VIPKID 安全响应中心（VKSRC）

安全漏洞处理和评分标准

（V3.0 版）

编写人	VIPKID 安全响应中心	
版本号	V3.0	
最后更新日期	2019-10-17	
修订记录	V1.0 2017-10-17	初版发布
	V2.0 2019-10-17	新增风险说明，提升季度个人奖励，漏洞接收范围新增蜂校业务
	V3.0 2020-10-25	提升漏洞奖励，提升季度奖个人奖励
实施日期	2020-10-25	

目录

一、 基本原则

VIPKID 非常重视自身产品和业务的安全问题，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。VIPKID 支持负责任的漏洞披露和处理，对于每位恪守白帽子精神、保护用户利益、帮助 VIPKID 提升安全质量的报告者，我们将给予感谢和回馈。

VIPKID 诚挚地邀请业界个人、组织及公司加入到“负责任的漏洞披露”过程中来，为业务的健康发展保驾护航，为共建互联网安全生态而共同努力。

如果您对本标准有任何的建议，欢迎通过VIPKID信息安全部官方邮箱（security@vipkid.com.cn）向我们反馈。

二、 风险说明

1. 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。对于发生上述行为的，VIPKID 将追究其法律责任；
2. 测试漏洞时应尽量避免直接修改页面、重复弹框（XSS 验证建议使用 log）、盗取 cookie、获取其他用户信息等攻击性较强的 payload（如果是测试盲打，请使用 dnslog）。如不慎使用了攻击性较强的 payload，请及时删除，否则 VIPKID 将追究其法律责任；
3. 测试结果应仅限能证明漏洞存在并可被利用即可（即 POC），严禁利用漏洞进行非法操作，包括但不限于拖库、内网渗透等，否则 VIPKID 将追求其法律责任；
4. 严禁使用自动化漏扫工具发起高频扫描行为，造成业务系统或网络不可用的情况，对于违反约定造成严重后果的 VIPKID 将追究其法律责任；
5. sql 注入要求至少到注出数据库名称，不允许获取超过 10 条数据，延时注射联系 VKSRC 管理人员，避免对业务造成影响；

三、 漏洞反馈及处理流程

1. 注册账号并完善资料

漏洞报告者应在 VIPKID 安全响应中心网站（security.vipkid.com.cn）注册账号并完善个人资料，为保证后续及时沟通与礼品发放，应确保所填资料真实有效。

2. 提交漏洞

漏洞报告者通过 VIPKID 安全响应中心网站（security.vipkid.com.cn）在线提交漏洞。（状态：待审核）

3. 漏洞处理

1) 一个工作日内，VIPKID 安全响应中心（以下简称：VKSRC）工作人员开始跟进评估问题。（状态：审核中）
2) 三个工作日内，VKSRC 工作人员处理问题、给出结论并评分，忽略的漏洞会说明原因。（状态：审核通过/已忽略）必要时，会与漏洞报告者沟通，请报告者给予协助。
3) 报告的漏洞被确认，漏洞报告者会得到相应的积分和安全币，安全币可用于兑换礼品。

4. 奖励发放

1) VKSRC 将不定期举行线上线下额外奖励活动，额外的安全币奖励在每次活动结束后统一结算至报告者的个人账户，额外的礼品奖励在每次活动结束后统一安排邮寄；
2) 报告者可以使用安全币在 VKSRC 的虚拟市场兑换礼品，每月的第一个工作日安排礼品发放；
3) 每个季度的第一周，发布上一季度的漏洞处理公告并向漏洞报告者致谢，依据《季度个人奖励规则》向漏洞报告者颁发相应的荣誉和奖励；

四、 漏洞评分和奖励标准

1. 积分奖励标准

漏洞危害 / 业务类型	严重	高危	中危	低危
核心业务	90-100	60-80	30-50	10-20
一般业务	36-40	24-32	12-20	4-8
边缘业务	9-10	6-8	3-5	1-2

2. 安全币奖励标准（税后金额，1 安全币=10 元人民币）

漏洞危害 / 业务类型	**严重**	**高危**	**中危**	**低危**
核心业务	500-800	200-400	40-60	10-20
一般业务	200-320	80-160	16-24	4-8
边缘业务	50-80	20-40	4-6	1-2
特别说明：核心业务严重漏洞额外奖励 500-1000 安全币				

3. 漏洞危害等级划分标准

根据漏洞的危害程度将漏洞划分为严重、高危、中危、低危、无影响（忽略）五个等级。每个等级的具体说明如下：

【严重】漏洞

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；

【高危】漏洞

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 DBSQL 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；

【中危】漏洞

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；

【低危】漏洞

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、非重要敏感操作的 CSRF、短信炸弹、未猜解到用户口令的暴力破解、JSONP 漏洞;
3) 越权操作非重要数据，比如越权查看别人的课程计划;
4) 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 以及内部 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;

【无影响】

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，包括但不限于难以利用的 SELF-XSS、非敏感操作的 CSRF、无敏感信息的 JSON HIJACKING、无意义的源码泄露、内网 IP 地址或域名泄露、后台信息泄漏、TFS 信息泄露、网站路径泄露等等；无任何证据的猜测;
3) 不能重现的漏洞，包括但不仅限于漏洞审核工作人员确认无法重现的漏洞;
4) 根据设备、系统、软件或框架的官方告警已经修复的漏洞;
5) 无安全影响的本地拒绝服务、重打包等其它危害过低的移动端漏洞;
6) 与本公司无关的安全漏洞;

4. 业务类型划分标准

【核心业务】

业务中涉及家长、学生、老师的敏感数据（手机号、邮箱等联系方式）、约课、在线教室等的核心业务。

【一般业务】

业务中不涉及家长、学生、老师的敏感数据（手机号、邮箱等联系方式）、约课、在线教室等的一般业务。

【边缘业务】

一般业务中的非核心业务，包括第三方供应商提供的系统。

五、 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、蜂校业务，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. 通用型漏洞，如 struts、weblogic 出现新漏洞，首位附 poc 报告者得漏洞对应等级最高分，报告时间 1 个月内其他该漏洞引起的问题忽略处理，报告时间 3 个月内其他该漏洞引起的问题最高中危处理，3 个月后如仍存在该问题则按漏洞对应级别评分；
7. 禁止未经 VIPKID 授权，私自公开漏洞的行为，一旦发现严肃处理，包括奖励取消、账户禁用等；
8. 网上已公开或内部已知的漏洞、不在奖励范围内；
9. VIPKID 员工不得参与或通过朋友参与漏洞奖励计划；
10. 漏洞奖励处理标准的解释权归 VIPKID 信息安全部所有；

六、 季度个人奖励规则

1. 奖励标准

等级称号		Lv5安全专家	Lv4安全专家	Lv3安全专家	Lv2安全专家	Lv1安全专家
评定要求	季度积分	≥480	≥240	≥120	≥60	≥60
	核心高危漏洞数量	≥4	≥3	≥2	≥1	无
奖励		20000元+荣誉证书	8000元+荣誉证书	4000元+荣誉证书	1500元+荣誉证书	感谢礼品+荣誉证书

2. 补充说明

1） 以季度（3 个自然月）为计算周期，评选截止时间为每个季度最后一天；
2） 每个季度的第一个工作日，对上一季度的季度奖励进行结算，并以安全币的形式发放至白帽子的个人账户；
3） 白帽子需同时满足季度积分和核心业务高危漏洞数量两个条件才能获得对应等级的奖励，若季度内无满足条件的白帽子，则该项奖励为空缺；

七、 关于安全币兑换现金的说明

1. 白帽子可以使用安全币通过 VKSRC 虚拟市场兑换现金；

2. 每月的第一个工作日，VKSRC 工作人员处理上个月的现金兑换订单并根据白帽子提供的个人信息发起财务流程，预计 15 个工作日内走完财务流程，具体到账时间以银行为准；

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，可以通过以下两种方式联系 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；

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。