VIPKID 安全应急响应中心(VK SRC)

安全漏洞处理和评分标准

V1.0 版

编写人	VIPKID 安全应急响应中心
版本号	V 1.0
更新日期	2017-10-17

目 录

我们承诺

1、 我们承诺，对每一位漏洞报告者反馈的问题都有专人进行跟进、分析和处理，并及时给予答复；

2、 VIPKID 支持合作式的漏洞披露和处理，对于每位恪守白帽子精神，保护用户利益，帮助 VIPKID 提升安全质量的用户，我们将给予感谢和回馈；

3、 VIPKID 反对和谴责一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的黑客行为，包括但不限于利用漏洞盗取用户隐私及虚拟财产、入侵业务系统、窃取用户数据、恶意传播漏洞等；

4、 VIPKID 认为每个安全漏洞的处理和整个安全行业的进步，都离不开各方的共同合作。希望企业、安全公司、安全组织、安全研究者一起加入到“合作式的漏洞披露和处理”过程中来，共建安全健康的互联网环境，共同保护广大互联网用户。

一、漏洞反馈和处理流程

1.1、预报告阶段

漏洞报告者登陆 VIPKID 安全应急响应中心漏洞反馈平台（security.vipkid.com.cn）注册账号。

1.2、报告阶段

漏洞报告者登陆 VIPKID 漏洞反馈平台，提交漏洞信息（状态：待审核）。

1.3、处理阶段

三个工作日内，VKSRC 工作人员处理问题，给出结论并评分（状态：审核通过/已忽略）。

必要时会与报告者沟通确认，请报告者予以协助。

1.4、完成阶段

VKSRC 每季度第一周内，发布上季度的漏洞处理公告，并向上季度的漏洞报告者致谢并发放礼品。

二、积分和安全币计算方法

1、 【积分】由漏洞对应的危害程度以及业务的重要程度决定：

积分的计算公式：**积分** = **基础积分** x **业务系数**

2、 【安全币】由漏洞对应的危害程度以及业务的重要程度决定：

安全币的计算公式：**安全币** = **基础安全币** x **业务系数**

3、 【示例】1 个直接获取核心 WEB 服务器权限的严重漏洞可获得 10,000 元人民币奖励

积分 = 基础积分（严重：10）x 业务系数（核心：10）= 100 积分

安全币 = 基础安全币（严重：50）x 业务系数（核心：10）= 500 安全币

额外奖励 5,000 元人民币 （其余漏洞评分依次类推）

注： “**业务系数**” 明细见下文内的第四点

2.1、积分对应表

基础积分 / 业务系数	严重 (9-10)	高危 (6-8)	中危 (3-5)	低危 (1-2)
核心业务(10)	90-100	60-80	30-50	10-20
一般业务(4)	36-40	24-32	12-20	4-8
边缘业务(1)	9-10	6-8	3-5	1-2

2.2、安全币对应表

基础安全币 / 业务系数	严重 (30-50)	高危 (10-30)	中危 (3-4)	低危 (1-2)	忽略 (0)
核心业务(10)	300-500	100-300	30-40	10-20	0
一般业务(4)	120-200	40-120	12-16	4-8	0
边缘业务(1)	30-50	10-30	3-4	1-2	0

安全币：人民币 = 1：10 元/RMB

三、漏洞等级

VKSRC 根据漏洞的危害程度将漏洞等级分为【严重】、【高危】、【中危】、【低危】、【无影响】五个等级。每个漏洞基础积分最高为 10，基础安全币最高为 50。由 VKSRC 结合利用场景中漏洞的危害程度、业务的重要程度、利用难度和影响范围等综合因素给予相应分值和漏洞定级，积分将用于礼品奖励发放。每种等级包含的评分标准及漏洞类型明细如下：

3.1、严重漏洞

基础积分【9~10】，基础安全币【30~50】

特别说明：额外奖励 5,000 元~10000 元（人民币）:

例如： 1 个核心业务严重漏洞 = 业务系数 x 基础安全币 x 人民币比例+额外奖励

= 10 *50 * 10 + 5,000 = 10,000 元

严重漏洞等级包括：

1、 直接获取基础架构系统权限包括但不限于：核心业务操作系统、核心业务数据库、防火墙等；

2、 直接获取 Web 服务器权限，包括但不限于：远程命令执行、上传并执行 Webshell、缓冲区域溢出等；

3、 严重的业务逻辑缺陷，可导致：大量用户经济损失，订单及支付系统业务逻辑绕过等；

4、 严重的程序设计缺陷，可导致：大量用户敏感信息泄露，公司内部核心数据泄露等；

5、 可直接导致核心系统瘫痪的拒绝服务攻击漏洞；

3.2、高危漏洞

基础积分【6~8】，基础安全币【10~30】

例如： 1 个核心业务高危漏洞 = 业务系数 x 基础安全币 x 人民币比例

= 10 * 30 * 10 = 3000 元

高危漏洞等级包括：

1、 越权访问重要应用系统，包括但不仅限于绕过认证直接访问管理后台，后台系统密码泄露等；

2、 影响一定范围用户账号或资金安全，包括但不限于：非核心 DB SQL 注入，可造成自动传播的存储型 XSS，涉及交易、资金、密码的 CSRF，可导致用户账号安全的应用系统漏洞或业务逻辑缺陷等；

3、 重要业务系统源代码、密钥或未鉴权的 API 的泄露；

4、 公司内部重要数据泄露；

3.3、中危漏洞

基础积分【3~5】，基础安全币【3~4】，

例如：1 个核心业务的中危漏洞现金奖励为 400 元

计算方法：核心业务系数 x 基础安全币 x 人民币比例 = 10 * 4 * 10 = 400 元

中危漏洞等级包括：

1、 需用户交互且在主流浏览器中才能产生影响的漏洞，包括但不仅限于针对重要系统的普通存储型 XSS 等；

2、 普通越权操作，包括但不仅限于不正确的直接对象引用，身份数据篡改等；

3、 少量的用户敏感信息泄露，包括但不限于：客户端明文存储密码、个别用户订单或身份信息泄露等；

4、 不涉及资金、订单和用户敏感信息的普通逻辑设计缺陷和业务流程缺陷；

5、 可导致资源滥用或造成对用户骚扰的漏洞，包括但不限于：短信炸弹、邮件炸弹等；

6、 一定量的非重要系统的普通代码泄露；

3.4、低危漏洞

基础积分【1~2】，基础安全币【1~2】，

例如：1 个核心业务的低危漏洞现金奖励为 200 元

计算方法：核心业务系数 x 基础安全币 x 人民币比例 = 10 * 2 * 10 = 200 元

低危漏洞等级包括：

1、 只在特定浏览器或客户端环境下才能执行，且影响较小的漏洞，包括但不限于反射型 XSS、非关键业务的存储型 XSS 等；

2、 难以利用但又可能存在安全隐患的问题。包括但不限于可能引起传播和利用的 Self-XSS 以及非重要敏感操作的 CSRF；

3、 低敏感度信息泄漏，包括但不限于路径泄漏、非核心代码 SVN 文件泄漏、phpinfo 等

4、 公司内部普通数据泄露，如：内部 IP、系统名称等；

5、 根据设备、系统、软件或框架的官方告警正在修复的漏洞；

3.5、无影响

积分及安全币均为 0，本等级包括：

1、 无关安全的 bug，包括但不限于网页乱码、网页无法打开、某功能无法用；

2、 无法利用的“漏洞”。包括但不限于没有实际意义的扫描器漏洞报告（如 Web Server 的

低版本）、无敏感信息的 JSON Hijacking、无敏感操作的 CSRF(如收藏、添加购物车、

非重要业务的订阅、非重要业务的普通个人资料修改等)；

3、 无任何证据的猜测；

4、 不可重现且无关紧要的漏洞；

5、 根据设备、系统、软件或框架的官方告警已经修复的漏洞；

四、业务系数

VKSRC 以业务相关性为依据，将此系数划分为三个等级：核心业务、一般业务、边缘业务

1、 “核心”业务系数为 **10**，包括：业务中涉及家长、学生、老师及员工敏感数据（手机号、邮箱等联系方式）、约课、在线教室等的核心业务；

2、 “一般”业务系数为 **4**，包括：业务中不涉及家长、学生、老师及员工敏感数据（手机号、邮箱等联系方式）、约课、在线教室等的一般业务；

3、 “边缘”业务系数为 **1**，包括：一般业务中的非核心业务，包括由 VIPKID 第三方供应提供的系统。

五、漏洞自动忽略说明

若首次提交漏洞后，审核暂未通过，我们将会以留言或邮件的方式，告知提供更进一步详细说明，待一周后，若白帽子未及时更新补充漏洞说明，则该漏洞将被自动忽略。

六、奖励兑换

6.1 兑换比例

安全币：人民币 = 1:10

6.2 兑换时间

处理时间：每月的最后一个工作日

最终到账时间：以银行为准

为了保障广大白帽子们的利益，VKSRC 会统一将需兑换现金的个人信息，在月底最后一个工作日之前，提交给公司财务，最终金额到账日期，以银行为准，请大家务必耐心等待，感谢理解！

七、评分标准通用原则

1、 奖励只针对通过 VKSRC 平台提交漏洞的白帽子。

2、 奖励机制只支持 VIPKID 业务，合作方、供应商等第三方公司系统不在此奖励范围内。

3、 同一漏洞产生的多个漏洞，按照最高级别的漏洞奖励标准执行，漏洞数量计为一。例如 PHPwind 的安全漏洞、同一个 JS 引起的多个 XSS 漏洞、同一个发布系统引起多个页面的 XSS 漏洞、框架导致的整站 XSS/CSRF 漏洞、泛域名解析产生的多个 XSS 漏洞、同一个 URL 多个参数的相同问题等。

4、 各等级漏洞的最终积分由漏洞利用难度及影响范围等综合因素决定，若漏洞触发条件非常苛刻，包括但不限于特定浏览器才可触发的 XSS 漏洞，则可跨等级调整积分。

5、 如果同一漏洞或同一问题漏洞的不同表现形式在漏洞修复前由多位漏洞报告者提交，在进行奖励时，我们会以最先提交并清晰表述、重现此漏洞问题的研究者为唯一受奖励者。

6、 漏洞挖掘过程应当以不影响 VIPKID 业务正常运作、不破坏、不传播漏洞为原则，否则 VIPKID 有权取消漏洞奖励。

7、 在漏洞未修复之前，被公开的漏洞不计分。

8、 网上已公开的漏洞不在奖励范围内。

9、 VIPKID 员工不得参与或通过朋友参与本活动。

10、 漏洞奖励处理标准的解释权归 VIPKID 信息安全部门所有。

八、争议解决办法

在漏洞报告处理过程中，如果报告者对流程处理、漏洞定级、漏洞评分等有异议的，可以通过以下三种方式联系 VKSRC 工作人员进行及时有效的沟通：

1、 漏洞详情页面的留言板；

2、 邮箱 security@vipkid.com.cn；

3、 微信公众号“VIPKID 安全应急响应中心”直接回复留言即可；

VKSRC 将按照漏洞报告者利益优先的原则处理，必要时将会引入外部安全人士共同裁定。