在漏洞检测模块中，为11类漏洞编写了检测插件，一共检测到了121处，共8类存在漏洞的代码，图 ？？？ 为其中两处漏洞代码示例。



图 ？？测试样本中的两处漏洞代码

漏洞1所示的问题代码在自实现的HostnameVerifier证书校验类中，校验函数verify()的返回值恒为1，没有实现有效校验，因此可能存在中间人攻击漏洞。

漏洞2所示的问题代码在加解密中，密钥直接明文存储在APK中，在图中可以看到加解密使用的密钥是29Blp39J，攻击者通过反编译即可拿到密钥

对测试样本中存在的121处漏洞代码的统计结果如表？？所示

表？？ 测试样本漏洞检测的统计结果

|  |  |
| --- | --- |
| 漏洞类型 | 数量 |
| checkServerTrusted()方法实现为空 | 4 |
| 检测到应用存在代码动态加载的行为 | 92 |
| HostnameVerifier非有效校验 | 3 |
| WebView明文存储密码漏洞 | 13 |
| 应用使用WebView，同时支持File协议 | 1 |
| WebView忽略SSL证书错误检测 | 2 |
| 应用程序加解密时密钥使用硬编码 | 5 |
| 应用外弹窗 | 1 |

在隐私泄露检测模块中，检测到了存在的隐私泄露问题共141条，图？？展示了其中两条隐私泄露代码



图？？？ 测试样本中的两处隐私泄露代码

在图？？中，第一处隐私泄露代码通过getLastKnownLocation ()函数获得用户位置，再通过Log.d()函数将其记录在日志中，造成用户隐私泄露。第二处隐私泄露代码通过getDeviceId()获得用户的设备ID，并通过网络请求将信息发送出去，造成用户隐私泄露。

对测试样本中存在的141处隐私泄露问题的统计结果如表？？所示

表9？？泄露的隐私类别统计

|  |  |
| --- | --- |
| 隐私类别 | 在测试中的发现数量 |
| 用户位置信息 | 1 |
| 用户唯一标志信息 | 18 |
| 用户网络访问相关信息 | 22 |
| 应用组件信息 | 1 |
| 程序运行间数据信息 | 99 |

表10 隐私数据发送方式统计

|  |  |
| --- | --- |
| 隐私类别 | 在测试中的发现数量 |
| 通过网络请求发送数据 | 2 |
| 通过日志记录数据 | 26 |
| 通过本地文件文件记录数据 | 27 |
| 通过应用组件传递数据 | 86 |