爱加密
IJIAMI.CN

爱加密安全检测系统

操作手册

北京智游网安科技有限公司

目录

1 引言 3

2 业务流程 3

2.1 实现流程 3
2.2 服务流程 4

3 产品模块及功能介绍 4

3.1 系统功能简介 4
3.2 系统功能模块介绍 4
3.2.1 用户登录及主页面 4
3.2.2 系统管理菜单介绍 5
3.3 检测功能模块介绍 7
3.3.1 漏洞检测 7
3.3.2 风险项排名 9
3.3.3 APP 安全排名 9
3.3.4 检测项设置 10

4 操作说明 11

4.1 管理员操作说明 11
4.1.1 登录系统 11
4.1.2 添加角色 12
4.1.3 添加用户 14
4.1.4 授权码修改 16
4.1.5 查看风险项排名 18
4.1.6 查看 APP 安全排名 20
4.1.7 设置检测项 22
4.2 普通用户操作说明 24
4.2.1 登录系统 24
4.2.2 APK 漏洞检测 24
4.2.3 查看检测结果 26
4.2.4 下载报告 27

5 服务响应 28

1 引言

本手册详细叙述爱加密安全检测系统的操作说明。

本文档预期的读者对象包括系统技术小组人员、测试人员、维护人员。

技术人员在进行实际操作前务必详细阅读本手册。

2 业务流程

2.1 实现流程

开发者只需将 APK 包上传至安检平台，平台自动完成安全检测，生成安全检测报告。开发者下载报告，即可查看分析结果。

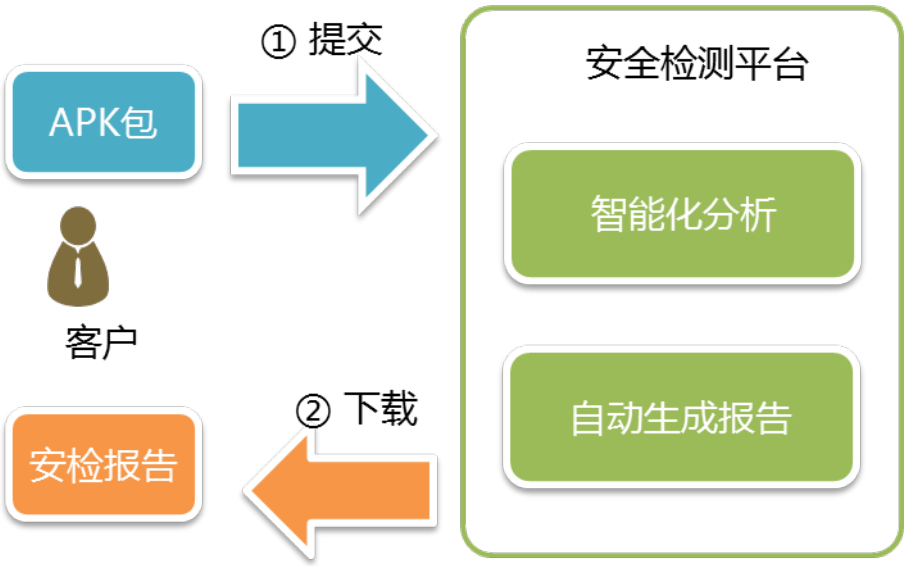

图2-1 实现流程

2.2 服务流程

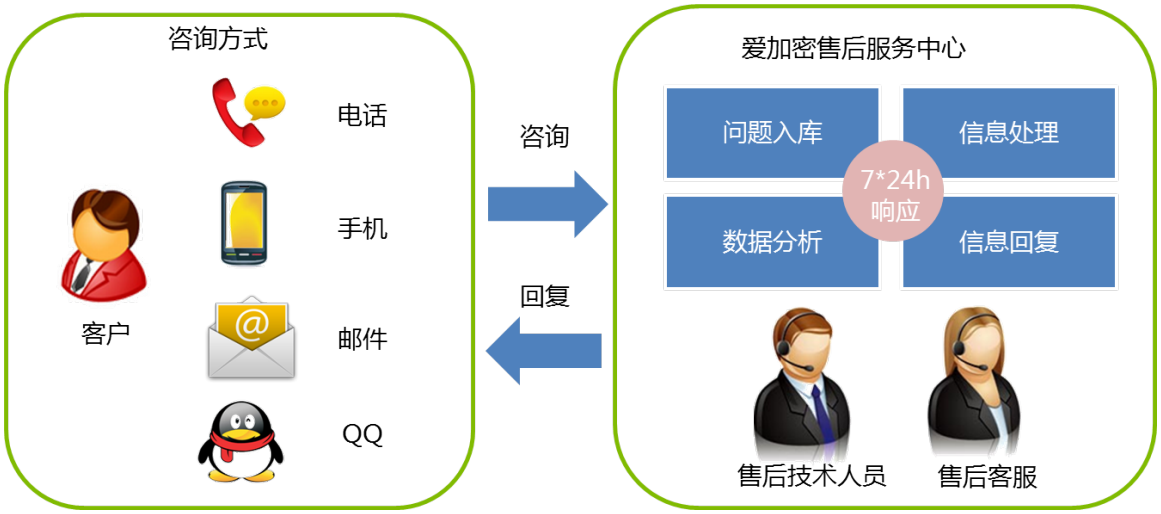

图2-2 服务流程

3 产品模块及功能介绍

3.1 系统功能简介

本系统具备核心功能和检测系统两部分，检测系统主要为普通用户对 APP 进行安全检测，核心功能主要为超级管理员管理用户、设置检测相关参数、查看 APP 安全排名、查看风险项排名等。

3.2 系统功能模块介绍

3.2.1 用户登录及主页面

打开浏览器，在浏览器中输入网址 http://xx.xx.xx.xx，xx.xx.xx.xx 为服务器 IP 地址。

图3-1

系统初始提供一个管理员账号，用户名 admin，密码 Admin_123。输入用户名和密码，点击“登录”。

图3-2

3.2.2 系统管理菜单介绍

3.2.2.1 角色管理

角色的作用：为不同使用权限的用户进行权限的分类授权。

系统初始有两个角色分别为超级管理员、普通员工。超级管理员角色默认已

添加系统所有权限，普通员工角色默认只添加了系统访问和加密相关权限。管理员可对初始角色的权限进行修改，添加更多的角色便于对不同类型的用户授权。

登录系统后，打开“核心功能”，点击左边的“角色管理”。

图3-3

3.2.2.2 用户管理

用户管理用来添加、删除、修改用户信息。系统初始有一个普通用户 ijiami，一个超级管理员用户 admin。admin 超级管理员用户默认不显示，超级管理员用户 admin 不允许做修改和删除操作。

登录系统后，打开“核心功能”，在左边的菜单栏中选择“用户管理”。

图3-4

3.2.2.3 系统管理

3.2.2.3.1 授权码管理

授权码管理是爱加密安全检测系统一套为用户使用系统授权的机制，在系统使用之前或者重新更换加密服务器之前都必须重新授权才能正常使用。

使用管理员登录后，打开左侧菜单栏中“核心功能”下的“授权码管理”，如图 3-5 所示。

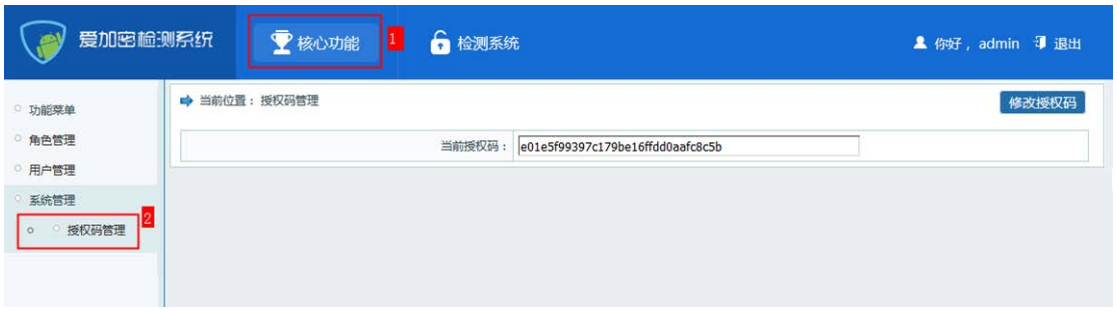

图3-5

3.3 检测功能模块介绍

3.3.1 漏洞检测

漏洞检测就是本系统的主要功能，根据设置的检查项对 APP 进行检测。

登录加密系统后打开左边菜单栏中“漏洞检测”。

图3-6

打开加密窗口后可以看到有查询和上传两个部分，“查询”是针对查看之前检测的记录，可通过应用名称、上传用户以及创建时间进行查询。

“上传应用”将 APK 上传至检测系统进行检测。

点击“查看详情”，如所示，查看漏洞检测的进度及检测结果，如图 3-7 所示。

图3-7

点击“下载报告”，下载安全检测报告。

3.3.2 风险项排名

风险项排名是对系统中所有应用检测出现安全风险的检测项的排名，根据检测项出现安全风险的次数进行排名。

打开左侧菜单栏中的“风险项排名”，如图 3-8 所示。

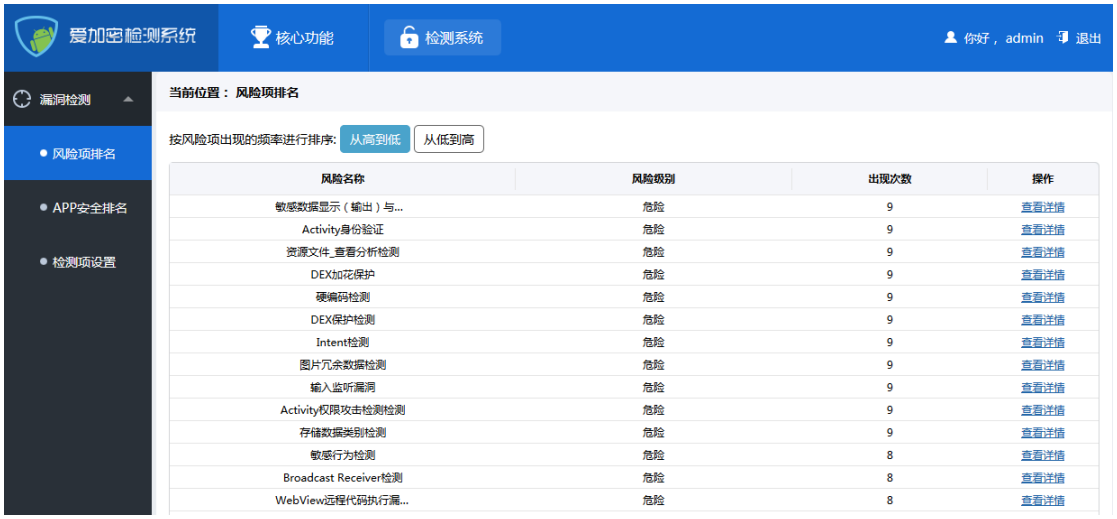

图3-8

点击“查看详情”，查看该检测项出现安全风险的应用，如图 3-9 所示。

图3-9

3.3.3 APP 安全排名

APP 安全排名是对 APP 安全性的排名，更加 APP 检测分数来排名，分数越高安全性越强。

打开左侧菜单栏中的“APP 安全排名”，如图 3-10 所示。

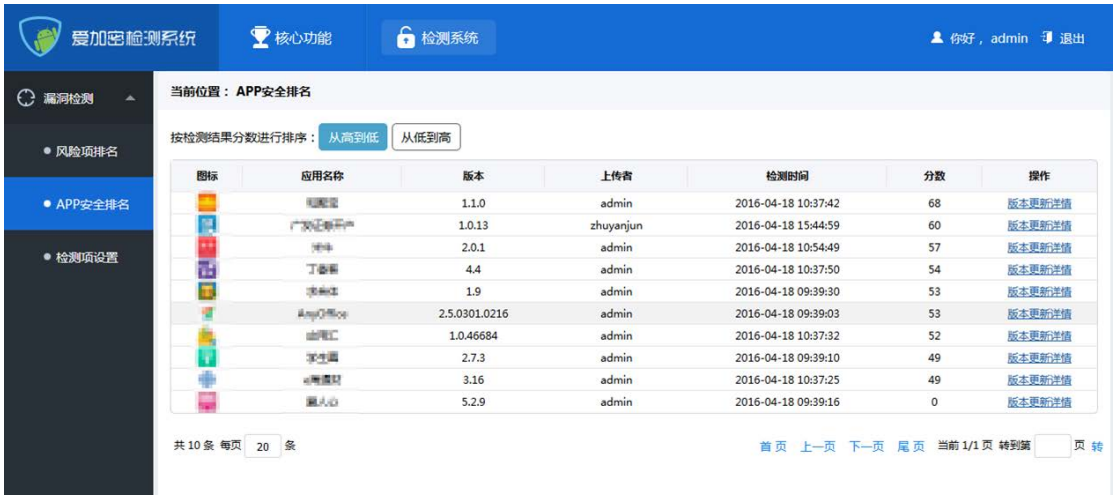

图3-10

点击“版本更新详情”，查看应用各版本的安全检测情况，如图 3-11 所示。

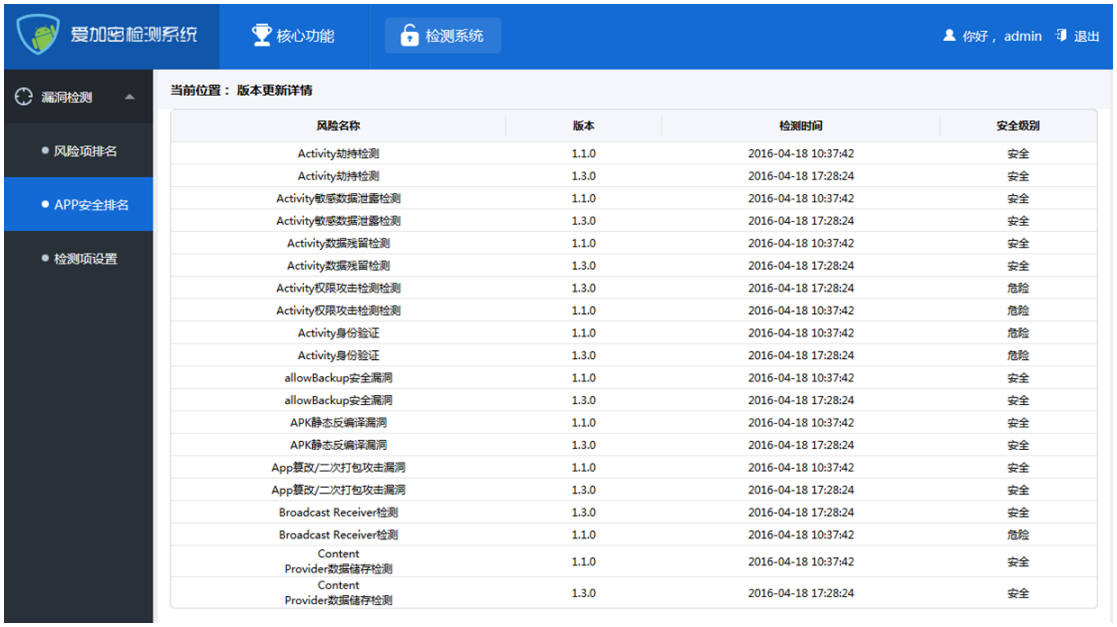

图3-11

3.3.4 检测项设置

检测项设置是 admin 用户设置应用进行安全检测时的检查项，如图 3-12 所示。

图3-12

4 操作说明

4.1 管理员操作说明

4.1.1 登录系统

1 打开浏览器，在浏览器中输入网址 http://xx.xx.xx.xx，xx.xx.xx.xx 为服务器 IP 地址。

2 输入用户名和密码，点击“登录”。

系统初始提供一个管理员账号，用户名 admin，密码 Admin_123。

4.1.2 添加角色

1 点击“核心功能”页签，如图 4-1 所示。

图4-1

2 点击左侧“角色管理”菜单，如图 4-2 所示。

图4-2

3 点击页面右上角的“添加角色”，如图 4-3 所示。

图4-3

4 在“核心功能-角色管理-添加”页面，添加“开发者”的角色，选择权限功能，点击“保存”，如图 4-4 所示。

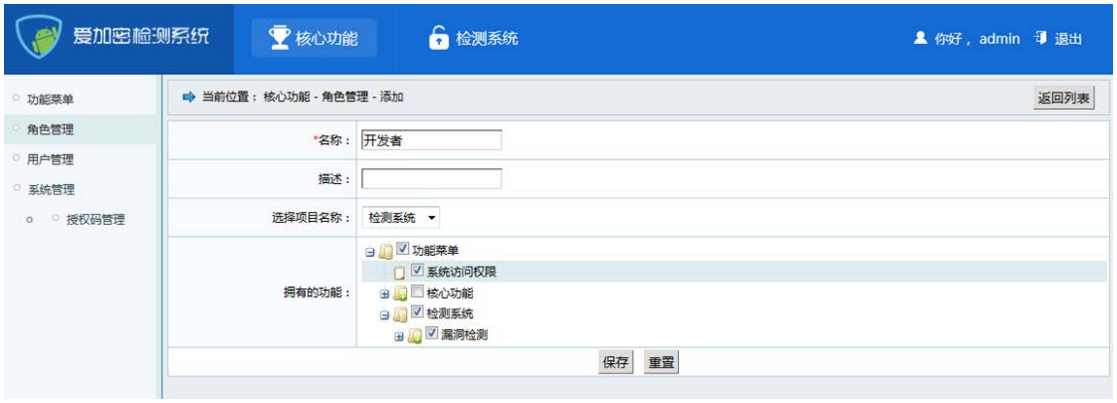

图4-4

权限可以按照实际需求在功能模块前选择即可（需注意“系统访问权限”决定该角色是否能够登录系统，因此必须添加）。

4.1.3 添加用户

1 点击“核心功能”页签，如图 4-5 所示。

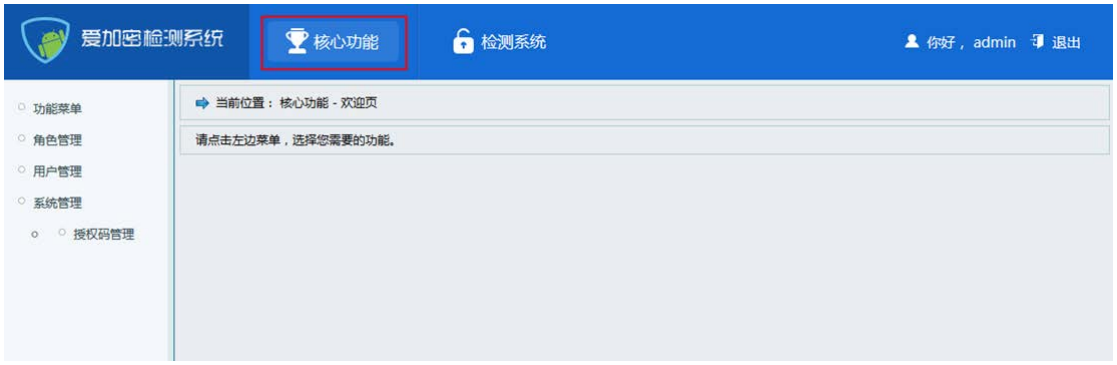

图4-5

2 点击左侧“用户管理”菜单，如图 4-6 所示。

图4-6

3 点击页面右上角的“添加用户”按钮，如图 4-7 所示。

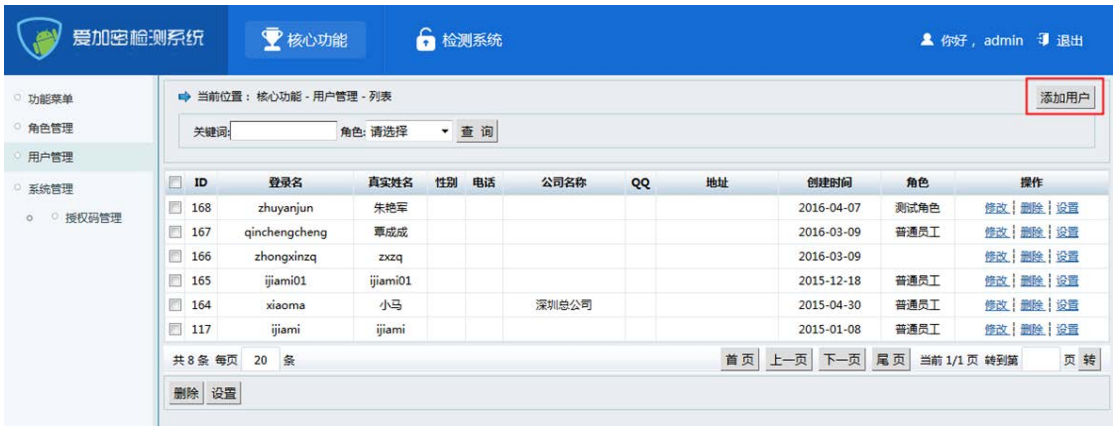

图4-7

4 在“核心功能-用户管理-添加”界面，设置用户信息，点击“提交”，如图4-8 所示。

图4-8

说明：登录时的“用户名”为用户信息中的“登录名”。

“禁用”选项表示禁止该用户登录本系统。

密码首字母必须大写，必须包含英文字母、数字、特殊字符，例如：(Ijiami_2015)。

5 点击“test”用户后面的“设置”选项，如图 4-9 所示。

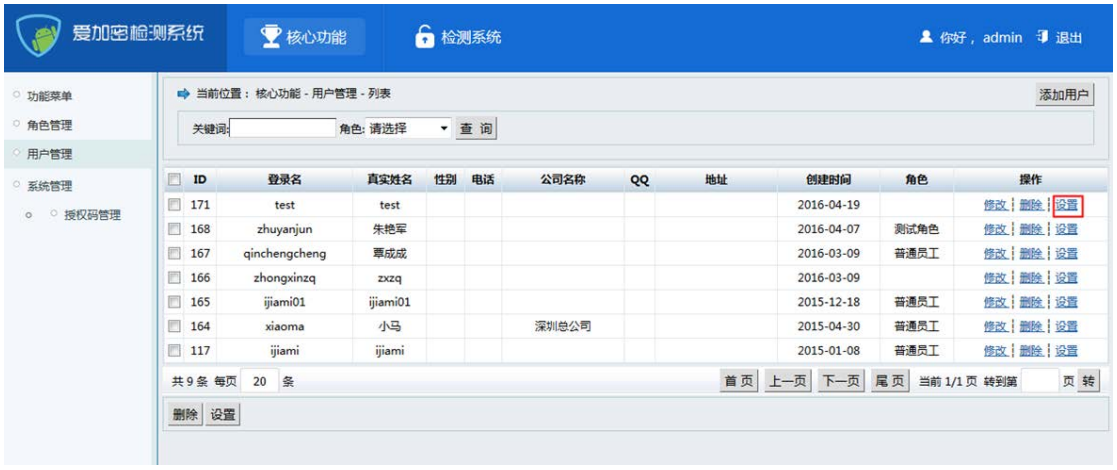

图4-9

6 在“角色”栏中的选择“开发者”，点击“保存”。这样“test”用户就赋予了“开发者”的权限，如图 4-10 所示。

图4-10

4.1.4 授权码修改

1 点击“核心功能”页签，如图 4-11 所示。

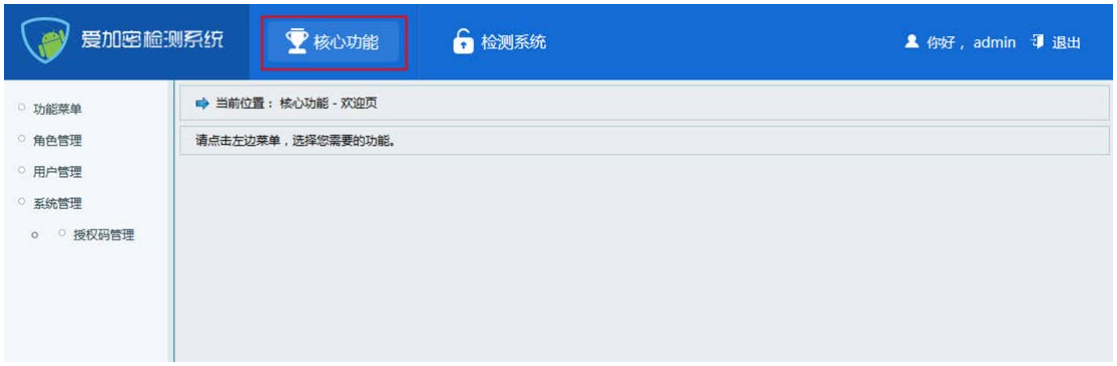

图4-11

2 点击左侧“授权码管理”菜单，如图 4-12 所示。

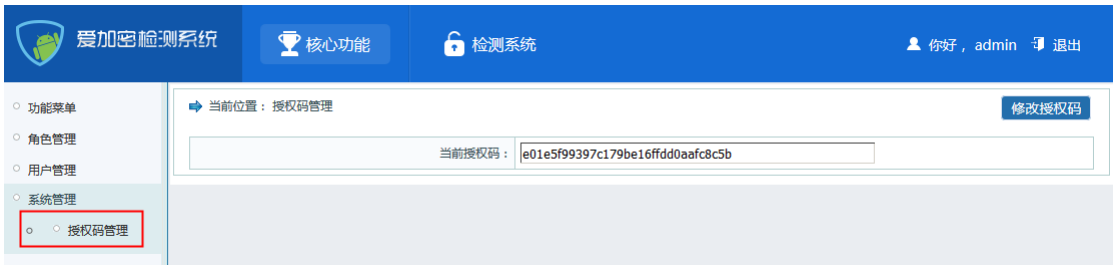

图4-12

3 点击页面右上角的“修改授权码”，如图 4-13 所示。

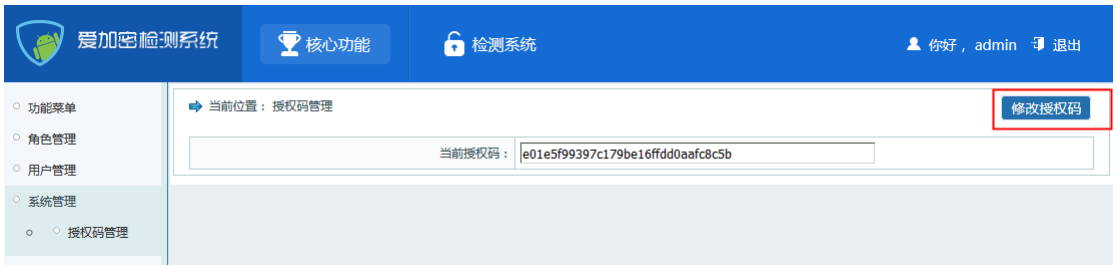

图4-13

4 点击“获取注册码”，如图 4-14 所示。

将注册码提供给我们的客服人员，我们的客服人员审核后会将新生成的授权码提供给贵司。

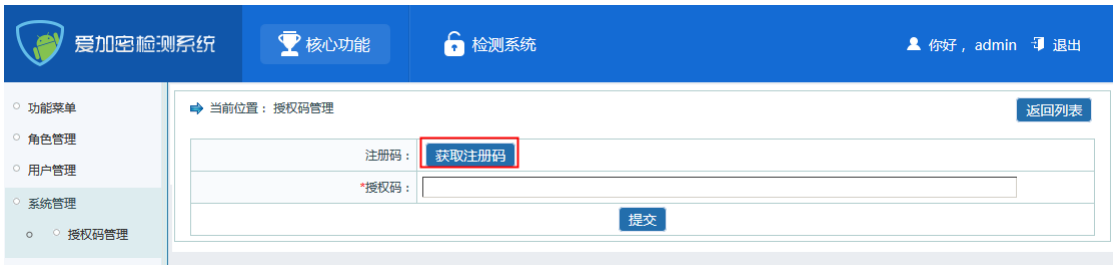

图4-14

5 输入新的授权码，点击“提交”，如图 4-15 所示。

修改授权码后，可正常使用加密系统。

图4-15

4.1.5 查看风险项排名

1 点击“检测系统”页签，如图 4-16 所示。

图4-16

2 点击左侧“风险项排名”菜单，如图 4-17 所示，查看检测项出现安全风险的情况。

图4-17

3 点击“查看详情”，如图 4-18 所示。在“风险详情”页面，查看该检测项出现安全风险的应用，如图 4-19 所示。

图4-18

图4-19

4.1.6 查看 APP 安全排名

1 点击“检测系统”页签，如图 4-20 所示，。

图4-20

2 点击左侧“APP 安全排名”菜单，如图 4-21 所示，查看检测项出现安全风险的情况。

图4-21

3 点击“版本更新详情”，如图 4-22 所示。查看应用版本更新后的安全检测情况，如图 4-23 所示。

图4-22

图4-23

4.1.7 设置检测项

1 点击“检测系统”页签，如图 4-24 所示，。

图4-24

2 点击左侧“检测项设置”菜单，如图 4-25 所示。

图4-25

3 在“检测项设置”界面，勾选需要检测的检测项，点击“保存”，如所示。

图4-26

4.2 普通用户操作说明

4.2.1 登录系统

1 打开浏览器，在浏览器中输入网址 http://xx.xx.xx.xx，xx.xx.xx.xx 为服务器 IP 地址。

2 输入用户名和密码，点击“登录”。

使用创建的普通用户“test”登录到加密系统。

4.2.2 APK 漏洞检测

1 点击左侧“漏洞检测”菜单，如图 4-27 所示。

图4-27

2 点击页面右上角“上传应用”，如图 4-28 所示。

图4-28

3 在“上传应用”页面中，选择需要检测的 APK，点击“提交”，如图 4-29 所示。

图4-29

4 系统自动返回“漏洞检测”页面，如图 4-30 所示。

图4-30

5 “状态”显示为“已完成”时，表示检测完成，如图 4-31 所示。

图4-31

4.2.3 查看检测结果

1 点击左侧“漏洞检测”菜单，如图 4-32 所示。

图4-32

2 点击应用操作栏的“查看详情”，如图 4-33 所示，查看漏洞检测的进度及检测结果。

图4-33

检测详情如图 4-34 所示。

图4-34

4.2.4 下载报告

1 点击左侧“漏洞检测”菜单，如图 4-35 所示。

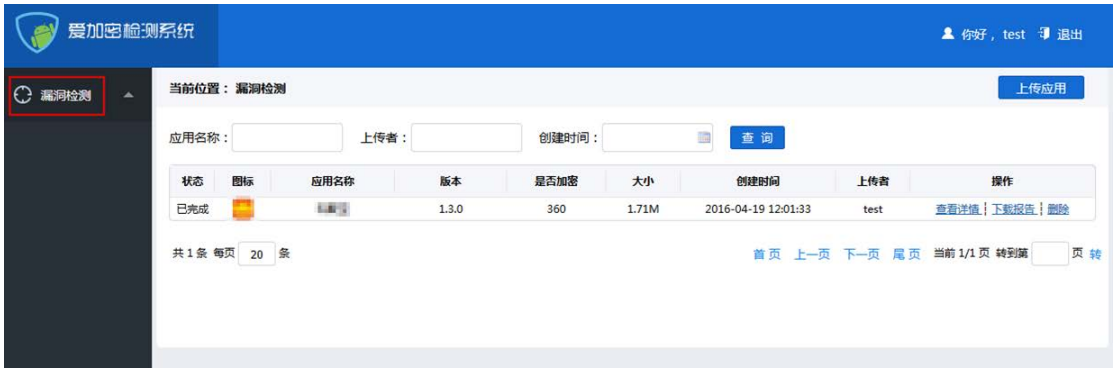

图4-35

2 点击“下载报告”，如图 4-36 所示，将安全检测报告保存到本地。

图4-36

5 服务响应

响应方式	线上响应	线下响应
内容	客户仔细记录故障现象，并将相关信息通过邮件方式发给送至项目售后服务中心	售后服务中心在接到客户系统/设备发生故障报告后，如出现较大问题后，项目支持小组派专业人员到达现场。
响应时间	半个小时内响应用户服务请求	1-2 个工作日内指派人员到达现场。