**第十四届全国大学生信息安全竞赛**

**创新实践能力赛出题说明**

**2021年6月**

目 录

[1 出题标准 3](#_Toc76024717)

[1.1 出题内容 3](#_Toc76024718)

[1.2 难度说明 3](#_Toc76024719)

[2 评分标准 6](#_Toc76024720)

[3 技术要求： 9](#_Toc76024721)

[4 注意事项： 9](#_Toc76024722)

# 出题标准

各参赛队伍可根据出题范围与难度要求自行选择应用场景开发功能与特性需求（包括二进制网络服务、Web应用服务），构建出靶标环节。

## 出题内容

|  |  |
| --- | --- |
| **内容** | **主要考察范围** |
| 二进制网络服务 | 涉及Linux平台网络服务程序的设计、安全开发，以及二进制常见漏洞类型（如栈溢出、堆溢出、格式化字符串、UAF、竞争条件等）的原理与漏洞代码形态，漏洞挖掘及利用机制理解等 |
| Web 应用服务 | 涉及Windows、Linux平台Web应用服务的设计、安全开发，以及Web应用服务常见漏洞类型（如SQL注入、XSS跨站脚本、CSRF跨站请求伪造、文件上传、文件包含、框架安全、越权、逻辑漏洞）原理与漏洞代码形态，漏洞挖掘及利用机制理解等 |

## 难度说明

| 难度等级 | 描述 | 用途 | 样例 | 分数 |
| --- | --- | --- | --- | --- |
| 简单 | 简单类赛题，这类赛题基本上要求选手只要对相关知识有初步涉猎即可解出。 | 1. 有时候会用于线上赛签到； 2. 适用于新手，让他们能学到更多的知识； 3. 常规赛题中的送分题类型。 | WEB-HTTP请求-来源头伪造 WEB-HTTP请求-UA头伪造 WEB-文件泄露-源码文件泄露 WEB-文件泄露-备份文件泄露 WEB-PHP-弱类型特性 WEB-PHP-其他语言特性 PWN-栈漏洞利用-ROP  参考例题： WEB-[BJDCTF2020]Mark loves cat | 14 |
|  |
| 中等偏易 | 赛题可能由多个简单的考点结合起来，或者是需要对安全知识具有一定的掌握才能能够解答出来的。该难度下，选手可能需要对赛题中的代码进行分析，需要有一定的代码基础。 | 1. 不太适用于新手，可作为对入门选手的难题或者拔高之类。 2. 比赛时这种题目的数量较多，需求量较大； 3. 中等难度的题目，对于不同的比赛都有可能出现此类题。 | WEB-PHP-命令执行 WEB-PHP-文件包含 WEB-SQL注入-WAF绕过注入 WEB-XSS-WAF绕过XSS WEB-SQL注入-报错注入 WEB-SSRF-内网探测 PWN-栈漏洞利用-ret2dlresolve PWN-栈漏洞利用-bypass-canary PWN-栈漏洞利用-stack\_pivoting PWN-堆漏洞利用-off-by-one PWN-堆漏洞利用-UAF PWN-堆漏洞利用-double free  参考例题： WEB-[极客大挑战 2019]BabySQL | 17 |  |
|  |
| 中等偏难 | 赛题开始出现了类型分化，对于不同类型的题，对于大部分选手来说不一定能全部掌握知识点，将会存在解答不出来的情况。在该难度下，选手通常需要几个人一起去进行比赛；需要选手对安全方面的研究要更加深入，分析代码问题。 | 1. 中等偏难题，适用于学习一年左右相关知识点的选手； 2. 对于偏类型选手来说不能够轻松解答。 | WEB-PHP-模板注入 WEB-PHP-代码混淆 WEB-SSRF-攻击内网应用 WEB-逻辑漏洞-业务逻辑漏洞 PWN-堆漏洞利用-House of orange PWN-堆漏洞利用-house of storm PWN-堆漏洞利用-IO\_FILE利用  参考例题： WEB-[网鼎杯 2020 玄武组]SSRFMe | 19 |  |
| 困难 | 针对不同类型的考点专一性更强，需要专门为此方向学习了解很长时间。该难度下，对于选手知识掌握有着较高的考验，学习好不好，扎不扎实，都能够得到很好的检验。 该难度等级中的每一题的知识点都需要选手长期不断的学习，跟着知识点技术的进步去一步一步的达到高难度的水平。 | 1. 解题较为困难，国内高校一般队伍难以解答； 2. 适用于通常比赛中的亮点题； 3. 作为难题出现。 | WEB-Java-反序列化 WEB-Node-原型链污染 WEB-Python-沙箱逃逸 PWN-realword-解释器 PWN-realword-VM PWN-realword-server  参考例题： WEB-[网鼎杯 2020 朱雀组]Think Java | 20 |  |
|  |

# 评分标准

| **评分项** | **评分内容** | | |
| --- | --- | --- | --- |
| **EXP通过率（0~15）** | **按运行选手exp程序后成功获取预设flag次数比例，给出EXP通过率得分** | **运行exp程序50次，能成功获得预设flag得次数为m，通过率=（m/50）\*15分；** |  |
| **能力符合度（0-20）** | **选手在题目说明中，预估难度分为（简单/中等偏易/中等偏难/困难）；** | **I）入选赛题的，经比赛后，计算方法： A、计算 解出率=成功解题队伍数/参赛总队伍数； B、难度分：简单 14 分、中等偏易 17 分、中等偏难 19 分、困难 20 分 B、题目实际难度=（困难：解出率0-20%；中等偏难：解出率21-40%；中等偏易：解出率41-70%；简单：解出率71-100%；）； C、实际难度与选手预测难度相等的，符合度=难度分；实际难度与预测难度不同的，相差等级数为n，符合度=难度-4\*n分；** | **II）未入选赛题的，按预估评价，由评委直接给出，计算方法： A、评委根据选手提供的wp、解题视频、程序源码等内容进行分析，给出题目的认定难度； B、难度分：简单 14 分、中等偏易 17 分、中等偏难 19 分、困难 20 分 C、选手预估难度与认定难度相等的，符合度=难度分，预估难度与认定难度不同的，相差等级为m，每差一个等级，扣4分，符合度=难度分-4\*m；** |
| **功能实现度-完整性（0-20）** | **根据选手提供的checker程序辅助，决定完整性** | **1）考点2个及以上，提示3个及以上；checker运行结果与赛题描述中思路相符合的，16-20分； 2）题目与思路符合，但题目考点不足2个；或者题目提示不足3点的；12-15分； 3）题目源码实现功能与题目描述不完全符合的；8-11分； 4）题目源码不符合题目描述，功能不完整的；0-7分；** |  |
| **功能实现度-可用性（0-15）** | **根据选手提供的checker程序，给出可用性得分** | **评测人员运行选手提供的checker程序，对场景服务处于开启和关闭状态下，能正确识别服务对应功能是否可用的，可用性=识别成功的比例\*15；** |  |
| **功能实现度-实用性（0-20）** | **根据选手提供的赛题说明和演示视频，判断题目场景中完成功能与所属类型结合程度，给出实用性得分。** | **1）题目场景完成的功能与题目所属类别中现实问题结合紧密，包括了场景中常见功能的（16-20分）； 2）提供的功能与实际问题有一定结合，包含场景中必要功能的（12-15分）； 3）提供的功能与实际问题结合较少，包含少量功能的（8-11分）； 4）提供的功能与实际问题没有结合，基本不提供应具备功能的（0-7分）** |  |
| **是否被选为大赛赛题（0或10）** | **一般根据完整性、可用性、实用性三项总分不低于45分的，可推荐作为赛题。** | **1）评委推荐赛题为大赛赛题的，10分；2）不推荐作为赛题的，0分；** |  |
| **备注** | **能力符合度填写，所有题目在评审环节，都按II）采用预估难度先评价打分；比赛中入选赛题的题目，比赛结束后，可由总决赛的技术委员按I）入选赛题计算方法，修改入选赛题的能力符合度（其他未入选题目，按II）结果不变。** |  |  |

# 技术要求：

1. 本次build使用“赛题验证平台”提交赛题。参赛团队的队长在竞赛官网（http://www.ciscn.cn/）登录后可使用此验证平台，具体请查看《赛题验证平台使用手册（参赛团队专用）》。
2. 参赛者需要制作1个赛题文件压缩包、1个资料包文件压缩包。

赛题文件是可运行的文件，例如 docker镜像。

资料包是指赛题的文档资料，请按照《第14届全国大学生信息安全竞赛创新实践能力赛赛题模板.zip》编制。

关于提交赛题时的要求，也请查看上面的《赛题验证平台使用手册（参赛团队专用）》。

1. 所有在赛题中提供的对外开放端口的服务（例如SSH端口），都应使用高强度密码（字符混杂、长度在15位以上）。
2. web题目的静态资源（如js、css）请不要使用外链，如有外链请下载到本地并改为使用本地链接。
3. 题目必须唯一解（也就是唯一flag），题目必须能成功复现；且题目只有一条攻击路径，禁止预设多种获取 flag 的途径。
4. 提交题目时提供check脚本。确保在check服务正常的情况下，能够修补漏洞。

# 注意事项：

1. 请仔细阅读该出题标准，并按照标准进行出题。
2. 题目设计上应该有一定的逻辑性、合理性，拒绝纯脑洞出题。
3. 题目的任何地方不允许出现任何敏感词汇，也不能出现出题人的姓名、邮箱、github等任何信息（如需要的话请提前说明）。
4. 题目原则上是必须原创内容。