Android应用安全开发

OWASP 中国

The Open Web Application Security Project

About Me

OWASP 中国
The Open Web Application Security Project

- 沈明星
- 网易安全专家

网易 NETEASE
www.163.com

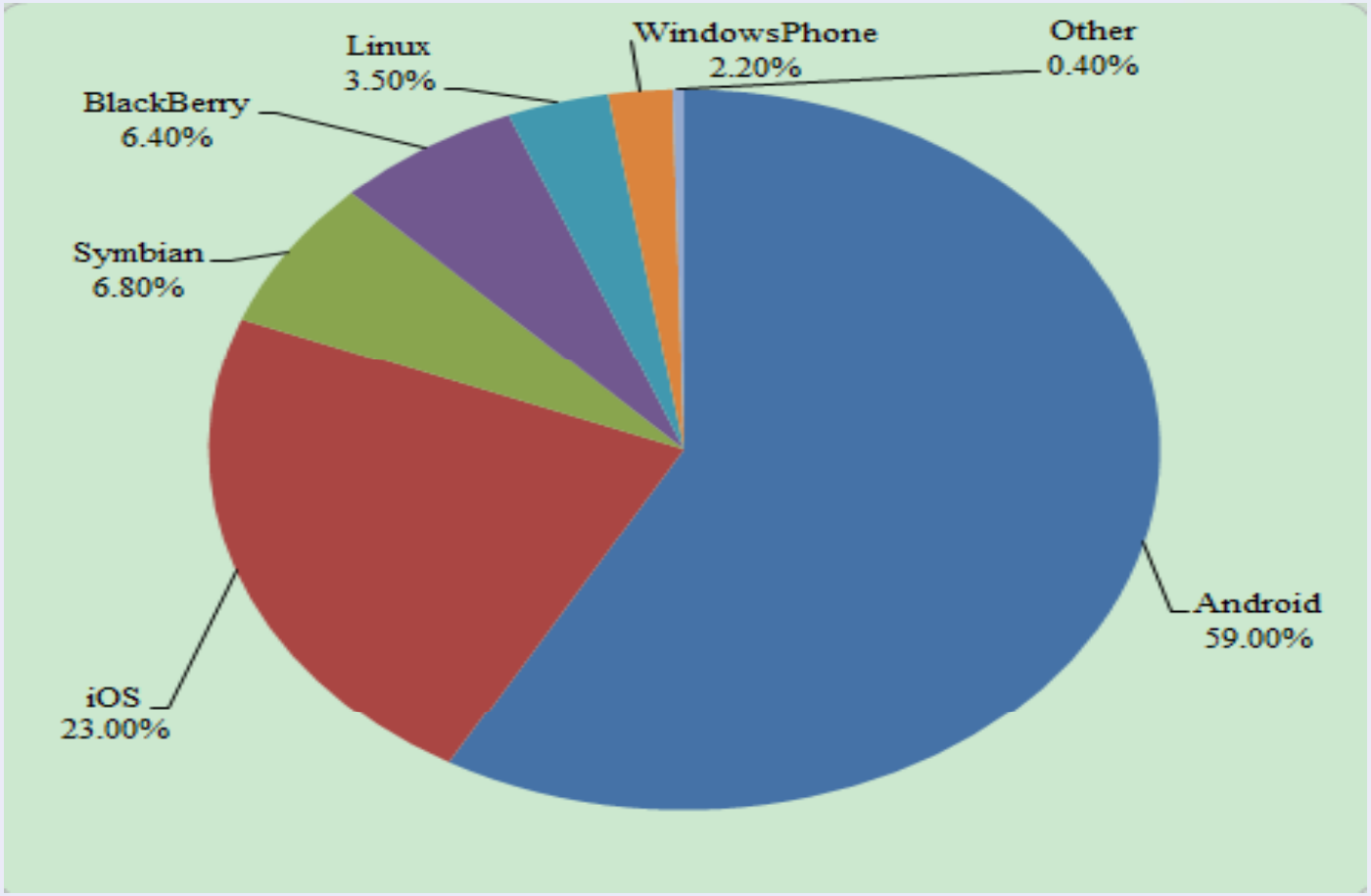
议程

OWASP 中国
The Open Web Application Security Project

- Android基础
- Android应用客户端安全
- Android应用通信安全
- Android应用服务端安全
- 总结

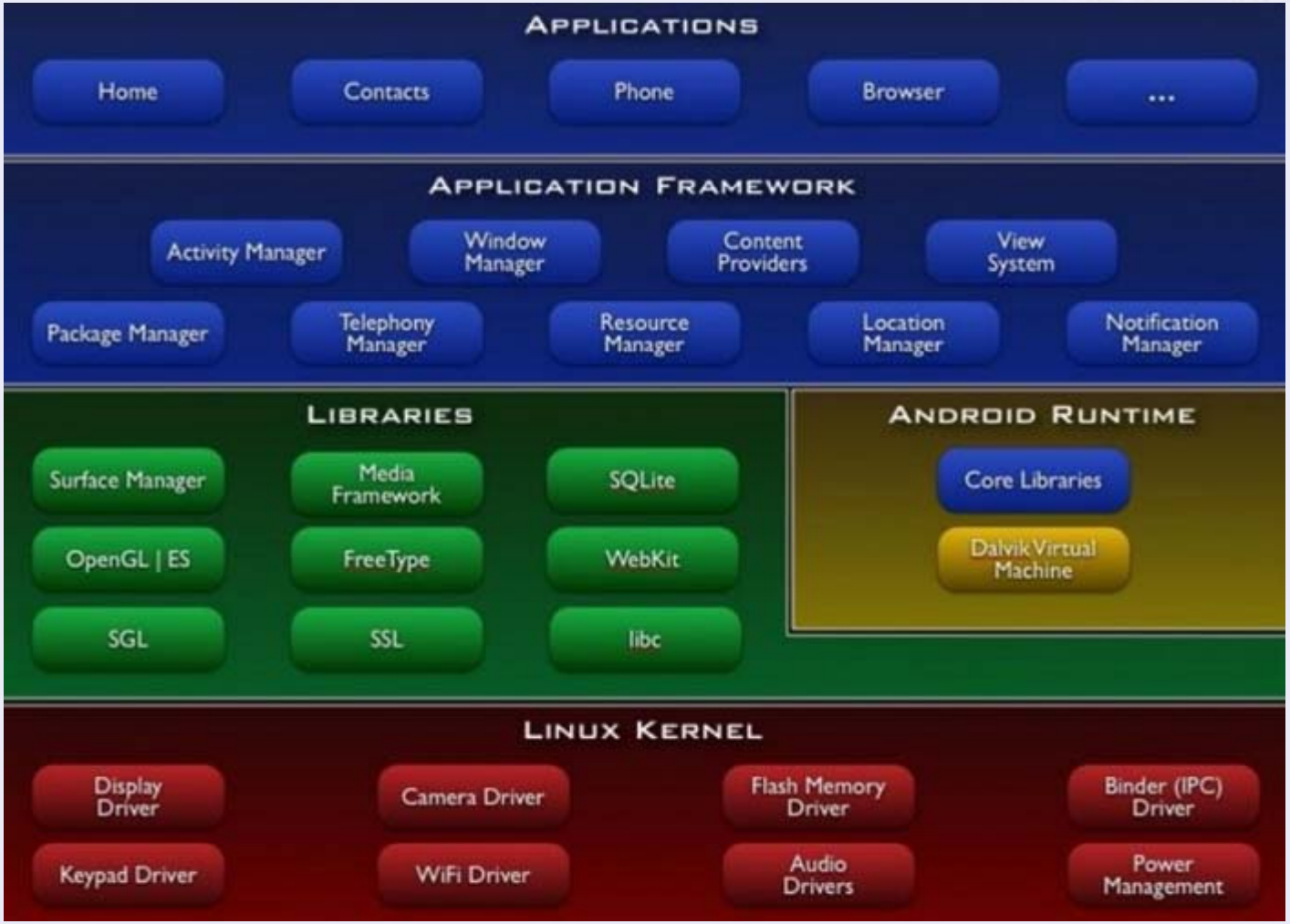
Android系统市场占有率巨大

OWASP 中国
The Open Web Application Security Project



Andriod整体构架

OWASP 中国
The Open Web Application Security Project



OWASP Mobile Top 10

OWASP 中国
The Open Web Application Security Project

OWASP Mobile Top 10 Risks	
M1- Insecure Data Storage	M6- Improper Session Handling
M2- Weak Server Side Controls	M7- Security Decisions Via Untrusted Inputs
M3- Insufficient Transport Layer Protection	M8- Side Channel Data Leakage
M4- Client Side Injection	M9- Broken Cryptography
M5- Poor Authorization and Authentication	M10- Sensitive Information Disclosure

与传统Web应用相比

OWASP 中国
The Open Web Application Security Project

- 手机上存的东西更隐私
- 手机直接关联运营商账号
- 手机更容易物理丢失
- 手机更多使用公用wifi上网
- Android系统的开放性
- Android机最大的乐趣-刷机（root）
- Android混乱的应用市场

OWASP 中国

The Open Web Application Security Project

Android客户端安全

从AndroidManifest.xml说起

OWASP 中国
The Open Web Application Security Project

- 每个Android程序中必须的文件
- 它位于整个项目的根目录
- 定义应用程序及其组件的结构和元数据
  - Permissions
  - Activities
  - Intents
  - Notifications
  - ContentProviders
  - 。。。

AndroidManifest.xml 实例

OWASP 中国
The Open Web Application Security Project

```
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.example.android.apis">

    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.WRITE_CONTACTS" />
    <uses-permission android:name="android.permission.VIBRATE" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.SET_WALLPAPER" />

    <!-- We will request access to the camera, saying we require a camera
         of some sort but not one with autofocus capability. -->
    <uses-permission android:name="android.permission.CAMERA" />
    <uses-feature android:name="android.hardware.camera" />
    <uses-feature android:name="android.hardware.camera.autofocus" android:required="false" />

    <application android:name="ApiDemosApplication"
            android:label="@string/activity_sample_code"
            android:icon="@drawable/app_sample_code" >

        <!-- This is how we can request a library but still allow the app
             to be installed if it doesn't exist. -->
        <uses-library android:name="com.example.will.never.exist" android:required="false" />

        <activity android:name="ApiDemos">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.DEFAULT" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
```

Permission

OWASP 中国
The Open Web Application Security Project

- 利用 Linux 已有的权限管理机制，为每一个 Application 分配不同的 uid 和 gid

- 在此基础上，对 Application 可以执行的某些具体操作进行权限细分和访问控制

Permission实例

OWASP 中国
The Open Web Application Security Project

Normal

android.permission.VIBRATE
com.android.alarm.permission.SET_ALARM

Dangerous

android.permission.SEND_SMS
android.permission.CALL_PHONE

Signature

android.permission.FORCE_STOP_PACKAGES
android.permission.INJECT_EVENTS

SignatureOrSystem

android.permission.ACCESS_USB
android.permission.SET_TIME

滥用权限

OWASP 中国
The Open Web Application Security Project

- android.permission.PROCESS_OUTGOING_CALLS
- android.permission.WAKE_LOCK,
- android.permission.READ_PHONE_STATE
- android.permission.INTERNET
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.ACCESS_NETWORK_STATE
- android.permission.ACCESS_COARSE_LOCATION
- android.permission.ACCESS_FINE_LOCATION
- com.google.android.googleapps.permission.GOOGLE_AUTH
- com.google.android.googleapps.permission.GOOGLE_AUTH.OTHER_SERVICES
- android.permission.GET_ACCOUNTS

组件间调用

OWASP 中国
The Open Web Application Security Project

- 四大组件
  - Activity
  - Service
  - Broadcast Receiver
  - Content Provider

- 如果配置不当，会被其他应用调用

- 为存储和获取数据提供统一的接口
- 可以在不同的应用程序之间共享数据
- ContentProvider提供的方法
  - query：查询
  - insert：插入
  - update：更新
  - delete：删除
  - getType：得到数据类型
  - onCreate：创建数据时调用的回调函数

滥用ContentProvider

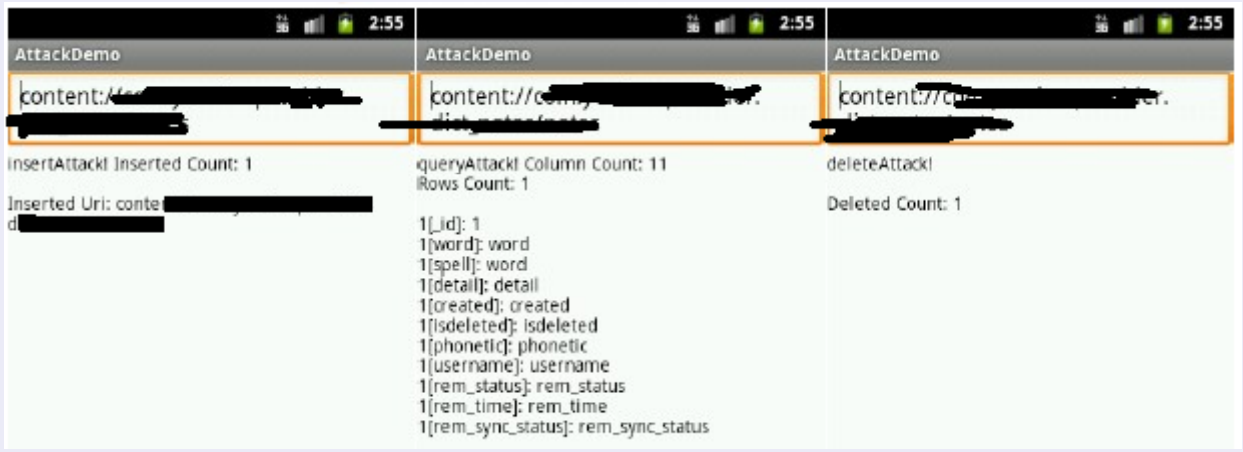
OWASP 中国
The Open Web Application Security Project

```
<provider android:name=".r[redacted]der" android:authorities="[redacted]tes" />
<provider android:name="[redacted]der" android:authorities="[redacted]ct" />
<provider android:name=".r[redacted]ovider" android:authorities="[redacted]review" />
<provider android:name=".d[redacted]ovider" android:authorities="d[redacted]" />
```

Content Provider Authority	Table Name
[redacted]	notes
[redacted]	user
[redacted]	rawnotes
[redacted]	note_tag_relations
[redacted]	words
[redacted]	counts
[redacted]	dicts

滥用ContentProvider

OWASP 中国
The Open Web Application Security Project

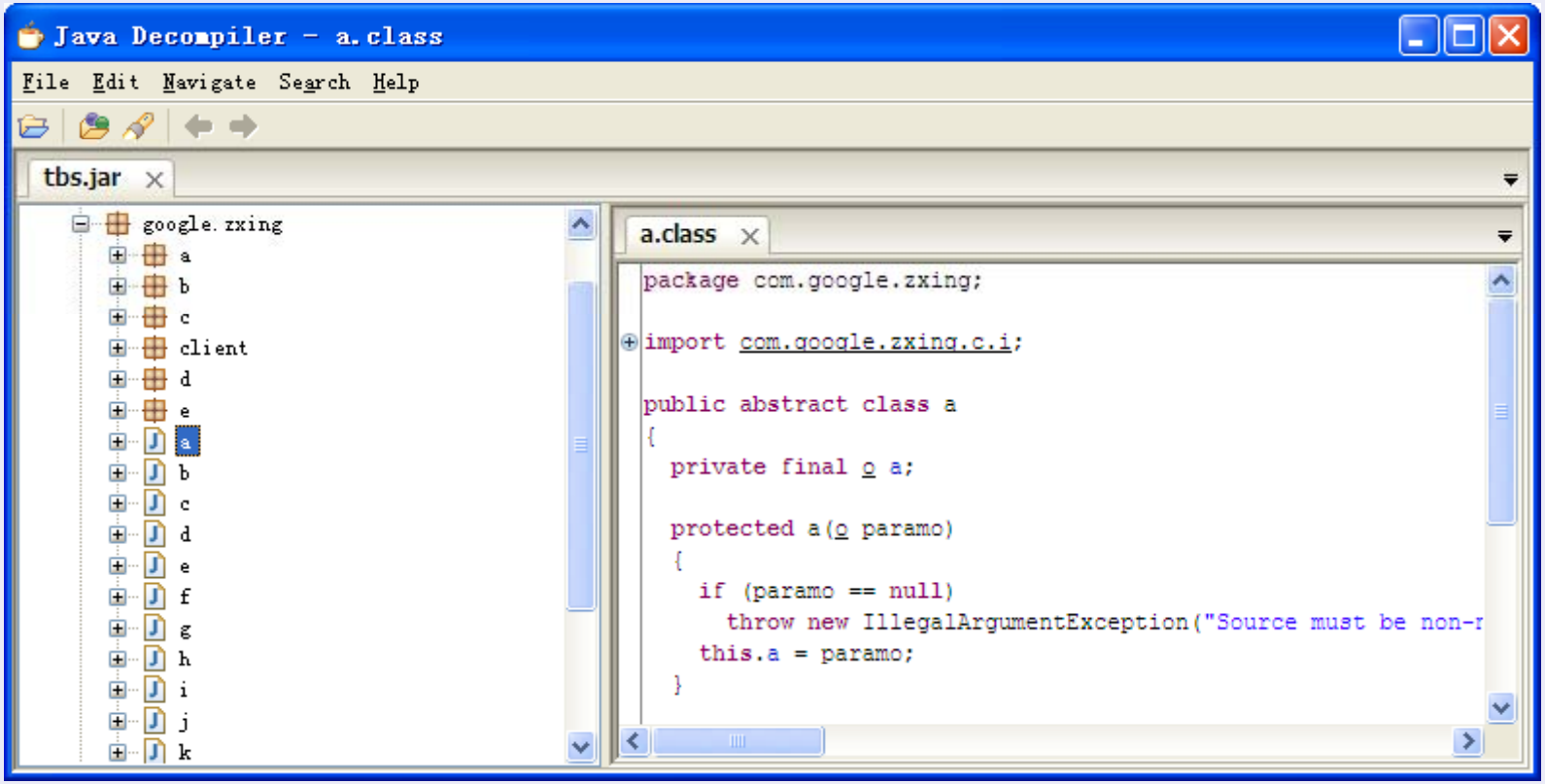


Andriod应用反编译

OWASP 中国
The Open Web Application Security Project

- Andriod 应用程序使用java开发，可通过反编译的方式获取对应的源码
- APK包其实就是个ZIP包，用WinRAR解开获得classes.dex
- 使用dex2jar将程序转换成jar文件
- 使用jad对jar文件进行反编译

反编译实例


Java Decompiler - a.class
File Edit Navigate Search Help
tbs.jar
google.zxing
a
b
c
client
d
e
a
b
c
d
e
f
g
h
i
j
k
a.class
package com.google.zxing;
import com.google.zxing.c.i;
public abstract class a
{
private final o a;
protected a(o paramo)
{
if (paramo == null)
throw new IllegalArgumentException("Source must be non-r
this.a = paramo;
}

对策

OWASP 中国
The Open Web Application Security Project

- ProGuard 是一个免费的 Java类文件的压缩，优化，混肴器
- 新建了一个Android工程之后，一个proguard.cfg文件会在工程的根目录下自动创建
- 文件定义了混淆器是怎样优化和混淆你的代码

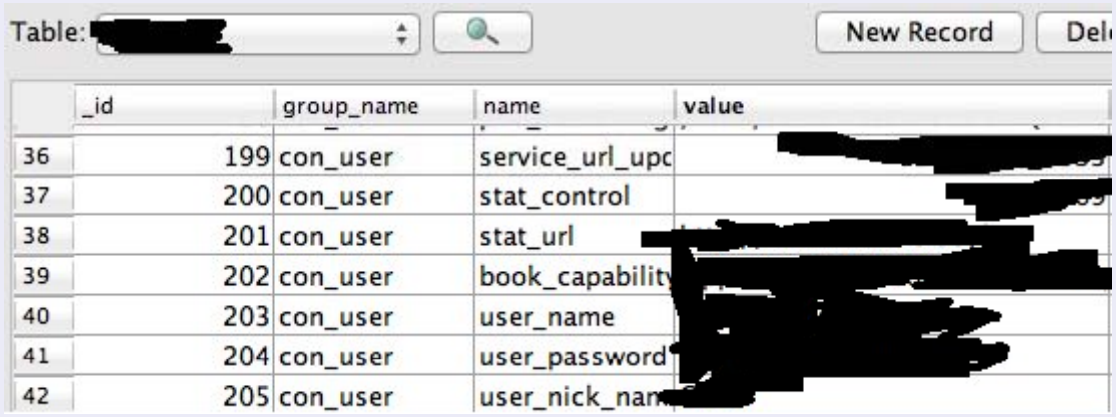
Andriod应用数据库

OWASP 中国
The Open Web Application Security Project

- Android使用开源的、与操作系统无关的SQL数据库SQLite
- 可以使用sqlite3查询sqlite数据库中的内容
- 同样可能受到SQLi攻击

对策

- 对于敏感数据要加密



- 预防SQLi

Android存储系统

OWASP 中国
The Open Web Application Security Project

- SD卡作为手机的扩展存储设备，在手机中充当硬盘角色，可以让我们手机存放更多的数据以及多媒体等大体积文件

- 内部存储 RAM，就是我们常说的真正意义上的内存

对SDCard进行读写操作

OWASP 中国
The Open Web Application Security Project

- 只需要在AndroidManifest.xml中声明

```
<uses-permission
    android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

- 我们存放在SD卡中数据很可能被其他恶意程序读取或者篡改

对RAM进行读写操作

OWASP 中国
The Open Web Application Security Project

- 存放在RAM中数据，被root之后也可以读取篡改
- 国内大部分机器都root了
- Android 2.2/2.3有大量可提权到root的漏洞

本地敏感信息保存实例

OWASP 中国
The Open Web Application Security Project

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="[redacted]_password">[redacted]</string>
<boolean name="[redacted]d_open" value="true" />
<string name="login_username">[redacted]</string>
<boolean name="first_open_app" value="false" />
<boolean name="is_pushing" value="true" />
<boolean name="show_guide" value="false" />
```

对策

OWASP 中国
The Open Web Application Security Project

- Encode vs. Serializable vs. Encrypt
- 加密之后的密钥存放？？
  - 算法密钥都在本地
- 对保存在客户端的敏感信息加密
  - 对于SD卡上的敏感信息一定要加密
  - 加密用的密钥放到RAM中

- Android底层是Linux和C
- 如果使用native本地库，那么可能存在缓冲区溢出
- 如果使用标准SDK库，那么把心放回肚子里

OWASP 中国

The Open Web Application Security Project

Android应用通信安全

Android手机信道

OWASP 中国
The Open Web Application Security Project

- SMS
- Socket
- HTTP
- Bluetooth

主要威胁

OWASP 中国
The Open Web Application Security Project

- 明文密码
- 明文会话id
- 其他敏感信息
- 手机信道更加危险

未加密的通信

OWASP 中国
The Open Web Application Security Project

```
⊞ Ethernet II, Src: HonHaiPr_58:f7:50 (44:37:e6:58:f7:50), Dst: Cisco_aa:78:bf (00:13:19:aa:78:bf)
⊞ Internet Protocol Version 4, Src: 192.168.161.237 (192.168.161.237), Dst: [redacted]
⊞ Transmission Control Protocol, Src Port: 59658 (59658), Dst Port: http (80), Seq: 1, Ack: 1, Len: 251
⊟ Hypertext Transfer Protocol
  ⊞ POST /[redacted] HTTP/1.0\r\n
    [redacted]\n
    Content[redacted]application/x-www-form-urlencoded\r\n
  ⊞ Content-Length:116\r\n
    \r\n
    [Full request URI: [redacted]]
⊟ Line-based text data: application/x-www-form-urlencoded
    &username=[redacted]&password=[redacted]&product=[redacted]&time
⊞ Hypertext Transfer Protocol
```

```
0000 [redacted]  ....X.D7 .X.P..E.
0010 [redacted]  .#Q.@...  .......
0020 [redacted]  S. 7..S2.P.
0030 [redacted]  .....PO ST[redacted]
0040 [redacted]
0050 [redacted]
0060 [redacted]  ent-Type
0070 [redacted]  : applic ation/x-
0080 [redacted]  www-form -urlenco
0090 [redacted]  ded..Con tent-Len
00a0 [redacted]  gth:116. ...&user
00b0 [redacted]  name=[redacted]m& password
00c0 [redacted]  =0[redacted]
00d0 [redacted]
00e0 [redacted]  &produc t=[redacted]
00f0 [redacted]  &pass type=0&s
0100 [redacted]  id=&fid= 0&time=.
0110 [redacted]
0120 [redacted]
0130 [redacted]
```

加密的通信

OWASP 中国
The Open Web Application Security Project

```
GET /[redacted]in=154831009&sess_id=bzwYsYNBIL7AtCURdaU63gali3jamESZ&data=45D4C8FAE3F7D4AC96C63B45F4CD19302AE52C644785EAFCE79B49A85BE1708879315C7528AD77EC HTTP/1.1
返回数据
{ "err": 0, "uin": 154831009, "isdna": 1, "setdir": 0, "have_mobile": 1, "mobile_mask": "152******12", "ques_appear": 1, "qqtoken_appear": 0, "tkn_usable": 1, "mobile_appear": 1, "mobile_sms_pref

GET [redacted]in=154831009&sess_id=bzwYsYNBIL7AtCURdaU63gali3jamESZ HTTP/1.1
返回数据
{ "err": 0, "uin": 154831009, "info": "" }
```

HTTPS的证书验证

OWASP 中国
The Open Web Application Security Project

- 大量自签名证书
- 系统设置，信任所有证书
- 绝大部分应用没有验证客户端

OWASP 中国
The Open Web Application Security Project

- 中间人攻击

```
public  SSLHttpClient (File keyStoreFile, String keyStorePass) throws Exception {
    initHttpClient();
    KeyStore keyStore = KeyStore.getInstance(KeyStore.getDefaultType());
    keyStore.load(new FileInputStream(keyStoreFile), keyStorePass.toCharArray());// 导入证书密钥库
    SSLSocketFactory socketFactory = new SSLSocketFactory("TLS", null, null, keyStore, new SecureRandom(),
            SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);
    Scheme sch = new Scheme("https", 443, socketFactory);
    httpClient.getConnectionManager().getSchemeRegistry().register(sch);
}
```

对策

OWASP 中国
The Open Web Application Security Project

- 使用安全的信道传输敏感信息
- 重载verification函数，hardcode强制验证证书的发行者
- 对客户端同样需要验证

OWASP 中国

The Open Web Application Security Project

Android应用服务端安全

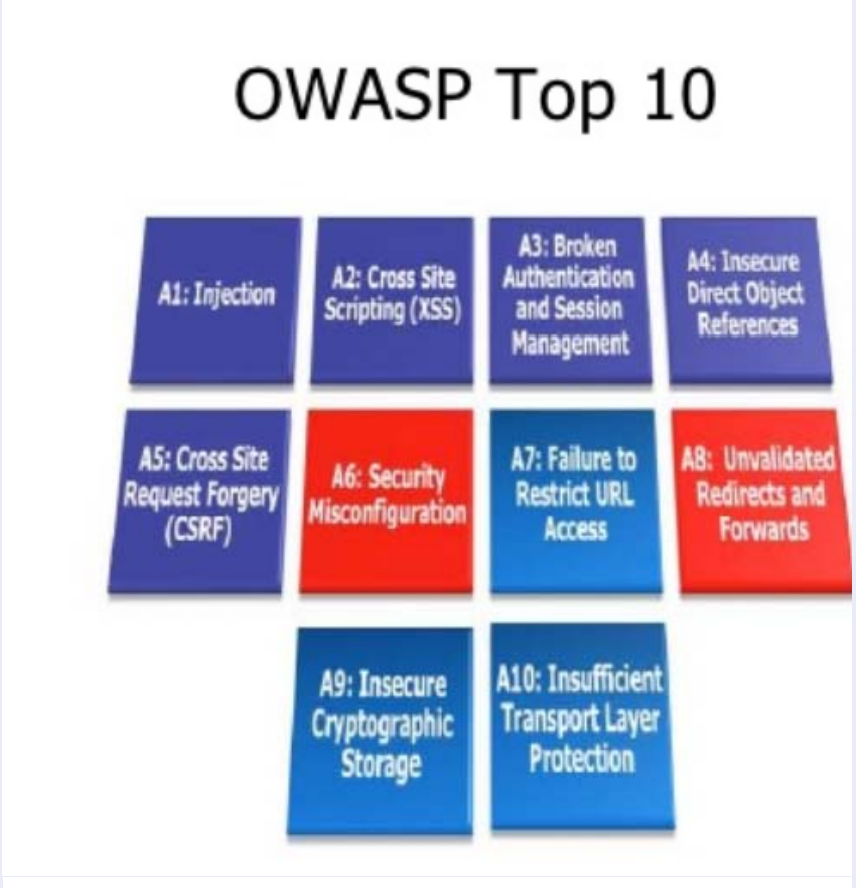
关于sessionid

OWASP 中国
The Open Web Application Security Project

- 唯一编号(IMEI，IMSI)，实际上并不唯一
- 任意程序可以读取上传
- 不适合当做认证凭证使用

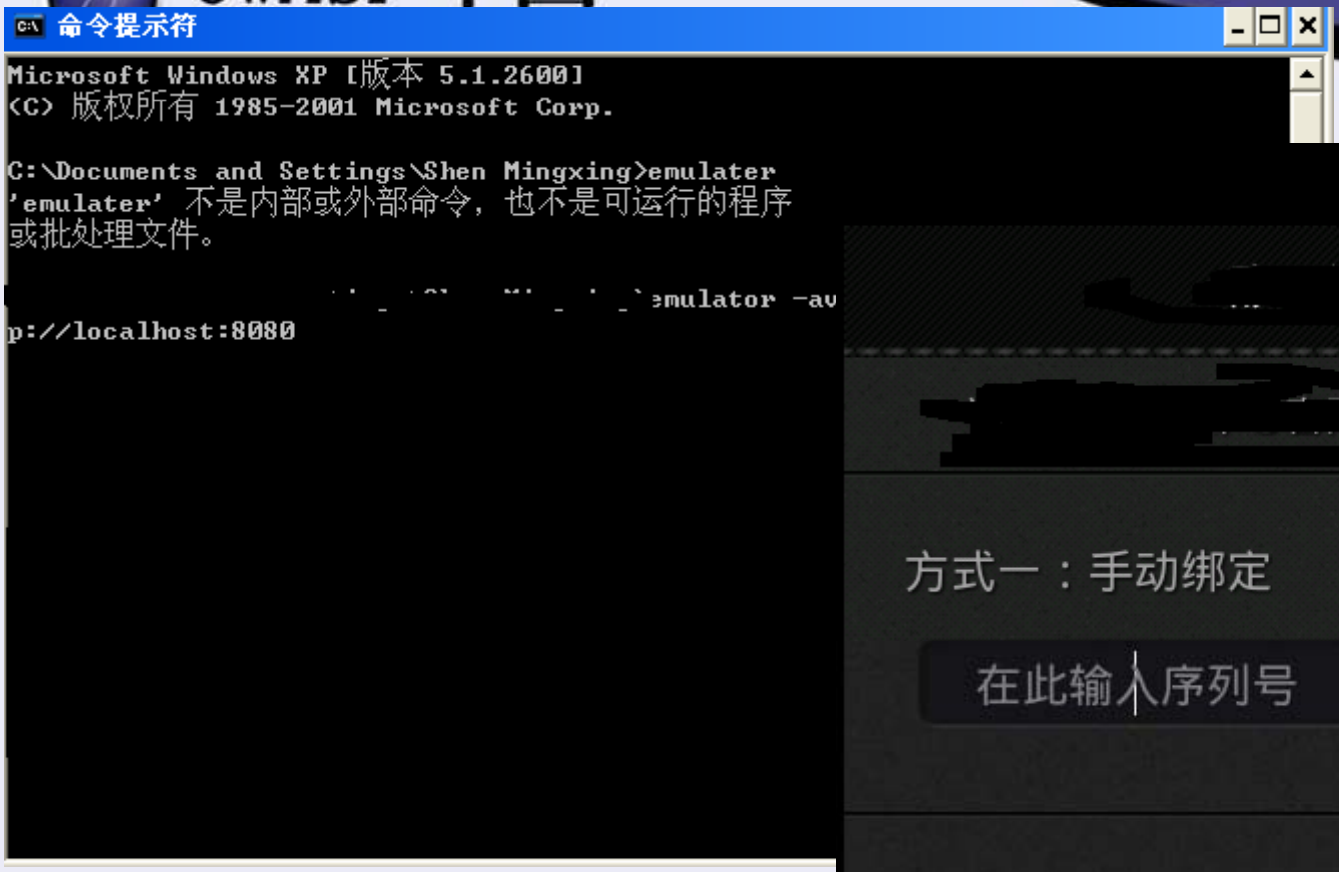
跟常规Web APP一样

OWASP 中国
The Open Web Application Security Project



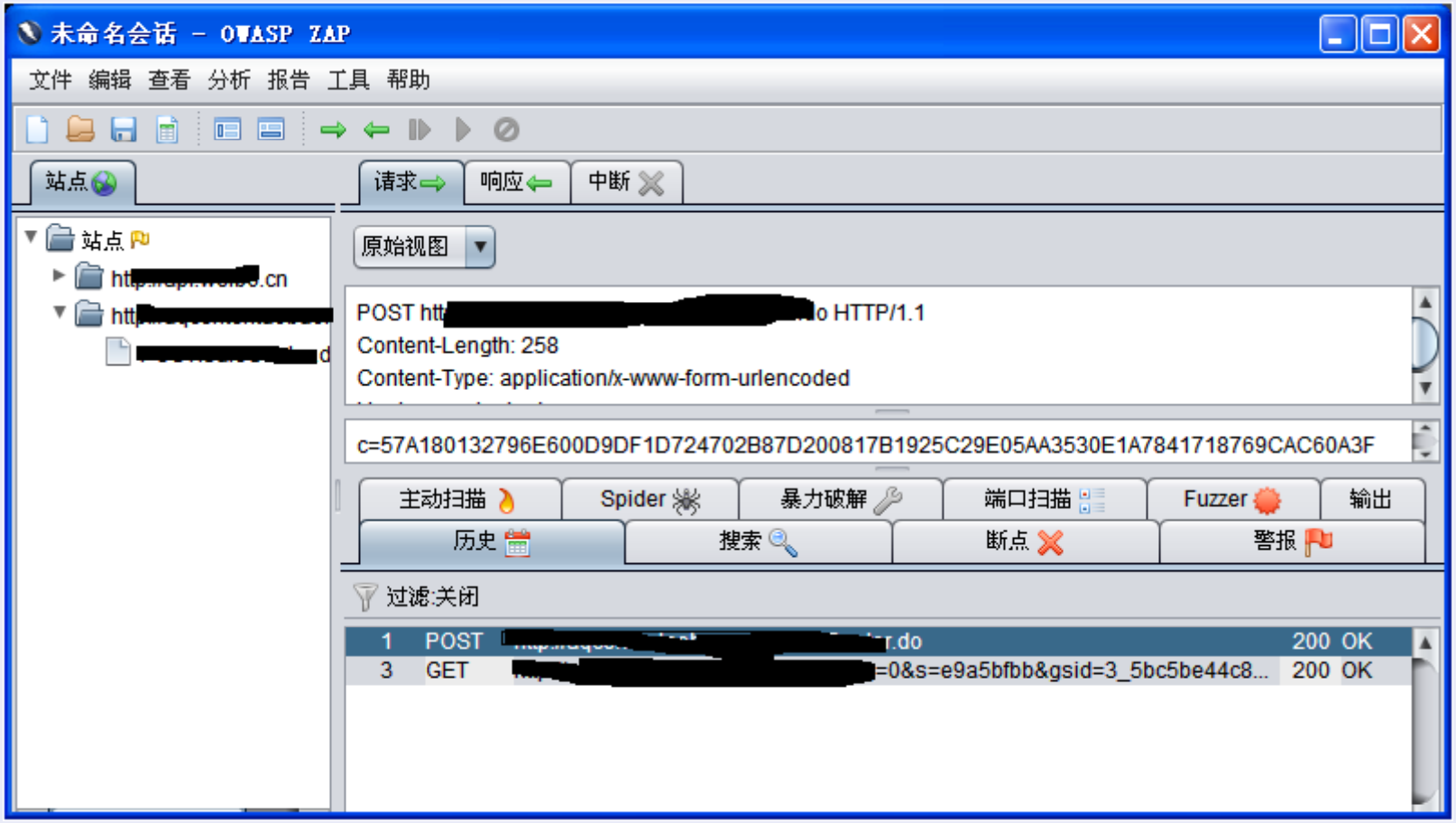
走HTTP的应用

OWASP 中国



走HTTP的应用– burp zap …

OWASP 中国
The Open Web Application Security Project



走 Socket的应用 - Mallory

OWASP 中国
The Open Web Application Security Project

Mallory

Streams

	Dir	Len	Source	Dest	tatu
0	c2s	37	10.0.0.10:62310	68.229.93.156:26637	U
1	c2s	102	10.0.0.10:62288	128.164.182.1:52976	U
2	c2s	38	10.0.0.10:62359	68.231.246.203:28137	U
3	c2s	58	10.0.0.10:62323	72.218.20.98:25744	S
4	c2s	29	10.0.0.10:62537	70.161.137.216:20134	U
5	c2s	62	10.0.0.10:62473	64.131.188.122:11560	U
6	c2s	35	10.0.0.10:62515	144.118.228.248:34603	U
7	c2s	30	10.0.0.10:62790	70.72.76.23:55019	U
8	c2s	30	10.0.0.10:62789	174.59.121.35:29103	U
9	c2s	30	10.0.0.10:62765	69.143.229.182:22479	U
10	c2s	57	10.0.0.10:62895	109.87.76.182:27477	U
11	c2s	85	10.0.0.10:62898	68.174.69.91:55625	U
12	c2s	56	10.0.0.10:62906	109.86.51.82:36823	U
13	c2s	106	10.0.0.10:62876	87.53.96.68:16652	U

Actions: Intercept Send Drop

Text Hex

Save Hex Changes

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	21	e3	5e	2c	d2	e8	7b	d7	e1	d3	a9	f9	0c	ec	06	46	!.^,..{.....F
2	d8	2f	e8	74	f6	7d	29	fd	9d	1c	34	e3	34	aa	01	bf	./.t.})...4.4...
3	5c	40	3a	ae	a9	11	6c	8b	95	a5	ba	5d	e3	50	60	b3	\@:...l....].P`.
4	42	15	f7	b2	e1	17	11	8c	06	b1							B.....

OWASP 中国

The Open Web Application Security Project

Thanks!

Q & A