

移动安全

快速入门

快速入门

登录 移动安全管理控制台。

单击 开通移动安全，即可开通。



以漏洞扫描升级专业版为例，步骤如下：

第一步 购买实例

（若已购买该服务专业版实例，跳过这一步）

[点击查看教程](#)

第二步 应用所有权认证

（若该应用已认证过，则跳过这一步）

为了保障应用开发者的隐私，在实例配置前需进行应用所有权认证

（1）进入管理控制台总览页

（2）选择要认证应用，点击该应用的【升级】下拉框

总览

续费管理

漏洞扫描剩余24个未配置实例，仿冒检测剩余11个未配置实例，应用加固剩余12个未配置实例

全部应用(7)

专业版(5)

上传应用(限APK)

应用名称	包名	版本	应用所有权	漏洞扫描	恶意代码扫描	仿冒检测	应用加固	操作
安全风险Demo	com.alibaba.wireless.jaq	1.0	认证成功	12 专业版	1	40 专业版	加固失败 专业版	删除
test_studio	com.example.xiaopai.test_studio	1.0	未认证	4	0	0	下载加固包 专业版	升级 删除
jaqtest_ft1	com.alibaba.wsqa.jaqtest.ft	1.0	认证成功	4	0	0	下载加固包 专业版	漏洞扫描 仿冒检测 应用加固
test8	com.alibaba.ws.jaq.test.demo8	8.0	认证成功	5	0	0	下载加固包	

(3) 选择欲升级的服务，进入所有权认证页面

(4) 参照验证原理，下载空白应用，使用页面所示命令进行签名后上传。

注意：认证已发布的应用，待认证应用、空白应用和官方应用的签名必须保持一致；如果你的应用还在开发中，则需保持待认证应用和空白应用的签名一致。

升级

返回上级

查看详细签名教程 >>

应用所有权认证

实例配置

认证原理

为保护应用隐私，我们将对您所要升级的应用进行所有权认证。请先下载空白包，使用与待认证应用相同的keystore进行签名后上传。

签名流程3步骤:

1

下载空白包

下载

2

对空白包进行签名 (签名工具和签名流程可咨询应用开发人员)

在命令行输入:
jarsigner -verbose -keystore [keystorePath] -signedjar [apkOut] [apkin] [alias]
* 命令格式及参数意义

3

上传签名后的空白包

上传

(5) 认证成功，总览页面会显示“认证成功”，同时您将会收到收到短信，邮件和站内信通知。

总览

续费管理

漏洞扫描剩余3个未配置实例，仿冒检测剩余0个未配置实例，应用加固剩余0个未配置实例

全部应用(3)

专业版(2)

上传应用(限APK)

应用名称	包名	版本	应用所有权	漏洞扫描	恶意代码扫描	仿冒检测	应用加固	操作
安全风险Demo	com.alibaba.wireless.jaq	1.0	认证成功	12 专业版	1	40 专业版	加固失败 专业版	删除
	com.example.xiaopai.test_studio	1.0	认证成功	4 专业版	0	开始检测	开始加固	删除
	com.alibaba.ws.jaq.test.demo7	7.0	认证成功	5	0	0	下载加固包	删除

(6) 若认证失败，则会在页面中提醒错误原因与解决办法，请解决后重新上传。



(7) 若出现以下页面，说明您的应用进入人工审核流程，请填写官网下载地址或大型应用市场下载页面地址，配合工作人员进行审核，预计需要1个工作日，请耐心等待。



第三步 实例配置

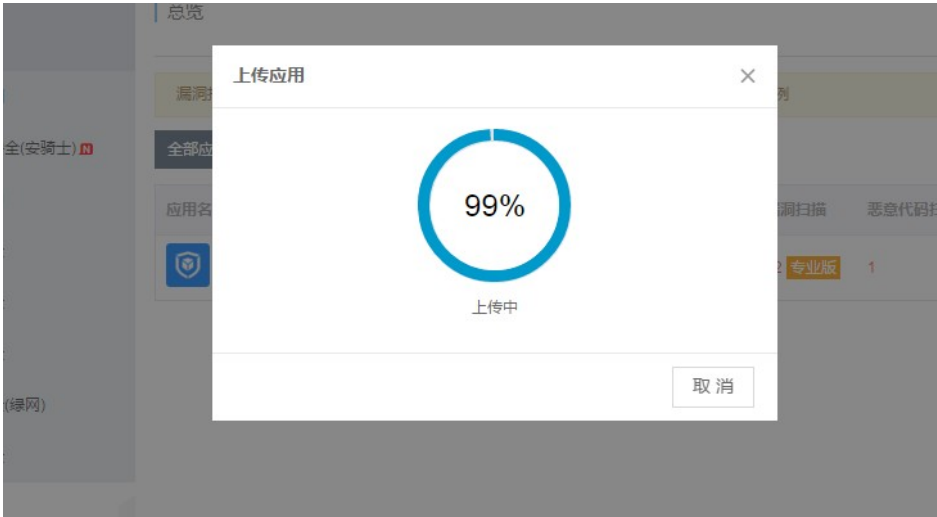
应用所有权通过后，则会自动跳转到实例配置页面。若是人工审核通过，则需点击总览页【升级】按钮进入。在实例列表中选择您要使用的实例，点击【确定】，将其配置到应用上。



单击左侧栏目【总览】，在页面右上角上传APK包。



等待上传应用，上传成功后勾选漏洞扫描功能（可以全部勾选），等待完成APK扫描。



单击漏洞扫描的数字，进入漏洞扫描页面查看漏洞具体详情。

漏洞扫描剩余0个未配置实例，仿冒检测剩余0个未配置实例，应用加固剩余0个未配置实例

全部应用(2)	专业版(1)	上传应用(限APK)						
应用名称	包名	版本	应用所有权	漏洞扫描	恶意代码扫描	仿冒检测	应用加固	操作
 安全风险Demo	com.alibaba.wireless.jaq	1.0	认证成功	12 专业版	1	40 专业版	加固失败 专业版	删除
			未认证	299	0	0	下载加固包	删除

页面上方显示为漏洞总数和漏洞分类，下方为漏洞名称、详情、修复建议等。

漏洞扫描

当前应用：安全风险Demo 1.0

漏洞总数：12

漏洞分类：4个 高危, 8个 中危, 0个 低危

漏洞名称	漏洞详情	修复建议	漏洞等级	操作
webview远程代码执行漏洞(1个)	addJavascriptInterface存在高危远程代码执行漏洞。应尽量避免使用API 17中用@JavascriptInterface代替addJavascriptInterface，移除系统webkit内置的危险接口searchBox.JavaBridge.accessibility.accessibilityTraversal	应尽量避免使用API 17中用@JavascriptInterface代替addJavascriptInterface，移除系统webkit内置的危险接口searchBox.JavaBridge.accessibility.accessibilityTraversal	高危	展开
随机数生成函数使用错误(1个)	使用SecureRandom时不要使用SecureRandom(byte[] seed)这个构造函数，会造成生成的随机数不随机。	建议通过devRandom或devRandom获取的随机数初始化伪随机数生成器PRNG	高危	展开
HTTPS禁止使用ALLOW_ALL_HOSTNAME_VERIFI				

展开漏洞详情，可查看具体漏洞位置。

漏洞名称	漏洞详情	修复建议	漏洞等级	操作
主机名弱效验(2个)	在实现的HostnameVerifier子类中未对主机名做效验，这样会导致恶意程序利用中间人攻击绕过主机名效验。利用HostnameVerifier子类中的verify函数效验服务器主机名的合法性。	在实现的HostnameVerifier子类verify函数中校验主机名的合法性。	中危	展开

漏洞名称	漏洞详情	修复建议	漏洞等级	操作
主机名弱效验(2个)	在实现的HostnameVerifier子类中未对主机名做效验，这样会导致恶意程序利用中间人攻击绕过主机名效验。利用HostnameVerifier子类中的verify函数效验服务器主机名的合法性。	在实现的HostnameVerifier子类verify函数中校验主机名的合法性。	中危	收起
当前试用的是免费版漏洞扫描，点击升级，查看详细漏洞位置 漏洞位置： 1、Lcom/fuya/smart**** 2、Lcom/squareup/okhttp****				

注意：如果您需要查看具体的漏洞位置，请 升级到专业版。

单击左侧栏目 **总览**，在页面右上角上传APK包。

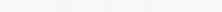


等待上传应用，上传成功后勾选应用加固功能（可以全部勾选）。



等待应用加固完成，下载加固包，并给 应用签名。

漏洞扫描剩余0个未配置实例，仿冒检测剩余0个未配置实例，应用加固剩余0个未配置实例

全部应用(2)	专业版(1)	上传应用(报APK)						
应用名称	包名	版本	应用所有权	漏洞扫描	恶意代码扫描	仿冒检测	应用加固	操作
 安全风险Demo	com.alibaba.wireless.jaq	1.0	认证成功	12 专业版	1	40 专业版	加固失败 专业版	删除
			未认证	299	0	0	下载加固包	删除

或者单击左边栏 应用加固，下载加固包并给应用签名。

产品与服务

云服务器 ECS

云数据库 RDS 版

负载均衡

对象存储 OSS

域名

云解析

服务器安全（安骑士）

态势感知

云盾

用户中心

账号管理

应用中心

资产管理

消息中心

云盾

态势感知

应用加固

安全组件

应用加固

返回上一页

重新加固

上传应用

升级

当前试用的是免费版应用加固，专业版在此基础上增加SO加固，JAVA常量加固，JAVA指令翻译和JAVA模拟执行等高级加固选项，还提供API接口满足自动化服务的需求。[点击查看](#)

当前应用：Test 1.0

免费版加固项：
DEX加固 对DEX文件进行加壳加密，保护JAVA层代码

专业版加固项：
SO加固 通过对SO进行加壳加密，防止应用被逆向破解
JAVA常量加固 加密DEX文件中的明文常量字符串，增大了逆向分析的难度
JAVA指令翻译 修改JAVA层业务逻辑的调用关系链，达到保护业务逻辑的效果
JAVA模拟执行 通过对DEX文件中的指令抽离，并使用一个自定义的执行环境进行模拟执行

下载加固包

升级专业版

专业版加固享有更多加固项

当前试用的是基础版应用加固，专业版在此基础上增加SO加固，JAVA常量加固，JAVA指令翻译和JAVA模拟执行等高级加固选项，还提供API接口满足自动化服务的需求。如有需求，请查看 升级专业版。

当前试用的是基础版应用加固，专业版在此基础上增加SO加固，JAVA常量加固，JAVA指令翻译和JAVA模拟执行等高级加固选项，还提供API接口满足自动化服务的需求。[点击查看](#)

当前应用：

基础版加固项：
DEX加固 对DEX文件进行加壳加密，保护JAVA层代码

专业版加固项：
SO加固 通过对SO进行加壳加密，防止应用被逆向破解
JAVA常量加固 加密DEX文件中的明文常量字符串，增大了逆向分析的难度
JAVA指令翻译 修改JAVA层业务逻辑的调用关系链，达到保护业务逻辑的效果
JAVA模拟执行 通过对DEX文件中的指令抽离，并使用一个自定义的执行环境进行模拟执行

下载加固包

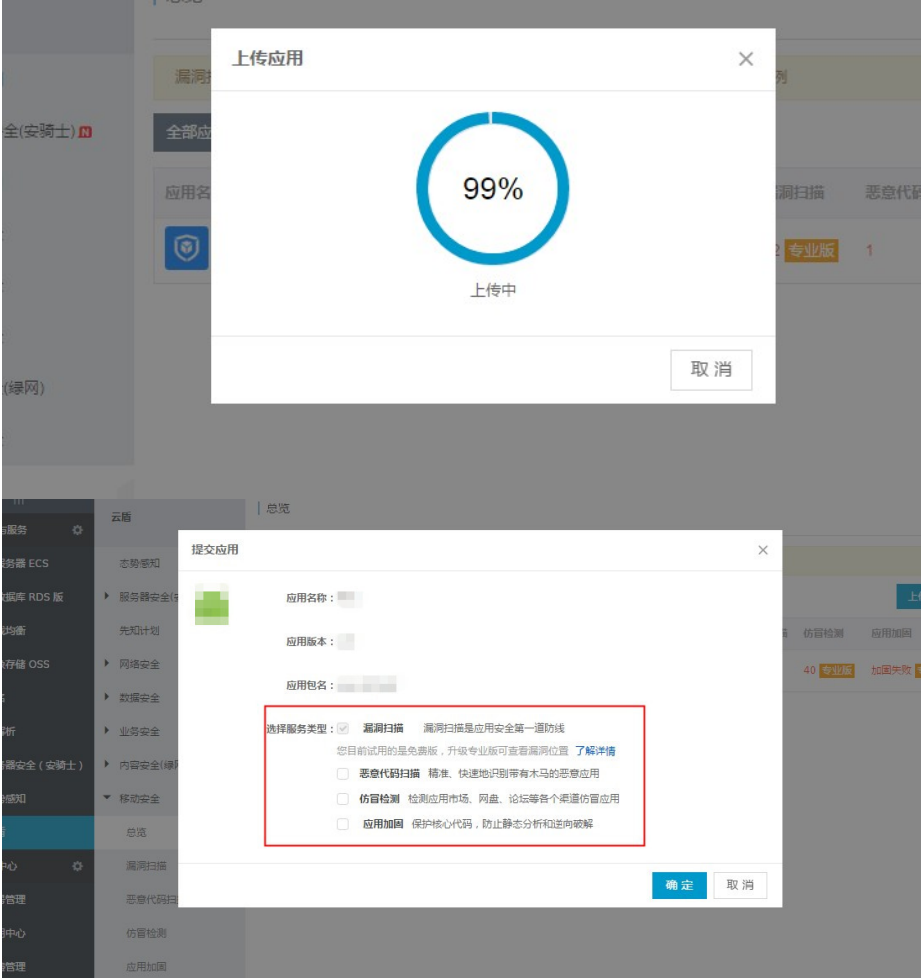
升级专业版

专业版加固享有更多加固项

1.点击左侧栏目【总览】，在页面右上角上传APK包



2.等待上传应用，上传成功后勾选仿冒检测功能（可以全部勾选），等待完成APK扫描



3.点击仿冒检测下的数字，进入扫描页面查看仿冒详情



4.页面显示为仿冒应用的名称、包名及仿冒应用地址

当前应用:

仿冒应用名称	包名	仿冒应用地址
		1、*****/api/v1/download?appkey=BIVKJJuXJKFlhVDw&sign=97606fd77a903427a680334ce13c6301&time=1465754455&file_md5=2c1cc2285167c3f073ee691eea5579b1&file_sha1=69e76a77666e98fabee3ef2c22c5c67ea03c322e
		1、*****/api/v1/download?appkey=BIVKJJuXJKFlhVDw&sign=ff831cc746abd7d1150166133112f40&time=1465241550&file_md5=647c523fa0ef53bb93c9e7db86dd2876&file_sha1=bc85aed055f95ec2ce8f522caf9a568482fa55ac
		1、*****/api/v1/download?appkey=BIVKJJuXJKFlhVDw&sign=ec7543b314772bc26b43ec7755944cb9&time=1464727706&file_md5=4f28dd8895f36678eebeb3e81d23df33&file_sha1=13ed9fe73d3a77d9895efcfe99d662941953d09
		1、*****/api/v1/download?appkey=BIVKJJuXJKFlhVDw&sign=81555541d0d962b0687ba39b67bd875c&time=1464294106&file_md5=01d590b6d341ee98537a2abd6ab74520&file_sha1=c2f8afd4ba57ddf5574694aee7a41305c250d0d
		1、*****/api/v1/download?appkey=BIVKJJuXJKFlhVDw&sign=65f8f5d870d9053f8dc5b4e21710b39&time=1464722421&file_md5=ad4eeba4ded2ae0a84fd4a15788ea081&file_sha1=144592068051b15f7c5bc4018114899f4f3fe71
		1、*****/api/v1/download?appkey=BIVKJJuXJKFlhVDw&sign=fb444bb9ebdac60f7462f950e97c7e9e&time=1465414403&file_md5=6ff4c308c636425d91dfe7b31240400&file_sha1=31d56e295a514c32fb7ba5d8cc1a4505da94b8

5.需要看到具体的仿冒应用地址需要升级到专业版

1.点击左侧栏目【总览】，在页面右上角上传APK包

漏洞扫描剩余0个未配置实例，仿冒检测剩余0个未配置实例，应用加固剩余0个未配置实例

全部应用(1)

专业版(1)

上传应用(限APK)

应用名称	包名	版本	应用所有权	漏洞扫描	恶意代码扫描	仿冒检测	应用加固	操作
 安全风险Demo	com.alibaba.wireless.jaq	1.0	认证成功	12 专业版	1	40 专业版	加固失败 专业版	删除

2.等待上传应用，上传成功后勾选恶意代码扫描功能（可以全部勾选），等待完成APK扫描

上传应用

99%

上传中

取消



3.点击恶意代码扫描下的数字，进入扫描页面查看恶意代码详情



4.页面上方显示为恶意代码的风险等级，下方为恶意代码详情



1.点击左侧栏目【总览】，在页面右上角上传APP



2.等待上传应用，上传成功后勾选安全组件功能（可以全部勾选）



3.下载免费版安全组件，按照接入文档接入集成

应用名称	版本	应用所有者	漏洞扫描	恶意代码扫描	仿冒检测	应用加固	安全组件	操作
安全风险Demo	1.0	已认证	12 专业版	1	41 专业版	加强防护 专业版	下载SDK	删除
		已认证	17	开始扫描	开始检测	开始加固	下载SDK	升级 • 删除

4.Android平台提供基础版和企业版，基础版为免费版本，用户可免费下载使用；企业版为收费版本，用户需在线付费购买后方可下载。

iOS平台仅提供收费的企业版，用户需在线付费购买后方可下载。

安全组件接入请查看接入教程

应用开发者在对加固包进行重签名时，建议使用之前对应用签名的keystore，以避免同一应用使用不同签名导致无法正常上传到应用市场的情况。

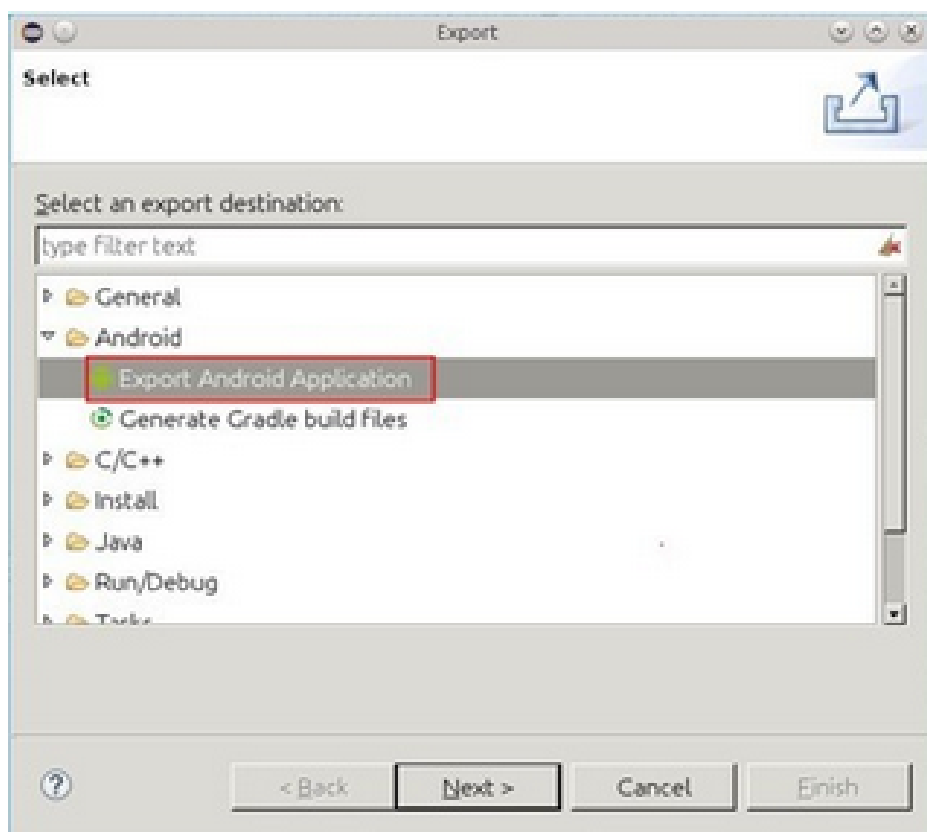
- 使用方法：jarsigner -digestalg SHA1 -sigalg MD5withRSA -verbose -keystore

```
[your_keystore_path] -signedjar [signed_apk_name] [unsigned_apk_name]  
[your_keystore_alias]
```

- 其中，your_keystore_path代表密钥所在位置的绝对路径；
- signed_apk_name代表签名后的安装包名称；
- unsigned_apk_name代表未签名的安装包名称；
- your_keystore_alias代表密钥的别名。

2.获取 keystore

在eclipse项目上点击右键，选择Export，选择Export Android Application并点击Next，Location项中显示的绝对路径即是之前使用过的keystore位置，将此作为步骤1 “使用方法 ”中的your_keystore_path。



3.获取 key alias

在keystore界面点击Next，进入key选择界面。在此界面中可以看到keystore中存储的所有可用key，选择之前对应用签名时使用的key alias，将此作为步骤1“使用方法 ”中的your_keystore_alias。

