# 移动应用安全检测项目

**系 统 测 试 用 例**

**（ 内部资料 ）**

|  |  |  |  |
| --- | --- | --- | --- |
| **拟定：** | 余西鹏 | **时间：** | 2016-05-12 |
| **审核：** | 赵猛 | **时间：** | 2016-05-14 |
| **批准：** | 赵猛 | **时间：** | 2016-05-14 |



北京洋浦伟业科技发展有限公司

版权所有 侵权必究

文档变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| 更新时间 | 版本 | 版本描述 | 作者 |
| 2016-05-12 | V1.0 | InSTial版本 | 余西鹏 |
|  |  |  |  |
|  |  |  |  |

**目 录**

[移动应用安全检测项目 1](#_Toc452395091)

[第1章 概述 4](#_Toc452395092)

[1.1 目的 4](#_Toc452395093)

[1.2 适用范围 4](#_Toc452395094)

[1.3 项目背景 4](#_Toc452395095)

[1.4 术语表 5](#_Toc452395096)

[第2章 测试环境 6](#_Toc452395097)

[2.1 系统物理结构 6](#_Toc452395098)

[2.2 系统结构 7](#_Toc452395099)

[第3章 系统测试用例 7](#_Toc452395100)

[3.1 功能部分 7](#_Toc452395101)

[3.1.1 静态扫描发起 7](#_Toc452395102)

[3.1.2 特征的扫描 8](#_Toc452395103)

[3.1.3 基于黑白名单扫描 9](#_Toc452395104)

[3.1.4 权限和行为分析引擎 9](#_Toc452395105)

[3.1.5 函数调用序列分析引擎 10](#_Toc452395106)

[3.1.6 开发者识别引擎 10](#_Toc452395107)

[3.1.7 程序变化引擎 11](#_Toc452395108)

[3.1.8 病毒扫描 11](#_Toc452395109)

[3.1.9 动态扫描发起 12](#_Toc452395110)

[3.1.10 动态扫描状态获取 13](#_Toc452395111)

[3.1.11 动态扫描结果 13](#_Toc452395112)

[3.1.12 安全管理控制台 14](#_Toc452395113)

[3.1.13 信息查询 14](#_Toc452395114)

[3.1.14 报告生成 14](#_Toc452395115)

[3.1.15 图文扫描引擎 15](#_Toc452395116)

[3.1.16 其他扫描引擎 16](#_Toc452395117)

[3.2 性能部分 16](#_Toc452395118)

[3.2.1 系统响应时间 16](#_Toc452395119)

[3.2.2 系统在线人数 17](#_Toc452395120)

[3.2.3 系统并发能力 17](#_Toc452395121)

# 概述

## 目的

通过对被测系统进行功能、性能、兼容等来验证是否满足了需求规格的定义，找出与需求规格不符或与之矛盾的地方，从而提出更加完善的方案。并对项目的可用性提供一定的指导性建议。

## 适用范围

本用例适用于该项目管理者、开发、测试等人员。

## 项目背景

随着3G的发展和智能手机的普及，手机安全问题越来越突出。如恶意扣费、恶意订购、主动发短信/彩信 ；窃取用户信息：通讯录、短信、银行账号 ；传播反动、色情等非法信息 ；破坏手机软硬件; 恶意流量消耗运营商带宽等。据运营商估算，恶意流量可能占10%-20%，极端情况下90%垃圾、恶意流量占用无线和分组域资源 。

目前市场上应用检测平台的软件扫描检测方法是基于病毒定义库来完成，这种杀毒软件只有捕获到病毒样本后，才能提取到病毒的特征码，而且对于新出现的未知病毒无法防范，病毒库也需要实时更新、升级才能即时跟踪。这些软件扫描检测方法都是从计算机领域学习过来的，也存在与计算机领域相同的问题。由于手机上的恶意软件的性质与计算机上的恶意软件存在很大不同，手机上的恶意软件在定义上与计算机上是不完全相同的，恶意软件在手机上很难进行大规模的传播。手机上的恶意软件的目的主要是窃取个人资料与信息、盗取银行账号、窃听电话等犯罪行为。因此，在目前的技术下，查杀效率和准确度都较低。

移动应用检测平台所提供基于静态和动态检测技术，主要采用行为分析技术，分析应用软件在安装过程中或安装后运行过程中都做了哪些行为、什么时候做的、以及这些行为到底具有什么危害都有详尽的分析和解析。让所有恶意和灰色软件无所遁形。为用户判别软件的可靠性提供重要和必不可少的 依据。在移动互联网领域，在世界范围内比较先进，无论从技术上还是从实用性上都具有先进性和前瞻性。

## 术语表

常规测试涉及的测试术语如下：

|  |  |  |
| --- | --- | --- |
| **序 号** | **术 语** | **描 述** |
| 01 | 单元测试 | 单元测试（unST testing），是指对软件中的最小可测试单元进行检查和验证。  单元测试（模块测试）是开发者编写的一小段代码，用于检验被测代码的一个很小的、很明确的功能是否正确。 |
| 02 | 集成测试 | 集成测试，也叫组装测试或联合测试。在单元测试的基础上，将所有模块按照设计要求（如根据结构图〕组装成为子系统或系统，进行集成测试。即，每个模块完成单元测试以后，将所有功能模块集成在一起的测试，以验证各模块的正确性和接口的正确性。 |
| 03 | 系统测试 | 系统测试，英文是System Testing。是将已经确认的软件、计算机硬件、外设、网络等其他元素结合在一起，进行信息系统的各种组装测试和确认测试，系统测试是针对整个产品系统进行的测试，目的是验证系统是否满足了需求规格的定义，找出与需求规格不符或与之矛盾的地方，从而提出更加完善的方案。  常见的、典型的系统测试分类包括功能测试、恢复测试、安全测试、压力测试。 |

# 测试环境

## 系统物理结构



图1 安检系统的物理结构图

## 系统结构

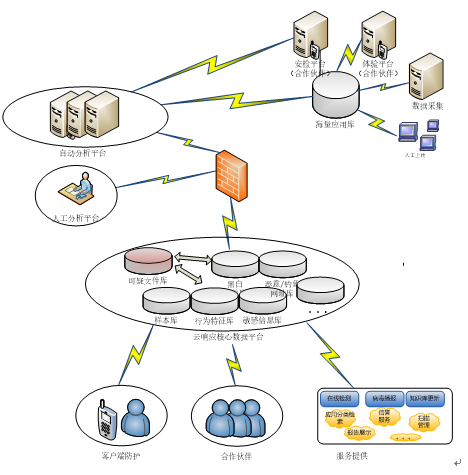


图2 移动云安全支撑系统结构

# 系统测试用例

## 功能部分

该部分主要针对移动应用安全检测项目的功能做全面的功能测试，来验证功能是否符合需求说明书，并对不符合要求的修正后来达到要求。

### 静态扫描发起

|  |  |
| --- | --- |
| 案例编号： ST\_001 | **案例描述：**发起扫描请求 |
| 案例目的：验证发起扫描请求是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 点击提交按钮 2. 检查提交状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 特征的扫描

|  |  |
| --- | --- |
| 案例编号： ST\_002 | **案例描述：**基于特征的扫描引擎 |
| 案例目的：验证基于特征的扫描引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查发起的请求状态，响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 基于黑白名单扫描

|  |  |
| --- | --- |
| 案例编号： ST\_003 | **案例描述：**基于黑白名单的扫描 |
| 案例目的：验证基于黑白名单的扫描引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查发起的请求状态，响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 权限和行为分析引擎

|  |  |
| --- | --- |
| 案例编号： ST\_004 | **案例描述：**权限和行为分析引擎 |
| 案例目的：验证权限和行为分析引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常   2、被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查扫描状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 函数调用序列分析引擎

|  |  |
| --- | --- |
| 案例编号： ST\_005 | **案例描述：**函数调用序列分析引擎 |
| 案例目的：验证函数调用序列分析引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常   2、被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查扫描状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 开发者识别引擎

|  |  |
| --- | --- |
| 案例编号： ST\_006 | **案例描述：**开发者识别引擎 |
| 案例目的：验证开发者识别引擎功能是否正确 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查扫描状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 程序变化引擎

|  |  |
| --- | --- |
| 案例编号： ST\_007 | **案例描述：**程序变化引擎 |
| 案例目的：验证程序变化引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查扫描状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 病毒扫描

|  |  |
| --- | --- |
| 案例编号： ST\_008 | **案例描述：**病毒扫描 |
| 案例目的：验证病毒扫描业务是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 检查病毒扫描项 2. 检查扫描状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 动态扫描发起

|  |  |
| --- | --- |
| 案例编号： ST\_009 | **案例描述：**发起扫描请求 |
| 案例目的：验证发起扫描请求是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 点击提交按钮 2. 检查提交状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 动态扫描状态获取

|  |  |
| --- | --- |
| 案例编号： ST\_010 | **案例描述：**获取动态扫描状态 |
| 案例目的：验证敏感行为分析项是否被检查到 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 检查获取动态扫描状态 2. 检查状态值，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 动态扫描结果

|  |  |
| --- | --- |
| 案例编号： ST\_011 | **案例描述：**获取动态扫描结果 |
| 案例目的：验证敏感行为分析项是否被检查到 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 检查获取扫描结果 2. 检查状态值，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 安全管理控制台

### 信息查询

|  |  |
| --- | --- |
| 案例编号： ST\_013 | **案例描述：**信息查询 |
| 案例目的：验证程序查询功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 完成信息查询请求 3. 检查信息查询的状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 报告生成

|  |  |
| --- | --- |
| 案例编号： ST\_014 | **案例描述：**报告生成 |
| 案例目的：验证程序查询功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 完成报告生成请求 3. 检查报告生成的状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 图文扫描引擎

|  |  |
| --- | --- |
| 案例编号： ST\_015 | **案例描述：**图文扫描引擎 |
| 案例目的：验证图文扫描引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查图文扫描引擎的状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

### 其他扫描引擎

|  |  |
| --- | --- |
| **案例编号：** ST\_016 | **案例描述：**其他扫描引擎 |
| 案例目的：验证其他扫描引擎功能是否正常 | |
| 预置条件：   1. 被测试端与测试端网络连接正常 2. 被测端符合测试要求 | |
| 执行步骤：   1. 提交静态扫描 2. 检查图文扫描引擎的状态，请求、响应的状态及参数值；   要求说明：  以上各个步骤（含异常结果情况），保证整个业务流的过程在程序模块间的逻辑、关键路径、错误及边界处理正确，以及各模块的正确性和接口的正确性。 | |
| 预期结果：   1. Http状态响应200，应该正常提交； 2. 消息体内容显示success及相关参数值。 | |
| 异常结果：  http请求响应状态非200“请求失败”（根据结果提示，修改后重新执行）；  sucess显示“请求成功”，但响应参数非规定值 | |
| 备注： | |

## 性能部分

### 系统响应时间

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **用例编号** | | | ST-Performance-001 | | | | | | | |
| **功能** | | | 测试扫描的性能 | | | | | | | |
| **用例目的** | | | 验证扫描的性能和负载情况是否符合用户要求 | | | | | | | |
| **方法** | | | 使用自动性能和负载测试工具模拟多个并发用户访问系统 | | | | | | | |
| **并发用户与事务执行情况** | | | | | | | | | | |
| **虚拟用户** | **事务相应时间MS** | | | | **平均每秒处理事务数** | **事务成功率%** | **错误比率%** | **拒绝比率%** | **每秒点击率** | **平均流量（字/每秒）** |
| **最大** | **最小** | | **平均** |
| 1000 | ≤600 | | | | ≥2 | ≥90 | ≤10 | ≤2 | ≥30 | ≥500 |
| 执行步骤 | 1. 提交扫描 2. 结果图表分析图 | | | | | | | | | |
| 测试结果 | * 正常 □测试重点1错误 □测试重点2错误 □重复测试 | | | | | | | | | |

### 系统在线人数

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **用例编号** | | ST-Performance-002 | | | | | | | | | | | | | | |
| **功能** | | 测试扫描的性能 | | | | | | | | | | | | | | |
| **用例目的** | | 验证扫描的性能和负载情况是否符合用户要求 | | | | | | | | | | | | | | |
| **方法** | | 使用自动性能和负载测试工具模拟多个并发用户访问系统 | | | | | | | | | | | | | | |
| **并发用户与事务执行情况** | | | | | | | | | | | | | | | | |
| **并发用户数** | **事务相应时间MS** | | | | **平均每秒处理事务数** | | **事务成功率%** | | **错误比率%** | | **拒绝比率%** | | **每秒点击率** | | **平均流量（字/每秒）** | |
| **最大** | | **最小** | **平均** | |  | |  | |  | |  | |  | |  | |
| 20 | ≤600 | | | | ≥2 | | ≥90 | | 0 | | ≤5 | | ≥30 | | ≥500 | |
| 30 | ≤600 | | | | ≥2 | | ≥90 | | 2 | | ≤5 | | ≥30 | | ≥500 | |
| 40 | ≤600 | | | | ≥2 | | ≥85 | | 4 | | ≤10 | | ≥30 | | ≥500 | |
| 50 | ≤600 | | | | ≥2 | | ≥80 | | 7 | | ≤15 | | ≥30 | | ≥500 | |
| 执行步骤 | 1. 提交扫描 2. 结果图表分析图 | | | | | | | | | | | | | | | |
| 测试结果 | * 正常 □测试重点1错误 □测试重点2错误 □重复测试 | | | | | | | | | | | | | | | |

### 系统并发能力

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **用例编号** | | ST-Performance-003 | | | | | | | | | | | | | | |
| **功能** | | 测试扫描的性能 | | | | | | | | | | | | | | |
| **用例目的** | | 验证扫描的性能和负载情况是否符合用户要求 | | | | | | | | | | | | | | |
| **方法** | | 使用自动性能和负载测试工具模拟多个并发用户访问系统 | | | | | | | | | | | | | | |
| **并发用户与事务执行情况** | | | | | | | | | | | | | | | | |
| **并发用户数** | **事务相应时间MS** | | | | **平均每秒处理事务数** | | **事务成功率%** | | **错误比率%** | | **拒绝比率%** | | **每秒点击率** | | **平均流量（字/每秒）** | |
| **最大** | | **最小** | **平均** | |  | |  | |  | |  | |  | |  | |
| 20 | ≤600 | | | | ≥2 | | ≥90 | | 0 | | ≤5 | | ≥30 | | ≥500 | |
| 30 | ≤600 | | | | ≥2 | | ≥90 | | 2 | | ≤5 | | ≥30 | | ≥500 | |
| 40 | ≤600 | | | | ≥2 | | ≥85 | | 4 | | ≤10 | | ≥30 | | ≥500 | |
| 50 | ≤600 | | | | ≥2 | | ≥80 | | 7 | | ≤15 | | ≥30 | | ≥500 | |
| 执行步骤 | 1. 提交扫描 2. 结果图表分析图 | | | | | | | | | | | | | | | |
| 测试结果 | * 正常 □测试重点1错误 □测试重点2错误 □重复测试 | | | | | | | | | | | | | | | |