完美世界安全应急响应中心

漏洞处理流程与奖励说明 V2.3

完美世界安全应急响应中心
security.wanmei.com

编写人	完美世界安全应急响应中心
版本号	V2.3
更新时间	2021-02-03

版本号	修订内容	发布日期
V1.0	发布第一版	2017-12-20
V1.1	完善评分原则	2018-1-17
V2.0	更新漏洞评分标准细则	2018-11-6
V2.1	更新适用范围及限制与指引	2019-05-05
V2.2	更新适用范围及限制与指引及安全漏洞评分原则	2019-10-14
V2.3	更新安全漏洞评分标准	2021-02-03

目录

一、 基本原则

1. 完美世界非常重视自身产品和业务的安全问题，我们承诺，每一位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. 完美世界承诺，对于每位恪守“白帽子精神”，保护用户利益，帮助完美世界提升安全质量的白帽子，我们会给予感谢和回馈；
3. 完美世界严禁一切以漏洞测试为借口，利用安全漏洞进行破坏、损害用户利益的恶意行为，包括但不限于利用漏洞盗取用户隐私数据及虚拟财产、入侵业务系统、恶意传播漏洞、暗藏木马后门等；
4. 完美世界希望通过此平台与白帽子和安全爱好者建立良好的关系，为完美安全添砖加瓦，为建设安全健康的互联网环境而努力。

二、 适用范围

本流程适用于处理完美世界 SRC 漏洞平台（http://security.wanmei.com）所收到的安全漏洞，公司内部人员的漏洞发现除外（内部员工请通过内部 SRC 渠道报告）。

三、 实施日期

本文档自发布之日起实行 。

四、 限制与指引

PWSRC 鼓励白帽子积极发现并报告属于完美世界产品或业务中的安全漏洞，但同时也希望您能遵循以下要求：

1）请勿在最低验证或者漏洞指标核实测试要求范围之外利用任何安全漏洞。

2）请勿进行拒绝服务（DoS 或 DDoS）的漏洞测试。

3）漏洞测试时，**严禁直接对正常用户数据进行操作，数据添加需要带【漏洞测试】字样，。**

4）在已经能够证明漏洞存在的情况下，严禁深入测试漏洞。例如：内网横向渗透、上传

WebShell 后下载服务器数据、在已经能够证明 SQL 注入存在的情况下，仍然大量获取用户数据用作他用等行为。**如果您无法确定能否继续进行测试，请与我们联系，**原则上用来证明漏洞存在操作如下：

i. SQL 注入类漏洞，证明能读取 user(),datebase()即可，禁止使用工具（sqlmap 等）进行测试.

ii. 邮箱/后台等弱口令漏洞，只需证明弱口令存在，严禁翻阅邮箱/后台内容。

iii. 命令执行类漏洞，仅允许执行验证性命令(ping/wget/curl)，严禁其他恶意操作，如反弹 shell、扫描内网等。

iv. 上传类漏洞，仅可上传 php 文件内容为 phpinfo()；或 echo md5(”123456”)。

v. SQL 注入或遍历类漏洞，原则上获取的用户数据不得超过 **10 组。**

5）请勿进行物理测试、社会工程学测试或任何其他非技术漏洞测试，例如向完美内部发送钓鱼邮件、社工手段获取内部员工账号进行测试。

6）请勿在任何情况下泄露漏洞测试过程中获知的任何数据，漏洞处理结束后请删除数据。

7）请以不影响其他正常用户及正常业务运行的方式进行漏洞测试。例如在测试越权、XSS 等漏洞时，可注册多个账号进行测试。若无意中改动到了正常用户的信息，请及时告知我们。

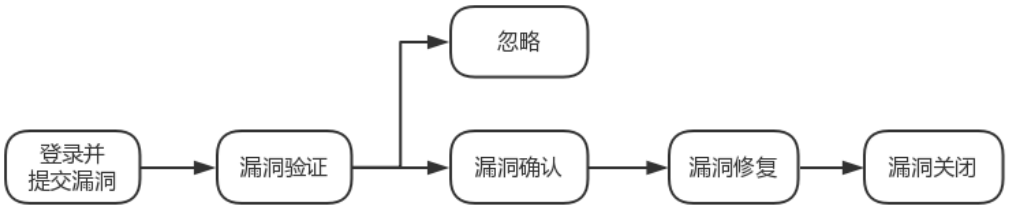
8）对于完美产品或业务漏洞的任何细节，请勿向 PWSRC 之外的任何人或机构提交，包括但不限于提交到第三方漏洞平台、将漏洞细节在 QQ 群或微信中公开讨论。

9）请务必遵守以上 1-8 条，如有违反，一经发现，PWSRC 有权取消奖励并根据具体情节追究相关责任。

10） 请您在提交漏洞时，标题内容尽量包括：**【业务名或子域名】【漏洞关键字】【造成危害】(常见漏洞类型危害可不写)，web 漏洞需要写出受影响的 URL，APP 及 PC 客户端**

漏洞需要给出具体的版本号、受影响组件名等。

五、漏洞处理流程



1. 预报告阶段

   报告者注册完美通行证账号，并访问 http://security.wanmei.com/（PWSRC 平台）进行登录。

2. 报告阶段

   报告者向 PWSRC 提交威胁报告（状态：未处理）

3. 处理阶段

   一个工作日内，PWSRC 工作人员会确认收到的报告并跟进评估问题（状态：处理中）。

   三个工作日内 PWSRC 工作人员处理问题、给出结论和积分（状态：已确认/忽略）。必要时会与报告者沟通确认，请报告者予以协助。

4. 修复阶段

   业务部门修复所报告的问题并安全修复上线（状态：已修复），修复时间根据问题严重程度、修复难度和业务情况而定。一般来说，在漏洞确认后，修复周期为：严重问题不超过 24 小时，高危问题不超过 3 天，中危问题不超过 7 天。如果存在特殊情况，修复时间根据具体情况而定，并与报告者商议修复周期。

5. 完成阶段

   <1> PWSRC 完成处理后，更新处理状态，报告者可见更新状态，可以通过积分在

PWSRC 平台兑换礼品。

<2> 对已修复漏洞,报告者可进行复测，若问题仍然存在，可再次报告。PWSRC 工作人员会对该问题进行审查确认，并再次计分或处理。

<3> 对已确认漏洞，3 个月后报告者复测依然存在且 PWSRC 工作人员未与报告者商议修复周期，可再次报告。

六、安全漏洞评分标准

漏洞的最终定级的评价标准在于漏洞对业务本身带来的影响，按照是否核心业务、利用难度、漏洞危害性、影响的用户规模、再现性和是否容易发现等因素，综合评价漏洞对业务的影响。同一漏洞类型，对业务的影响不一致会有不同的漏洞等级。

注：1 积分=5 RMB。具体积分奖励情况请参考下表：

表 6.1 漏洞积分奖励标准

漏洞等级 / **业务等级**	严重 (100-140)	高危 (40 - 60)	中危 (8 - 12)	低危 (1 - 3)
核心业务（10）	1000 - 1400	400 - 600	80 - 120	10 - 30
一般业务（5）	500 - 700	200 - 300	40 - 60	5 - 15
边缘业务（1）	100 - 140	40 - 60	8 - 12	1 - 3

漏洞等级、业务等级及其定义最终以完美世界审核结果为准

【严重】

1）直接获取核心系统服务器权限的漏洞。包括但不仅限于核心系统服务器的任意命令执行、上传获取 WebShell、SQL 注入获取系统权限、远程代码执行漏洞等；

2）严重的逻辑设计缺陷。包括但不仅限于任意账号登陆、批量任意账号密码修改、任意账

号资金消费、支付交易方面的严重漏洞；

3）严重的敏感信息泄露。包括但不仅限于重要数据的 SQL 注入（例如重要的账号密码）、包含敏感信息的源文件压缩包泄露。

4）针对游戏类漏洞：

1. 客户端设计缺陷，包括客户端远程命令执行（WEB、二进制）
2. 支付设计缺陷，包括本地篡改商品价格并能够成功完成交易、交易整数溢出漏洞。
3. 并发漏洞，包括游戏内重要价值商品被多次刷取。

【高危】

1）高风险的信息泄露，包括但不限于可以获取一般数据的 SQL 注入漏洞、源代码泄露以及任意文件读取和下载漏洞等；

2）越权访问，包括但不限于绕过验证直接访问管理后台、后台登录弱口令、以及其它服务的弱口令等。

【中危】

1）需交互才能影响用户的漏洞。包括但不限于能够造成切实危害的存储型 XSS，重要的敏感操作 CSRF；

2）普通信息泄露。包括但不仅限于获取用户敏感信息等；

3）普通越权操作。包括但不仅限于越权查看非核心的信息、记录等；

4）普通逻辑设计缺陷。包括但不仅限于短信验证绕过、邮件验证绕过。

【低危】

1）有一定价值的轻微信息泄露。比如 phpinfo、测试数据泄露等；

2）逻辑设计缺陷。包括但不仅限于图形验证码绕过；

3）有一定轻微影响的反射型 XSS、URL 跳转、非重要的敏感操作 CSRF 漏洞等。

【忽略】

1）不涉及安全问题的 BUG。包括但不仅限于网页乱码、无意义的测试页面等；

2）客户端拒绝服务漏洞和消耗资源的拒绝服务漏洞。包括但不仅限于 DDOS、客户端本地拒绝服务、组件参数未验证导致的拒绝服务漏洞；

3）无法利用的漏洞。包括但不仅限于 Self-XSS、无敏感操作的 CSRF、无敏感信息的 JSON 劫持、没有回显且没有内网探测证明的 SSRF、401 基础认证钓鱼；

4）无敏感信息的信息泄露。包括但不限于无意义的源码泄漏、无意义的内网 IP 地址/域名/测试账号密码泄漏、程序路径信任问题、跨域策略文件（crossdomain.xml）泄露、无敏感信息的 logcat/.htaccess/web.config/备份文件等信息泄漏；

5）无法重现的漏洞。包括但不仅限于纯属用户猜解、未经过验证的问题、无实际危害证明的扫描器结果；

6）其它类型的问题，包含但不接收针对多用户的短信问题、单一的用户名爆破（如手机号、用户名等）、邮箱 SPAM、有条件的 URL 跳转、低版本的 XSS、本地提权漏洞、部分 android 漏洞如二次打包、组件泄露等。

七、安全漏洞评分原则

1. 评分标准适用于完美世界的所有产品和服务。包括完美世界各 PC、移动和 web 端的网游等。
2. 由于业务调整，我们不再接收重庆星游传媒有限公司所属网站的相关漏洞，包含但不限于：stargame.com、178.com、tgbus.com、a9vg.com、dospy.com、nga.cn、ngacn.cc、ptbus.com、766.com、xyous.com 等
3. 针对完美世界使用的第三方系统及部分子公司，或与我们相关的一些边缘业务，漏洞和情报可能将不完全按照上述评分标准，而是根据业务实际运营情况及所涉及的业务数据

进行综合评分。

4. 同一漏洞最早提交者得分，在其它平台上提交过的不计分，与完美世界无关的漏洞不计分。
5. 同一漏洞源引起的多个问题仅记录为 1 个（按引起的最高风险问题计算）。
6. 同一个漏洞，若内外部几乎同时发现（24h 之内），外部提交的当新漏洞处理，超过该时间漏洞不计分。
7. 通用型漏洞，多处出现时，若合并提交，视漏洞危害提升级别，最高双倍积分；若分散提交，则只收一次，其余的按低危处理。

8、对于网上已公开的通用漏洞/威胁，因补丁下发及修复需要一定的时间，故在补丁下发 30 天内提交不计分。

八、奖励兑换

PWSRC 工作人员会在**每个月第一个工作日进行订单确认并进行礼品采购**，首次在平台兑换现金奖励的用户，应公司要求，需要根据平台的引导进行实名认证。如有任何疑问，请联系 src@pwrd.com。奖励的发放需要一定的时间，请各位白帽子耐心等待，感谢理解!

九、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 src@pwrd.com 与工作人员及时沟通。

本流程由完美世界集团信息安全部负责修订和解释。