**移动APP检测平台测试报告**

**2016年1月**

**目录**

[一、测试概述 3](#_Toc7545)

[1.1.测试目的 3](#_Toc29931)

[1.2.测试对象 3](#_Toc8943)

[1.3.测试场景 3](#_Toc31560)

[1.4.测试地点 4](#_Toc3264)

[1.5.测试时间 4](#_Toc960)

[二、测试结论与总结 5](#_Toc27571)

[2.1测试结论 5](#_Toc8052)

[2.2测试总结 6](#_Toc2580)

[2.2.1检测项目测试 6](#_Toc7809)

[2.2.2检测项目测试详细对比 7](#_Toc29312)

[2.2.2.1.基本信息对比 7](#_Toc22558)

[2.2.2.2.组件安全对比 9](#_Toc544)

[2.2.2.3发布规范对比 10](#_Toc13431)

[2.2.2.4应用完整性对比 10](#_Toc2444)

[2.2.2.5程序机密性对比 10](#_Toc3702)

[2.2.2.6数据安全对比 13](#_Toc23018)

[2.2.3APP用例测试 16](#_Toc29927)

[2.2.3.1 10款app发现的漏洞情况 16](#_Toc18452)

[2.2.3.2 漏洞检测结果重点差距分析 18](#_Toc19857)

# 一、测试概述

## 1.1.测试目的

为开展行业移动应用安全检测服务，结合国内已有的移动APP应用的安全检测规范，我们特组织本次针对国内主流移动APP应用的安全检测工具测试，为移动安全检测工具提供选型参考。

## 1.2.测试对象

我们对国内主流移动APP应用厂商进行调研，选择了支持本地设备部署、支持远程多用户访问、支持B/S架构的检测平台进行测试。

|  |  |  |  |
| --- | --- | --- | --- |
| 检测工具名称 | 厂商 | 版本号 | 备注 |
| 爱加密移动安全检测平台 | 爱加密 | V1.2 |  |
| 梆梆移动安全检测平台 | 梆梆 | V2.2.0 |  |
| 思锐联移动安全检测平台 | 思锐联 | v2.0.1 |  |
| 娜迦移动安全检测平台 | 娜迦 | V2.1.2 |  |

## 1.3.测试场景

（1）测试人员通过浏览器登录检测平台；

（2）上传APP，平台完成检测并提供报告。共选择10个行业app应用进行测试，名称见下表。

表1：10个行业app应用列表

|  |  |  |  |
| --- | --- | --- | --- |
| 应用名称 | 版本 | 所属机构 | 备注 |
| 博时基金 | V1.1 | 博时基金 |  |
| 华夏基金管家 | V3.0.2 | 华夏基金 |  |
| 嘉实理财嘉 | V1.4.06 | 嘉实基金 |  |
| 财达大智慧 | V6.40 | 财达证券 |  |
| 小方 | V1.10.2 | 方正证券 |  |
| E海通财 | V3.11 | 海通证券 |  |
| 平安证券 | V5.7.0.5 | 平安证券 |  |
| 首创证券 | V5.3.4.15 | 首创证券 |  |
| 大商所 | V1.1 | 大商所 |  |

## 1.4.测试地点

北京市西城区金融街4号金益大厦4楼

## 1.5.测试时间

|  |  |  |
| --- | --- | --- |
| 厂商 | 时间 | 厂商参与人员 |
| 爱加密 | 2015.11.19-20 | 郭训平、曾志峰、苗慧明 |
| 梆梆 | 2015.11.18-19 | 李春蝶、于守清、杜楠 |
| 娜迦 | 2015.11.18-18 | 邹纲、张德文 |
| 思锐联 | 2015.11.17-17 | 赵小鹏、张展鹏 |

# 测试结论与总结

## 2.1测试结论

从本次测试的性能来看，各厂商信息扫描速度、并发支持、多任务同时处理、检测项目明确性、透明性、准确性、代码定位的支持均满足要求。其中自动报告生成，除娜迦一家厂商不支持外，其他厂商均支持自动报告生成。本次测试除了衡量各厂商检测的性能、检测结果外，检测项目更为重要。检测项目测试中，总体测试项包含：应用信息、组件安全、发布规范、应用完整性、程序机密性、数据安全。共50项检测内容。在检测项测试中部分厂商产品存在部分测试结果不满足的情况。爱加密、绑绑在应用基本信息获取全面准确。漏洞扫描速度很快，支持并发，多任务同时处理。检测项目目标明确，检测依据详细透明。扫描结果准确，界面直观，可直接定位到问题。自动生成报告格式规范，项目准确，描述清晰。支持开放接口，可二次开发整合。系统效率高，CPU和内存消耗小。支持超大安装包检测。尤其爱加密在漏洞检测方面比其它三家检测较为突出。

综合四家厂商产品在对检测项目支持、10个APP测试用例测试结果。综合考虑得出最终的测试结果。

**首选：爱加密**

**次选：梆梆**

**关注：思锐联、娜迦**

## 2.2测试总结

### 2.2.1检测项目测试

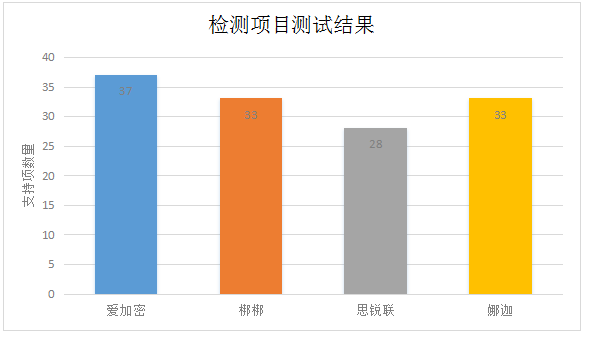
本次检测项目测试共测试50项。检测项目分为：基本信息检测、组件安全检测、发布规范检测、应用完整性检测、程序机密性检测、数据安全检测。各厂商的检测平台在检测项目中均有不通过情况，各厂商不通过情况如下：

1. 爱加密：检测平台共支持检测项目37项，达到检测项目50项要求的74%。检测信息全面、准确。
2. 梆梆：检测平台共支持检测项目33项，达到检测项目50项要求的66%。检测信息相对准确。
3. 娜迦：检测平台共支持检测项目33项，达到检测项目50项要求的66%。检测平台不支持自动检测报告的导出。
4. 思锐联：检测平台共支持检测项目28项，达到检测项目50项要求的56%。检测信息准确度差。

厂商测试项对比表：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 项目 | 爱加密 | 梆梆安全 | 思锐联 | 娜迦 |
| 基本信息 | 应用信息 | √ | √ | √ | √ |
| 签名信息 | √ | √ | √ | √ |
| 行为信息 | √ | √ | √ | √ |
| 权限信息 | √ | √ | √ | √ |
| 病毒检测 | √ | √ | × | × |
| 加固壳识别 | √ | √ | × | √ |
| 组件安全 | Activity安全 | √ | √ | √ | √ |
| Broadcast Receiver安全 | √ | √ | √ | √ |
| Service安全 | √ | √ | √ | √ |
| Content Provider安全 | √ | √ | √ | √ |
| Intent安全 | √ | √ | × | √ |
| 发布规范 | 测试数据移除 | √ | √ | √ | √ |
| 日志信息移除 | √ | √ | √ | √ |
| 内网测试信息残留 | √ | √ | √ | √ |
| 应用完整性 | 程序签名 | √ | × | × | √ |
| 完整性校验 | √ | √ | √ | √ |
| 程序机密性 | 代码混淆 | √ | √ | √ | √ |
| Dex保护 | √ | × | × | × |
| SO保护 | √ | × | × | × |
| 资源文件保护 | √ | × | × | × |
| 敏感函数调用风险 | × | √ | × | × |
| 调试日志调用 | √ | √ | √ | √ |
| 动态调试攻击 | √ | √ | √ | √ |
| 动态代码注入攻击 | √ | √ | √ | √ |
| 明文数字证书风险 | √ | √ | √ | √ |
| WebView明文储存密码风险 | √ | √ | √ | × |
| WebView远程代码执行漏洞 | √ | √ | √ | √ |
| 权限管理 | × | × | × | × |
| 模拟器检测 | √ | × | × | √ |
| 第三方SDK安全 | × | × | √ | × |
| 数据库注入漏洞 | √ | √ | × | √ |
| 随机数使用不当漏洞 | × | × | × | √ |
| secureRandom猜解 | × | × | √ | × |
| 数据安全 | 敏感数据显示 | √ | √ | √ | √ |
| 输入监听 | × | × | × | × |
| 存储数据类别 | × | × | × | × |
| 数据访问控制 | √ | √ | × | √ |
| 敏感数据加密 | √ | √ | × | √ |
| 内存数据安全 | √ | × | × | × |
| 远程数据通讯协议 | √ | √ | √ | √ |
| 证书验证 | √ | √ | √ | √ |
| 远程数据通信加密 | √ | √ | √ | × |
| 数据传输完整性 | × | √ | √ | √ |
| allowBackup安全漏洞 | √ | √ | √ | √ |
| 会话安全 | × | × | × | × |
| 重放攻击 | × | × | × | × |
| 资源文件中包含apk | × | × | √ | × |
| 调试信息 | √ | × | × | × |
| Java层ssl中间人攻击漏洞 | × | × | × | √ |
| 运行设备是否被Root风险 | × | × | × | √ |

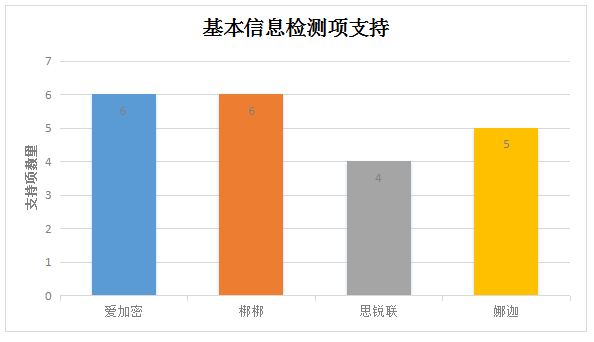
检测项目测试汇总结果如下图：



### 2.2.2检测项目测试详细对比

#### 2.2.2.1.基本信息对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 功能测试项 | 爱加密 | 梆梆 | 思锐联 | 娜迦 |
| 应用信息 | **√** | **√** | **√** | **√** |
| 签名信息 | **√** | **√** | **√** | **√** |
| 行为信息 | **√** | **√** | **√** | **√** |
| 权限信息 | **√** | **√** | **√** | **√** |
| 病毒检测 | **√** | **√** | **╳** | **╳** |
| 加固壳识别 | **√** | **√** | **╳** | **√╳** |



结论:

基本信息检测一共检测6项,爱加密、梆梆6项全部支持，娜迦支持5项，思锐联支持4项。

在应用信息获取方面全部支持，基本一致。签名信息获取方面，爱加密输出报告格式比较清晰直观，娜迦获取信息比较丰富。

权限获取方面，爱加密获取权限丰富，梆梆安全在权限上获取比较突出。

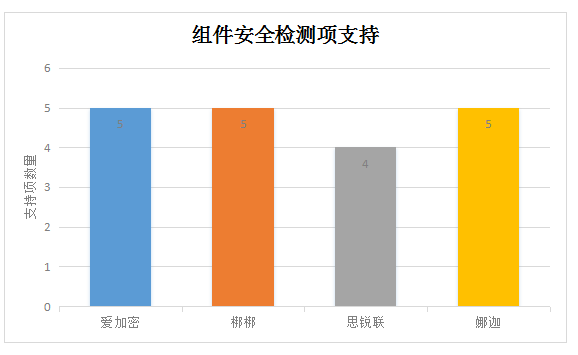
行为信息获取方面，四个平台全部支持，基本一致。

病毒检测方面，爱加密与梆梆具备该功能，思锐联与娜迦不具备该功能。

加固壳识别方面，爱加密、梆梆、娜迦具备该功能，思锐联不具备该功能。

#### 2.2.2.2.组件安全对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 功能测试项 | 爱加密 | 梆梆 | 思锐联 | 娜迦 |
| Activity安全 | **√** | **√** | **√** | **√** |
| Broadcast Receiver安全 | **√** | **√** | **√** | **√** |
| Service安全 | **√** | **√** | **√** | **√** |
| Content Provider安全 | **√** | **√** | **√** | **√** |
| Intent安全 | **√** | **√** | **╳** | **√** |



结论:

组件安全检测项方面共检测5个方面，爱加密、娜迦、梆梆5个方面全部支持，思锐联支持4项。

在四家厂商之中，除思锐联不具备Intent安全检测功能之外，其它三家全部支持。在漏洞详细信息输出方面，娜迦较为清晰直观，其它三家基本一致。

#### 2.2.2.3发布规范对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目 | 爱加密 | 梆梆 | 思锐联 | 娜迦 |
| 测试数据移除 | **√** | **√** | **√** | **√** |
| 日志信息移除 | **√** | **√** | **√** | **√** |
| 内网测试信息残留 | **√** | **√** | **√** | **√** |

结论:

通过测试发现四家厂商在发布规范方面全部支持，爱加密较为清晰直观，其它三家基本一致。

#### 2.2.2.4应用完整性对比

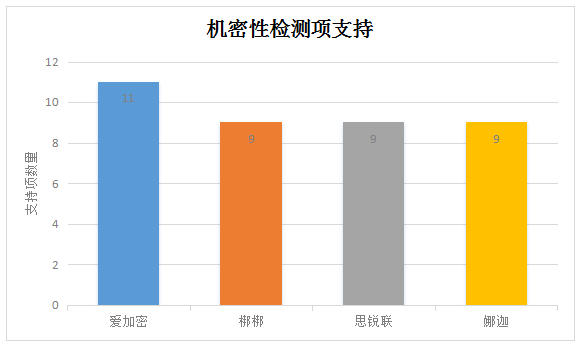
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目 | 爱加密 | 梆梆 | 思锐联 | 娜迦 |
| 程序签名 | **√** | **╳** | **╳** | **√** |
| 完整性校验 | **√** | **√** | **√** | **√** |

结论：

程序签名、完整性校验方面，爱加密检测结果最为准确检测方案最为合理，梆梆与思锐联不具备该功能检测。

#### 2.2.2.5程序机密性对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目 | 爱加密 | 梆梆 | 思锐联 | 娜迦 |
| 代码混淆 | **√** | **√** | **√** | **√** |
| Dex保护 | **√** | **╳** | **╳** | **╳** |
| SO保护 | **√** | **╳** | **╳** | **╳** |
| 资源文件保护 | **√** | **╳** | **╳** | **╳** |
| 敏感函数调用风险 | **╳** | **√** | **╳** | **╳** |
| 调试日志调用 | **√** | **√** | **√** | **√** |
| 动态调试攻击 | **√** | **√** | **√** | **√** |
| 动态代码注入攻击 | **√** | **√** | **√** | **√** |
| 明文数字证书风险 | **√** | **√** | **√** | **√** |
| WebView明文储存密码风险 | **√** | **√** | **√** | **╳** |
| WebView远程代码执行漏洞 | **√** | **√** | **√** | **√** |
| 权限管理 | **╳** | **╳** | **╳** | **╳** |
| 模拟器检测 | **√** | **╳** | **╳** | **√** |
| 第三方SDK安全 | **╳** | **╳** | **√** | **╳** |
| 数据库注入漏洞 | **╳** | **√** | **╳** | **√** |
| 随机数使用不当漏洞 | **╳** | **╳** | **╳** | **√** |
| secureRandom猜解 | **╳** | **╳** | **√** | **╳** |
| 支持数量 | 11 | 9 | 9 | 9 |



结论：

在程序机密性对比方面：爱加密支持11项功能要求，梆梆、娜迦、思锐联支持9项。

通过平台检测对比发现，各平台的调试日志调用、动态调试攻击、动态代码注入攻击、明文数字证书风险、WebView远程代码执行漏洞方面，四个平台全部支持，基本一致。

Dex保护方面，爱加密检测结果与分析过程清晰直观，梆梆、思锐联、娜迦不具备该功能检测。

SO保护方面，爱加密检测结果与分析过程清晰直观，梆梆、思锐联、娜迦不具备该功能检测。

资源文件保护方面，爱加密检测结果与分析过程清晰直观，梆梆、思锐联、娜迦不具备该功能检测。

模拟器检测方面，目前只有爱加密、娜迦支持检测，其它两家家均不支持。

WebView明文储存密码风险方面，爱加密、梆梆检测结果清晰直观并且分析方案最为详细，娜迦不具备该功能检测。

secureRandom猜解、第三方SDK安全方面，目前只有思锐联支持检测，其它三家均不支持。

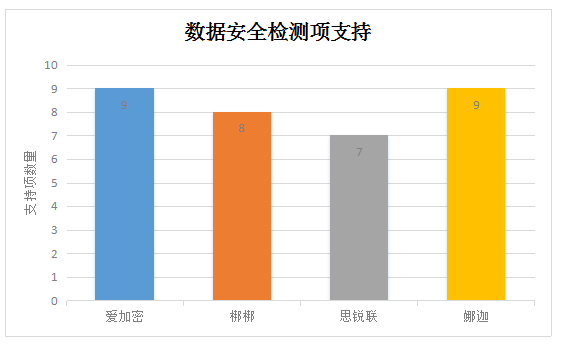
数据库注入漏洞目前只有梆梆、思锐联支持检测，其它二家均不支持。

随机数使用不当漏洞方面，目前只有娜迦支持检测，其它三家均不支持。

敏感函数调用风险方面，目前只有梆梆支持检测，其它三家均不支持。

#### 2.2.2.6数据安全对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 项目 | 爱加密 | 梆梆 | 思锐联 | 娜迦 |
| 敏感数据显示 | **√** | **√** | **√** | **√** |
| 输入监听 | **╳** | **╳** | **╳** | **╳** |
| 存储数据类别 | **╳** | **╳** | **╳** | **╳** |
| 数据访问控制 | **√** | **√** | **╳** | **√** |
| 敏感数据加密 | **√** | **√** | **╳** | **√** |
| 内存数据安全 | **√** | **╳** | **╳** | **╳** |
| 远程数据通讯协议 | **√** | **√** | **√** | **√** |
| 证书验证 | **√** | **√** | **√** | **√** |
| 远程数据通信加密 | **√** | **√** | **√** | **╳** |
| 数据传输完整性 | **╳** | **√** | **√** | **√** |
| allowBackup安全漏洞 | **√** | **√** | **√** | **√** |
| 会话安全 | **╳** | **╳** | **╳** | **╳** |
| 重放攻击 | **╳** | **╳** | **╳** | **╳** |
| 资源文件中包含apk | **╳** | **╳** | **√** | **╳** |
| 调试信息 | **√** | **╳** | **╳** | **╳** |
| Java层ssl中间人攻击漏洞 | **╳** | **╳** | **╳** | **√** |
| 运行设备是否被Root风险 | **╳** | **╳** | **╳** | **√** |
| 支持数量 | 9 | 8 | 7 | 9 |



结论：

在数据安全性方面：爱加密、娜迦支持9项功能，梆梆支持8项、思锐联支持7项功能。

通过平台检测对比发现，各平台的敏感数据显示、证书验证、远程数据通信加密、allowBackup安全漏洞方面，四个平台全部支持，基本一致。

内存数据安全方面，爱加密检测结果与分析过程清晰直观，梆梆、思锐联、娜迦不具备该功能检测。

调试信息方面，爱加密支持，其他三件均不支持。

数据访问控制、敏感数据加密方面，爱加密、梆梆、娜迦支持检测，思锐联不支持。

远程数据通信加密方面、爱加密、梆梆、思锐联支持检测。娜迦不支持。

资源文件中包含apk方面，思锐联支持，其他不支持

Java层ssl中间人攻击漏洞、运行设备是否被Root风险方面，娜迦支持检测，其他三家不支持。

### 2.2.3APP用例测试

#### 2.2.3.1 10款app发现的漏洞情况

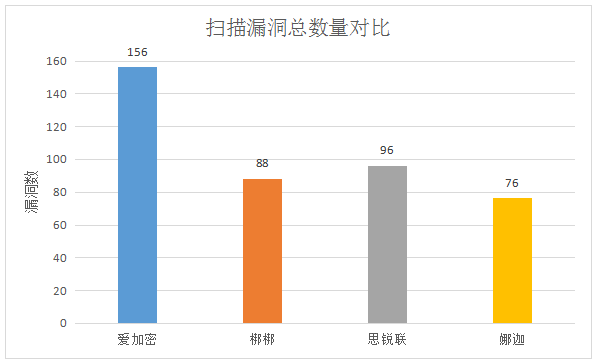
本次测试通过10款APP进行测试，10款APP分别为：大商所、方正证券、海通证券、财达证券、平安证券、首创证券、华夏基金、嘉实基金、博时基金、招商基金。各厂商对10款APP进行漏洞扫描结果如下：

1. 各厂家发现漏洞总数情况

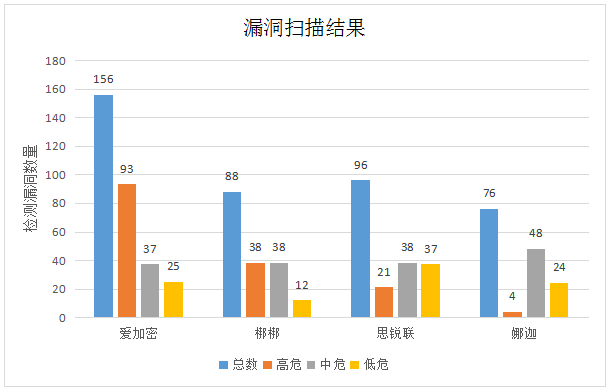
* 爱加密：发现漏洞总数为156个漏洞，其中高危漏洞93个，中危漏洞37个，低危漏洞25个。
* 思锐联：发现漏洞总数为96个漏洞，其中高危漏洞21个，中危漏洞38个，低危漏洞37个。
* 梆梆：发现漏洞总数为88个漏洞，其中高危漏洞38个，中危漏洞38个，低危漏洞12个。
* 娜迦：发现漏洞总数为76个漏洞，其中高危漏洞4个，中危漏洞48个，低危漏洞24个。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 厂商名称机构名称 | **爱加密** | | | | **梆梆** | | | | **思锐联** | | | | **娜迦** | | | |
| 高危 | 中危 | 低危 | 汇总 | 高危 | 中危 | 低危 | 汇总 | 高危 | 中危 | 低危 | 汇总 | 高危 | 中危 | 低危 | 汇总 |
| 大商所 | 11 | 4 | 3 | **18** | 5 | 5 | 0 | **10** | 2 | 3 | 5 | **10** | 1 | 4 | 3 | **8** |
| 方正证券 | 10 | 5 | 2 | **17** | 6 | 4 | 3 | **13** | 4 | 5 | 6 | **15** | 1 | 7 | 5 | **13** |
| 海通证券 | 10 | 5 | 3 | **18** | 6 | 4 | 3 | **13** | 4 | 4 | 4 | **12** | 1 | 7 | 3 | **11** |
| 财达证券 | 9 | 3 | 3 | **15** | 4 | 3 | 0 | **7** | 1 | 3 | 1 | **5** | 0 | 3 | 0 | **3** |
| 平安证券 | 9 | 4 | 3 | **16** | 8 | 6 | 2 | **16** | 3 | 5 | 5 | **13** | 1 | 7 | 3 | **11** |
| 首创证券 | 10 | 3 | 3 | **16** | 4 | 4 | 1 | **9** | 2 | 4 | 3 | **9** | 0 | 5 | 1 | **6** |
| 华夏基金 | 8 | 4 | 2 | **14** | 0 | 3 | 0 | **3** | 1 | 4 | 3 | **8** | 0 | 4 | 3 | **7** |
| 嘉实基金 | 8 | 3 | 2 | **13** | 0 | 3 | 0 | **3** | 1 | 3 | 3 | **7** | 0 | 4 | 2 | **6** |
| 博时基金 | 10 | 3 | 3 | **16** | 4 | 3 | 3 | **10** | 3 | 4 | 4 | **11** | 0 | 3 | 2 | **5** |
| 招商基金 | 8 | 3 | 1 | **13** | 1 | 3 | 0 | **4** | 0 | 3 | 3 | **6** | 0 | 4 | 2 | **6** |
| 漏洞总数 | 93 | 37 | 25 | **156** | 38 | 38 | 12 | **88** | 21 | 38 | 37 | **96** | 4 | 48 | 24 | **76** |

扫描结果，漏洞数量：



扫描结果详情对比图(包含扫描出高危、中危、低危数量)：

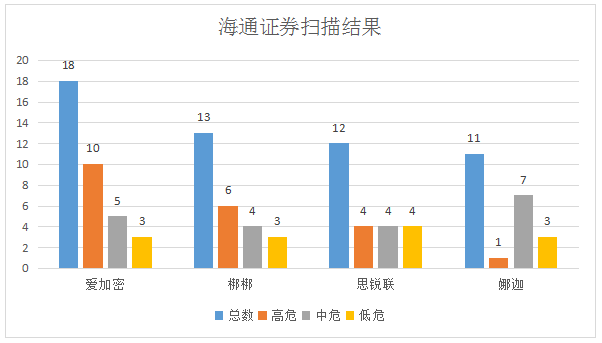


#### 2.2.3.2 漏洞检测结果重点差距分析

重点对海通证券、平安证券、华夏基金3个APP的漏洞检测情况进行分析，结果如下：

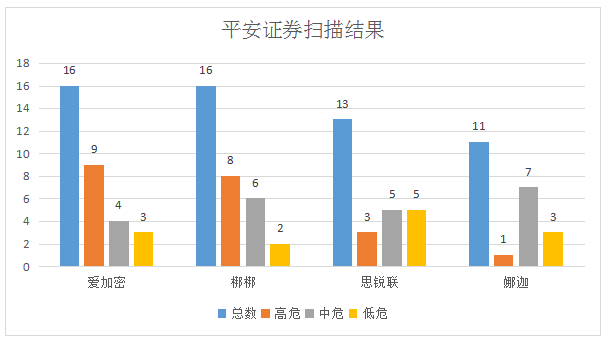
1. 海通证券：对海通证券APP客户端的扫描检测结果是：

* 爱加密：一共发现18个漏洞，其中高、中、低危漏洞数量分别为：10个、5个、3个。
* 梆梆：一共发现13个漏洞，其中高、中、低危漏洞数量分别为：6个、4个、3个。
* 思锐联：一共发现12个漏洞，其中高、中、低危漏洞数量分别为：4个、4个、4个。
* 娜迦：一共发现11个漏洞，其中高、中、低危漏洞数量分别为：1个、7个、3个。



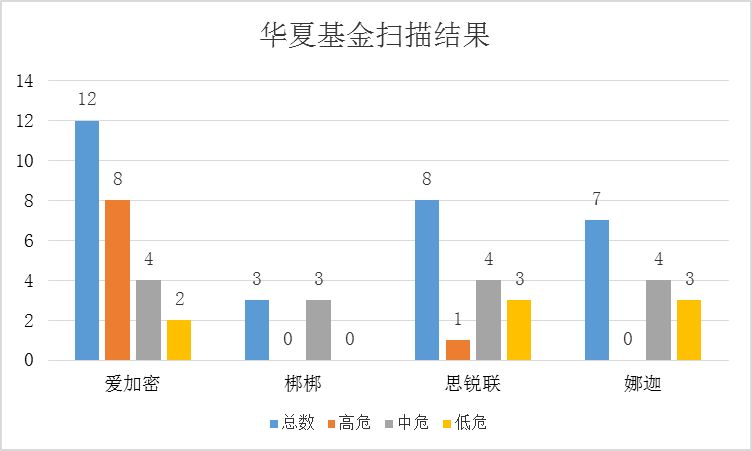
1. 平安证券：对平安证券APP客户端的扫描检测结果是：

* 爱加密：一共发现16个漏洞，其中高、中、低危漏洞数量分别为：9个、4个、3个。
* 梆梆：一共发现16个漏洞，其中高、中、低危漏洞数量分别为：8个、6个、2个。
* 思锐联：一共发现13个漏洞，其中高、中、低危漏洞数量分别为：3个、5个、5个。
* 娜迦：一共发现11个漏洞，其中高、中、低危漏洞数量分别为：1个、7个、3个。



1. 华夏基金：对华夏基金APP客户端的扫描检测结果是：

* 爱加密：一共发现12个漏洞，其中高、中、低危漏洞数量分别为：8个、4个、2个。
* 梆梆：一共发现3个漏洞，其中高、中、低危漏洞数量分别为：0个、3个、0个。
* 思锐联：一共发现8个漏洞，其中高、中、低危漏洞数量分别为：1个、4个、3个。
* 娜迦：一共发现7个漏洞，其中高、中、低危漏洞数量分别为：0个、4个、3个。



注:华夏基金APP因采用梆梆加密，所以在检测漏洞有所差距。