**第三方**

**产品安全引入流程指引**

# 1.引入流程

社交网站的手机截图

描述已自动生成

1. 第三方产品引入前，腾讯产品引入团队到磐石平台下载**”第三方产品安全准入文档”，并把文档交付给第三方公司填写。**
2. 第三方厂商需要自行寻找第三方安全公司给产品做安全评估**（渗透测试或代码审计二选一）**，腾讯推荐第三方安全公司列表见**附录3,**安全测试验收标准见**附录4**
3. 第三方厂商需按实际情况填写**《第三方安全自检表》**和**《安全检查材料交付清单》**

**请完整填写《第三方安全自检表》，若产品未涉及自检表部分栏目，填写未涉及并说明理由即可。**

1. 第三方厂商将文档以上文档打包交付产品引入团队，产品引入团队通过磐石系统提交准入申请，准入过程中同时需要经过云鼎实验室的安全审批才能准入。

# 2. 研发环境安全要求

### 2.1.合作开发的代码托管研发的形式

如需要与合作厂商进行合作开发的，需由引入产品团队腾讯同事进行报备，经过引入产品团队GM审批后，可使用**腾讯云外网工蜂git.tencent.com**进行协作开发。

# 3研发安全要求

### 3.1.安全设计

开发人员在系统设计时应充分考虑安全问题，降低设计方案本身不合理或考虑不全面导致的安全风险。验证设计环节是否存在与原则相悖或不符合自查项之处，并填写**《第三方安全自检表》**。安全设计应遵循以下几个原则：

##### 3.1.1简单易懂

越复杂越容易出错，越难以审查，越难以全面测试，从而使一些安全缺陷遗留在系统中。随着系统复杂度增加，安全风险也在升高。减少冗余，提高组件重用度。集中控制接口，避免系统中分布式的安全性代码，维护困难。一个入口检票的难度远低于一堆入口的难度。

##### 3.1.2最小特权

只授予执行操作所必需的最小访问权，并且对于该访问权只准许使用所需的最少时间。

##### 3.1.3故障安全化

许多系统以各种形式出现故障时，他们都归结为不安全行为。在这样的系统中，攻击者只需要造成恰当类型的故障，或者等待恰当类型的故障发生。安全模块要避免单点故障，保证冗余度，考虑可用性。避免兼容逻辑以及降级逻辑，容易产生漏洞。

##### 3.1.4保护最薄弱环节

执行一个好的风险分析，标识出系统最薄弱的组件应该非常容易。首先应该消除看起来最严重的风险，而不是最容易减轻的风险。

##### 3.1.5纵深防御

使用多重防御策略来管理风险，以便在一层防御不够时，在理想情况下，另一层防御将会阻止完全的破坏。

##### 3.1.6隔离

如果我们将系统分成尽可能多的独立单元，那么我们可以将对系统可能造成的损害的量降到最低。隔离的使用必须适度，因为如果每一个功能都隔离，那么系统将难以管理。

##### 3.1.7默认不信任

参数不合法导致的漏洞、直接对象引用、缺乏访问控制等问题都是由于默认信任导致的。

##### 3.1.8保护隐私

有些数据是绝对不能存储的（比如信用卡磁道信息、卡背面的cvv2码等）；有些数据如身份证号是必须加密存储的；有些信息如密码是必须以不可逆的加盐Hash算法存储的。

##### 3.1.9总体调节

应用的访问授权和安全策略保持一致，保持每次访问都进行安全检查。

##### 3.1.10公开设计

不假设应用中存在隐藏的秘密，比如后台、数据库不会被外界发现。

# 4安全的编码要求

### 4.1.安全编码原则

为保障腾讯公司业务安全以及第三方产品安全，请填写《第三方安全自检表》，并遵循以下几点安全编码原则：

4.1.1 选择基础组件时应使用腾讯云平台统一提供的组件库，禁止直接复用或在代码中引入外部未经安全评估的开源代码和组件来实现基础功能。新引入组件需要报备安全团队进行安全评估通过后方可在业务中使用，针对struts、phpmyadmin等黑名单组件任何条件下均禁止使用。

4.1.2 禁止开发恶意程序，例如病毒、木马以及非授权采集和处理用户敏感信息等的代码。

4.1.3 禁止在代码中加入与需求无关的功能，禁止在代码中留下特殊权限和通用漏洞等后门。

4.1.4 对敏感数据的传输及存储，使用强加密算法进行加密处理。

### 4.2.安全组件

4.2.1 开源组件选择，推荐使用的开源清单

4.2.2 推荐使用腾讯镜像源的组件：[http://mirrors.tencent.com/#/index](http://mirrors.tencent.com/" \l "/index)

4.2.3 严禁使用黑名单的组件，组件黑名单见附录1

4.2.4 近半年内，官方有版本更新记录

4.2.5 版本必须为不存在已公开安全漏洞的安全稳定版本，建议从官网下载最新稳定版本

4.2.6 当应用出现高危安全漏洞时，能快速升级应用

4.2.7 禁止私建代码编译、数据库任意SQL查询、任意命令执行类应用或者接口

# 5.附录

### 附录1 组件黑名单

|  |  |  |  |
| --- | --- | --- | --- |
| **来源** | **组件** | **正确方式** | **备注** |
| 下载 | Struts | 禁用所有版本 |  |
| PhpMyAdmin | 禁用所有版本 | 严重漏洞频出，存在入侵和数据泄漏风险，易被黑客GetShell；授权、访问控制、审计能力不满足标准要求。 |
| Jetty | 外网业务禁用（如需外网，需部署前置Nginx+门神） | 内部源保留 |
| Pypi/pip | Opencv | 官方网站下载安装 | 201706添加的第一批pypi组件，这些都是黑客上传至pypi的钓鱼组件（仿冒常用开源组件名称），仅影响pip 安装方式 |
| Tkinter | 通过yum安装 |
| mkl | 官方网站下载安装 |
| Python-dev | 通过yum安装 |
| git | 通过yum安装或官方下载安装 |
| openssl | 通过yum安装 |
| caffe | 官方网站下载安装 |
| ffmpeg | 官方网站下载安装 |
| phantomjs | 官方网站下载安装 |
| smb | pip install pysmb |
| pygpu | 官方网站下载安装 |
| vtk | 官方网站下载安装 |
| acqusition | pip install acquisition（伪造包少一个字母） | 20170919增补第二批 |
| apidev-coop | pip install apidev-coop\_cms |
| bzip | pip install  bz2file |
| crypt | pip install crypto（伪造包少一个字母） |
| jango-server | pip install jango  pip install jango-server-guardian-api |
| pwd | pipinstall pwdhash |
| setup-tools | pip install  setuptools（伪造包多一个符号） |
| telnet | 禁用Telnet服务（仿冒的是telnetsrv、telnetsrvlib） |
| urlib3 | pip install  urllib3（伪造包少一个字母） |
| urllib | pip install  urllib3（伪造包少一个数字） |
| npm | crossenv | npm install  across-env（伪造包少一个符号） | Node.js源 //20170919增补 |

### 附录2 用户个人敏感信息参考

|  |  |
| --- | --- |
| 个人基本资料 | **个人姓名**、生日、性别、民族、国籍、家庭关系、**住址、个人电话号码、电子邮件地址**等 |
| **个人身份信息** | **身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等** |
| **个人生物识别信息** | **个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等** |
| 网络身份标识信息 | 个人信息主体账号、IP地址、个人数字证书等 |
| **个人健康生理信息** | **个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、**  **手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以**  **往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康**  **状况相关的信息，如体重、身高、肺活量等** |
| 个人教育工作信息 | 个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、  成绩单等 |
| **个人财产信息** | **银行账户、鉴别信息**  **(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息** |
| 个人通信信息 | **通信记录和内容、**短信、彩信、电子邮件，以及描述个人通信的数据（通常  称为元数据）等 |
| 联系人信息 | 通讯录、好友列表、群列表、电子邮件地址列表等 |
| 个人上网记录 | 指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等 |
| 个人常用设备信息 | 指包括硬件序列号、设备MAC地址、软件列表、唯一设备识别码（如IMEI/Android  ID/IDFA/OpenUDID/GUID/SIM卡IMSI信息等）等在内的描述个人常用设备基本情况的信息 |
| 个人位置信息 | 包括行踪轨迹、精准定位信息、住宿信息、经纬度等 |
| **其他信息** | **性取向、婚史、宗教信仰、未公开的违法犯罪记录、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等** |

**注：定义来自GB/T 35273-2020《信息安全技术 个人信息安全规范》，加粗字体为个人敏感信息**

### 附录3 可供选择的第三方安全厂商

安全厂商需满足以下条件中的任意一条

3.1腾讯投资的安全公司

3.2具有国家**风险评估三级以上**的资质证书（包括不限于CRCC、国家信息安全测评信息安全服务资质证书、中国通信企业协会通信网络安全服务能力），**只要拥有该资质的公司都可以**。

3.3腾讯云渗透测试方向安全供应商

### 附录4安全测试标准

测试漏洞类型包括不限于：

|  |  |
| --- | --- |
| **测试分类** | **漏洞类型** |
| 应用层 | SQL注入攻击 |
| 跨站脚本攻击 |
| 代码执行 |
| 命令执行 |
| 文件上传 |
| 文件读取 |
| 文件包含 |
| 跨站点请求伪造(CSRF) |
| 服务端请求伪造(SSRF) |
| URL重定向 |
| 点击劫持 |
| XML外部实体注入攻击 |
| LDAP注入攻击 |
| CRLF注入攻击 |
| 跨域资源共享攻击(CORS) |
| 反序列化攻击 |
| 加密算法使用不当 |
| XPATH注入攻击 |
| 服务端 | 敏感信息泄露 |
| 弱点端口检测 |
| 弱点服务检测 |
| 运维不当 |
| 目录遍历 |
| Git/SVN文件泄露 |
| 不安全的HTTP请求方法 |
| 默认凭证 |
| 栈异常跟踪 |
| 弱密码规则测试 |
| 缓冲区溢出 |
| Host绑定不安全因素 |
| DNS域传送 |
| Squid不安全代理 |
| 第三方组件安全 |
| CI安全检测 |
| Web应用上线Debug未关闭 |
| 中间件 | 中间件弱口令测试 |
| 中间件文件解析漏洞 |
| Java中间件已知安全漏洞 |
| 中间件配置不当 |
| 中间件默认管理页面泄露 |
| 中间件示例页面泄露 |
| 业务逻辑 | 用户身份体系 |
| 垂直权限测试 |
| 水平权限测试 |
| 授权绕过 |
| 暴力破解 |
| 在线支付逻辑测试 |
| OAuth授权测试 |
| 验证码复用 |
| 密码重置测试 |
| 手机SMS接口安全问题 |
| 人员安全意识 | 员工弱口令 |
| Github敏感信息泄露 |
| 社会工程学攻击 |
| 云环境 | 云网络环境安全测试 |
| 云服务器安全测试 |
| 容器服务安全测试 |
| 云数据库安全测试 |
| 大数据处理套件安全测试 |
| 云函数安全测试 |
| AI服务安全测试 |
| 计费系统安全测试 |
| 云对象存储系统安全测试 |

# 验收要求

安全服务商需将发现的安全问题进行全面分析后编写直观的服务报告，报告内需包含：

* 测试IP地址、网站域名、软件版本信息
* 测试厂商信息、人员联系方式
* 漏洞详情
* 漏洞复现方法及工具
* 漏洞修复建议
* 漏洞修复情况（存在高中危漏洞必须进行修复，审核才能通过）