基础APP安全测试

姓名：XXX

目录

CONTENTS

概述

图1：2017年12月通过360显危镜检查的约1.8万款安卓主流APP应用中，发现了99.5%的安卓应用存在威胁风险，平均每个应用威胁风险数量为38.6个。可见安卓市场上的APP存在严重的安全隐患

概述

表1：2017年十大Android软件漏洞

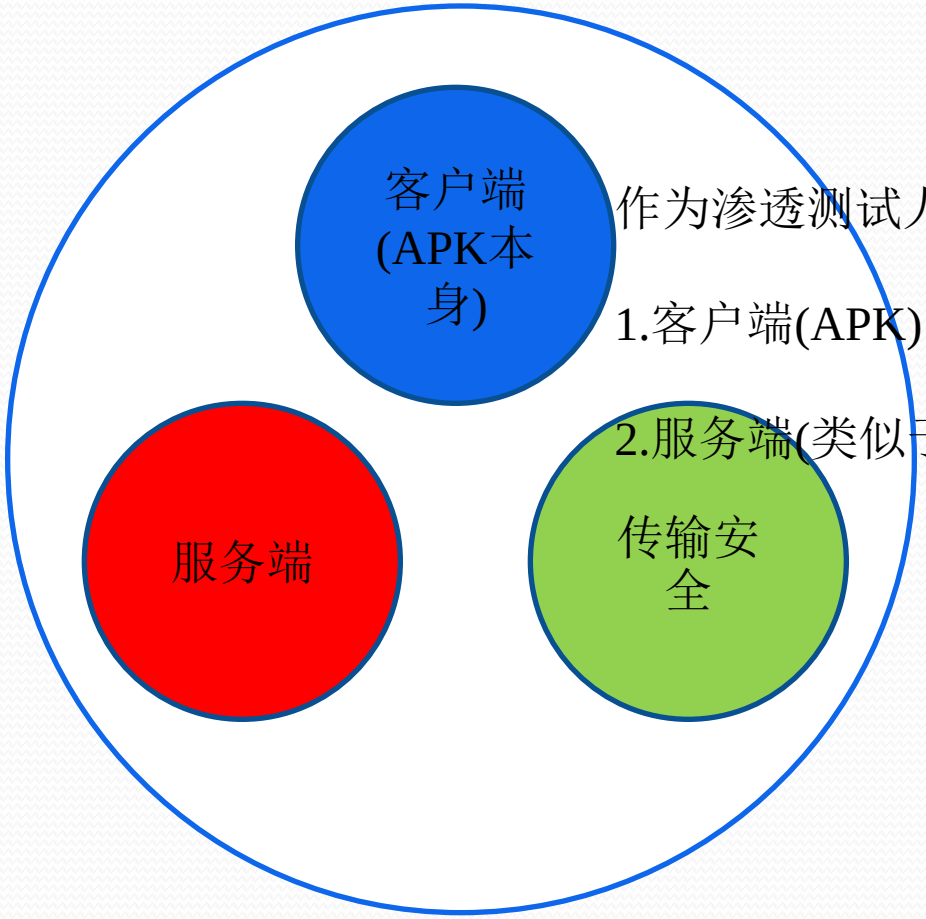
序列	漏洞名称
1	WebView远程代码执行漏洞
2	界面劫持漏洞
3	权限漏洞
4	篡改和二次打包漏洞
5	SharedPref读写安全漏洞
6	WebView组件忽略SSL证书验证错误漏洞
7	固定端口监听风险漏洞
8	数据弱加密漏洞
9	动态注册广播暴露风险
10	业务逻辑漏洞

概述

那么作为基础的安全人员或者说一个新手该如何入门进行app的基础安全测试呢？又该从哪些方面去检测呢？

APK渗透测试基础点

Android安全分类



作为渗透测试人员主要检测以下两点：

1.客户端(APK)

2.服务端(类似于WEB安全测试)

APK渗透测试基础点

- 客户端(APK)
  - 签名问题
  - 组件问题
  - 日志问题
  - 本地存储问题
  - 客户端完整性问题
  - Webview相关问题
  - Androidmanifest配置问题

APK渗透测试基础点

◆签名问题

问题描述：

安装包签名的目的是为了便于升级，便于模块化程序设计和开发，代码或者数据的共享，区别app防止被恶意第三方程序覆盖或者替换掉。有些apk程序签名有问题，则说明程序存在安全问题。

检测工具：jarsigner.exe, Android右键工具

检测方法：jarsigner.exe –verify –verbose –certs XXX

APK渗透测试基础点

◆组件问题

问题描述：

Activity 活动

Service 服务

Content Provider 内容提供者

Broadcast Receiver 广播接收器

组件暴露，使得攻击者可以调用组件去实现一些复杂攻击。比如：利用APP组件间相互协作泄露程序敏感信息。

检测工具：Jd_GUI（java decompile），右键工具，Android killer等

检测方法：通过查看Androidmanifest.xml文件，判断exported="true"是否存在

APK渗透测试基础点

◆日志问题

问题描述：

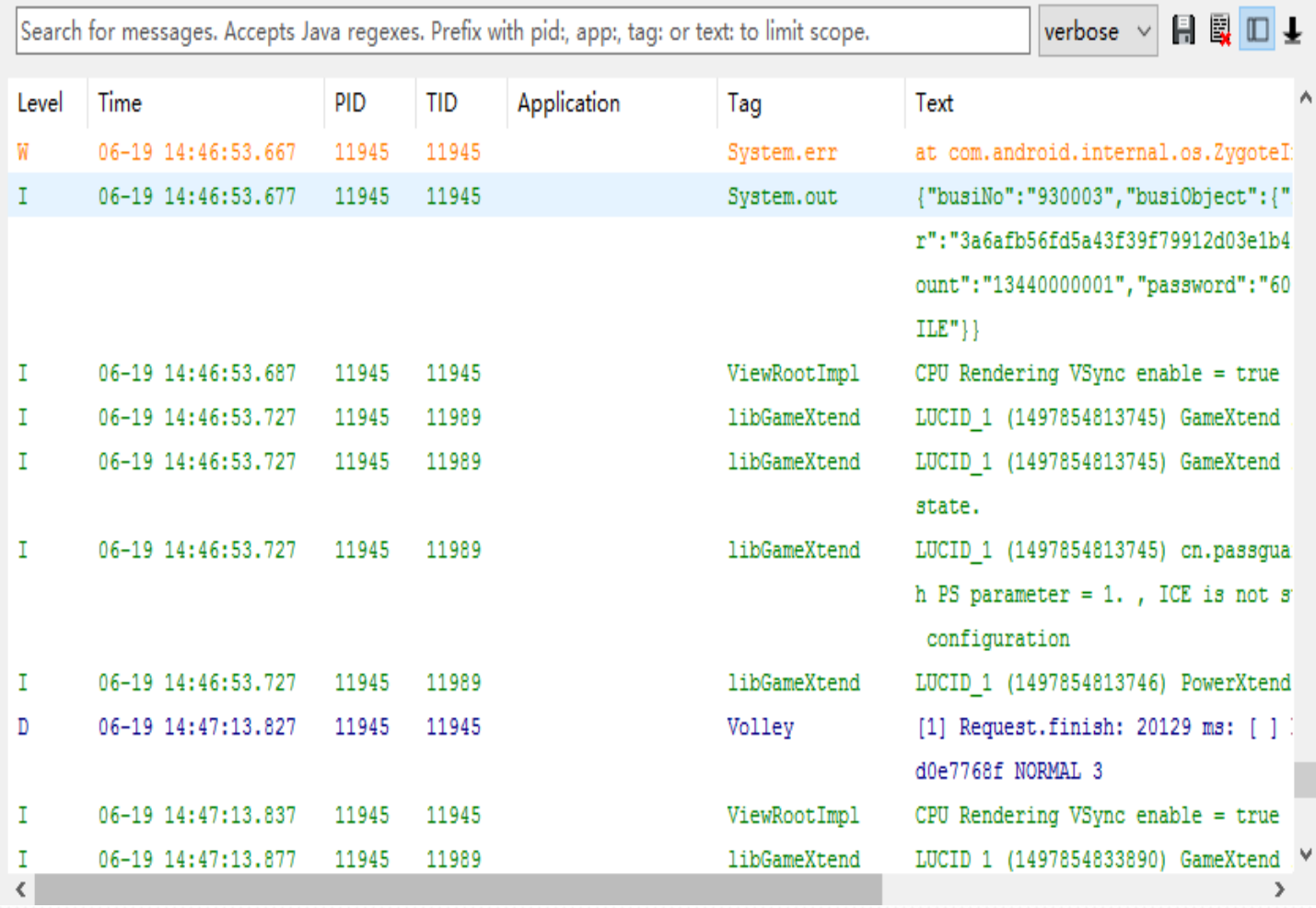
有时候开发人员为了便于调试往往在日志里面输入大量敏感信息，这些信息可能包含了用户密码信息等。攻击者通过分析，可以进行有效的攻击。

检测工具：adb.exe ,或者aapt.exe，DDMS等

检测方法：借助adb.exe，输入logcat可以查看所有日志信息。可以指定进程名，然后获取指定程序的日志信息。Adb logcat | grep XXXX

APK渗透测试基础点

检测客户端对应的Logcat日志是否会打印一些用户或服务器的敏感信息。



APK渗透测试基础点

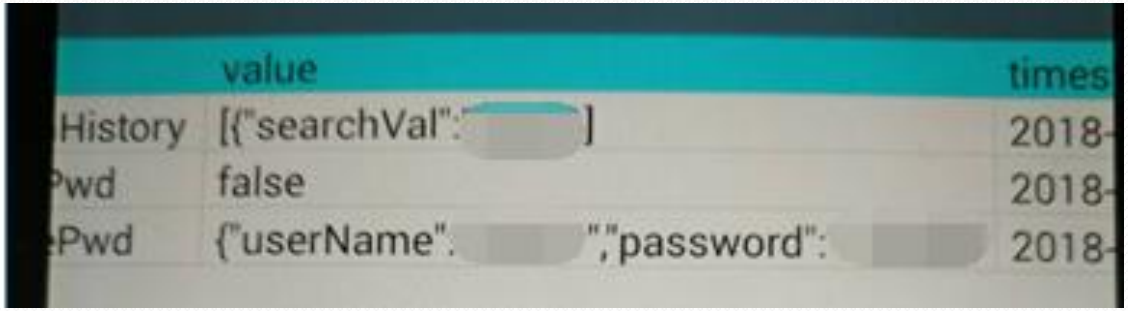
◆本地存储问题

问题描述：

Android的Webview组件中默认打开了提示用户是否保存密码的功能，如果用户选择保存，用户名和密码将被明文存储到该应用目录databases/webview.db中。

检测工具：Android killer，adb等工具

检测方法：代码审计，或者直接检查app对应的data数据库，打开检查是否存储有敏感信息。如果有就会存在如下所示效果。



APK渗透测试基础点

◆客户端完整性问题

问题描述：

对客户端程序添加或修改代码，修改客户端资源图片，配置信息，图标，添加广告，推广自己的产品，再生成新的客户端程序，可导致大量盗版应用的出现分食开发者的收入；恶意的二次打包还能实现应用的钓鱼、添加病毒代码，添加恶意代码，从而窃取登录账号密码、支付密码、拦截验证码短信，修改转账目标账号，金额等

检测工具：Android killer,C32asm,梆梆扫描等工具

检测方法：对dex文件或者so文件修改，然后重新打包。判断程序是否仍能正常运行。

APK渗透测试基础点

◆Webview相关问题

问题描述：

webview明文存储。 mWebView.setSavePassword(true)

webview远程代码执行。

webview域控制不严格问题。（克隆漏洞） WebView如果打开了对JavaScript的支持，同时未对file:///形式的URL做限制，则会导致coookie、私有文件、数据库等敏感信息泄露

检测工具：梆梆扫描工具，或者进行人工代码审计

检测方法： setAllowFileAccess

setAllowFileAccessFromFileURLs

setAllowUniversalAccessFromFileURLs（导致远程泄露敏感信息）

webSettings.setJavaScriptEnabled(true);

APK渗透测试基础点

◆Androidmanifest其他配置问题

问题描述：

AndroidManifest.xml文件是整个应用程序的信息描述文件。这里面包含了很多重要信息，比如版本信息，权限信息，文件备份等配置信息。这些信息也会暴露出安全问题。

检测工具：android右键工具，APKtool，梆梆扫描平台等

检测方法：在检查的时候主要检查以下几点：

检查是否最小sdk版本是否大于16；

检查是否存在任意文件备份的问题；android:allowBackup=“true”

检查是否存在动态调试的问题；android:debuggable=“false”。

其他等等；

APK渗透测试基础点


<uses-permission android:name="android.hardware.camera"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.RESTART_PACKAGES"/>
<uses-permission android:name="android.permission.READ_LOGS"/>
<uses-permission android:name="android.permission.SET_DEBUG_APP"/>
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
<uses-permission android:name="android.permission.SYSTEM_OVERLAY_WINDOW"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.USE_CREDENTIALS"/>
<uses-permission android:name="android.permission.MANAGE_ACCOUNTS"/>
<application android:allowBackup="true" android:configChanges="keyboardHidden|orientati
"com.hundsun.winner.application.base.WinnerApplication" android:screenOrientation="porti
<receiver android:exported="false" android:name=
Receiv
<intent-filter>
<action android:name="android.intent.action.BOOT_COMPLETED"/>
<action android:name="android.net.conn.CONNECTIVITY_CHANGE"/>
<action android:name="
/>
</intent-filter>
</receiver>
<service android:enabled="true" android:exported="false" android:name="cn.jpush.and
<intent-filter>
<action android:name="cn.jpush.android.intent.REGISTER"/>
<action android:name="cn.jpush.android.intent.REPORT"/>
<action android:name="cn.jpush.android.intent.PushService"/>
<action android:name="cn.jpush.android.intent.PUSH_TIME"/>
</intent-filter>

APK渗透测试基础点

- 服务端(APK)
  - 用户遍历
  - 弱口令以及暴力破解
  - SQL注入
  - 短信轰炸
  - 短信绕过
  - 任意文件上传
  - 敏感信息明文传输
  - 越权
  - 其他

APK渗透测试基础点

◆用户遍历

问题描述：

用户在登录或者注册时，往往会遇到一种情况，当输入不存在用户时会返回用户不存在，当密码不正确时，会返回密码信息不正确，这种情况会导致用户枚举.

检测工具：Burpsuite，Fillder等抓包工具

检测方法：Burpsuite抓包分析数据，或者什么工具也不需要直接登录查看页面返回信息

APK渗透测试基础点

◆弱口令与暴力破解

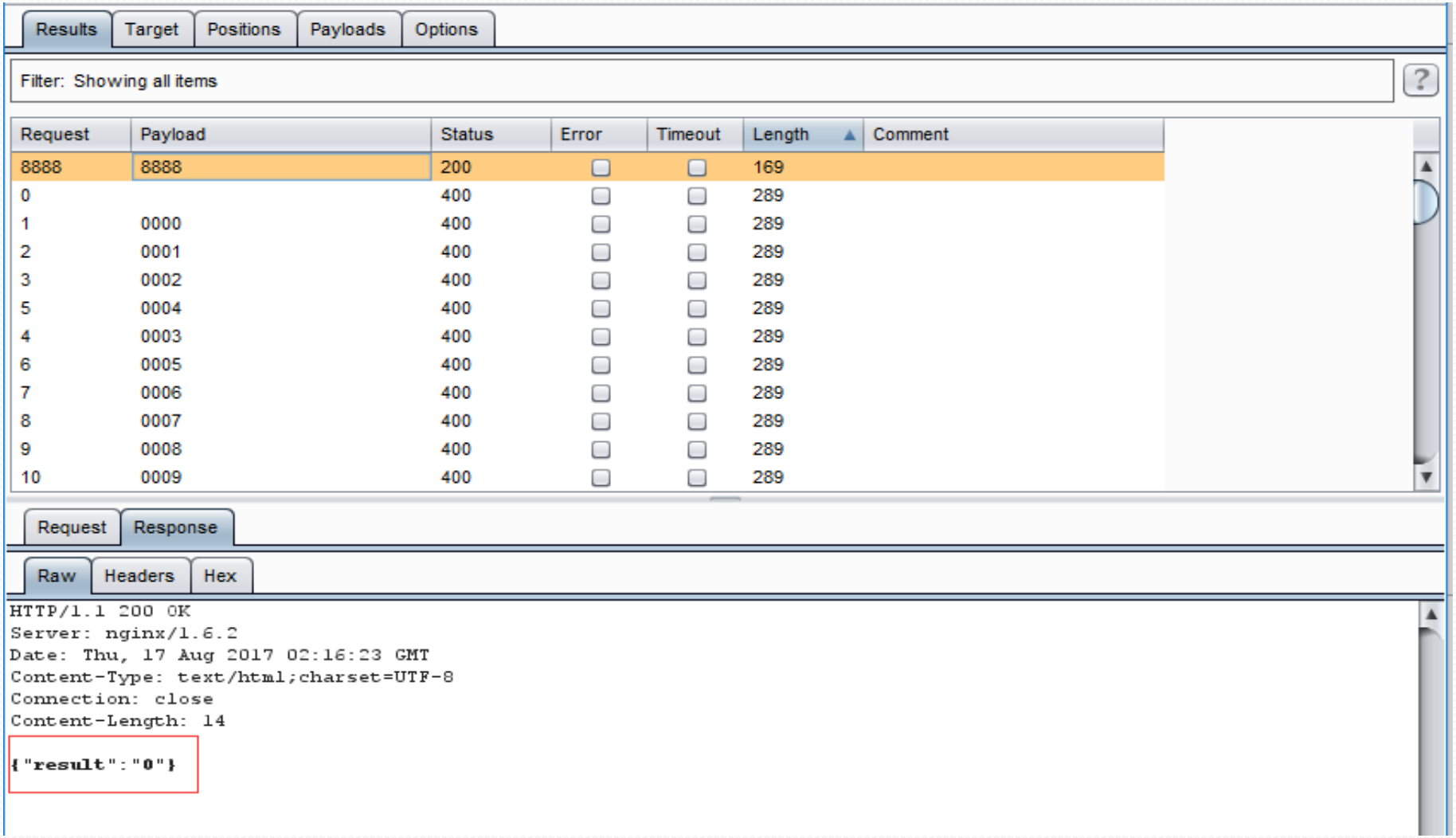
问题描述：

在某些情况下，系统登录的口令是简单的弱口令，这样导致攻击者可以通过简单尝试登录系统。比如：admin/admin

检测工具：Burpsuite等工具

检测方法：使用burp抓包以后，然后使用暴力破解功能进行尝试。如下图所示，是使用burp暴力破解功能进行尝试的情况。

APK渗透测试基础点


Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
8888 8888 200 169
0 400 289
1 0000 400 289
2 0001 400 289
3 0002 400 289
5 0004 400 289
4 0003 400 289
6 0005 400 289
7 0006 400 289
8 0007 400 289
9 0008 400 289
10 0009 400 289
Request
Response
Raw
Headers
Hex
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Thu, 17 Aug 2017 02:16:23 GMT
Content-Type: text/html;charset=UTF-8
Connection: close
Content-Length: 14
{"result":"0"}

APK渗透测试基础点

◆SQL注入

问题描述：

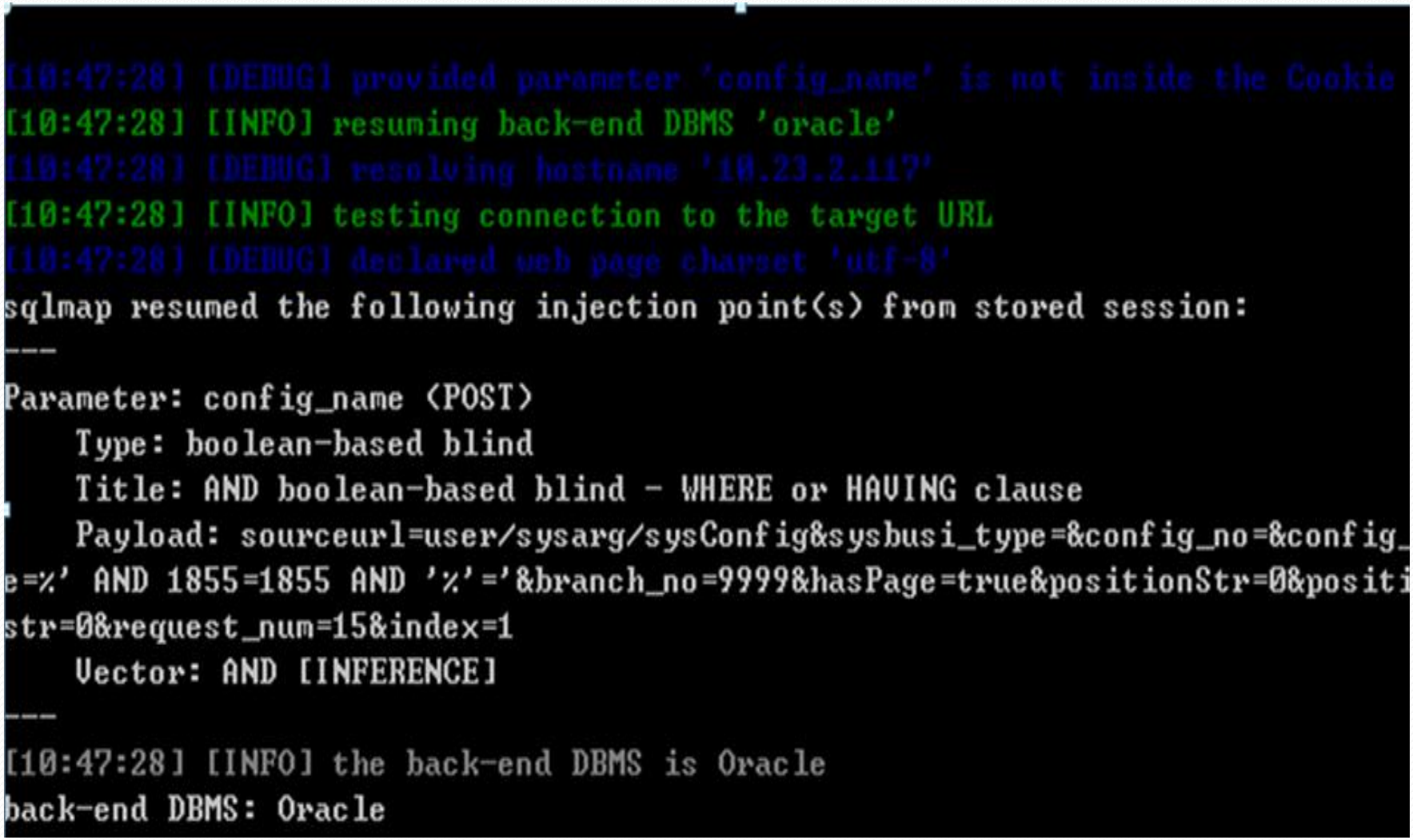
程序未对程序的输入进行限制，从而造成攻击者输入指令被作为SQL语句执行。最终泄露数据库相关的信息。。

检测工具：SQLMAP或者使用手工尝试

检测方法：如果是get类型参数：sqlmap –u “url”；

如果是post类型参数：可以拷贝出整个数据包，然后使用命令:sqlmap –r “拷贝到文件的地址”

APK渗透测试基础点


[10:47:28] [DEBUG] provided parameter 'config_name' is not inside the Cookie
[10:47:28] [INFO] resuming back-end DBMS 'oracle'
[10:47:28] [DEBUG] resolving hostname '10.23.2.117'
[10:47:28] [INFO] testing connection to the target URL
[10:47:28] [DEBUG] declared web page charset 'utf-8'
sqlmap resumed the following injection point(s) from stored session:

Parameter: config_name (POST)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: sourceurl=user/sysarg/sysConfig&sysbusi_type=&config_no=&config_
e=%' AND 1855=1855 AND '%'='&branch_no=9999&hasPage=true&positionStr=0&positi
str=0&request_num=15&index=1
Vector: AND [INFERENCE]

[10:47:28] [INFO] the back-end DBMS is Oracle
back-end DBMS: Oracle

APK渗透测试基础点

◆短信轰炸

问题描述：

现在很多系统在登录或者注册的时候要求用户输入手机号，然后发送验证码。该过程如果配置不当可能造成短信轰炸，攻击者可以一直发送短信验证码。

检测工具：Burpsuite等抓包工具

检测方法：抓取发送验证码的数据包，然后不断的进行重放，判断返回结果。

APK渗透测试基础点

◆短信绕过

问题描述：

在某些登录场景下，短信是可以被成功绕过的。而绕过最常见的三种种形式是：第一、验证码是4位，可以被暴力破解猜测。第二、验证码在本地校验没有在服务端进行。第三、服务端根本没有验证短信信息是否正确。。

检测工具：Burp，Fillder等工具

检测方法：在用户登录或者注册的地方，抓取数据包，依次判断上述几点哪个成立。

APK渗透测试基础点

◆任意文件上传

问题描述：

现在众多系统都存在用户上传的地方，比如上传照片，上传文档。这些地方很容易存在任意文件上传的问题。该问题最大的危害是可以允许getshell。造成这种问题方法是多样的，比如文件上传限制不严，比如利用服务器的文件解析漏洞，比如配置文档设置不安全等等。。

检测工具：burpsuite,fillder等工具

检测方法：常用的方法是使用burp抓包，然后不断修改数据包进行文件上传，具体的需要结合情况分析。

APK渗透测试基础点

```
POST /13/?action=upload HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------120333047721284
Content-Length: 522
Referer: http:[redacted]
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

---------------------------120333047721284
Content-Disposition: form-data; name="file"; filename="sec.php"
Content-Type: application/octet-stream

<?php
$file_path = str_replace('\\','/',realpath(dirname(__FILE__).'/')).'/';
echo $file_path;
$file=scandir($file_path);
 print_r($file);
//if(file_exists($file_path)){
//$str = file_get_contents($file_path);//将整个文件内容读入到一个字符串中
//$str = str_replace("\r\n","<br />",$str);
//echo $str;
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 24 May 2018 02:36:01 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=k92i5ulf2crcbmlpat26pgmea4; path=/web-serveur/ch20/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Length: 515

<html><body><h1>Photo gallery v 0.02</h1><span id="menu"/> | <span><a
href='?galerie=emotes'>emotes</a></span> | <span><a
href='?galerie=apps'><b>apps</b></a></span> | <span><a
href='?galerie=upload'>upload</a></span> | <span><a
href='?galerie=devices'>devices</a></span> | <span><a
href='?galerie=categories'>categories</a></span> | <span><a
href='?galerie=actions'>actions</a></span><br><hr><p style='color: red'>Wrong file extension
!</p></body></html>
```

APK渗透测试基础点

◆敏感信息明文传输

问题描述：

程序使用明文传输敏感信息，这些信息包括用户密码，身份证等信息。该信息存在被监听的可能。

检测工具：抓包工具，Fillder,或者burpsuite

检测方法：抓包查看敏感信息是否是明文传输

```
POST /oss-api-app/client/login HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Host: 183.129.145.245:9060
Connection: close
Accept-Encoding: gzip
User-Agent: okhttp/3.4.2

password=88888888&op_station=[redacted]&mobile_tel=[redacted]
```

APK渗透测试基础点

◆越权

问题描述：

越权问题是apk很容易存在的问题。越权可以分为水平越权和垂直越权。比如在渗透测试的时候，遇到一个场景，在登录时仅仅通过userid来获取用户信息，而这个userid是可以遍历的，这样造成的危害是可以越权读取其他人的身份信息或者账单信息等。

检测工具：抓包工具，Fillder,或者burpsuite

检测方法：通过抓包工具，主要对参数进行检查，特别是一些带有敏感关键字的参数，比如userid,username等。这些地方都是需要格外注意的地方.

APK渗透测试基础点

◆越权

水平越权

```
https.
hs_openid=20140917000000107&os=Android_4.4.2&serviceType=queryIntegralTaskInfo&channel=umeng&version=5.2.0
```

Hs_openid是一个敏感的参数，通过修改其id就可以越权读取其他用户的信息。

垂直越权

直接构造url就可以越权读取信息。

实验

抓包环境搭建

Burp+夜神模拟器

常用工具及环境搭建

工具	作用
Adb	操作管理android模拟器和真机
AndroidKiller	静态分析攻击，重打包等
Burpsuite	抓包工具
Fillder	抓包工具
Ida	强大静态和动态分析工具
Jeb	强大静态和动态分析工具
Android右键工具	自动化、快捷app信息查看工具
Drozer	Android app安全评估工具

常用工具及环境搭建

1. 工具名称 Apktool

   工具用途 GOOGLE提供的APK编译工具，能够反编译及回编译apk。

   相关信息https://code.google.com/p/android-apktool/

2. 工具名称 Dex2jar

   工具用途 将Android的dex文件反编译为java源码。

   相关信息https://code.google.com/p/dex2jar/w/list

3. 工具名称 Jd-gui

   工具用途 反编译代码阅读工具。

   相关信息http://jd.benow.ca/

4. 工具名称 Portecle

   工具用途 证书管理工具，可以进行证书维护。

   相关信息http://www.oschina.net/p/portecle

常用工具及环境搭建

5. 工具名称 SuperOneClick

   工具用途 Android手机root工具

   相关信息http://www.superoneclick.cc/

6. 工具名称 Proxydroid

   工具用途 Android手机用代理软件。

   相关信息https://github.com/madeye/proxydroid

7. 工具名称 MemSpector

   工具用途 Android手机内存修改工具

   相关信息http://www.nosec.org

8. 工具名称 BurpSuite

   工具用途 HTTP数据包修改、转发工具

   相关信息http://portswigger.net/burp/

常用工具及环境搭建

9. 工具名称 Fiddler

   工具用途 HTTP数据包修改、转发工具

   相关信息http://www.fiddler2.com/fiddler2/

10. 工具名称 Xposed框架

    工具用途 系统级框架，用于开发底层插件进行测试

    相关信息http://repo.xposed.info/module/de.robv.android.xposed.installer

11. 工具名称 SwipeBack

    工具用途 Xposed插件，用于绕过登陆界面

    相关信息http://repo.xposed.info/module/us.shandian.mod.swipeback

12. 工具名称 Android Development Tools

    工具用途 支持Android开发的工具

    相关信息http://developer.android.com/tools/help/adt.html

总结

APK基础安全测试即是一种新的安全测试也是一种旧的安全测试。要想对其熟练掌握还需要多动手联系。

另外，诸如梆梆扫描可以多使用一下，多仔细分析一下其列出来的安全漏洞点。

本期课件

1、本期PPT（PDF版）

2、Android渗透测试工具（含jd-gui）

3、2017年度移动App安全漏洞相关报告

4、Root Explorer-3.3.8(3.0+).apk

QUESSTION&THANKS