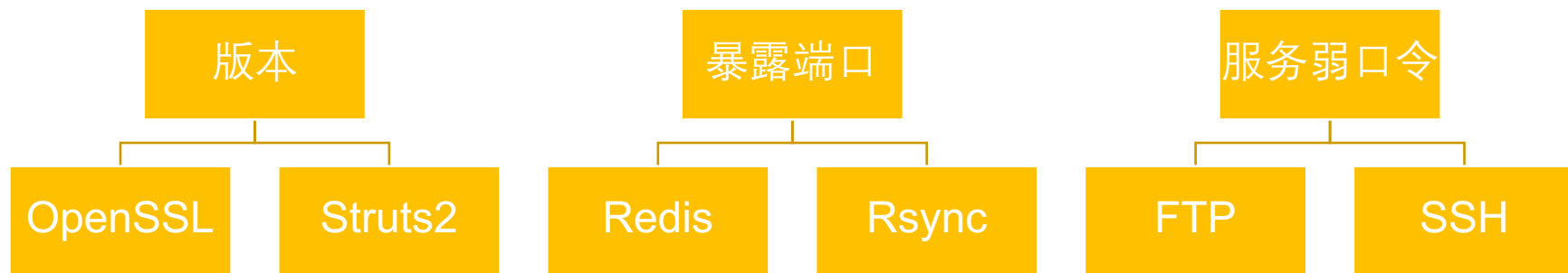
```
INSERT INTO `p_admin` (`id`, `groupid`, `username`, `realname`, `password`,  
(1, 1, 'admin', '贺', '2e4121014', 1436152259, '  
(2, 2, 'f', '风', '4db335d5a', 1436233253,
```

案例1

The screenshot displays a web management interface. At the top, a browser address bar shows the URL `www. /index.php?r=admin/index/index`. Below the address bar, there are four navigation 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). On the left side, there is a sidebar menu with categories: "全局设置" (Global Settings), "后台功能" (Backend Functions), "网站缓存" (Website Cache), "前台模板" (Frontend Templates), "后台登陆管理" (Backend Login Management), and "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: `✓`
- 允许使用URL打开文件(`allow_url_fopen`): `✓`

运维



Redis暴露导致公众号被控制

- 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) "yqmxbyqrf"  
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

群发钓鱼信息

微信内打开钓鱼网址

不显示网址

欺骗输入账号信息

自动化监控

基本思路



实施步骤

- 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

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

文本消息包含链接

猛戳【[阅读原文](#)】进入

[阅读原文](#) 阅读 100

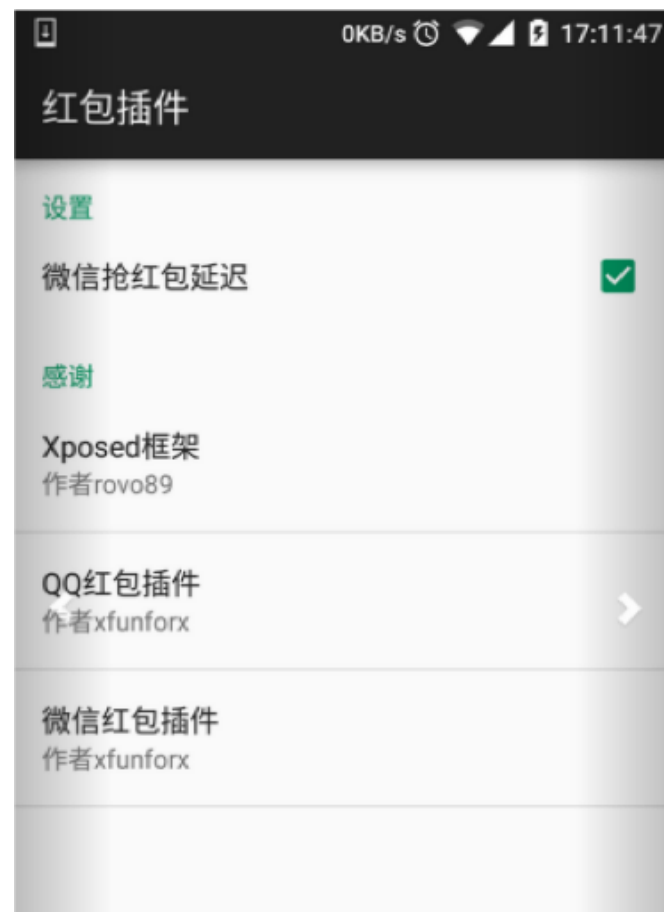
图文消息的原文链接

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

```
=====
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
务办理； ③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
服务电话：95511
图标地址：http://wx.qlogo.cn/mmhead/Q3auHgzwzM7wYXpyZQ52ygWQ0LBjPeVG0ibwf5hYZp1qW8Can31BDUg/0
查看历史消息：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
l%3Dhttp%3A%2F%2Fm.pingan.com%2Fc3%2Flife%2Frefxiaochanpin.shtml%26weappNo%3DPARS95511_01&response_type=code&scope=snsap
    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=
ttps%3A%2F%2Fwww.pingan.com.cn%2Flife_insurance%2Fandroid%2Ftemplates%2Fmanager_index.html%3Ffrom%3Dweixin%26weappNo%3D
at_redirect"
    二级按钮：代理人专区 "https://open.weixin.qq.com/connect/oauth2/authorize?appid=wx1b9ff1efb826794a&redirect_uri=ht
ps%3A%2F%2Fsales.pa18.com%2Fwechat.sxBindStatus.loginFree%3Ffrom%3Dweixin%26weappNo%3DPARS95511_01&response_type=code&s
=====
```


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



总结

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

银河一号

nabla 管理员

仪表盘 信息状态尽在眼前

首页 / 仪表盘

| 项目数量 | EXP数量 | 插件数量 | 漏洞数量 |
|---------|------------|--------|-----------|
| 1 | 28 | 0 | 2 |
| 当前创建的项目 | 即成的EXP监测脚本 | 集成插件数量 | 系统发现的漏洞数量 |

业内资讯

- 从底层分析eval和assert的区别
- Android安全开发之通用签名风险
- WAF攻防研究之四个层次Bypass WAF
- IPS Community Suite PHP远程代码执行漏洞分析(CVE-2016-6174)
- Stuxnet纪录片-零日 Zero.Days (2016) 【中文字幕】
- Linux服务器TCP连接曝高危漏洞：只要接入网络就可能被攻击
- 浅谈互联网隐私安全
- 揭秘：俄罗斯APT漏洞利用工具包

漏洞信息

- Rapid7 AppSpider 6.12 - Local Privilege Escalation
- Barracuda Web App Firewall 8.0.1.007/Load Balancer 5.4.0.004 - ...
- Barracuda Spam & Virus Firewall 5.1.3.007 - Remote Command ...
- MediaCoder 0.8.43.5852 - .m3u SEH Exploit
- Drupal CODER Module 2.5 - Remote Command Execution (Metasploit)
- CodoForum 3.2.1 - SQL Injection
- CoolPlayer+ Portable 2.19.6 - .m3u Stack Overflow (Egghunter+ASLR ...
- GRR Système de Gestion et de Réservations de Ressources 3.0.0-RC1 ...



点融秋季安全沙龙

谢谢

<http://rk700.github.io>

微信：lrk700

