SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

CSDN
全球最大中文IT社区

安卓应用安全解析

Who am i

- 乌云漏洞报告平台核心白帽子

http://www.wooyun.org/whitehats/瘦蛟舞

- 乌云知识库资深作者

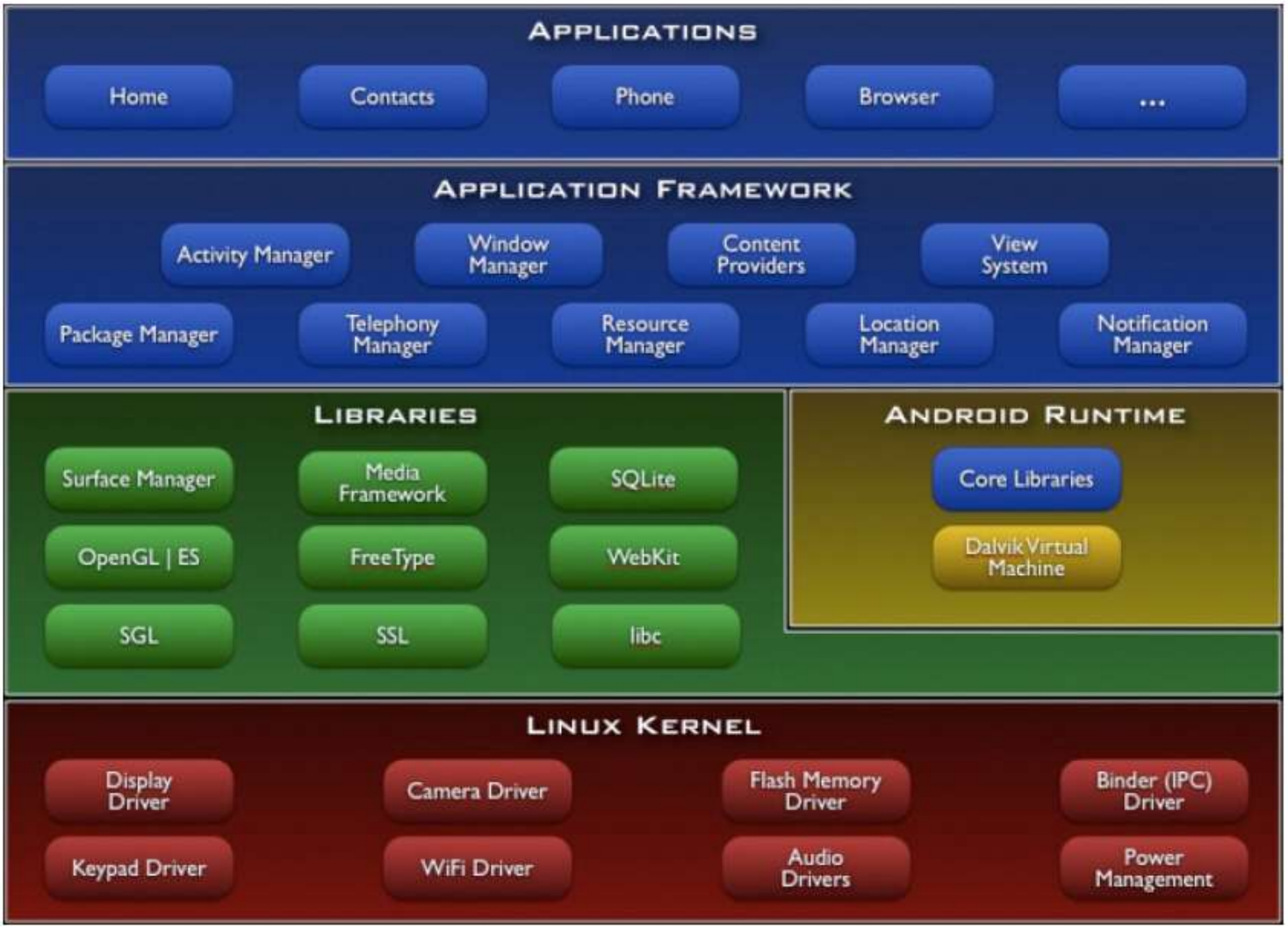
http://drops.wooyun.org/author/瘦蛟舞

- 互联网安全公司安全研究员

议题大纲

- 主流攻击手法
- 常见漏洞
- 乌云经典案例
- 安全开发小技巧
- 总结

Framework



Application Security

Device Security

SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

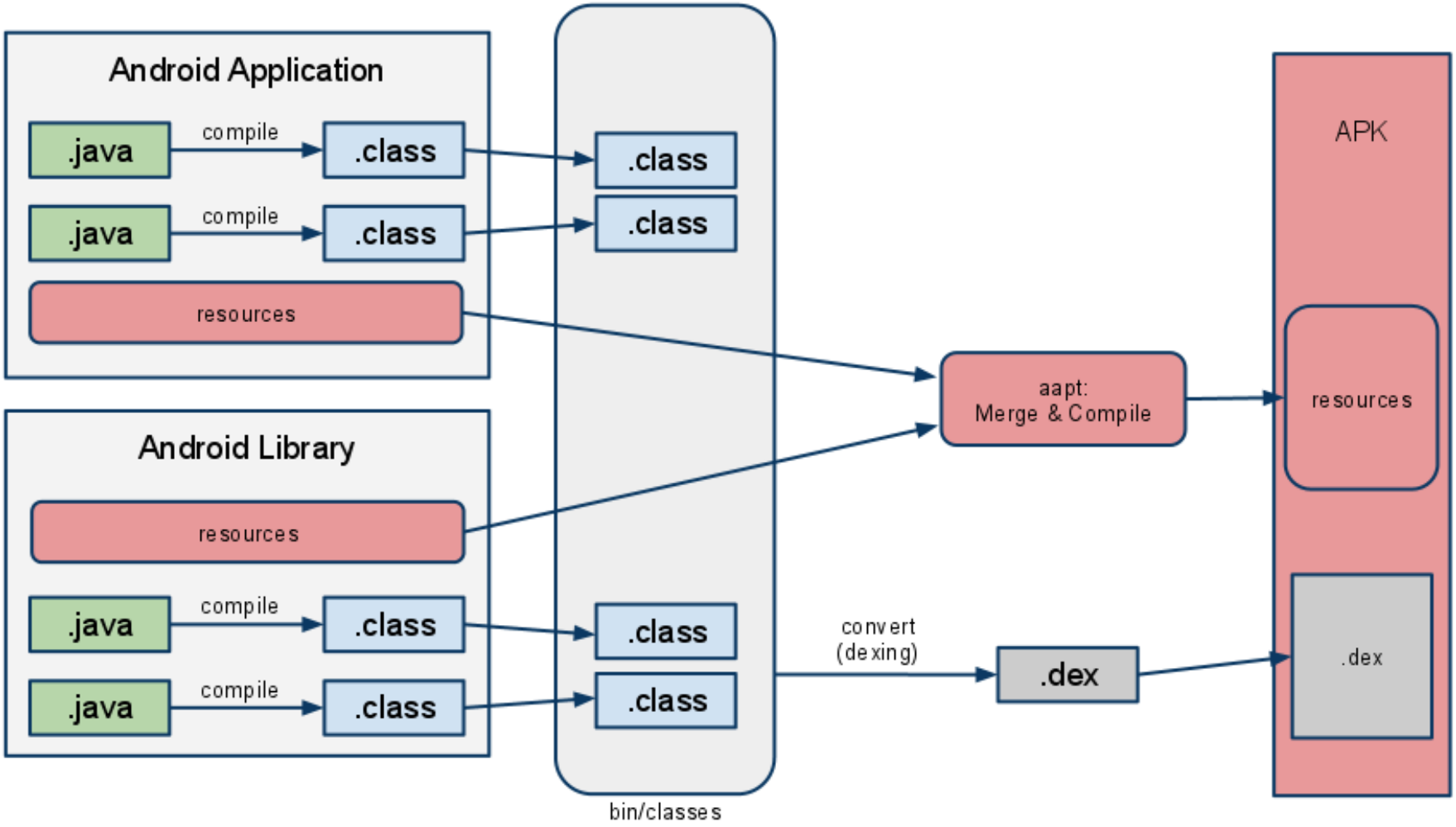
CSDN
全球最大中文IT社区

安卓平台主流攻击手法

Android平台下主流攻击手法

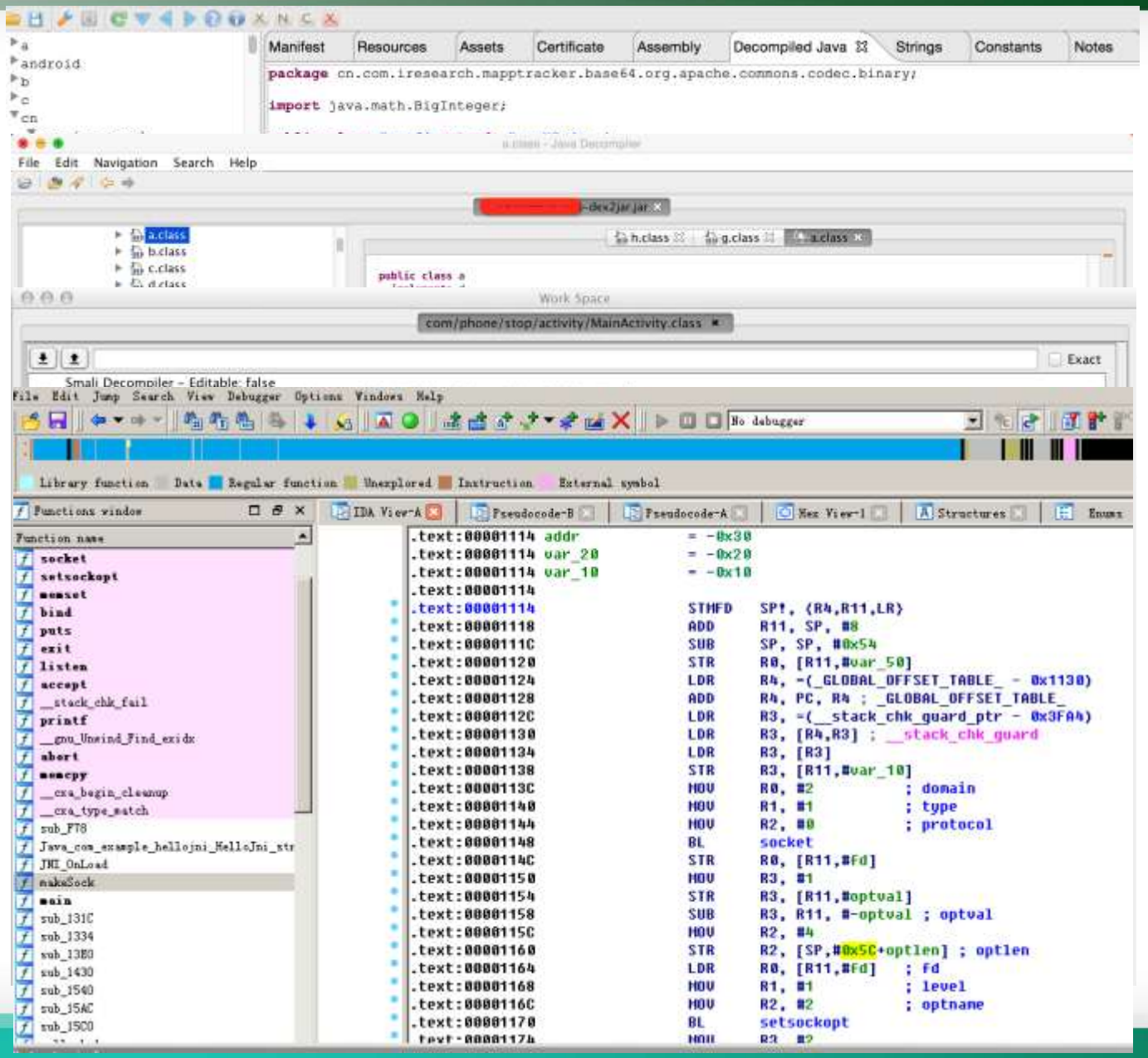
- 逆向反编译
- 代理抓包分析云端 API
- 无源码动态调试
- 插桩
- Hook

APK file

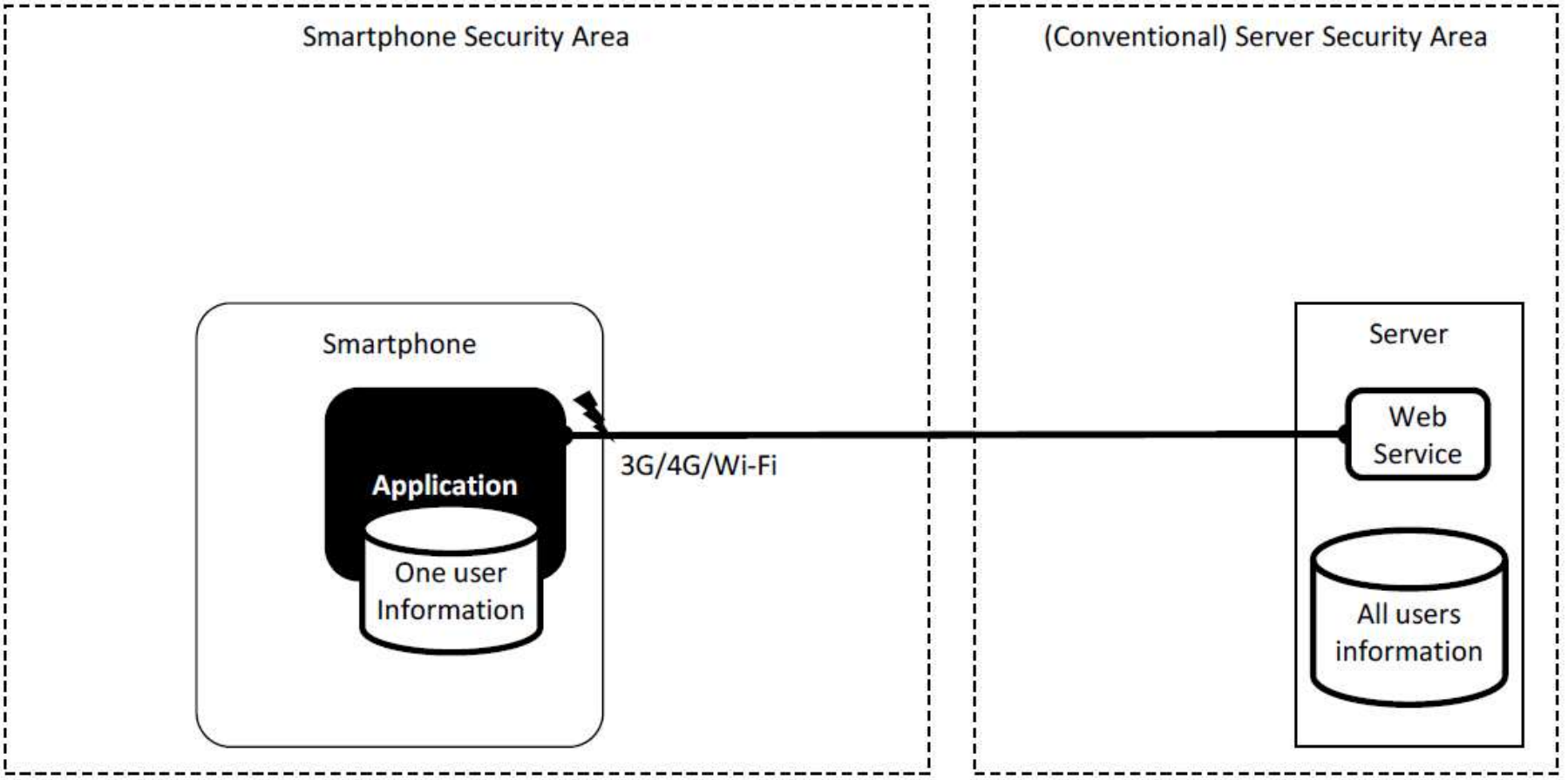

Android Application
.java
compile
.class
.java
compile
.class
resources
Android Library
resources
.java
compile
.class
.java
compile
.class
.class
.class
.class
.class
bin/classes
aapt:
Merge & Compile
convert
(dexing)
.dex
APK
resources
.dex

反编译

- Smali
- Dex2jar
- Jeb
- IDA
- Enjarify

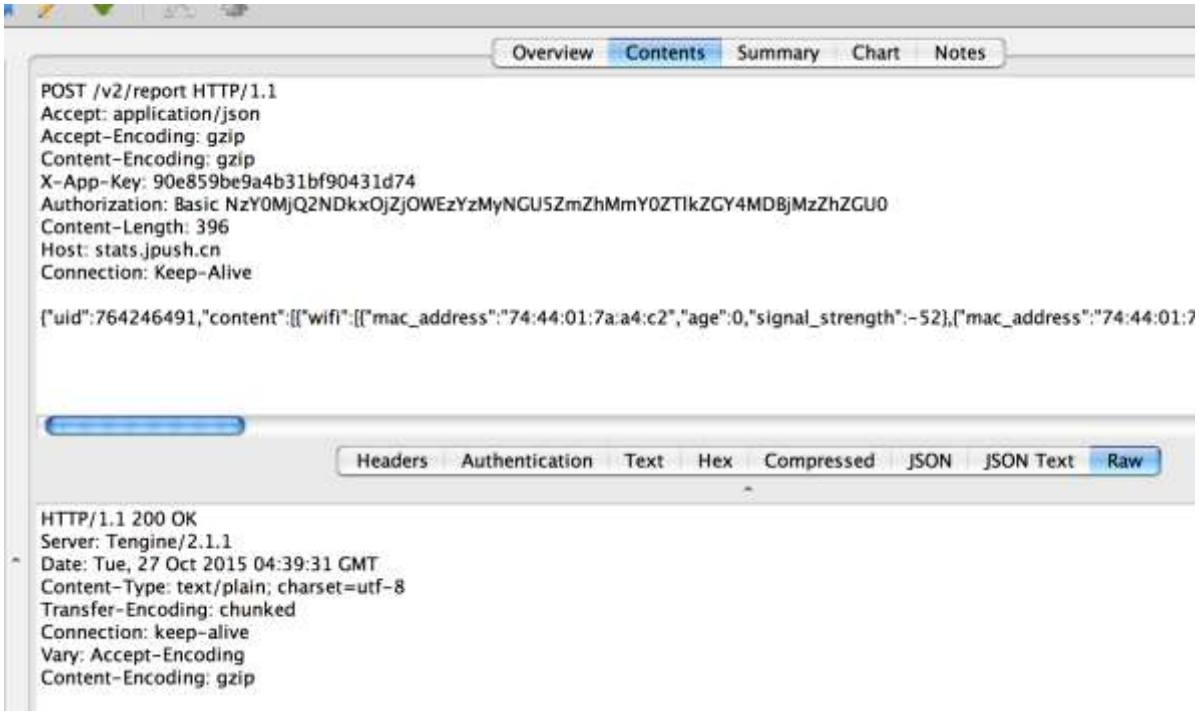


C/S


Smartphone Security Area
(Conventional) Server Security Area
Smartphone
Application
One user Information
3G/4G/Wi-Fi
Server
Web Service
All users information

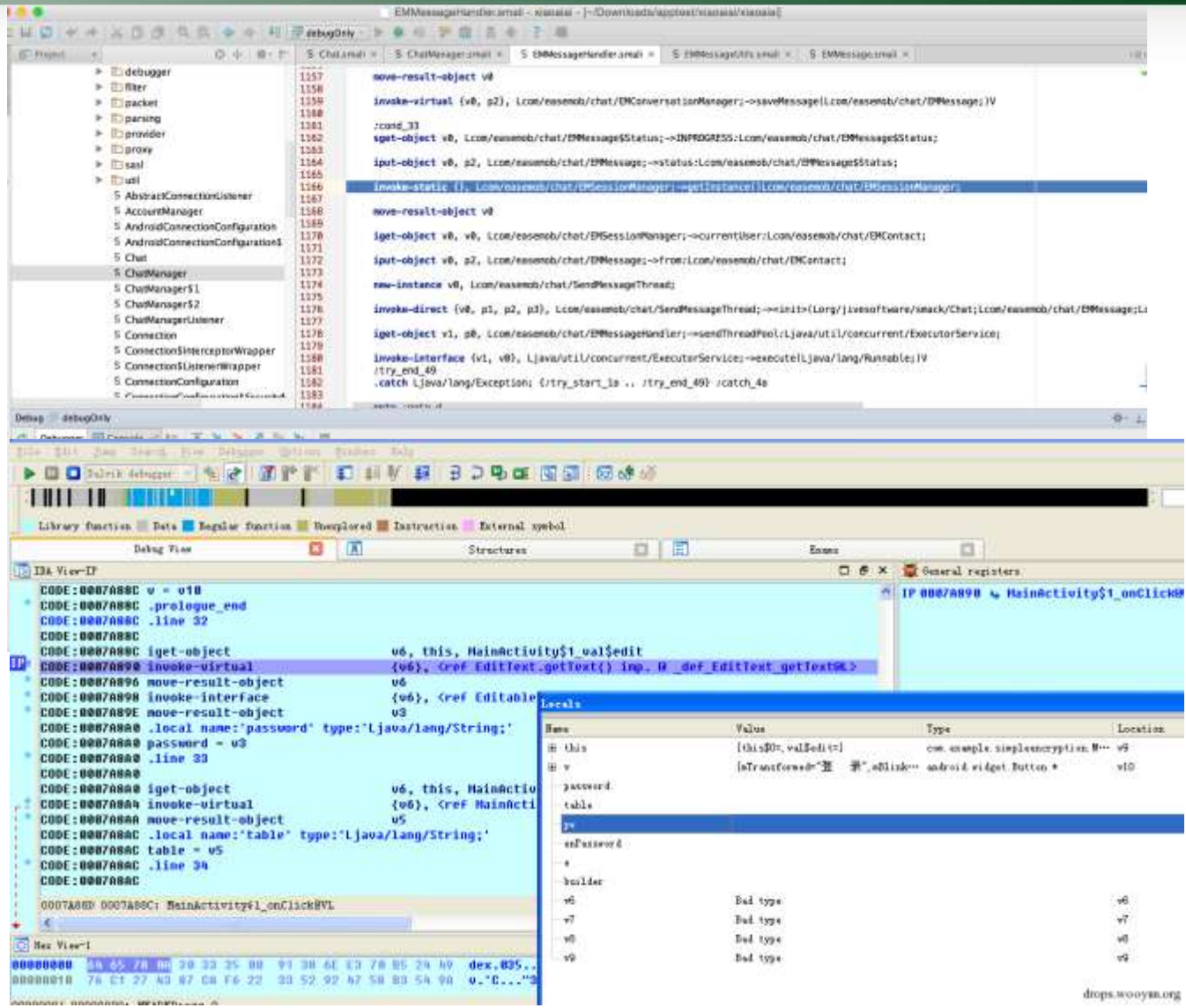
代理分析服务端 API

- ProxyDroid
- Charles
- BurpSuite
- WireShark



无源码调试

- Smalidea
- IDA
- Eclipse
- …



Hook

- Xposed
- Cydia
- ADBI

插桩

- smali 注入
- dalvik 插桩

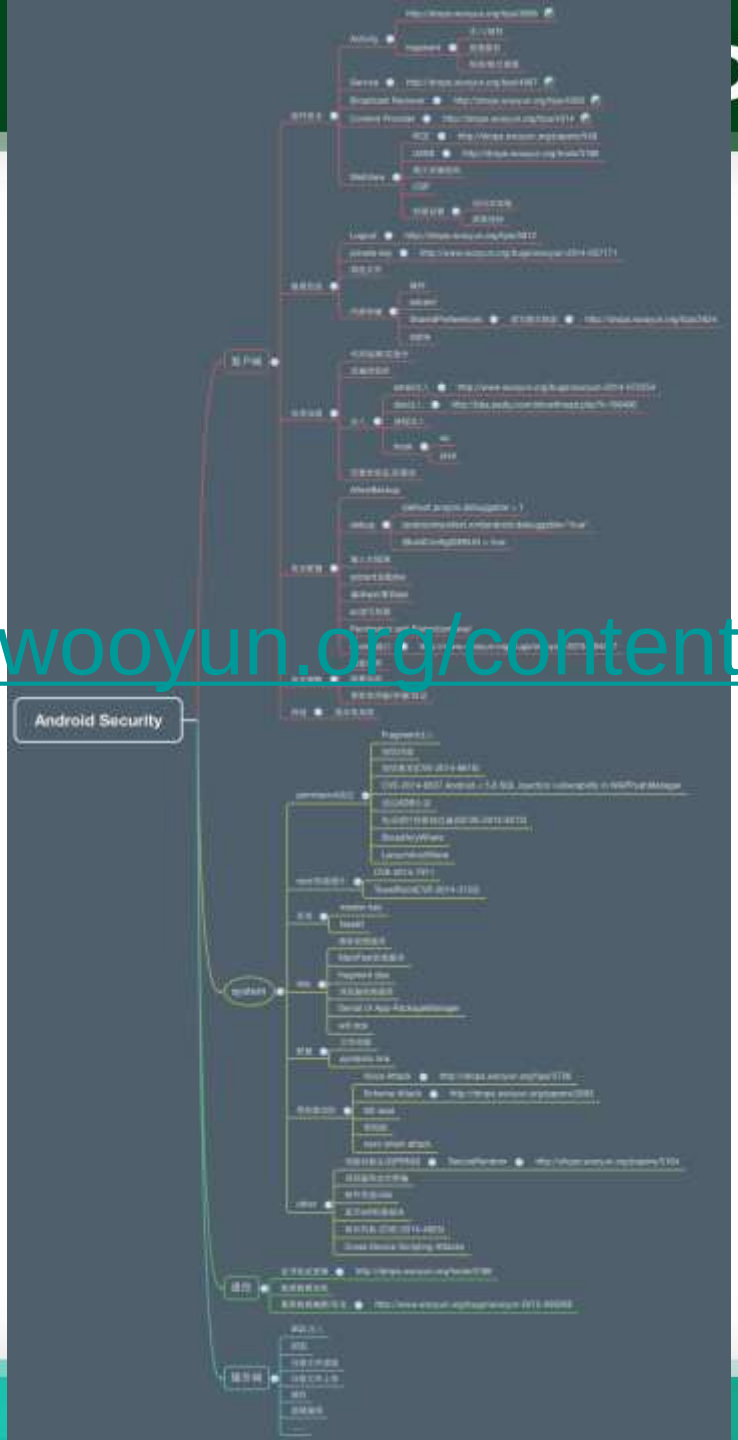
SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

CSDN
全球最大中文IT社区

安卓平台下应用常见漏洞

Attack surface

- 人祸
- 天灾
- http://zone.wooyun.org/content/19039



常见漏洞

- 权限泄露
- 信息泄露
- 组件安全
- ...
- http://wiki.wooyun.org/android:client

WEBVIEW漏洞

- RCE:http://drops.wooyun.org/webview.html
- UXSS:http://uxss.sinaapp.com/index.php

SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

CSDN
全球最大中文IT社区

乌云上安卓应用经典漏洞

如家酒店Android客户端程序支付漏洞

- http://
  2015

2.对于漏洞2，通过反编译App并且修改支付金额 漏洞可以利用

code 区域

```
public void onClick(View paramView)
    {
      if ((isAlipay) || (isHomeInnPay
      {
        if (paramView.getId() == 2131
          getActivity().getIntent().p
        while (true)
        {
          ((PaymentOperateActivity)ge
          return;
          getActivity().getIntent().p
        }
      }
      noSupportAlert.show();
    }
```

PPTV客户端批量刷会员漏洞

-

JsExternal.class | MD5.class | UUIDDatabaseHelper.class

```
}

public static void onCreate(SQLiteDatabase paramSQLiteDatabase)
{
  a(paramSQLiteDatabase);
}

public static void onUpgrade(SQLiteDatabase paramSQLiteDatabase, int paramInt1, int paramInt2)
{
}

public String getUUID()
{
  return getUUID(((TelephonyManager)this.b.getSystemService("phone")).getDeviceId());
}

// ERROR //
```

www.wooyun.org

百度某SDK设计缺陷导致手机敏感信息泄露

- 

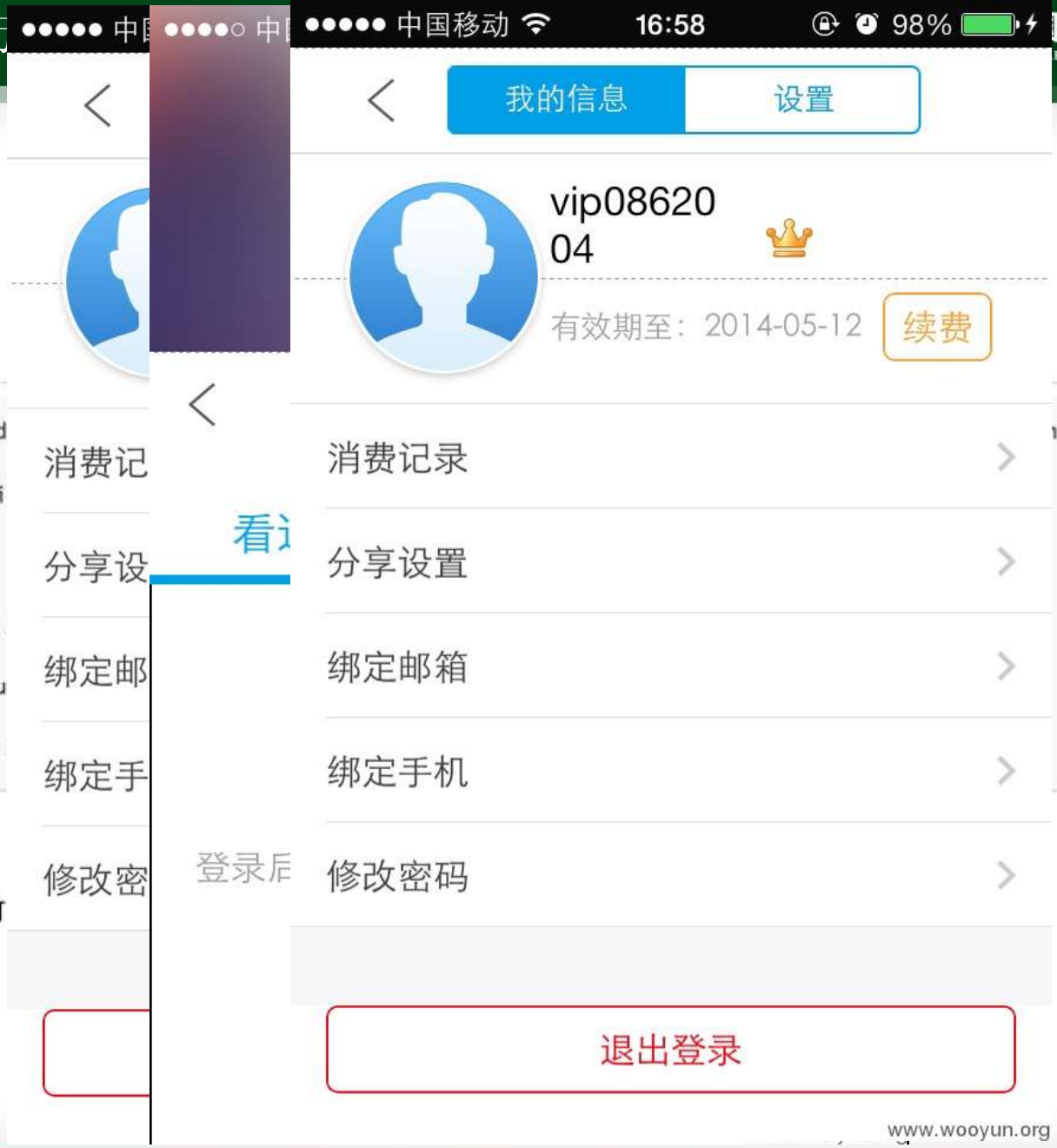
- 登录抓包吧

code 区域

```
GET /android
Host: dynami
Connection:
Accept-Langu
User-Agent:
```

```
=5.0 HTTP/1.1
```

修改任意uid即可



SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

CSDN
全球最大中文IT社区

安全开发小技巧

Tips

- 使用第三方安全框架
- 安全配置检测
- 小心使用第三方库/SDK/工具类
- 应用初期考虑安全设计
- 定制开发规范
- 系统漏洞规避

使用第三方安全框架

- sqlcipher
- secure-preferences

安全配置检测

- debug 开关
- proguard 使用
- export 属性
- API 选择
- Backup 属性

小心使用第三方库/SDK/工具类

- weiboSDK
- Android-PullTo
- Jpush

漏洞概要

缺陷编号： WooYun-2014-52339
漏洞标题： 新浪微博sdk设计缺陷可导致网络传输中窃取敏感信息
相关厂商： 新浪微博
漏洞作者： hqdvista

漏洞概要

缺陷编号： WooYun-2015-138620
漏洞标题： 极光推送错误实现可能导致某些安全风险
相关厂商： jpush.cn
漏洞作者： 么么哒
提交时间： 2015-09-02 15:37
公开时间： 2015-12-05 10:29
漏洞类型： 远程代码执行
危害等级： 低
自评Rank： 1
漏洞状态： 厂商已经确认
漏洞来源： http://www.wooyun.org
Tags标签： 无

应用初期考虑安全设计

- 传输协议
- 数据加密
- 签名效验

定制开发规范

- 测试代码移除logcat 移除
- 测试接口移除
- 最小权限原则
- Don‘t Copy without
- thinkOWASP_Mobile_Security

系统漏洞规避

- LanchAnywhere
- WebView RCE/UXSS
- BroadAnywhere
- master key
- 签名漏洞
- ...

总结

SDCC
中国软件开发者大会
SOFTWARE DEVELOPER CONFERENCE CHINA

CSDN
全球最大中文IT社区

THE END

THANK YOU

sdcc.csdn.net