

# 腾讯云手游安全测试

产品简介

产品文档



腾讯云

## 【版权声明】

©2015-2016 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

## 【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

## 【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

## 文档目录

|                |    |
|----------------|----|
| 文档声明.....      | 2  |
| 产品简介 .....     | 4  |
| 使用场景 .....     | 7  |
| SR扫描漏洞列表 ..... | 9  |
| 漏洞定级标准.....    | 12 |
| 手游外挂八大危害 ..... | 14 |

## 产品简介

### 产品概述

手游安全测试 ( Security Radar ) 为企业提供私密安全测试服务，通过主动挖掘游戏业务安全漏洞 ( 诸如钻石盗刷、服务器宕机、无敌秒杀等40多种漏洞 ) ，提前暴露游戏潜在安全风险，提供解决方案及时修复，最大程度降低事后外挂危害与外挂打击成本。该服务为腾讯游戏开放的独家手游安全漏洞挖掘技术，杜绝游戏外挂损失，[查看手游外挂危害](#)。

### 产品优势

#### 1. 预知风险

##### 预知风险并修复

提前挖掘漏洞，并提供修复方案，让外挂无机可乘。

##### 与安全加固的区别

一般安全加固产品都是提高外挂制作门槛，不会从根本上消除漏洞和外挂。该产品是直接找到漏洞并修复，让外挂无机可乘。

##### 与App安全扫描的区别

游戏安全扫描，不仅通过智能自动化工具扫描，还与游戏具体的玩法和功能紧密相关，理解游戏的功能后，分析正常功能背后的作弊点，找到能够通过非正常途径的获益点。

#### 2. 专注游戏

支持Unity3D、UE4、Cocos2D等主流引擎的游戏，从游戏通信协议、客户端函数安全、脚本逻辑、内存安全、静态资源安全等多个维度挖掘业务安全漏洞。

#### 3. 专家团队

工程师来自腾讯IEG手游漏洞测试团队，具有极为丰富的实战经验，

曾服务过腾讯自研、累积服务产品版本700+，使用行业独创渗透测试方案提供专业级服务。

## 4. 星级标准

腾讯游戏6星级质量标准，获得与《王者荣耀》、《穿越火线-枪战王者》、《龙之谷》等腾讯顶级手游同等测试服务品质。

## 5. 降低成本

按效果付费，无漏洞，不收费。

## 6. 方便安全

无需接入SDK，对游戏本身无影响；保证产品高度私密性，不公开任何漏洞细节。

# 产品功能

## 1. 漏洞挖掘

### 风险分析

熟悉游戏，进行风险分析，设计测试风险点。

### 漏洞挖掘

安全测试专家分组进行安全渗透测试，提交漏洞。

- 漏洞类型：包含服务器宕机、盗刷钻石、无敌秒杀、全屏攻击、游戏加速等40多种漏洞，不同游戏类型不一样。查看[更多漏洞类型](#)
- 测试维度：游戏通信协议、服务器健壮性、客户端函数安全、脚本逻辑安全、内存安全、静态资源安全、变速测试等。

### 报告汇总

汇总游戏风险评估结果和漏洞，发送测试报告。查看[测试报告](#)

## 2. 灰盒与黑盒测试说明

漏洞挖掘，包含两种测试方式：灰盒测试、黑盒测试。根据您的情况进行选择。

#### 灰盒深度测试

- 对游戏进行深度风险分析和漏洞挖掘，覆盖全量游戏功能，并提供安全漏洞修复方案。
- 支持所有游戏。
- 需产品方提供游戏协议结构文件。
- 耗时5-8个工作日。

#### 黑盒深度测试

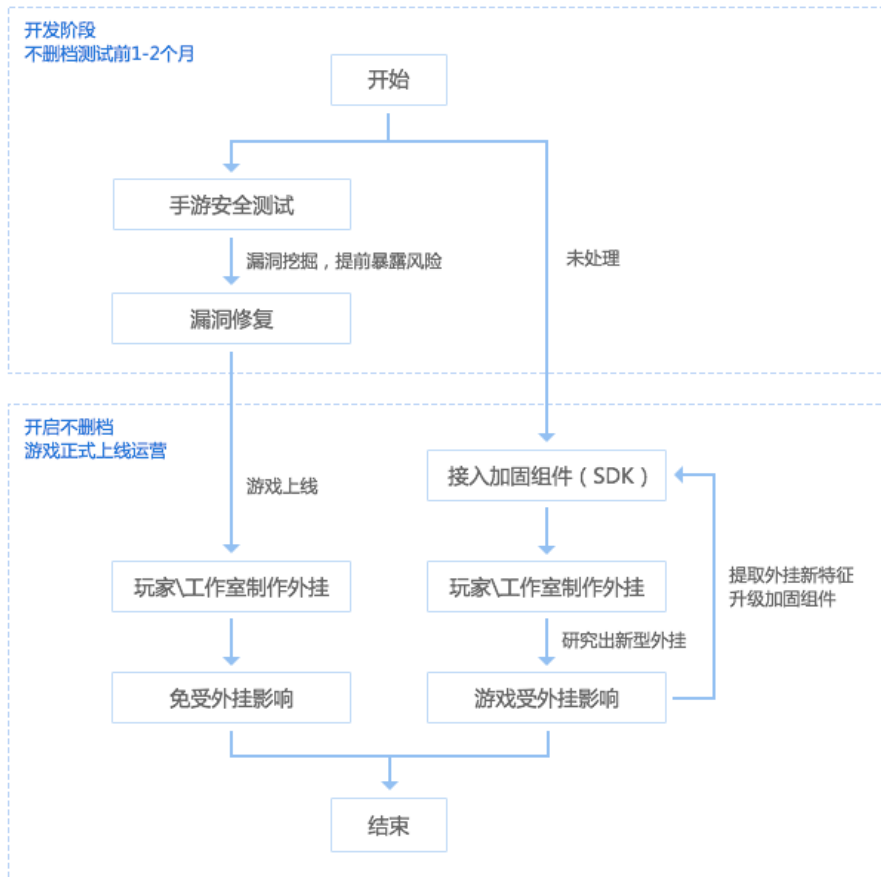
- 对游戏进行深度风险分析和漏洞挖掘，覆盖全量游戏功能，并提供安全漏洞修复方案。
- 支持Unity3D和UE引擎开发的游戏。
- 无需提供游戏协议结构文件。
- 耗时15个工作日。

## 使用场景

### 产品使用场景

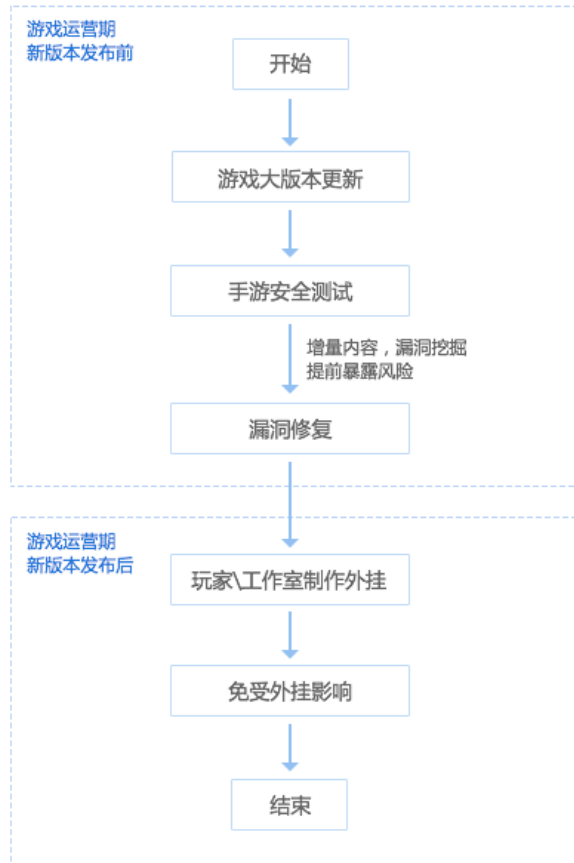
#### 1. 在开发阶段，或者不删档测试前1-2个月

在开发阶段，或者不删档测试前1-2个月，此时测试出游戏的漏洞，减少漏洞的修复成本，在上线后游戏更加安全无忧。



#### 2. 游戏正式运营，版本更新

一个大的新版本发布时，也有可能发现较严重漏洞。





## SR扫描漏洞列表

### SR扫描漏洞列表

| 手游安全风险项 | 风险解释                           | 风险等级 |
|---------|--------------------------------|------|
| 服务器宕机   | 破坏服务器进程或造成异常，停止游戏服务            | 致命风险 |
| 刷钻石     | 可无限量获得游戏代币，不用再进行充值             | 致命风险 |
| 刷属性     | 可无限量获提升角色各种属性值                 | 致命风险 |
| 无敌      | 角色永久免受伤害                       | 致命风险 |
| 秒杀      | 伤害无限大，一招击毙对手                   | 致命风险 |
| 全屏攻击    | 攻击距离无限延长                       | 致命风险 |
| 刷道具     | 可无限量获得游戏道具                     | 致命风险 |
| 刷游戏币    | 可无限量获得游戏币                      | 致命风险 |
| 加速修改    | 提升移动、攻击速度                      | 高危风险 |
| 技能无CD   | 去除技能冷却时间，可无间隔释放                | 高危风险 |
| 攻击必爆    | 每次攻击100%暴击                     | 高危风险 |
| 无限闪避    | 100%闪避敌人攻击                     | 高危风险 |
| 无限回血    | 快速无限量回复生命值                     | 高危风险 |
| 无限HP    | 可无限量提升生命值上限                    | 高危风险 |
| 无限MP    | 可无限量提升魔法值上限                    | 高危风险 |
| 弱化怪物    | 使怪物无法移动，无法攻击，或弱化怪物攻击力          | 高危风险 |
| 飞天遁地    | 在空中或地面以下移动，一般在FPS游戏中出现         | 高危风险 |
| 瞬移      | 向指定坐标点瞬间移动                     | 高危风险 |
| 隐身      | 角色永久隐身                         | 高危风险 |
| 全图显示    | 消除地图阴影，显示全地图玩家的动向，一般在Moba游戏中出现 | 高危风险 |
| 透视      | 透过障碍物看到后面，一般在FPS游戏中出现          | 高危风险 |
| 冒充他人/盗号 | 登录其他玩家的号、冒充他人执行游戏内任意操作         | 高危风险 |
| VIP破解   | 非VIP获的VIP高级福利                  | 高危风险 |

| 手游安全风险项    | 风险解释                         | 风险等级 |
|------------|------------------------------|------|
| 内购破解       | 使用未拥有、未购买的角色、宠物、卡牌等道具        | 高危风险 |
| 越权踢人       | 成员踢出帮主或队长，Moba游戏任意踢人         | 高危风险 |
| 强制投降       | 强制性使对手投降，直接获得胜利，一般在Moba游戏中出现 | 高危风险 |
| P2P交易绑定物品  | 交易绑定的物品，一般在MMORPG游戏中出现       | 高危风险 |
| 减速修改       | 降低游戏运行速度，使游戏难度降低，一般在跑酷类游戏出现  | 中危风险 |
| Buff强化     | 加强buff增益效果，延长buff持续时间        | 中危风险 |
| 修改关卡摆件     | 移除关卡中所有障碍物，降低关卡难度，一般在跑酷类游戏出现 | 中危风险 |
| 无限冲刺/飞行    | 永久保持冲刺飞行的状态，一般在跑酷类游戏出现       | 中危风险 |
| 超远距离攻击     | 超远距离攻击对手，破坏游戏平衡              | 中危风险 |
| 无限传送       | 不限次数传送到任意位置                  | 中危风险 |
| 无限复活/无消耗复活 | 不限次数，不消耗金钱或物品复活              | 中危风险 |
| 无限弹药       | 攻击不消耗弹药，一般在FPS游戏中出现          | 中危风险 |
| 主动释放被动技能   | 被动技能不用触发，直接主动释放              | 中危风险 |
| 关闭阻挡       | 无视障碍物的阻挡，穿越一切障碍物             | 中危风险 |
| 草丛可见       | 显示草丛内的敌人，一般在Moba游戏中出现        | 中危风险 |
| 自动瞄准       | 自动识别敌人，快速自动瞄准，一般在FPS游戏中出现    | 中危风险 |
| 无后坐力       | 移除任意枪械的后坐力，一般在FPS游戏中出现       | 中危风险 |
| 秒换弹夹       | 瞬间完成更换弹夹的动作，一般在FPS游戏中出现      | 中危风险 |
| 强制交易/强制组队  | 强制与他人交易，强制加入他人的队伍            | 中危风险 |
|            |                              |      |

| 手游安全风险项 | 风险解释                               | 风险等级 |
|---------|------------------------------------|------|
| 远程任务/仓库 | 远程交接任务，远程使用仓库功能，<br>一般在MMORPG游戏中出现 | 中危风险 |

## 漏洞定级标准

### SR漏洞定级标准

| 漏洞等级 | 定级标准   |
|------|--|
| 致命级  | <ol style="list-style-type: none"> <li>1. 拒绝服务漏洞。包括但不限于导致服务器端游戏服务进程崩溃、无响应，或导致游戏某个核心玩法无法正常使用的远程拒绝服务漏洞。</li> <li>2. 无限量盗刷游戏代币的漏洞。以任意方式无限量刷取游戏代币，包括但不限于钻石、元宝、点券、绑定点券的漏洞。</li> <li>3. 无限量盗刷游戏高价值物品的漏洞。以任意方式无限量刷取高价值物品，包括但不限于游戏金币，可交易流通的物品，代币商店中贩卖的物品，所有可无限且永久提升人物总战斗力的物品、或可导致游戏拍卖行物价崩溃的物品的漏洞</li> <li>4. 导致全服排行榜数据明显异常的漏洞。包括但不限于以任意方式达到全服任意排行榜前3名，造成数据明显异常影响游戏口碑的漏洞。</li> <li>5. 可应用于PVP模式或游戏核心玩法中的外挂漏洞。外挂漏洞类型包括但不限于无敌、秒杀、技能无CD、全屏攻击、变速、飞天遁地、瞬移、隐身、越权踢人、强制投降、全图显示、100%暴击、快速通关等对游戏平衡性造成严重破坏的漏洞。</li> <li>6. 盗号漏洞。以任意方式（不包含木马盗号）登录他人账号，并造成高价值物品转移或销毁，或直接删除他人账号中的游戏角色的漏洞。</li> <li>7. 伪造系统身份的漏洞。包括但不限于伪造系统身份在游戏内发送系统公告，或已系统身份在游戏聊天的系统频道中发送虚假消息的漏洞。</li> </ol> |
| 高危级  | <ol style="list-style-type: none"> <li>1. 可应用于PVE模式或游戏非核心玩法中的外挂漏洞。外挂类型包括但不限于无敌、秒杀、技能无CD、全屏攻击、弱化怪物、加速、飞天遁地、瞬移、隐身、全图显示、100%暴击、快速通关等一些游戏中正常无法实现的变态行为的漏洞。</li> </ol>   |

| 漏洞等级 | 定级标准  |
|------|---|
|      | <p>2. 有限量刷取游戏代币的漏洞。 以任意方式刷取一定量的游戏代币，包括但不限于钻石、元宝、点券、绑定点券的漏洞。</p> <p>3. 有限量刷取游戏高价值物品的漏洞。 以任意方式刷取一定量高价值物品，包括但不限于游戏金币，可交易流通的物品，代币商店中贩卖的物品，所有可以有有限量永久提升人物总战斗力的物品的漏洞</p> <p>4. 伪造其他玩家身份的漏洞。 包括但不限于伪造其他玩家身份进行世界聊天、交易、工会管理的漏洞。</p> <p>5. 聊天刷屏漏洞。 快速发送聊天消息持续刷屏，导致聊天功能无法正常使用的漏洞。</p> <p>6. 恶意攻击其他玩家账号，导致一部分游戏功能无法正常使用或造成游戏财产损失漏洞。 包括但不限于使用垃圾邮件覆盖他人邮箱中带有附件的邮件，已任意方使令他人游戏客户端出现100%崩溃的漏洞</p> |
| 中危级  | <p>以任意手段绕过游戏客户端或服务器限制，形成有异于正常的游戏行为，但影响较小，或收益甚微的漏洞。</p> <p>包括但不限于：屏蔽物品采集或技能引导的进度条、用户自定义输入内容错误显示或突破游戏限制、购买商品列表之外的物品等</p>  |

## 手游外挂八大危害

### 手游外挂八大危害

| 外挂危害   | 详细描述   |
|--------|--|
| 破坏游戏平衡 | 使用外挂篡改游戏正常数值，迅速超过正常玩家在游戏中长时间的积累，极大地损坏游戏公平性。                |
| 缩短游戏寿命 | 随着外挂介入，游戏数值异常，游戏制作者预先准备的装备、材料、关卡等版本内容被加速消耗，高价值道具肆意盗刷。      |
| 丧失游戏乐趣 | 玩家长期依赖于外挂的帮助，无法体验到游戏的乐趣与精彩，更不可能尽情地投入到游戏中。                  |
| 游戏用户流失 | 外挂玩家投入产出远高于正常玩家，游戏不平衡加剧，正常玩家权益受到破坏，被迫离开。                   |
| 暗藏恶意病毒 | 外挂程序内容得不到任何安全审核和保证，一般包含木马、病毒程序，盗取用户手机短信、银行卡等资料，严重危害用户信息安全。 |
| 增加运营成本 | 游戏服务器宕机，安全事故层出不穷，游戏客服、研发、策划、运营等角色疲于救火。                     |
| 降低企业收益 | 游戏难度变低，游戏竞技性下降，用户付费动力减弱，导致整体收益下滑。                          |
| 品牌口碑受损 | 外挂之所以对游戏的破坏巨大，是因为摧毁玩家心中最根本的信任感，随着外挂的病毒式传播，游戏厂商品牌口碑荡然无存。    |