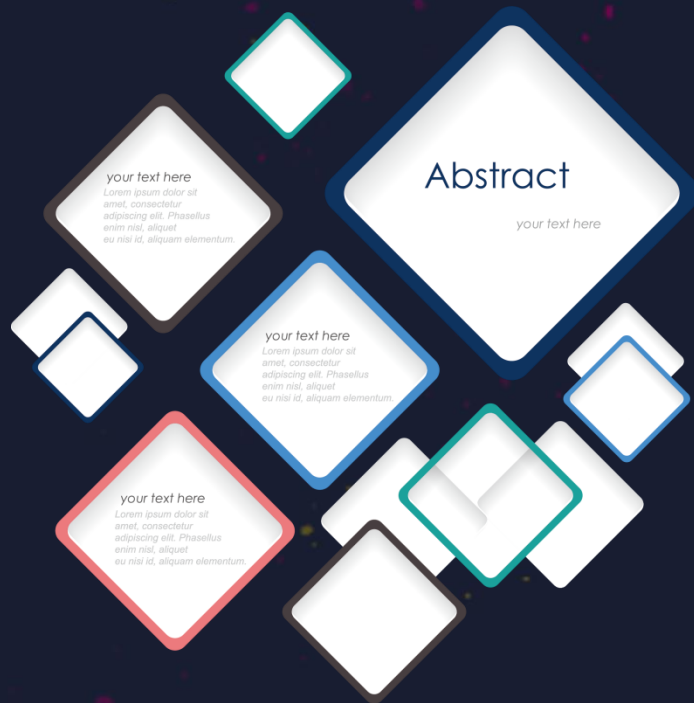


隐私合规测试实践



沈海涛
OPPO子午互联网安全
实验室负责人



目录

CONTENTS



1

背景

2

技术需求分析

3

方案优化演进

4

Q&A



01

章节

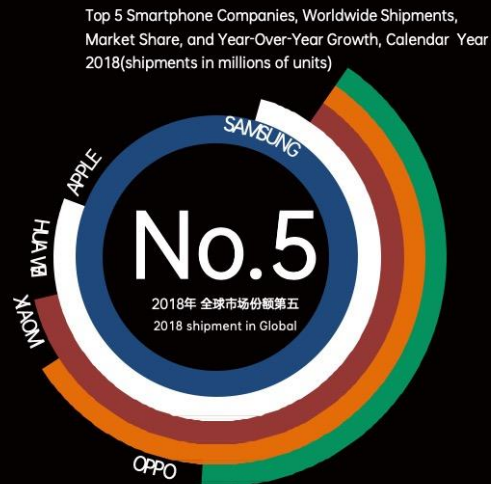
PART

背景





Source: 《IDC中国季度手机市场跟踪报告.2018年第四季度》



Source: IDC Quarterly Mobile Phone Tracker, January 30, 2019

2018年，OPPO取得中国市场份额第2，世界市场份额第5
In 2018, OPPO's shipment in China ranked No.2 and its shipment in the world No.5

背景-业务

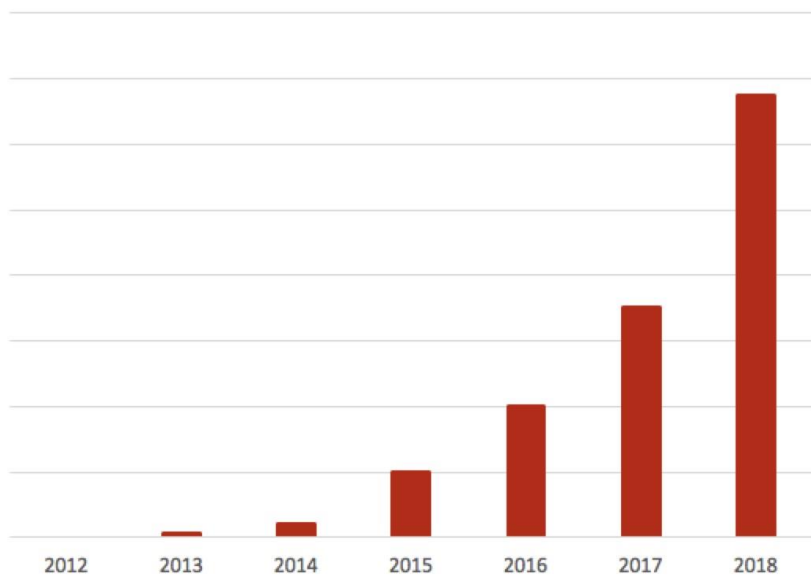
oppo

手机销往全球**30+**国家和地区

Color OS全球月活用户数**3.1亿**



互联网业务增长趋势



背景-法律法规

一、《欧盟GDPR》

-堪称史上最严格的数据保护条例-

最高处以2千万欧元或上年度全球营业额4%的行政处罚

Google受罚首例。2019年1月，法国数据保护机构CNIL宣布，对Google处以5000万欧元(约合5700万美元)的罚款。机构称，在用户使用Android手机时，Google未能遵守欧盟隐私法——《通用数据保护条例》（GDPR）。Google没有向用户正确披露获取数据的目的、数据的储存期以及哪些数据用于个性化广告等。例如，用户想知道他们的数据如何用于个性化广告，一般需要5或6次点击。CNIL表示，通常很难理解你的数据是如何被使用的，因为谷歌的措辞是广泛而且模糊不清的。



背景-法律法规

二、《中华人民共和国网络安全法》&《个人信息安全规范》

-《个人信息安全规范》-中国版的GDPR-

虽然《个人信息安全规范》性质上为推荐性国家标准，不具有强制执行力，但作为《网络安全法》等法律法规的配套技术规范，对于行政主体、司法机关和企业都具有普遍的适用性。《个人信息安全规范》本身只设定适用条件和行为模式，并未设定相应的行为后果，但该规范将是行政主体和司法机关判断事实和构成要件的依据，如果违反其中体现《网络安全法》等法律关于个人信息保护的强制性要求的，行政主体和法院可以依据相关法律设定的行为后果作出处罚和判决，企业可能承担相应的民事、行政和刑事责任。

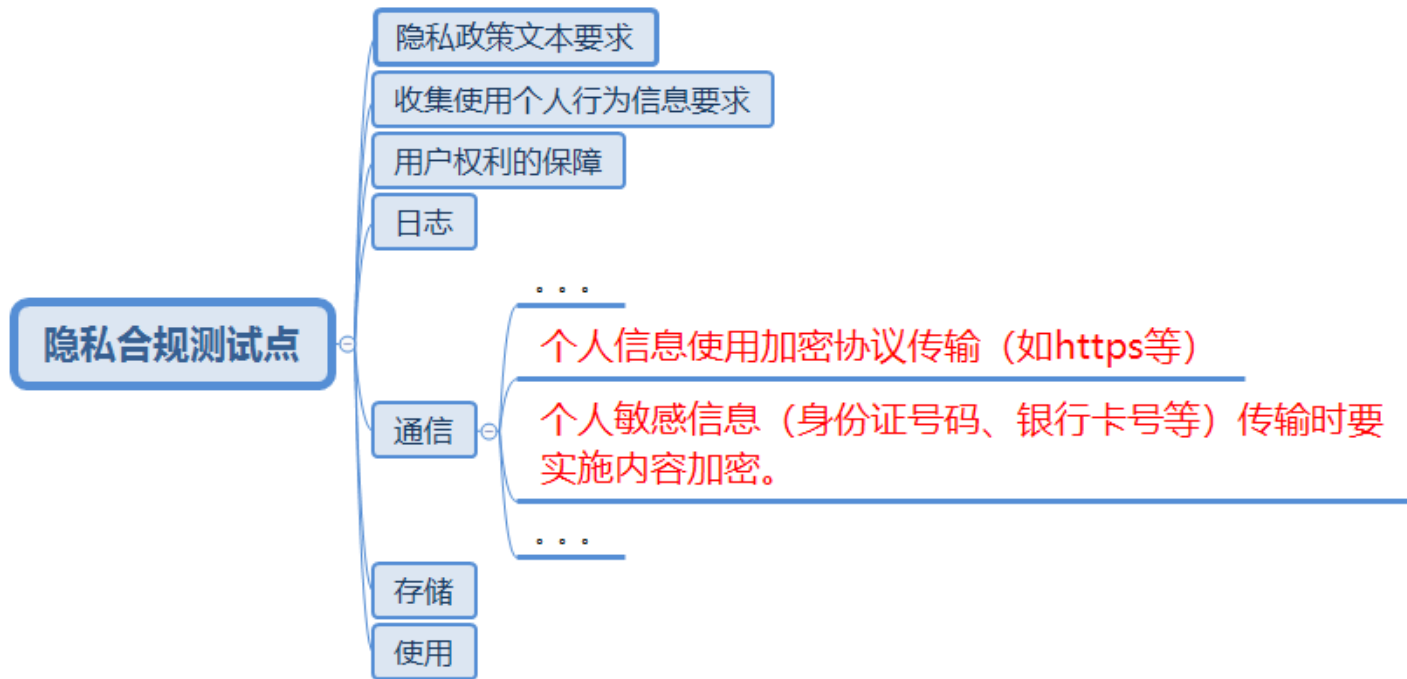


02

章节

PART

技术需求分析



需求点

oppo

能够分析SSL/TLS
加密流量

能够识别流量中的
个人敏感数据



现状分析

oppo

手机：最新出货版本

权限：adb root

系统：android 9

权限：修改系统文件难度较大



技术方案选型

oppo

手机安装代理证书抓包

Xposed + TrustTrustMe

Frida + bypass.js + Burp





03

章节

PART

方案优化演进

Round 1

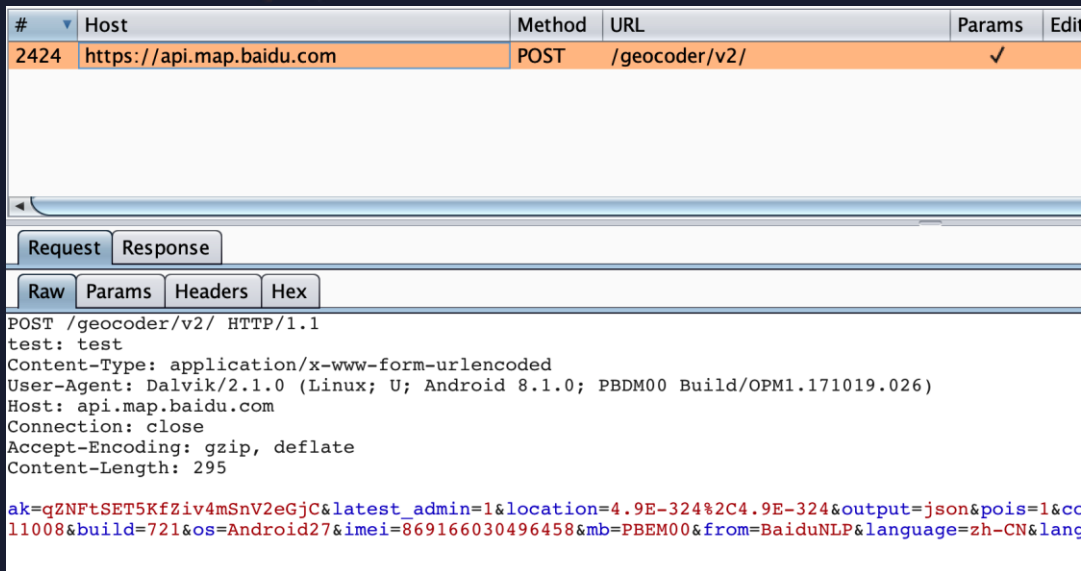
oppo



Frida bypass 脚本

<https://codeshare.frida.re/browse>

针对具体情况可能要有一些定制
原则是尽量hook系统底层



Round 2

oppo

开发：我不走系统代理，看你怎么抓包

URLConnection:

```
URL url = new URL(urlStr);  
URLConnection = (URLConnection) url.openConnection(Proxy.NO_PROXY);
```

OkHttp:

```
OkHttpClient client =  
    new OkHttpClient().newBuilder().proxy(Proxy.NO_PROXY).build ();
```



Round 2

oppo

攻防：我有hook大法，想抓就抓

```
try {
    var URL = Java.use("java.net.URL");
    URL.openConnection().overload('java.net.Proxy').implementation = function() {
        return this.openConnection();
    }
} catch(e) {
    console.log("" + e);
}

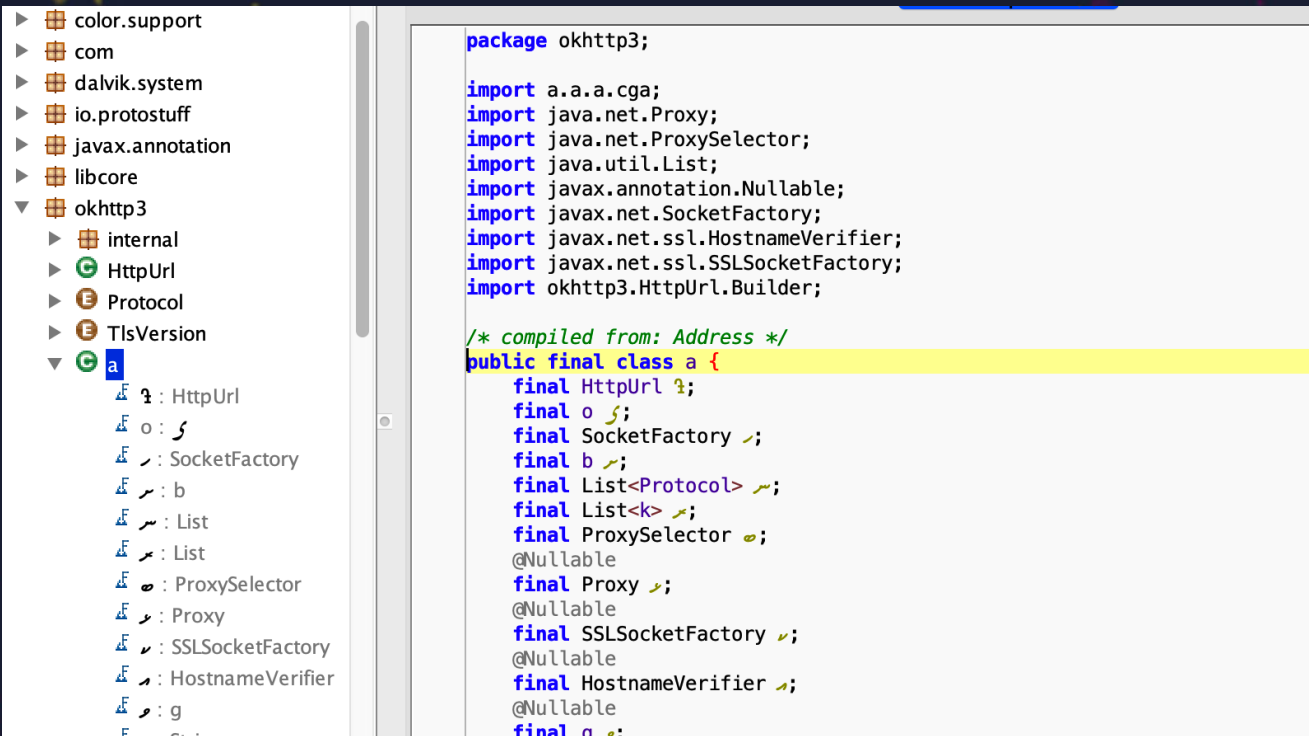
try {
    var Builder = Java.use("okhttp3.OkHttpClient$Builder");
    var mybuilder = Builder.$new();
    Builder.proxy().overload('java.net.Proxy').implementation = function(arg1) {
        return mybuilder;
    }
} catch(e) {
    console.log("" + e);
}
```



Round 3

oppo

开发：让你找不到hook的点，且每次变，看你咋办



Round 3

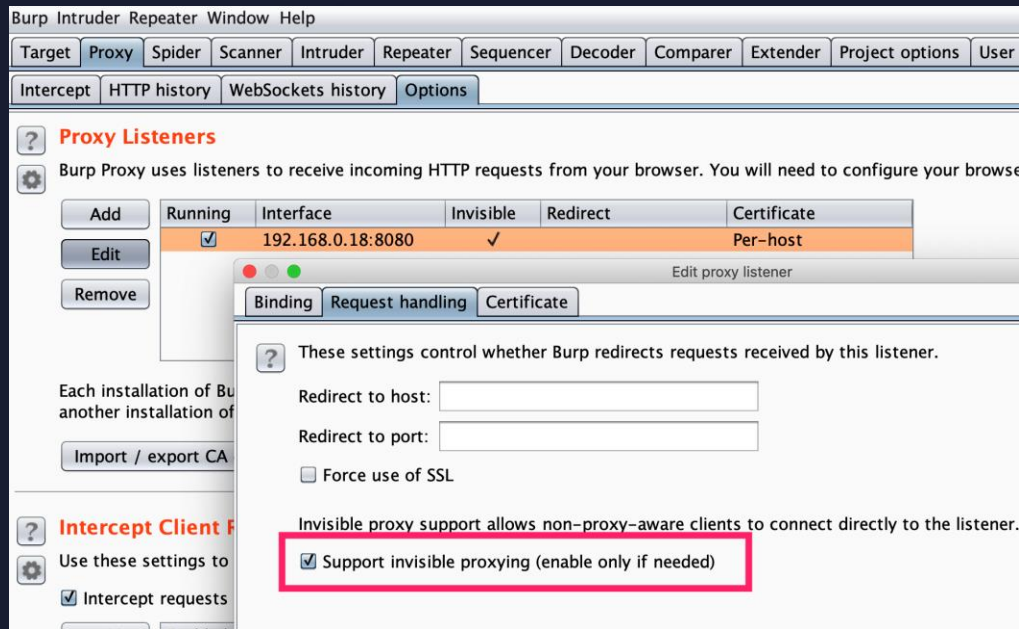
oppo

攻防：看来只能降维打击了

使用 iptables 转发应用流量：

`iptables -t nat -A OUTPUT -p tcp -m owner --uid-owner 应用uid -j DNAT --to-destination ip:端口`

同时需要设置 burp 透明代理



Round 4



开发：哎呦，不错哦。那我们走 TCP/UDP 吧

```
Socket s = new Socket("192.168.0.8", 12345);
OutputStream out = s.getOutputStream();
PrintWriter output = new PrintWriter(out, true);
output.println("Hello IdeasAndroid tcp!");
BufferedReader input = new BufferedReader(
    new InputStreamReader(s.getInputStream()))
);
final String message = input.readLine();
```




```
String message = "Hello IdeasAndroid udp!";
int server_port = 12345;
DatagramSocket s = null;
try {
    s = new DatagramSocket();
} catch (SocketException e) {
    e.printStackTrace();
}
InetAddress address = null;
try {
    address = InetAddress.getByName("192.168.0.8");
} catch (UnknownHostException e) {
    e.printStackTrace();
}
int msg_length = message.length();
byte[] messageByte = message.getBytes();
DatagramPacket p = new DatagramPacket(messageByte, msg_length, address, server_port);
try {
    s.send(p);
} catch (IOException e) {
    e.printStackTrace();
}
```

Round 4

oppo

攻防：还真的有点难住我了。。。

嗯，burp 抓不到，直接 Frida hook 打印出来好啦。



```
[*] Intercepting on ddns.android.netcapture (pid:23245)...  
[-] OpenSSLSocketImpl pinner not found  
org.conscrypt.Platform not found!  
com.android.org.conscrypt.NativeSsl not found!  
org.conscrypt.NativeSsl not found!  
Hello IdeasAndroid tcp!
```

```
udp data:
```

```
Hello IdeasAndroid udp!
```

Round 5

oppo

开发：换个思路，流量任你抓吧，让你看不懂总行了吧

```
POST /update/v3/check HTTP/1.1
host: i[REDACTED]m
sign: 7455120284fb14603072f4312efcl2e9
Accept: application/x-protobuf; charset=UTF-8
Content-Type: application/x-protobuf; charset=UTF-8
Content-Length: 5148
Connection: close
Accept-Encoding: gzip, deflate

O
&gggggggggwgwgc[REDACTED]core [REDACTED]
[REDACTED] (/com.[REDACTED].UpgradeRequygfs
G
com.[REDACTED]sync [REDACTED] (*com.[REDACTED].dto.UpgradeReq1
K
com.android.browser [REDACTED] ([REDACTED])com.[REDACTED].UpgradeReq
K
com.android.calendar [REDACTED] ([REDACTED])com.[REDACTED].UpgradeReq
L
com.[REDACTED].thespace [REDACTED] ([REDACTED])com.[REDACTED].UpgradeReq
P
com.[REDACTED].rom [REDACTED]
([REDACTED])com.[REDACTED].UpgradeReq
S
```

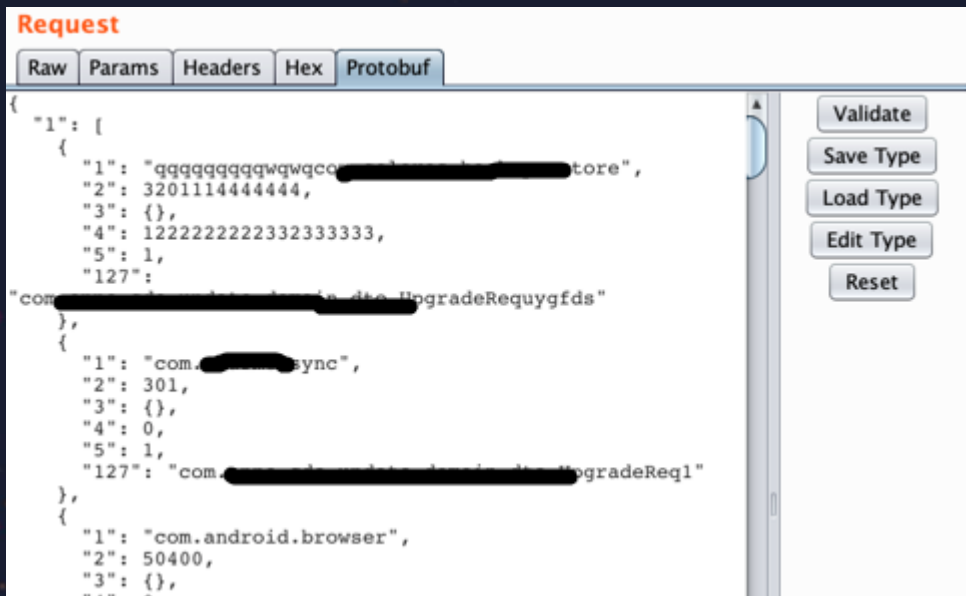


Round 5

oppo

Protobuf 是 google 开源的一种平台无关、语言无关、可扩展且轻便高效的序列化数据结构的协议，可以用于网络通信和数据存储。其具有体积小、序列化和传输速度快、维护简单的特点，被越来越多的安卓 APP 使用。

Burp插件：<https://github.com/nccgroup/blackboxprotobuf>



Round 6



开发：真是拿你没办法，埋个坑送给你。

于是开发将不同出货区域、不同定制版集成到了同一个 app 中。

意味着：不同的环境会触发不同的代码分支，可能会携带不同的数据请求不同的域名。进行隐私合规测试的时候，需要模拟大量的环境，且不能保证没有遗漏。

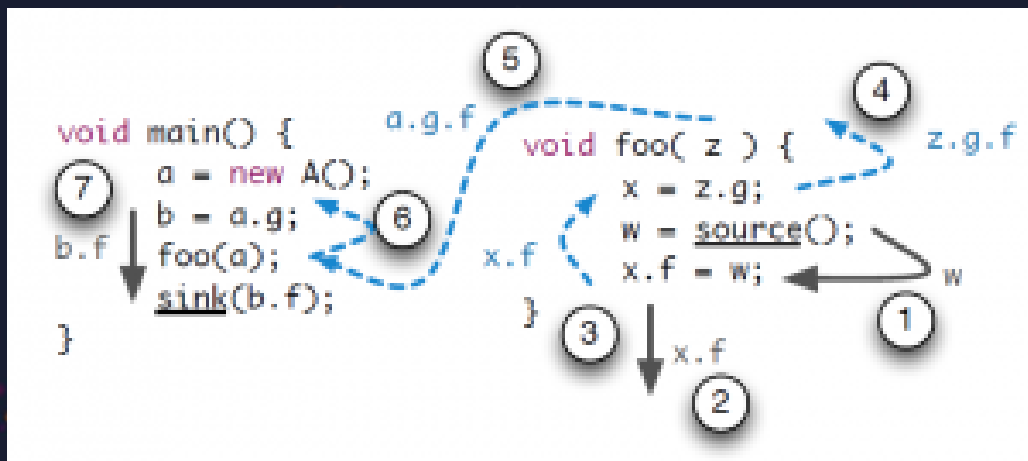


Round 6

oppo

攻防：嗯，干得漂亮。。。

不过，我们还有一招：基于污点的静态分析。



Round 6

oppo

```
String imei = telephonyManager.getDeviceId();

switch (areaType) {
    case CHINA:
        Log.d(tag: "neixiao_log", imei);
        break;
    case INDIA:
        Log.d(tag: "waixiao_log", imei);
        break;
    case FRANCE:
        Log.d(tag: "gdpr_log", imei);
        break;
}
```

Path0:

```
-> <ddns.android.privacytest.MainActivity: void onCreate(android.os.Bundle)>
    -> $r6 = virtualinvoke $r3.<android.telephony.TelephonyManager: java.lang.String getDeviceId()>()
-> <ddns.android.privacytest.MainActivity: void onCreate(android.os.Bundle)>
    -> staticinvoke <android.util.Log: int d(java.lang.String, java.lang.String)>("gdpr_log", $r6)
```

Path1:

```
-> <ddns.android.privacytest.MainActivity: void onCreate(android.os.Bundle)>
    -> $r6 = virtualinvoke $r3.<android.telephony.TelephonyManager: java.lang.String getDeviceId()>()
-> <ddns.android.privacytest.MainActivity: void onCreate(android.os.Bundle)>
    -> staticinvoke <android.util.Log: int d(java.lang.String, java.lang.String)>("waixiao_log", $r6)
```

Path2:

```
-> <ddns.android.privacytest.MainActivity: void onCreate(android.os.Bundle)>
    -> $r6 = virtualinvoke $r3.<android.telephony.TelephonyManager: java.lang.String getDeviceId()>()
-> <ddns.android.privacytest.MainActivity: void onCreate(android.os.Bundle)>
    -> staticinvoke <android.util.Log: int d(java.lang.String, java.lang.String)>("neixiao_log", $r6)
```



更多优化 - 效率

oppo

	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
k.earme.com...	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php				223
k.earme.com...	POST	/index.php?q=index/subfeed	✓		200	447	JSON	php		13330994619 13252054003		223
pp.earme.com	GET	/generate_204			204	323						14.7
du.com	POST	/			302	1212	HTML					14.7
ers.google.cn	GET	/generate_204			204	102						203
k.earme.com...	GET	/index.php?q=index/feedbacktype	✓		200	504	JSON	php				223
k.earme.com...	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php				223
k.earme.com...	GET	/index.php?q=index/comquedetail&ci...	✓		200	2182	JSON	php				223
.baidu.com	POST	/statloc	✓		200	159	JSON					163
p.baidu.com	POST	/geocoder/v2/	✓		200	5301	script			001003289013420	✓	163
k.earme.com...	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php				223
k.earme.com...	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php				223
k.earme.com...	GET	/index.html			200	11024	HTML	html				223
k.earme.com...	GET	/index.html			200	11024	HTML	html				223
ou.com	POST	/q	✓		404	184	HTML					111
.finz.earme.com...	POST	/api/pin/v1/reset-pin	✓		200	719	JSON			001003289013420	✓	223
p.baidu.com	POST	/sdk.php	✓		200	540	text	php			✓	163
p.baidu.com	POST	/sdk.php	✓		200	540	text	php			✓	163
.finz.earme.com...	POST	/api/pin/v1/rule-check	✓		200	738	JSON			001003289013420	✓	223
p.baidu.com	POST	/sdk.php	✓		200	540	text	php			✓	163
p.baidu.com	POST	/sdk.php	✓		200	540	text	php			✓	163
.com	POST	/			302	366	HTML		30...			183
pp.earme.com	GET	/generate_204			204	325						14.7
ogle.cn	GET	/generate_204			204	102						203
.baidu.com	POST	/statloc	✓		200	159	JSON					163
.finz.earme.com...	GET	/favicon.ico			404	747	HTML	ico	40...		✓	223
.finz.earme.com...	GET	/static/icon_remove.png			200	2376	PNG	png			✓	223
.finz.earme.com...	GET	/static/shouqi.png			200	755	PNG	png			✓	223
.finz.earme.com...	GET	/static/js/views/resetPassAuth.39a56...			200	29582	script	js			✓	223
.finz.earme.com...	GET	/views/resetPassAuth.html?target=_bl...	✓		200	2591	HTML	html	ã¿...	001003289013420	✓	223
.finz.earme.com...	GET	/generate_204			204	203				001003289013420		121
.finz.earme.com...	POST	/api/auth/identify/v1/four-element	✓		200	1500	JSON			æ ñè¼*ã¼ 13330994619 001003289013420	✓	223
p.baidu.com	POST	/sdk.php	✓		200	540	text	php			✓	163

更多优化 - 覆盖率

oppo

静态污点分析:

Source不仅要覆盖系统函数 (IMEI、GPS、电话号码等), 还要覆盖用户输入的信息 (身份证号码、地址等)。

Sink要尽可能的覆盖全, 如日志打印、各种网络请求库。

A screenshot of the OPPO login interface. At the top, the status bar shows the time 12:17 and various icons. The page title is "OPPO 帐号". Below it is a large input field labeled "手机号码/邮箱地址" with a green border. Underneath is a password input field labeled "请输入密码" with a toggle icon. A "登录" button is centered below the password field. At the bottom, there are links for "忘记密码" and "新用户注册". A Google Assistant suggestion bar is visible at the very bottom, showing a search bar and a keyboard.

04

章节

PART

Q&A

子午互联网安全实验室

oppo

专注于隐私保护、IoT安全、红
蓝对抗等领域的安全技术研究。



OGeek

oppo

OGeek

2019网络安全挑战赛



—谢谢—



Abstract

your text here

your text here
Lorem ipsum dolor sit
amet, consectetur
adipiscing elit. Phasellus
enim nisi, aliquet
eu nisi id, aliquam elementum.

your text here
Lorem ipsum dolor sit
amet, consectetur
adipiscing elit. Phasellus
enim nisi, aliquet
eu nisi id, aliquam elementum.

your text here
Lorem ipsum dolor sit
amet, consectetur
adipiscing elit. Phasellus
enim nisi, aliquet
eu nisi id, aliquam elementum.