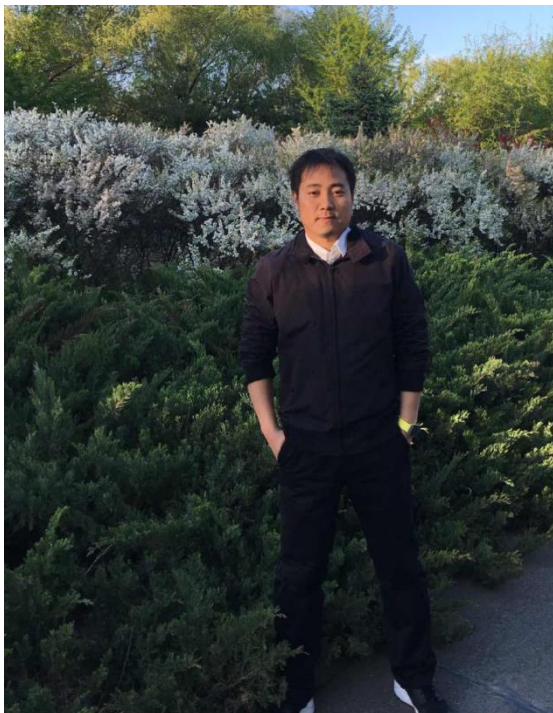


移动端产品安全



@许章毅

个人简介



知名白帽子/依旧
新浪安全技术负责人
安全软件ProxyScan作者

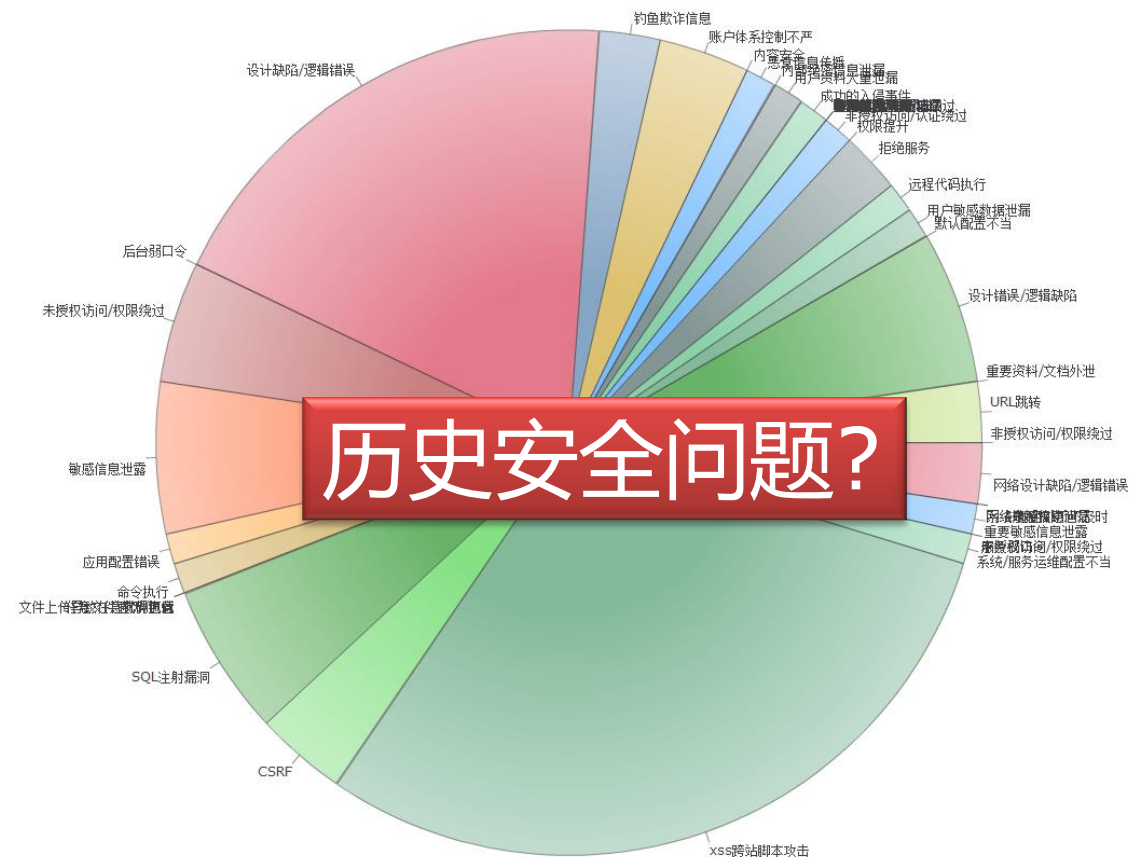
现负责新浪业务和产品的安全保障工作。专注应用和移动端安全，漏洞智能检测等。

移动端产品安全现状

谁知道?



移动端产品安全现状



主要议题

- 移动端产品安全保障
 - 数据安全
 - Acitvity组件安全、Webview代码执行漏洞、明文存储、模版交互、隐私数据、核心算法保护
 - 开发安全
 - 安全意识、环境和测试安全、第三方SDK安全开发
 - 业务及接口安全
 - 输入与输出、验证与授权、核心接口保护
 - 安全运维
 - 配置错误、匿名、弱口令
 - 安全工具
 - 漏洞智能检测
- 移动端产品最佳实践

数据安全

- Activity组件安全
- Webview代码执行漏洞
- 明文存储
- 模版交互
- 隐私数据
- 核心算法保护

Activity组件安全

```
<activity android:name=".activity.ForwardRecentActivity"
android:launchMode="singleTop" android:screenOrientation="portrait"
android:configChanges="locale|keyboardHidden|orientation"
android:alwaysRetainTaskState="true" android:windowSoftInputMode="adjustPan"> <
intent-filter> <action android:name="com.██████████_FORWARD" /> <category
android:name="android.intent.category.DEFAULT" /> </intent-filter> </activity>
```

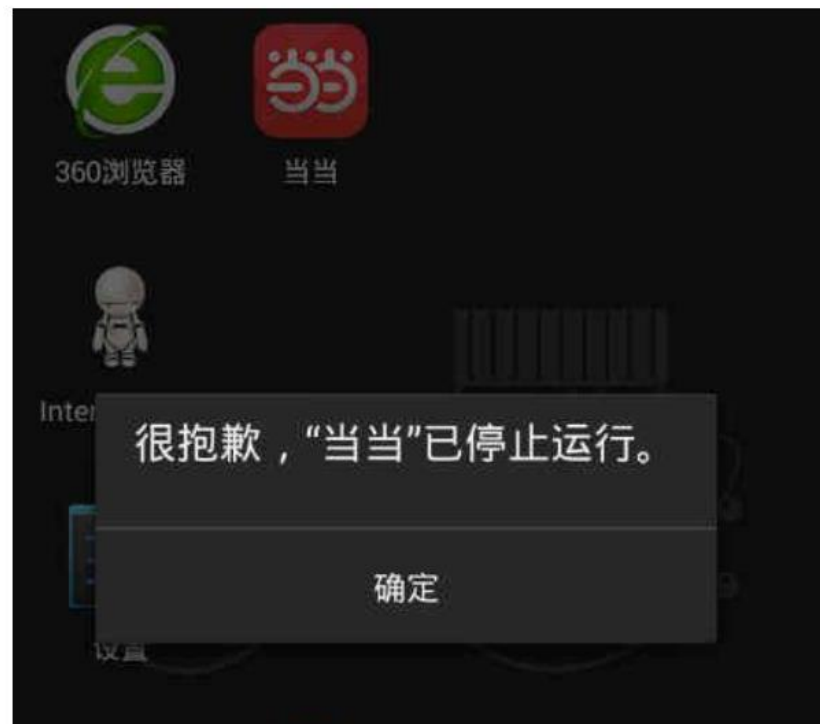
默认发布[android:exported="false"]
私有Activity不应被其他应用启动

Acitvity组件安全

客户端版本，v5.9.4 #### 组件拒绝服务，向组件发送空的intent，导致客户端app崩溃退出，存在该问题的组件有多个，如下

code 区域

Activity: buy2.activities.FirenzeDetailsActivity buy2.activities.MyMessageListActivity Servi



Activity组件安全

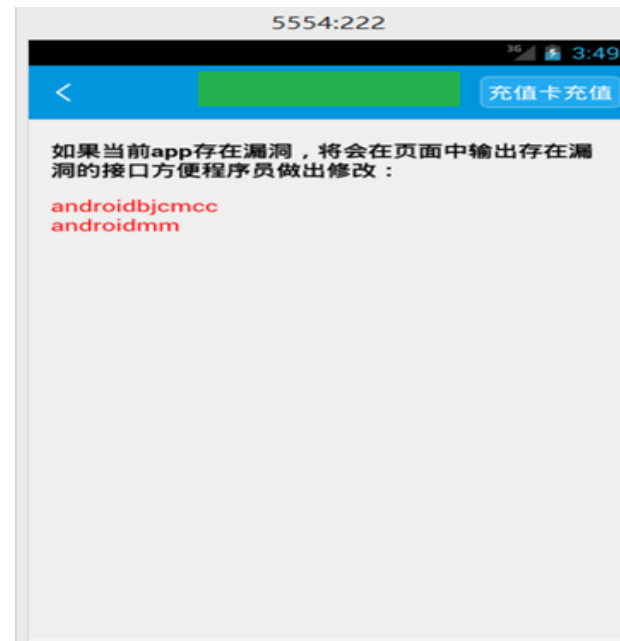
- 当Activity返回数据时候需注意目标Activity是否有泄露信息的风险?
- 验证目标Activity是否恶意app，规避受到intent欺骗，可用hash签名验证。
- 签名验证内部（in-house）app

Webview代码执行漏洞

```
1127     move-result-object v1
1128
1129     invoke-virtual {p1, v1}, Landroid/webkit/WebView;->setWebChromeClient(Landroid/webkit/We
1130
1131     invoke-virtual {v0}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
1132
1133     move-result-object v0
1134
1135     invoke-virtual {p1, v0}, Landroid/webkit/WebView;->loadUrl(Ljava/lang/String;)V
1136
1137     return-void
1138 .end method
```

ReChargeWebActivity.class x f.class

```
this.h.getSettings().setAllowFileAccess(true);
this.h.getSettings().setAppCacheEnabled(true);
this.h.addJavaScriptInterface(new g(), "androidmm");
if ((this.k.equals("流量消费分析") == true) || (this.k.equals("趣味账单") == true))
    localWebSettings.setCacheMode(2);
while (true)
{
    this.h.addJavaScriptInterface(new g(), "androidbjcmcc");
    ga localca = new ga(this);
    this.h.setWebViewClient(localca);
    gh localcb = new gh(this);
    this.h.setWebChromeClient(localcb);
    this.h.setDownloadListener(new gg(this));
    this.h.loadUrl(this.j);
    this.h.addJavaScriptInterface(new g(), "androidbjcmcc");
    setVisible(false);
    f.s("http_URL", this.j);
    f.s("li", "web loadUrl");
    this.h.loadUrl(this.j);
    if (this.q != null)
    {
        this.q.setVisibility(0);
        this.q.setOnClickListener(this);
    }
    if ((BApplication)getContext() != null)
    {
        this.d = WXAPIFactory.createWXAPI(this, "wxa48f0b9e1ed8f680", false);
        this.d.registerApp("wxa48f0b9e1ed8f680");
    }
    if (this.q != null)
    {
        this.q.setVisibility(8);
        this.a.c(false);
        this.a.a(PullToRefreshBase.k.s);
    }
}
```



明文存储

```
srini@srini:~$ cat userdetails.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="password">pass123</string>
  <string name="username">Infosec Institute</string>
</map>
srini@srini:~$ █
```

明文存储

```
D/tracelog( 7379): add log: ##[eventType=102][eventTypeStr=theone_ppx_home06_ck][sessionId=2D596A7F8C3E859E9DC044EF2F779629][area=17][phone=15048713ab06a3e1e3][imei=352887EBE9900CF1A3][deviceId=26d713ab06a3e1e3][deviceType=Nexus 5][appKey=taxiPassengerAndroid][osName=AndroidOS][osVersion=4.4.4][appVersion=4.2.5][time=20160304214546][channel=38][lng=103.984507][lat=30.581288][cid=68edc8a150487c144f9b4c5ca4df72a4][content=成都西门][ftab=Flash][stab=null]
D/tracelog( 7379): add log: ##[eventType=102][eventTypeStr=theone_ppx_home32_sw][sessionId=2D596A7F8C3E859E9DC044EF2F779629][area=17][phone=15048713ab06a3e1e3][imei=352887EBE9900CF1A3][deviceId=26d713ab06a3e1e3][deviceType=Nexus 5][appKey=taxiPassengerAndroid][osName=AndroidOS][osVersion=4.4.4][appVersion=4.2.5][time=20160304214546][channel=38][lng=103.984507][lat=30.581288][cid=68edc8a150487c144f9b4c5ca4df72a4][ftab=Flash][stab=null]
D/tracelog( 7379): add log: ##[eventType=102][eventTypeStr=theone_ppx_home07_ck][sessionId=2D596A7F8C3E859E9DC044EF2F779629][area=17][phone=15048713ab06a3e1e3][imei=352887EBE9900CF1A3][deviceId=26d713ab06a3e1e3][deviceType=Nexus 5][appKey=taxiPassengerAndroid][osName=AndroidOS][osVersion=4.4.4][appVersion=4.2.5][time=20160304214547][channel=38][lng=103.984507][lat=30.581288][cid=68edc8a150487c144f9b4c5ca4df72a4][content=成都西门][ftab=Flash][stab=null]
D/DIDIPsg ( 7379): | sending----- CollectSvrCoordinateReq{phone=15048713ab06a3e1e3, lng=103.984507, lat=30.581288, type=GCJ_02, accuracy=150.0, pull_peer=true, pre_lng=103.984507, pre_lat=30.581288, state=0, gps_source=GPS, time=20160304214547}
```

模版交互

交互参数过滤



模版交互



隐私数据

<

银行卡

工商银行-储蓄卡

97 879

下一步

<

银行卡

持卡人姓名

银行预留手机号

13

持卡人身份证号

44

财付通支付密码

☒ 同意 《快捷支付服务及相关协议》

下一步

打码模糊

核心算法保护

中国移动 0.36K/s 08:26

< 图案密码

请绘画图案密码

密文: F8218F3E5F939A92BE368D

类型: md5

解密

查询结果:
0124678

[添加备注](#)

中国移动 0.36K/s 08:26

< 图案密码

请绘画图案密码

忘记密码

#Fri Ja
PP=F821
PQ=

算法强度

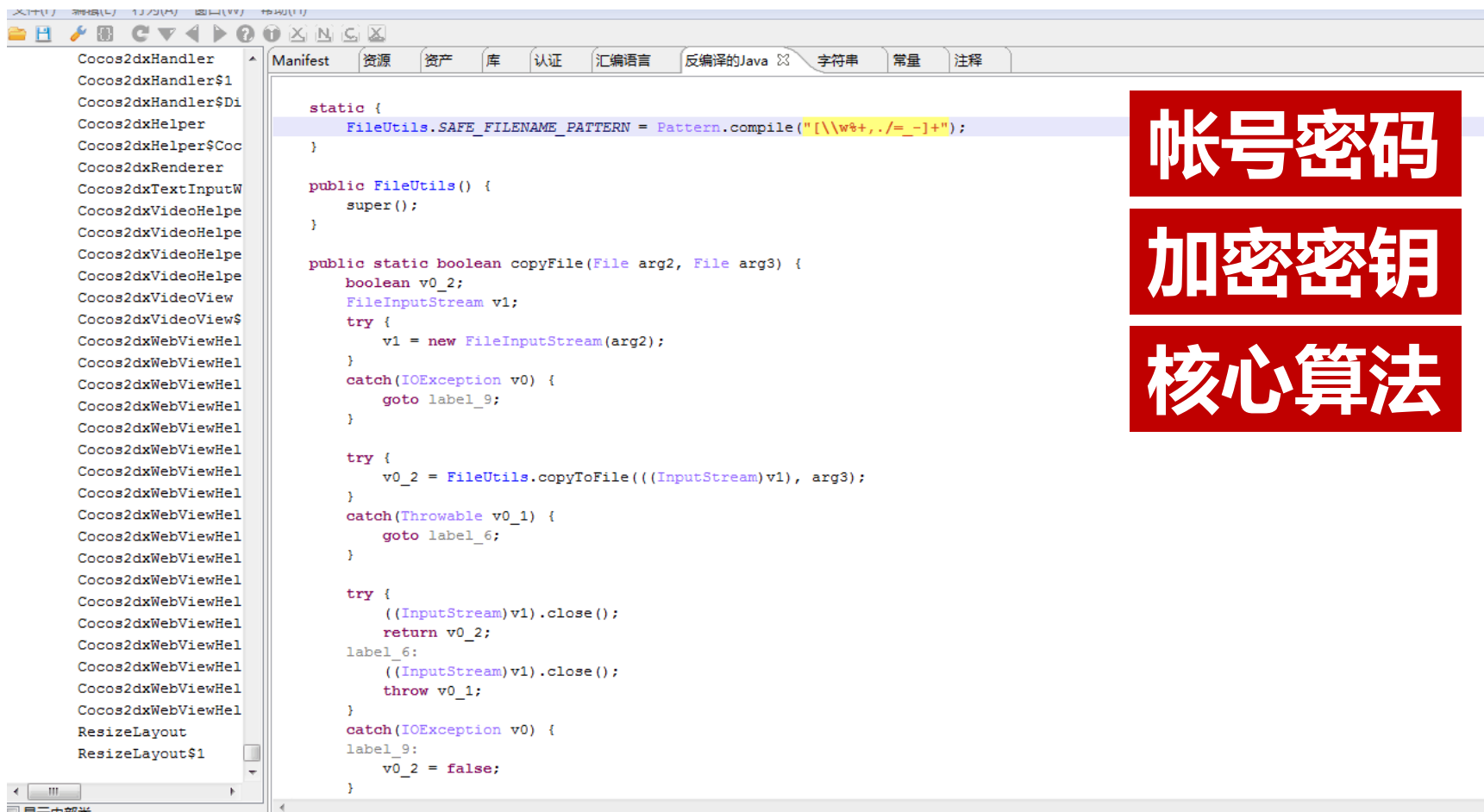
核心算法保护

Manifest	资源	资产	库	认证	汇编语言	反编译的Java	字符串	常量	注释
编号	值								
Cocos2dxHandler									
Cocos2dxHandler\$1									
Cocos2dxHandler\$Di									
Cocos2dxHelper	63427	选择录制的视频宽为:							
Cocos2dxHelper\$Coc	63428	选择机位失败。。。							
Cocos2dxRenderer	63429	选择机位, 当前选择机位:							
Cocos2dxTextInputW	63430	选择此功能, 您自己也将无法查看附近的人, 是否继续?							
Cocos2dxVideoHelpe	63431	选择联系人							
Cocos2dxVideoHelpe	63432	通							
Cocos2dxVideoHelpe	63433	通知							
Cocos2dxVideoHelpe	63434	通知 newNotifyCount =							
Cocos2dxVideoView	63435	通讯录为空							
Cocos2dxVideoView\$	63436	通讯录好友							
Cocos2dxWebViewHel	63437	通讯录好友:							
Cocos2dxWebViewHel	63438	通讯录获取失败							
Cocos2dxWebViewHel	63439	连接							
Cocos2dxWebViewHel	63440	连接计数取消							
Cocos2dxWebViewHel	63441	连接计数取消 设置收藏							
Cocos2dxWebViewHel	63442	退							
Cocos2dxWebViewHel	63443	邀请qq好友							
Cocos2dxWebViewHel	63444	邀请你安装人人客户端, 新用户安装注册立得5元话费。下载地址 http://2014.renren.com/mobile 安装完记得进入赚金币页面填写我的ID:							
Cocos2dxWebViewHel	63445	邀请好友							
Cocos2dxWebViewHel	63446	邀请微信好友							
Cocos2dxWebViewHel	63447	邀请微博好友							
Cocos2dxWebViewHel	63448	邀请, 加入XX群, 同意按钮点击后返回的数据值 -							
Cocos2dxWebViewHel	63449	邓							
Cocos2dxWebViewHel	63450	邢							
Cocos2dxWebViewHel	63451	那							
Cocos2dxWebViewHel	63452	郇							
ResizeLayout	63453	郗							
ResizeLayout\$1	63454	邵							
	63455	邹							

重要参数

老版本泄露

反编译



帐号密码

加密密钥

核心算法

开发安全

人员

- 安全意识
- 专业知识

环境

- 开发环境
- 测试环境

第三方

- SDK调用
- 安全开发

开发人员安全意识

<> Code

Issues 0

Pull requests 0

Wiki

Pulse

规范分享源代码

哔哩哔哩（B站）Android客户端源码（非最新版，可以运行，可看视频）

6 commits

1 branch

0 releases

2 contributors

Branch: master New pull request New file Upload files Find file HTTPS https://github.com/Summe Download ZIP

SummerRC Edit README.md Latest commit 0a8a1cf on 16 Feb

ABPlayer	哔哩哔哩简版	4 months ago
OneXListViewLibrary	哔哩哔哩简版	4 months ago
VitamioBundle-4	哔哩哔哩简版	4 months ago
VitamioDemo-master	哔哩哔哩简版	4 months ago
ZI-master	哔哩哔哩简版	4 months ago
appcompat_v7	哔哩哔哩简版	4 months ago
gradle/wrapper	哔哩哔哩简版	4 months ago
main	哔哩哔哩简版	4 months ago
viewPagerlibrary	哔哩哔哩简版	4 months ago
.gitignore	哔哩哔哩简版	4 months ago
.travis.yml	add .travis.yml	2 months ago
README.md	Edit README.md	2 months ago
build.gradle	哔哩哔哩简版	4 months ago
gradlew	哔哩哔哩简版	4 months ago

开发人员安全意识

code 区域

https://github.com/muyuyuan007/check_private_information/blob/64f3054402952030a1d41362aa1d540b

保护帐号和密码

```
# 邮箱账户设置
host = "smtp.oppo.com"
auth = "z[REDACTED]"
passwd = "zh[REDACTED]"
subject = "Please check your information"
# 调试模式 (1 or 0) 当为1时邮件将全部发送给auth.
debug = "1"
```

开发环境和测试环境

关于使用非苹果官方XCODE存在植入恶意代码情况的预警通报

来源：CNCERT 时间：2015-09-14



近日，CNCERT监测发现，开发者使用非苹果公司官方渠道的XCODE工具开发苹果应用程序（苹果APP）时，会向正常的苹果APP中植入恶意代码。被植入恶意程序的苹果APP可以在App Store正常下载并安装使用。该恶意代码具有信息窃取行为，并具有进行恶意远程控制的功能。

目前，CNCERT正在加强分析，并将此预警信息通报相关开发者或互联网企业，在开发苹果APP过程中，切勿使用非苹果官方渠道的XCODE工具，以维护广大用户的个人信息安全。

开发工具和代码包来源的安全性

第三方SDK安全开发

```
static
{
    a.put("geolocation", b + "GetLocLiteString");
    a.put("getsearchboxinfo", b + "GetSearchboxInfo");
    a.put("getapn", b + "GetApn");
    a.put("getserviceinfo", b + "GetServiceInfo");
    a.put("getpackageinfo", b + "GetPackageInfo");
    a.put("sendintent", b + "SendIntent");
    a.put("getcuId", b + "GetCuId");
    a.put("getlocstring", b + "GetLocString");
    a.put("scandownloadfile", b + "ScanDownloadFile");
    a.put("addcontactinfo", b + "AddContactInfo");
    a.put("getapplist", b + "GetAppList");
    a.put("downloadfile", b + "DownloadFile");
    a.put("uploadfile", b + "UploadFile");
}
```

```
"com.baidu.hello.moplus.action.BIND";

= 20;
S = "class";
AGE = "package";
alService";
/daemon";
http://127.0.0.1:40310/daemon?package=%s&class=%s";
http://127.0.0.1:40310";
on = new a();
```



百度WormHole虫洞漏洞
开放40310端口
无验证授权高权限操作

写入URL地址

APP列表信息

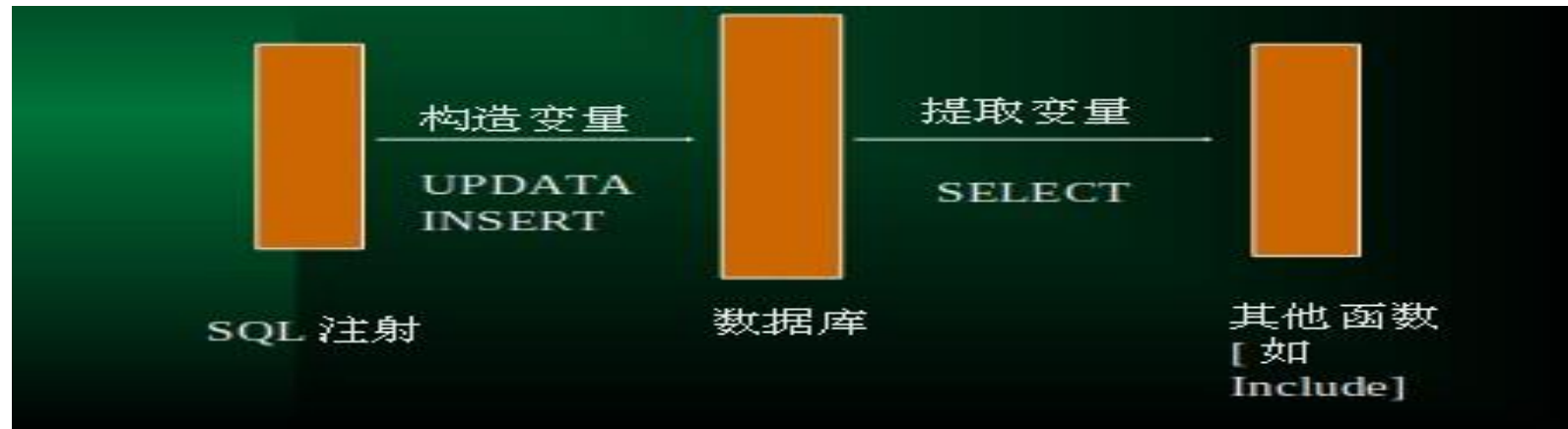
```
0.4-302030", "package_name": "com.android.soundrecorder",
name": "com.android.sdksetup", "package_state": 1, "version_c
"package_state": 1, "version_code": 15, {"version_name": "4.0
on_code": 15, {"version_name": "4.0.4-302030", "package_name":
name": "4.0.4-302030", "package_name": "com.android.contacts",
name": "com.android.inputmethod.latin", "package_state": 1
d.phone", "package_state": 1, "version_code": 15, {"version_na
, "version_code": 15, {"version_name": "4.0.4-302030",
, {"version_name": "1.0", "package_name": "com.android
me": "4.0.4-302030", "package_name": "com.android.providers
e name": "com.android.customLocale2", "package_state": 1
, "calendar", "package_state": 1, "version_code": 15, {"version
version_code": 15, {"version_name": "4.1-eng.ondo.20111206
code": 15, {"version_name": "4.0.4-302030", "package_name":
0.4-302030", "package_name": "com.android.netspeed", "package
0.4-302030", "package_name": "com.android.widgetpreview", "package_state": 1, "version_code":
15, {"version_name": "4.0.4-302030", "package_name": "com.example.android.livecubes", "package_state": 1, "version_code": 15, {"version_name":
"4.0.4-302030", "package_name": "com.android.providers.downloads.ui", "package_state": 1, "version_code": 15, {"version_name": "4.0.4-302030",
, "package_name": "com.android.providers.userdictionary", "package_state": 1, "version_code": 15, {"version_name": "4.0.4-302030", "package_name":
```

业务及接口安全

- 数据库操作【Sql注入】
- 文件操作【上传 下载】
- 输入与输出【xss】
- 验证与授权【CSRF、登陆】
- 核心接口保护

Sql注入

Web应用程序在操作数据库的Sql语句中插入了用户可控的变量，导致可以通过可控变量组合Sql执行语句恶意操作数据库。



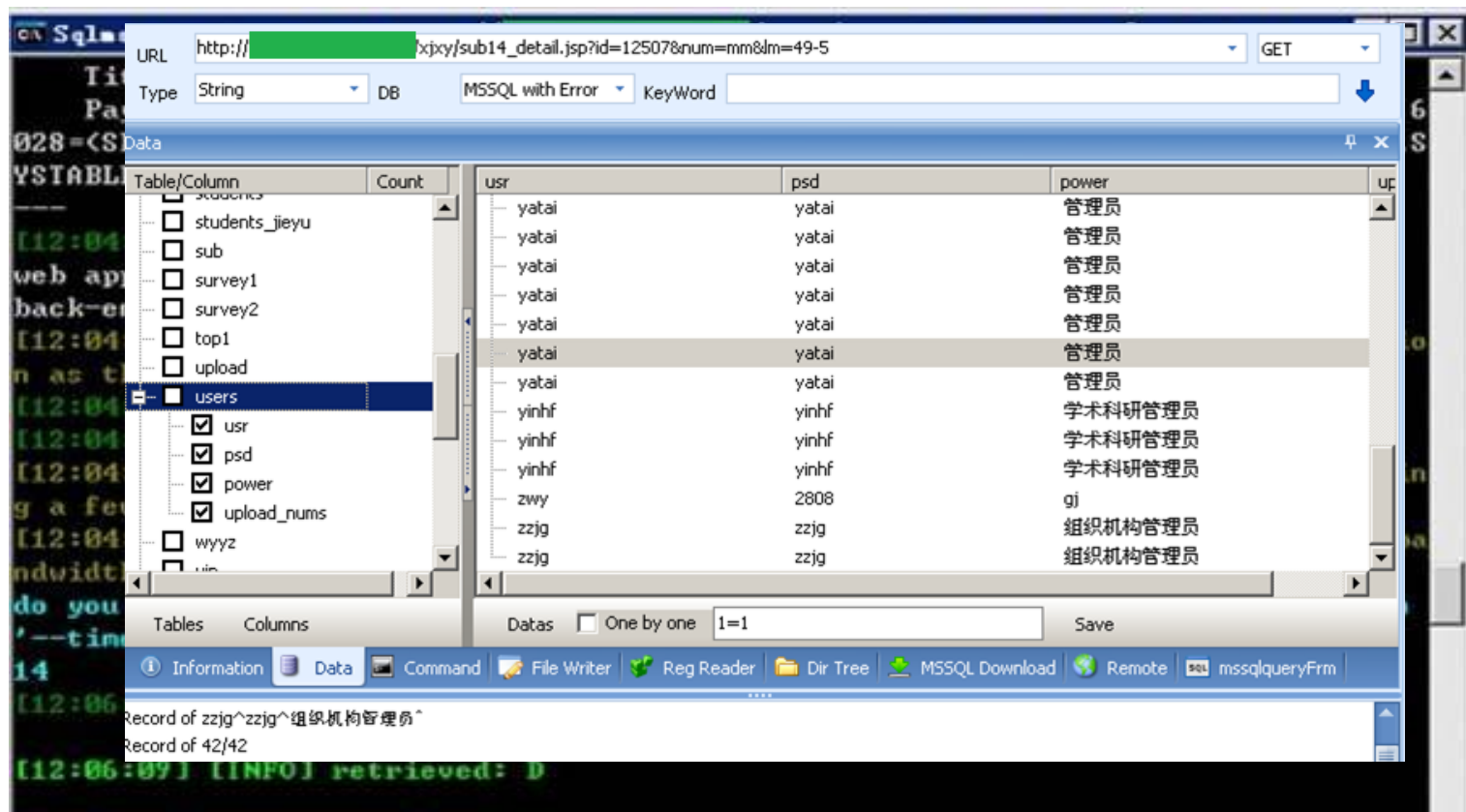
Sql注入漏洞

```
clean-based blind
title: AND boolean-based blind - WHERE or HAVING clause
Payload: http://[REDACTED]:80/ystpatient2.3/part.do?method=getJbPageBy
PartId&true=doJsonp_cfcc9621_553d_46cb_8b7b_909f8f148fd9&pageNo=1&partId=2&searchStr=-1' or 1=1 ) AND 9908=9908 AND ( 5226=5226 or 'a'='&functionName=doJsonp_cfcc9621_553d_46cb_8b7b_909f8f148fd9&_ =1464676214454
---
[03:27:42] [INFO] the back-end DBMS is Oracle
web application technology: JSP
back-end DBMS: Oracle
[03:27:42] [INFO] fetching current user
[03:27:42] [INFO] retrieving the length of query output
[03:27:42] [INFO] retrieved: 3
[03:27:46] [INFO] resuming partial value: AM
[03:27:46] [INFO] retrieved: S
current user: 'AMS'
[03:27:48] [INFO] testing if current user is DBA
current user is DBA: False
[03:27:48] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
www.jkwin.com.cn'

[*] shutting down at 03:27:48
```

searchStr参数存在注入

可直接操作数据库



Sql注入 - 推荐修复

- 代码实例

- String username = "admin' or 1=1--";
- String password = "foo"
- Statements s = connection.prepareStatement("select * from users where username = ? And password = ?")
- s.setString(1,username);
- S.setString(2,password);

Sql注入 - 安全性增强

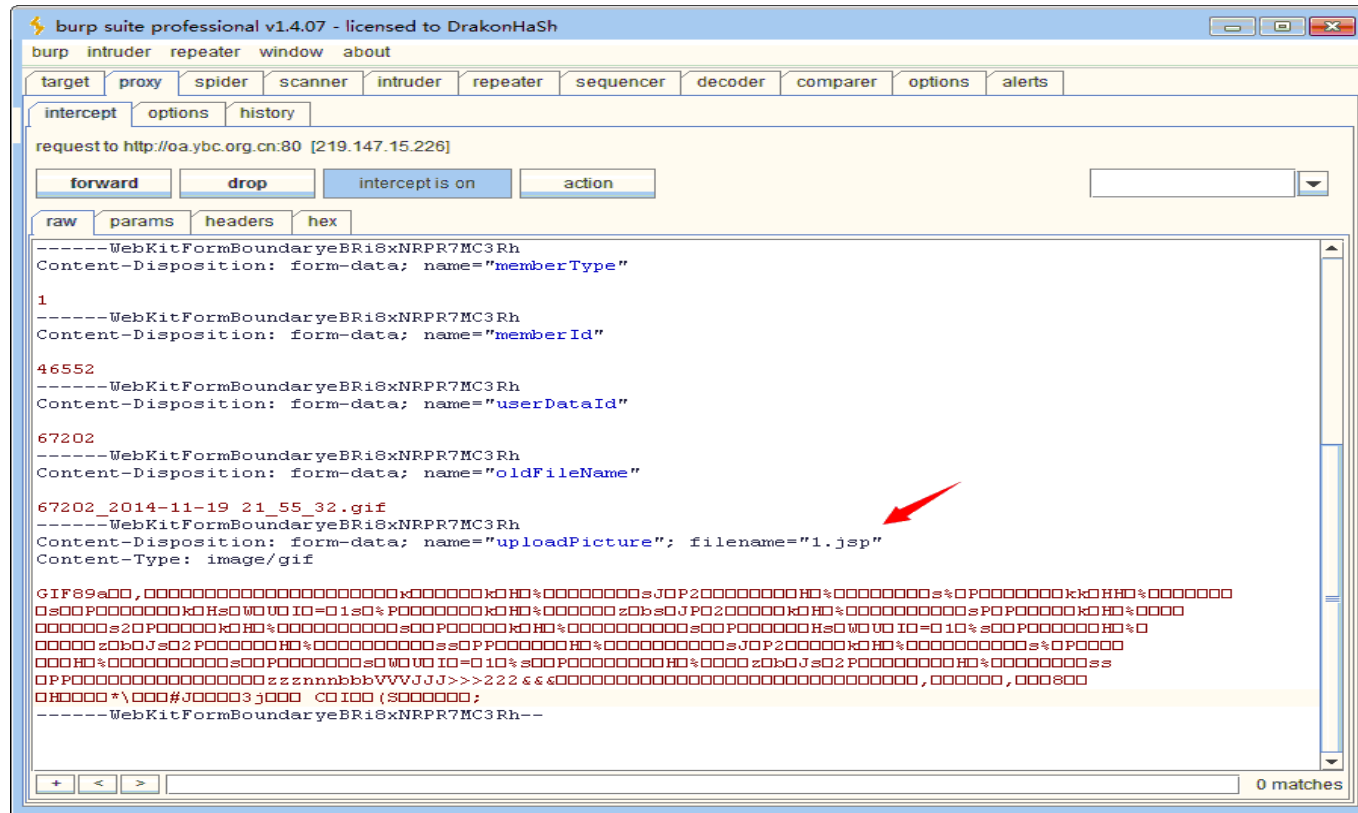
- 数据库连接帐号权限
- 对用户输入验证数据类型检验
- 使用数据先检验

文件操作

- `Java.IO.FileInputStream`
- `Java.io.FileOutputStream`
- `Java.io.FileReader`
- `Java.io.fileWriter`

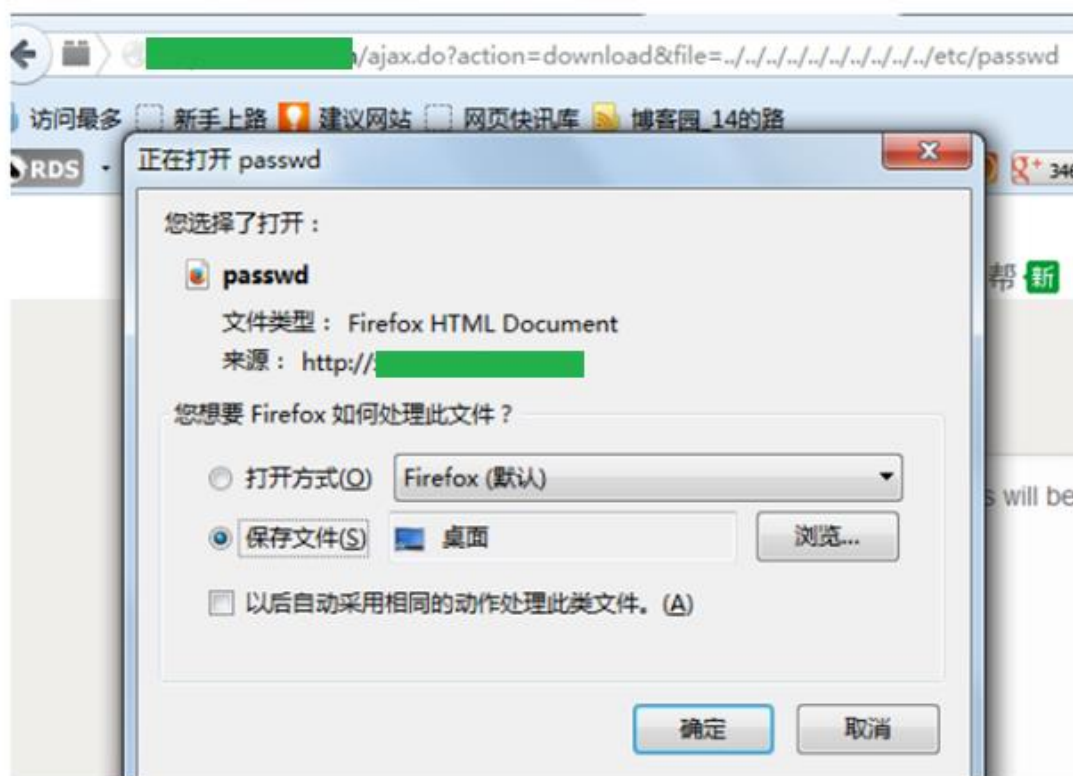
- `/../../..`

文件上传 - 文件名绕过



文件下载

http://[redacted]ajax.do?action=download&file=../../../../../../../../etc/passwd



XSS

- Web网页里输出内容包含用户可控制的内容，导致嵌入的恶意代码得到执行而进行攻击。

```
sae在反馈提交时没有过滤变量app_name,导致存储型xss.  
POST http://sae.sina.com.cn/?m=feedback&a=save HTTP/1.1  
Accept: text/javascript, text/html, application/xml, text/xml, */*  
X-Requested-With: XMLHttpRequest  
Content-Type: application/x-www-form-urlencoded; charset=utf-8  
Referer: http://sae.sina.com.cn/?m=feedback  
Accept-Language: zh-cn  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)  
Host: sae.sina.com.cn  
Content-Length: 200  
Connection: Keep-Alive  
Pragma: no-cache  
  
title=aaaa&fdtype=bug&app_name=%3Cimg+src%3D1+onerror%3Dalert(1)%3E&app_version=  
&err_url=http%3A%2F%2Fwww.baidu.comasdfasdf  
&reproduce=asdfasdfsdfasdfsdf&attachements=&content=asdfasdfsdfasdfsdf&vcode=42MK  
app_name变量没有过滤,导致漏洞产生
```



XSS-常见漏洞

- 数据交互的地方
 - Get Post Cookies Headers
 - 反馈与留言
 - 富文本编辑
 - 各类标签插入和自定义
- 数据输出的地方
 - 用户资料
 - 关键词，标签，说明
 - 文件上传

XSS-常见地方

```
<img src={$输出在这里}></img>
<span class="xxx">{$输出在这里}</span>
<div style="background-color:{$输出在这里};">
</div>
<script> var vultest='{$输出在这里}';</script>
```

```
<script>
  var s = "\u003con";
  alert(s);
</script>
```

来自网页的消息

1

确定

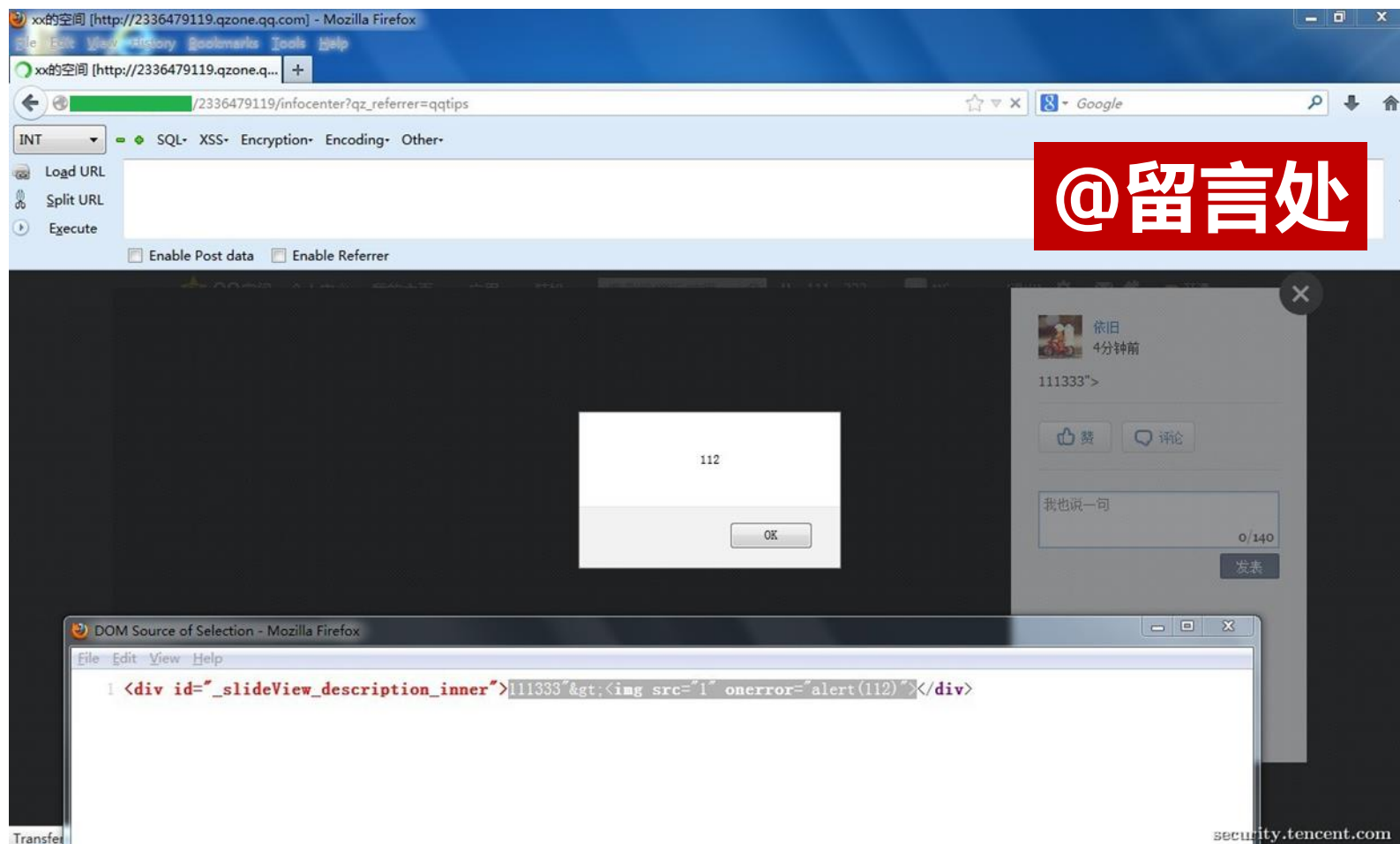
来自网页的消息

<on

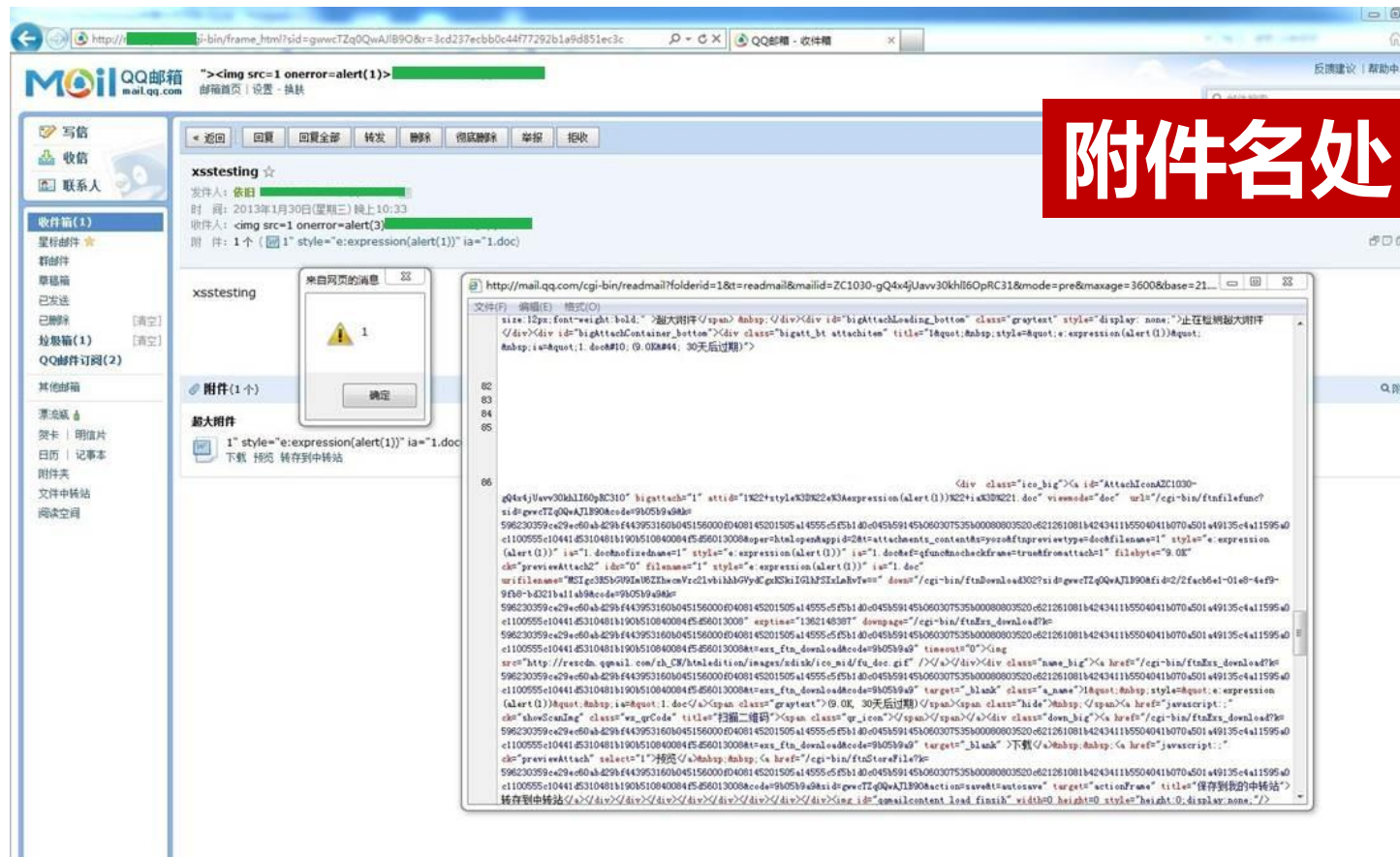
确定

```
<img src=alert(1)></img>
<span class="xxx"><script>alert(1)</script></span>
<div style="background-color:expression(alert(1))"> xss</div>
<script> alert(1);var mn = '1';</script>
```

XSS-常见漏洞



常见XSS漏洞



XSS-推荐修复

- (1)
html
以下字
- (2)
type:
- (3)
- (4)
- (5)

安全修复:

> (1) 通过对标签调用进行白名单过滤, 或者对标签进行检测后取出其值重新组合。(推荐使用)

> (2) 标签的黑名单过滤。(可能存在绕过的风险):

> (一) 建议标签不要支持伪协议, 防范Html属性值的协议攻击内容, 检测src属性值必须以"http://"开发, 或者是检测属性值, 重新构造。

> 可利用的属性:

> dynsrc=

> href=

> lowsrc=

> src=

> background=

> value=

> action=

> bgsound=

> 可利用的伪协议:

> 脚本伪协议

> vbscript:

> javascript:

> 文件类协议

> ms-its:

> mhtml:

> data:

> 第三方协议

> firefoxurl:

> mocha:

> livescript:

> 要求检测属性值是不是"http"字符开头,

> (二) 利用style属性的攻击, 严格过滤富文本标签中的\+数字和&#的字符串, 如 (style="\0078\0073\0073:\0065?\0;

<div STYLE="x:\0065expression(alert(/aaaaaaa/));"> > ;

过滤注释符和\, 如 (style="xss:expr/*xss*/ession(alert(111))">;style="background-image:url(ja\vas\\c\ript:alert(111))">> ;

> 过滤"expression, background, binding ,String.fromCharCode字符,

如 (<div style="x:expression((window.r==1)?':eval('r=1;alert(String.fromCharCode(88,83,83));'))">>

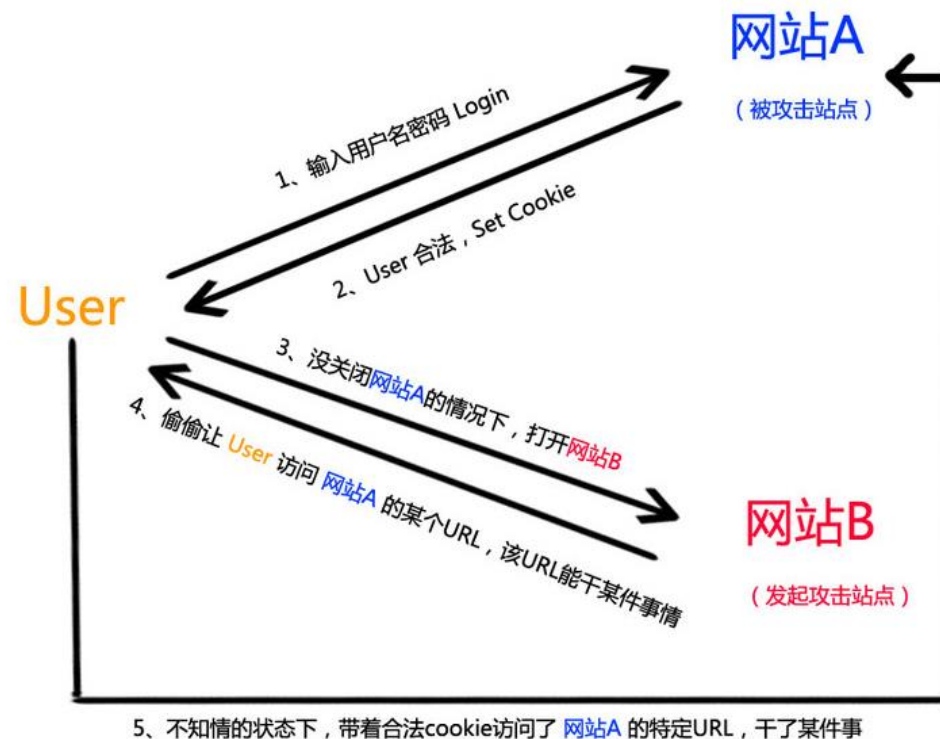
> (三) 利用标签的事件触发的攻击, 过滤以下事件onload、onerror、onmousemove、onmouseout、onmouseover、onmouseup、

onmouseenter、onmouseleave、onmousewheel、onscroll, .

), 转义

CSRF

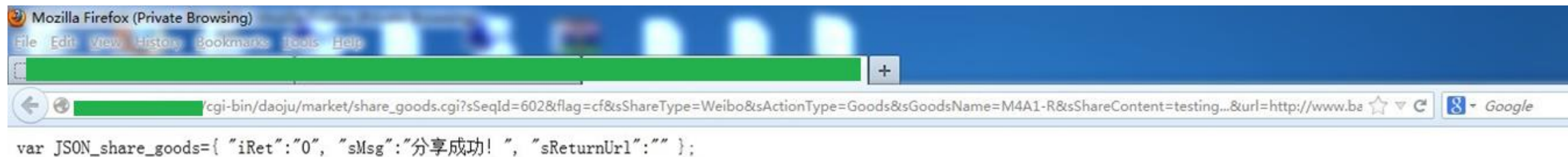
- ❑ 攻击者通过调用第三方网站的恶意脚本或者利用程序来伪造请求。
- ❑ 利用用户的浏览器向攻击的应用程序提交一个已经预测好请求参数的操作数据包。
- ❑ 利用的实质是截持用户的会话状态。



CSRF-浏览器

- 本地Cookie
 - 拦截IE6/IE7/IE8/Safari
 - 发送FireFox 2/firefox3/Opera/Chrome
- 内存Cookie
 - 均发送
- 多标签浏览器
 - 同一进程，内存Cookie没有清除

发微博处



CSRF-推荐修复

- 验证请求来路（不允许为空）
- 验证码
- 一次性令牌

验证与授权

831 http:// GET /api/v2/sms/13344445555/login?f...

Request Response

Raw Headers

HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Tue, 01 Sep 2015 16:55:16 GMT
Content-Type: application/json; charset=UTF-8
Connection: keep-alive
Content-Length: 31

{"message": "7852", "status": 1}

832 http://app POST /api/v2/login?format=json 200 331
833 http://au POST /api/check_app_update 200 173
834 https://ap POST /api/crash 200 341
835 http://loc POST /sdk.php 200 420

Request Response

Raw Params Headers Hex

POST /api/v2/login?format=json HTTP/1.1
Cookie:
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
User-Agent:
Host: app.
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 80

mobile=13344445555&code=7852&um_d_t=AiDcSMv-PjP_CMmeHtY8Wu9N07QA6cFUZe1SL1a9IyMx

任意用户登陆漏洞

验证与授权

```
GET http://app. api/user/forgetPassword?phone=18 HTTP/1.1
cookie: JSESSIONID=A41E4F433D7D434ED218A0DC11A276C1; Path=/; HttpOnly;
User-Agent: Dalvik/2.1.0 (Linux; U; Android 5.0.2; MI 2SC MIUI/V6.6.1.0.LXACNCF
Host: app.eapchina.net
Connection: Keep-Alive
Accept-Encoding: gzip
```

```
HTTP/1.1 200 OK
Server: nginx/1.6.0
Date: Sat, 19 Sep 2015 03:27:57 GMT
Content-Type: application/json;charset=UTF-8
Pragma: no-cache
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Cache: MISS from netentsec-nps-10.10.101.9
Connection: keep-alive
Content-Length: 56
```

```
{"message":"","result":"success","data":{"code":"8411"}}
```

手机号

手机验证码泄露

短信验证码

验证与授权

Request	Payload	Status	Error	Timeout	Length	Comment
30	5729	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
31	5730	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
32	5731	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
33	5732	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
34	5733	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
35	5734	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
36	5735	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
37	5736	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
38	5737	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
39	5738	200	<input type="checkbox"/>	<input type="checkbox"/>	331	

RequestResponse

RawHeadersHex

Connection: close
Content-Type: text/html; charset=utf-8

1

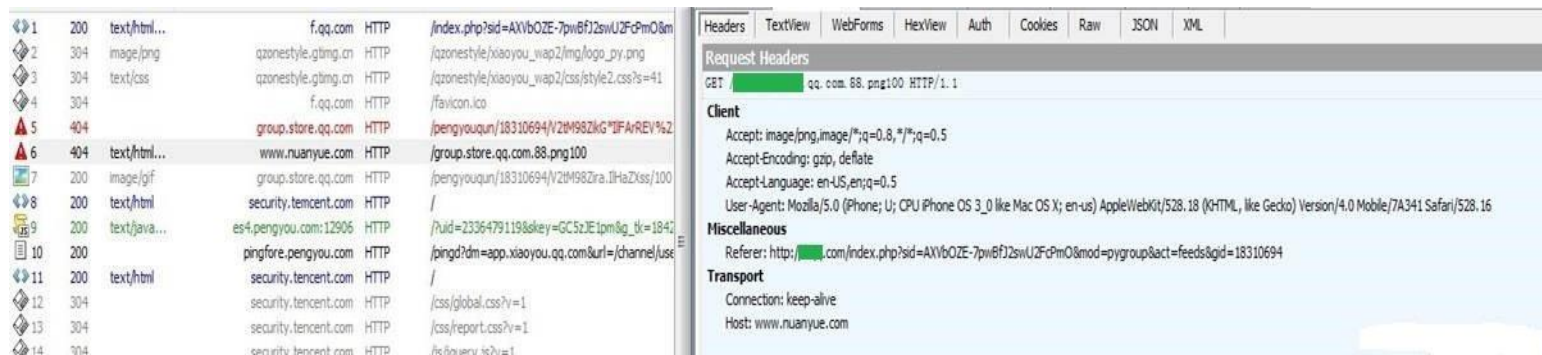
?<+>

Type a search term

Finished

手机验证码暴力破解

验证与授权



重要参数通过Referer泄露

核心接口保护



The screenshot shows a web browser with two tabs: "百度新闻搜索——全球最..." and "国美在线-国美电器官方网...". The address bar shows "news.baidu.com". The page content includes the Baidu News logo, navigation links, and a list of news items. The console log on the right shows a jQuery AJAX call to a URL that includes a Baidu account ID. The response is a JSON object containing address details. The console log also shows the success callback function, which logs the response to the console. A red box with the text "Json劫持" (JSON Hijacking) is overlaid on the bottom right of the console log.

news.baidu.com

登录 | 注册 | 百度新闻无线版 | 百度首页

新闻 网页 贴吧 知道 音乐

Baidu 新闻

新闻全文 新闻标题

首页 百家 个性推荐 互联网 传媒 汽车

热点要闻 个性推荐 登录更懂

盘点习近平勉励高三学子的真情话语
李克强：鼓励地方设立创业基金 中央部署沉船救援12字方针

“东方之星”遇难者人数已升至396人
未配备自动报警系统和黑匣子 驾驶舱实景还原 搜救基本结束

全民造车大幕拉开 各路人马纷纷涌进
科技公司造车 可笑还是可怕？ 互联网公司“造车”的真实逻辑

直升机坠入北京密云水库2人遇难 村民称飞机撞树

7日“头七” 将在沉船打捞现场举行悼念活动

北京自住房摇号出现多个重号 网友质疑有“猫腻”

网曝湖南某局长携女下属游玩 当地纪委立案调查

我国首例输入性mers病例全基因组序列测定已完成

Elements Network Sources Timeline Profiles Resources Audits Console

<top frame> Preserve log

```
> $.ajax({type:"get",url:"http://[redacted]/myaccount/address/getSecondaryAddress?timer=1433606988720",dataType:"jsonp",jsonp:"callback",jsonpCallback:"ckdata",success:function(json){console.log('上面是在百度域名下获取到国美的内容');console.log(json);console.log('上面是在百度域名下获取到国美的内容');});}
Object {readyState: 1}
下面是百度域名下获取到国美的内容
Object {result: Object}
  result: Object
    pAddressDetails: Array[1]
      0: Object
        address: "sddfsfdf"
        city: "11010000"
        cityName: "北京市"
        county: "11011400"
        countyName: "东城区"
        firstName: "test4"
        id: "16756624420"
        isDefault: false
        mobile: "188[redacted]"
        modifyTime: 1433606128908
        nickname: "1428639188907"
        state: "11000000"
        stateName: "北京"
        town: "110114001"
        townName: "全部区域"
        userId: "2030614"
        __proto__: Object
        length: 1
        __proto__: Array[0]
        __proto__: Object
        __proto__: Object
上面是在百度域名下获取到国美的内容
> |
```

Json劫持

核心接口保护

老旧接口兼容

- 及时更新统一
- 下线旧接口

兼容各个端

- 移动端接口隔离
- 禁止互相调用

调用保护

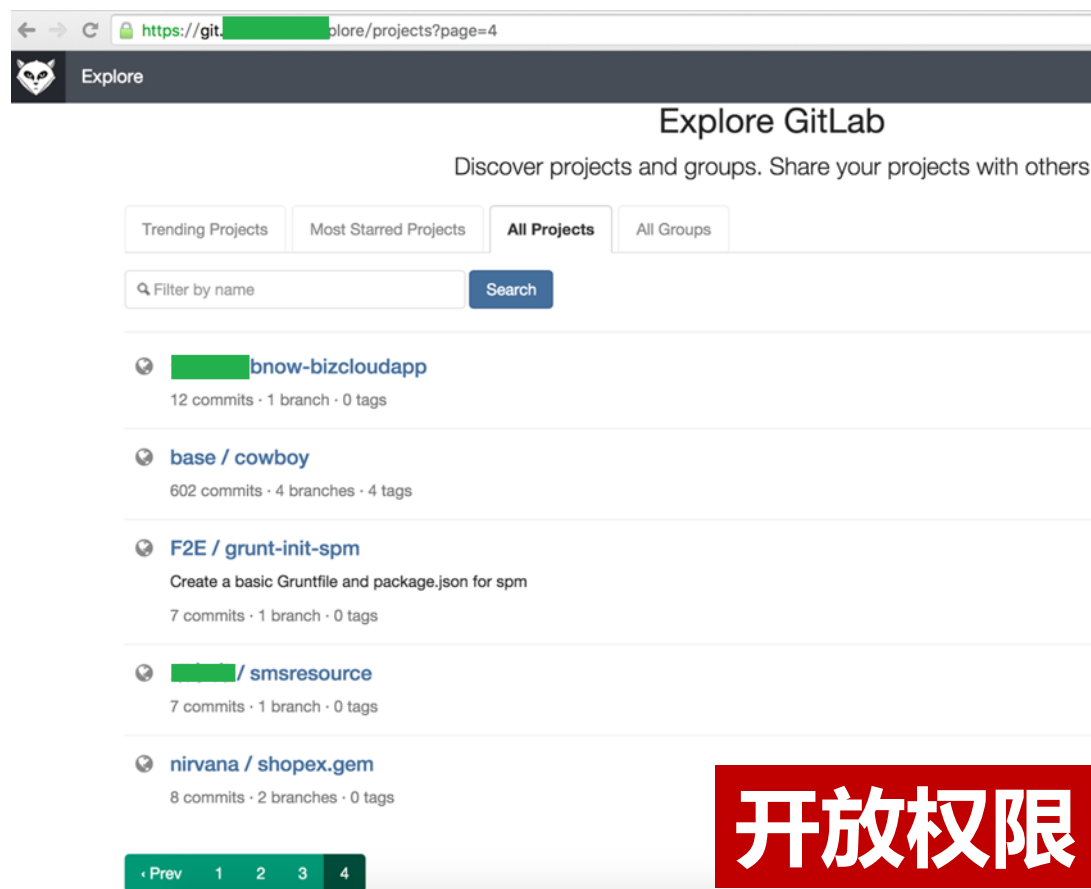
- 参数跟踪
- 次数限制
- 来源白名单

安全运维- 匿名

```
fan@websec00: ~/code
fan@websec00: ~/test
fan@websec00:~/code$ rsync 172.16.6.105::ghchun
drwxr-xr-x      4,096 2014/12/11 11:22:08 .
-rw-r--r--      9,114 2014/12/11 20:24:43 .bash_history
-rw-r--r--       33 2008/10/09 09:46:37 .bash_logout
-rw-r--r--      176 2008/10/09 09:46:37 .bash_profile
-rw-r--r--      125 2012/10/24 18:10:56 .bashrc
-rw-r--r--       35 2014/12/09 18:32:28 .lessht
-rw-r--r--    49,492 2014/10/20 16:26:27 .mysql_history
-rw-r--r--     9,729 2014/12/11 11:22:08 .viminfo
-rw-r--r--      658 2008/10/09 09:46:37 .zshrc
-rwxrwxr-x     8,063 2014/12/09 18:33:40 a.out
-rw-r--r--       42 2013/07/25 11:28:12 g.sh
-rwxr-xr-x      370 2010/09/07 19:43:17 go.sh
-rw-r--r--  47,634,806 2012/06/06 18:53:27 pub2.tar.gz
-rw-r--r-- 528,531,464 2012/10/16 16:04:42 pub20121016.tar.gz
-rw-r--r--   293,277 2012/06/07 14:49:31 pub3.tar.gz
-rw-r--r--   276,152 2012/06/26 18:42:28 pub4.tar.gz
-rw-r--r--     3,105 2013/07/19 20:18:41 t.sh
-rw-rw-r--      406 2014/07/11 10:01:24 t2.txt
-rw-r--r--      835 2012/06/08 15:34:16 transfer.php
-rw-r--r--   5,085 2014/12/09 18:33:35 vsprintf.c
-rw-r--r--  3,385,372 2012/08/03 15:52:16 web.tar.gz
drwx-----    4,096 2008/10/09 09:46:38 .ssh
drwxrwxr-x    4,096 2013/12/25 17:35:21 .subversion
```

内网未授权访问

安全运维 - 配置错误



The screenshot shows the GitLab Explore page. The browser address bar displays `https://gitlab.com/explore/projects?page=4`. The page header includes the GitLab logo and the word "Explore". Below the header, the text "Explore GitLab" is followed by the subtitle "Discover projects and groups. Share your projects with others". There are four tabs: "Trending Projects", "Most Starred Projects", "All Projects" (which is selected), and "All Groups". A search bar with the placeholder "Filter by name" and a "Search" button is present. The main content area lists several projects:

- bnow-bizcloudapp**: 12 commits · 1 branch · 0 tags
- base / cowboy**: 602 commits · 4 branches · 4 tags
- F2E / grunt-init-spm**: Create a basic Gruntfile and package.json for spm. 7 commits · 1 branch · 0 tags
- [redacted] / smsresource**: 7 commits · 1 branch · 0 tags
- nirvana / shopex.gem**: 8 commits · 2 branches · 0 tags

At the bottom left, there is a pagination bar with "Prev", "1", "2", "3", and "4". At the bottom right, a red box contains the white text "开放权限" (Open Permissions).

安全运维 - 弱口令

admin/123456
test/1234qwer
manage/1qaz@WSX
root/123456

太弱密码

统一密码

安全运维 – 密码保护

- 密码选择 易记不易猜
 - FLZX3000cY4yhx9day
 - 飞流直下三千尺，疑似银河下九天
- 密码策略
 - 大于8位 数字+字母+特殊符号组
 - 定期更换(三个月)
 - 一个密码不能多用

安全工具 - 漏洞智能检测



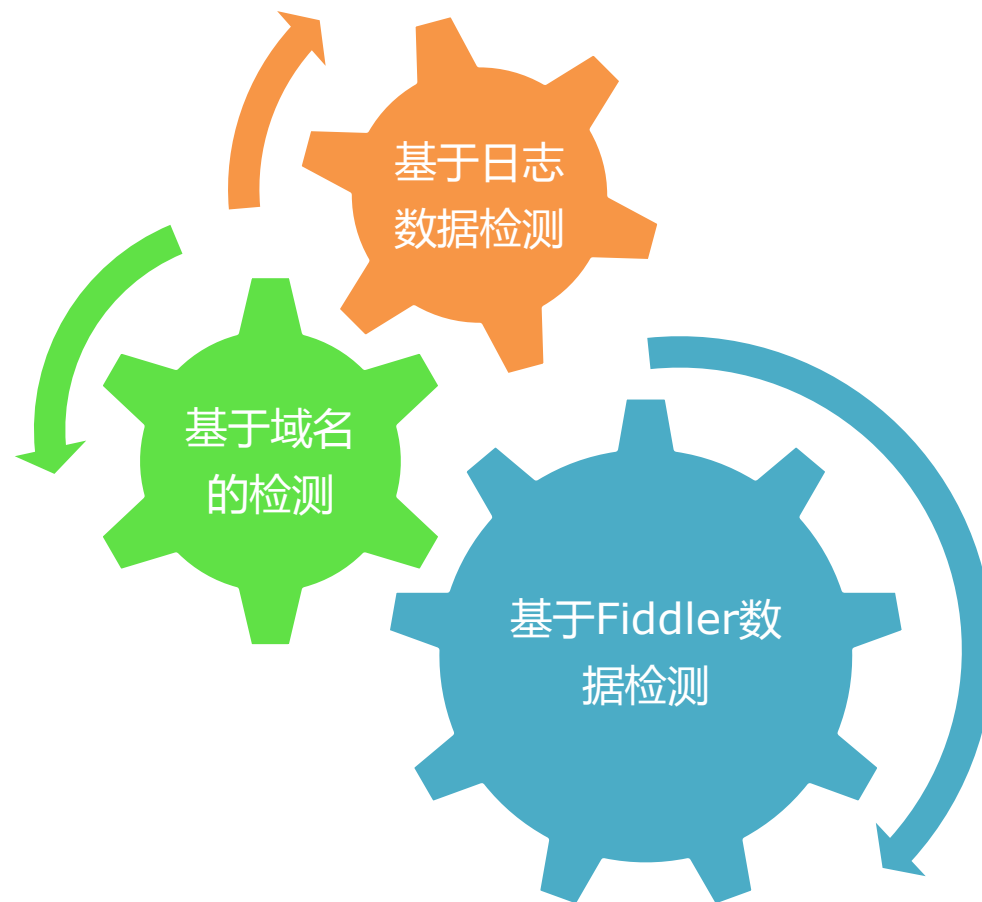
最简模式

扩展插件

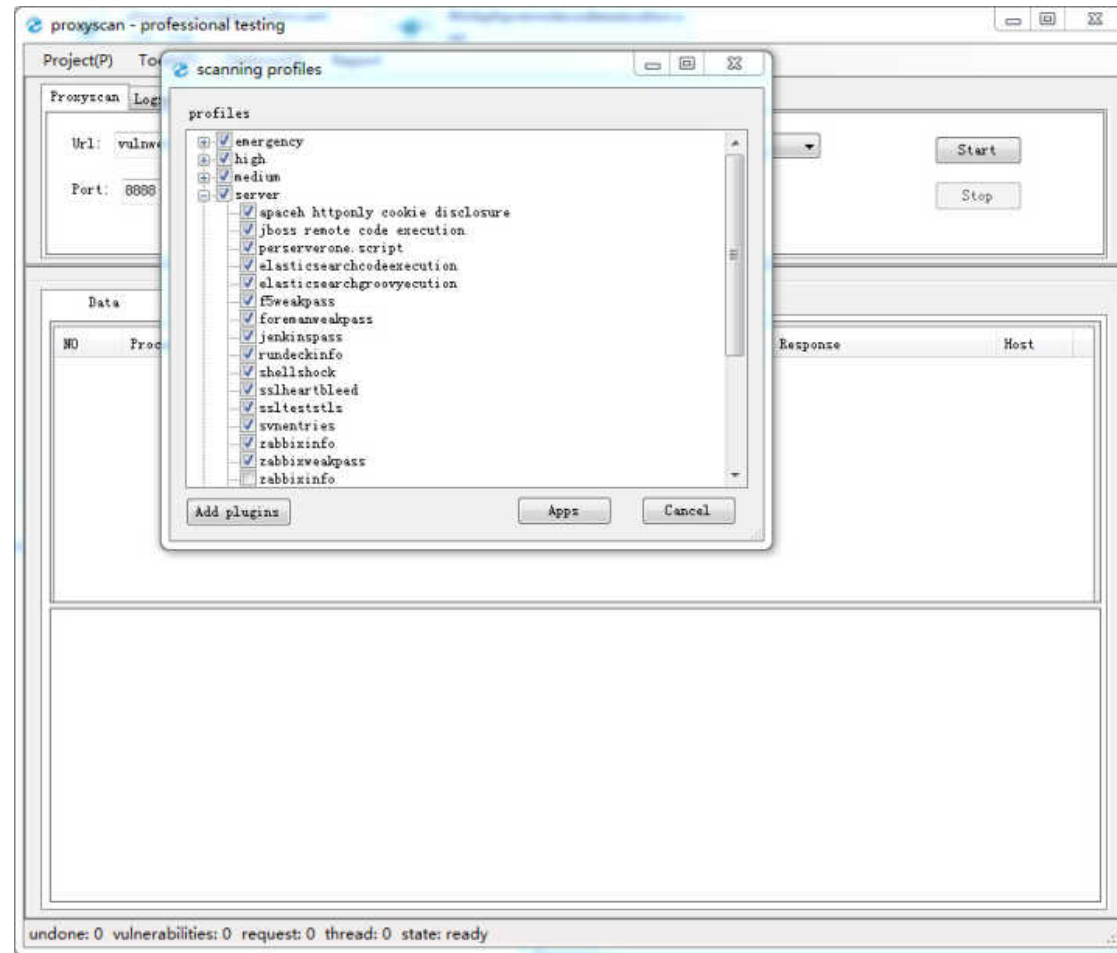
细分精准

自定义协议

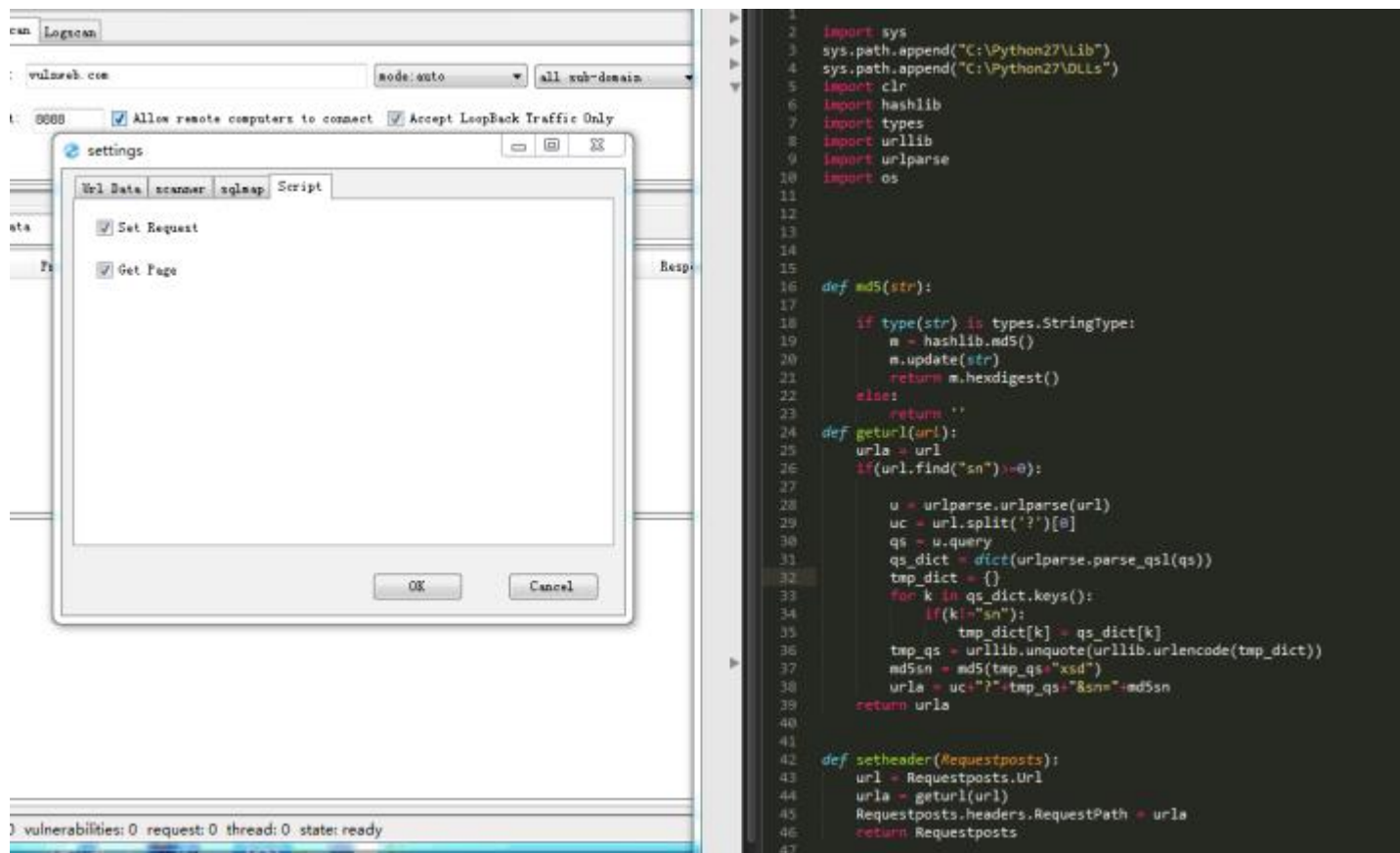
安全工具 – ProxyScan



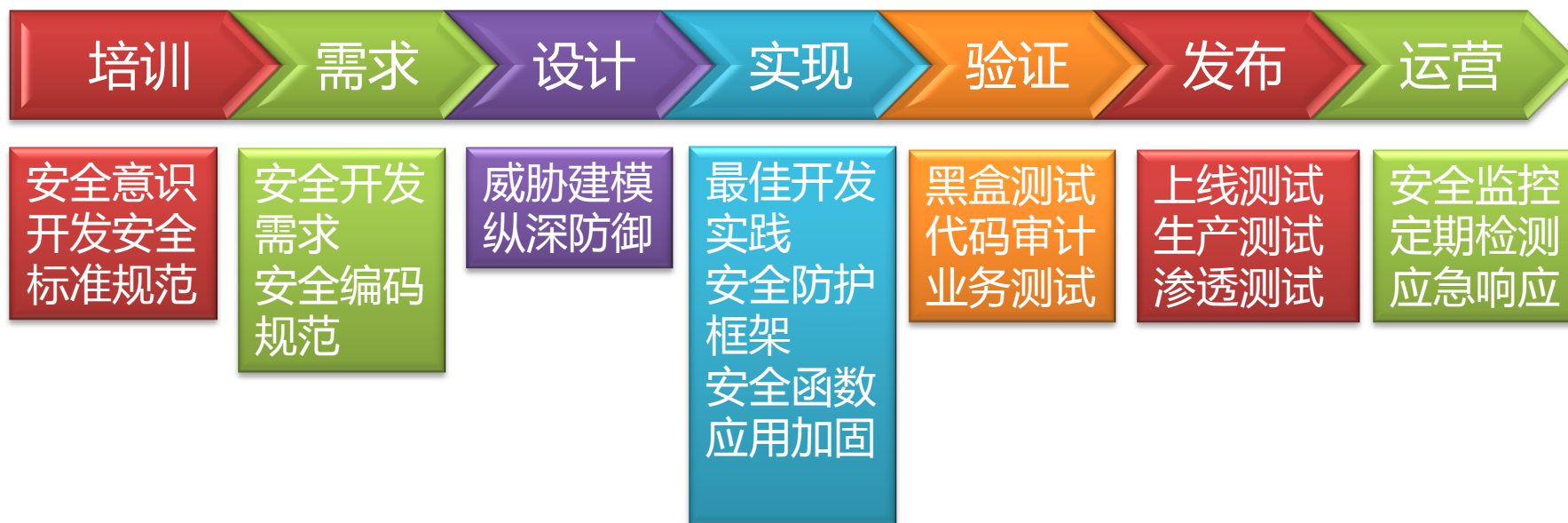
安全工具 – ProxyScan



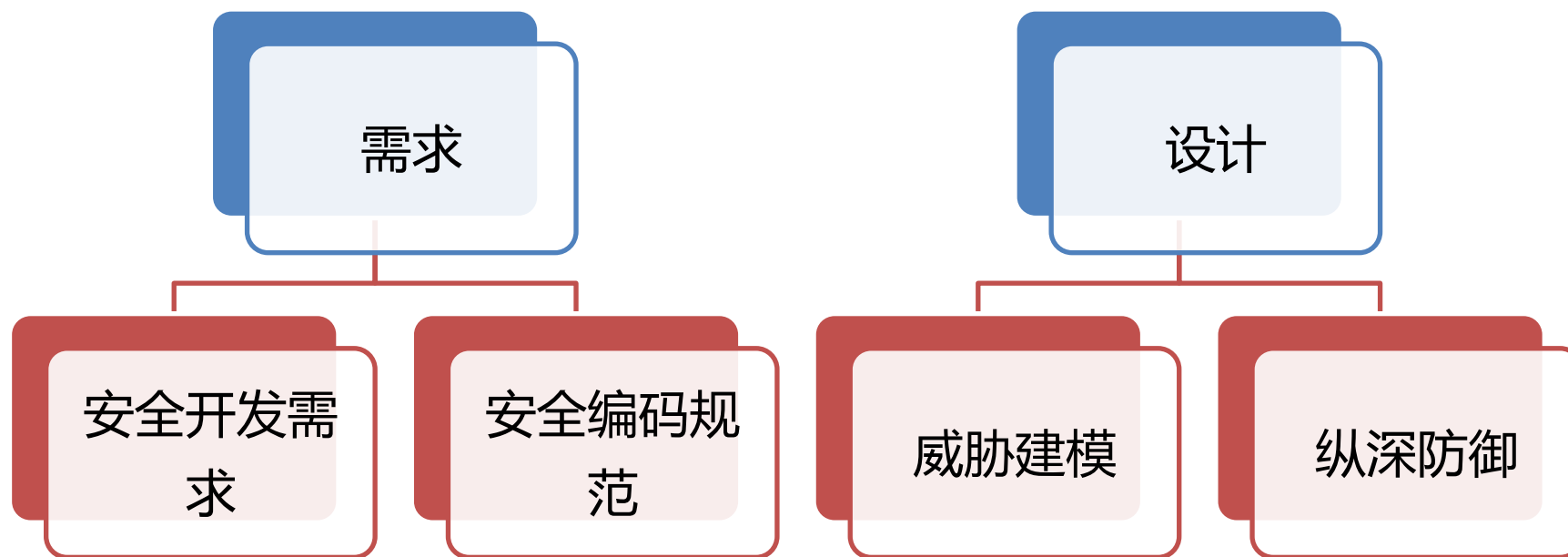
安全工具 – ProxyScan



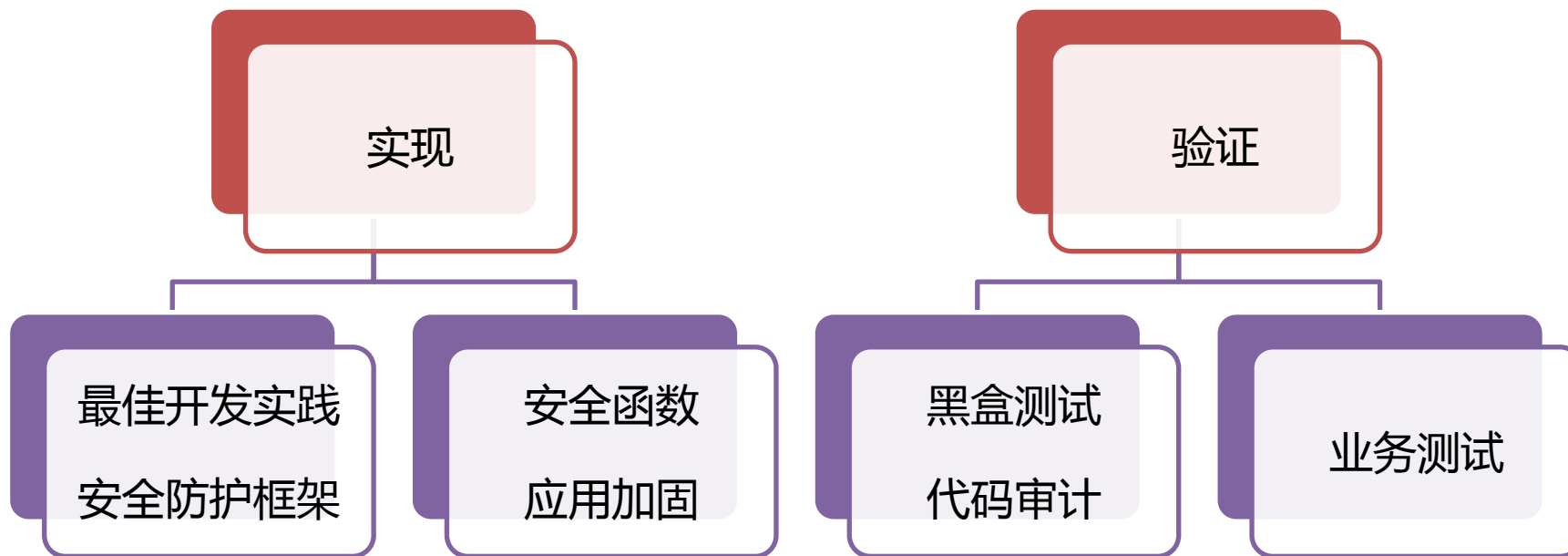
移动端产品最佳实践



移动端产品最佳实践



移动端产品最佳实践



移动端产品最佳实践

发布

上线测试

生产测试

渗透测试

运营

安全监控

定期检测

应急响应

议题总结

- 移动端产品安全保障
 - 数据安全
 - Acitvity组件安全、Webview代码执行漏洞、明文存储、模版交互、隐私数据、核心算法保护
 - 开发安全
 - 安全意识、环境和测试安全、第三方SDK安全开发
 - 业务及接口安全
 - 输入与输出、验证与授权、核心接口保护
 - 安全运维
 - 配置错误、匿名、弱口令
 - 安全工具
 - 漏洞智能检测
- 移动端产品最佳实践

移动端产品安全

谢谢观看！

