2022 年第三届“网鼎杯”网络安全大赛半决赛人工智能漏洞挖掘赛（RHG）赛制细则

一、 比赛形式

本赛段比赛将在“春秋云境 RHG 人工智能攻防竞赛平台”中进行。

第三届“网鼎杯”网络安全大赛半决赛所有参赛战队均可参与。此阶段允许参赛战队采取人工解题或利用自己准备的机器人程序，通过平台接口自动完成题目获取、分析、利用及提交答案等工作中的全部或部分。所有赛队无论何种参与方式都统一进行积分排名。如果参赛队采用编写机器人的方式答题，需依照如下标准及规范：

机器人程序通过平台的特定接口获取赛题信息，并下载每道赛题的二进制文件进行本地漏洞挖掘、分析和漏洞利用代码的开发。在靶场平台内，靶场会为每个战队分配特定的虚拟靶机作为赛题的运行环境，每道赛题在对应的靶机上开放特定的端口提供网络服务，战队机器人可直接与赛题通信，发送 payload，进行漏洞利用获取服务器权限，从而获取靶机内与该题目相关的 flag。

每支战队的靶机相互隔离，战队机器人的网络也相互隔离，保证每个机器人拥有安全独立的比赛环境。每支战

队的每道赛题 flag 均为动态生成，只有正确提交本队赛题的 flag 才能获得积分。

二、 比赛规则

（一）半决赛当天 10:00-13:00 为测试阶段，将有 1 道题目用于测试，此阶段不计算得分；13:00-18:00 为正式比赛阶段，该阶段共设置 9 道题目。

（二）机器人程序需要通过平台接口获取相关信息并完成相关动作，如赛题下载、得分情况、答案提交等。

（三）赛题在靶机上以开放端口的网络服务形式存在，每个战队的统一赛题具有唯一的 flag，机器人需通过漏洞利用的方式读取靶机上的 flag，并提交至平台，经验证正确后方可得分。

（四）赛题为 32 位 x86 二进制文件的形式，静态编译动态编译均有，并关闭堆栈保护。

三、 积分规则

参赛队伍通过正确作答题目，并提交 flag 获取得分，RHG 排名分为 5 个档：

1 档	第 1~第 10 名
2 档	第 11~第 30 名
3 档	第 31~第 50 名

4 档	第 51~第 100 名
5 档	第 101~第 500 名

注：

1. 相同档内得分一致。

2. 本环节的得分数，会在统计“最佳突破奖”时以双倍积分的方式计入到赛队得分中。

四、 赛题环境

（一） 赛题操作环境

1. 操作系统：Ubuntu 16.04.4 LTS(32-bit)

参考下载地址：

https://mirrors.aliyun.com/oldubuntu-releases/releases/16.04.4/ubuntu-16.04-server-i386.iso

2. 系统内核版本：4.4.0-116-generic

3. glibc 版本：2.23

4. GCC 版本：gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.9)

5. 单进程，单线程

6. 关闭 ASLR

7. 静态编译

8. GCC 编译选项参数（无优化）

9. 为保证比赛公平性，在人工智能漏洞挖掘环节中各参赛队伍**仅可以使用笔记本电脑运行机器人程序，不可使用服务器等相关设备**。

（二） 赛题运行环境

[Ubuntu 16.04.4 Server (32-bit)]

[内核版本: 4.4.0-116-generic]

[glibc 版本: 2.23]

（三） 赛题漏洞类型

人工智能漏洞挖掘（RHG）环节的漏洞类型包括所有的内存访问异常类漏洞，包括但不限于栈溢出、整数溢出、格式化字符串、堆溢出、UAF 等。

五、 平台接口

平台会为每个队伍分配唯一 ID 和对应权限，机器人需要使用接口进行 Flag 提交

（一） 接口描述以及使用流程图

1. 读取题目信息 ：比赛开始后首先调用【api/get_question_status】接口获取所有题目信息；

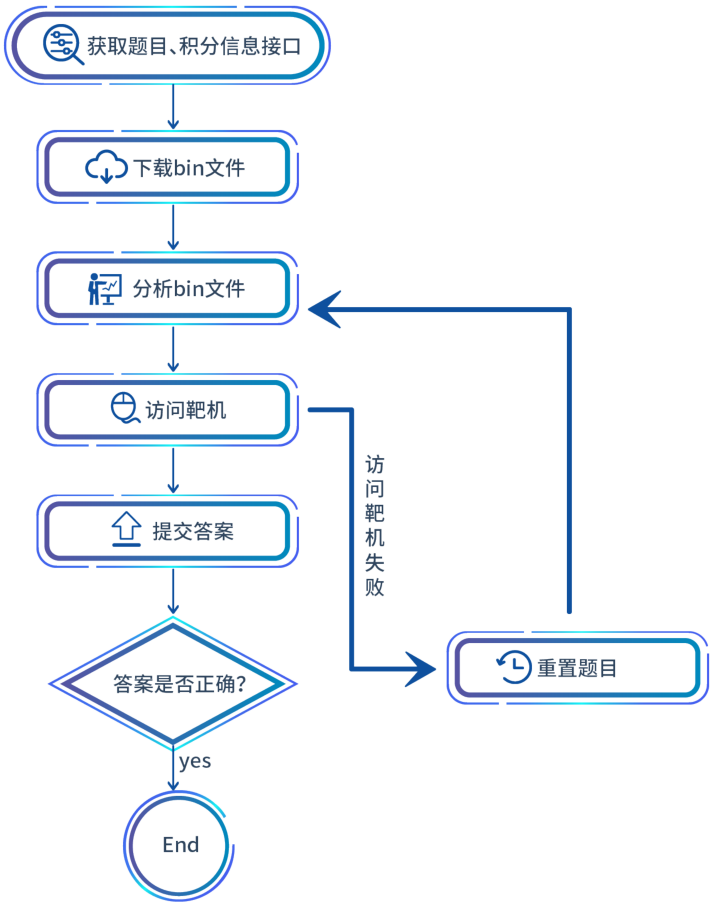
2. 下载 bin 文件 ：根据获取题目信息中 bin 文件的下载地址，下载所有题目的 bin 文件；

3. 分析 bin 文件 ：根据自己编写的脚本分析 bin 文件，找出 flag；

4. 提交题目答案 ：通过【api/sub_answer】接口提交获取到的 flag；

5. 重置题目机器 ：若链接不到题目机器，可调取【api/reset_question】接口申请重置，该接口 60 秒内限制请求一次；

6. 获取机器信息 ：可以调取【api/get_machines_info】接口获取机器信息，获取机器信息该接口 60 秒内限制请求一次；



接口需要 http authorization 身份验证，使用各个队伍的用户名密码。

（二） 获取题目、积分信息接口

1. 地址：

https://172.20.1.11/api/get_question_status

2. 请求方式：GET

3. 例：curl -k -X GET --user user:pwd https://172.20.1.11/api/get_question_status

4. 返回格式：JSON

5. 频率限制：1 秒

6. 内容：

```
{
    "status":1,//接口状态，成功。0 为失败
    "AiChallenge": [//ai 比赛当前开放题目
        {
            "challengeID": 1,//题目编号
            "vm_ip": "127.0.0.1",//虚拟机 ip
            "question_port": 8080,//题目开放端口
            "binaryUrl": "https://172.20.1.11/resources/fileupload/xxx/bin",//二进制文件下载地址
            "flag_path": "/home/flag1.txt",//flag 所在地址
            "first_blood": 0,//0 或 1 或 2 或 3,0 代表题目未被攻破，1 代表题目一血已经产生，2 代表题目二血已经产生，3 代表题目三血已经产生
            "current_time": 1547717696,//平台
```

```
当前时间戳
                "attacks_count":0,//本题有多少个队伍解答出来
                "current_score":128,//本题目前价值多少分
                "score":0,//本队得分
                "question_type": 1,//题目类型，1 是栈，2 是堆
            }
        ],

        "PointsInfo": [//总得分情况
            {
                "aiPoints": 60,//ai 比赛得分
            }
        ]
    }
```

（三） 提交答案接口

1. 地址：https://172.20.1.11/api/sub_answer

2. 请求方式：POST

3. 参数：

参数	答案
Answer	flag{XXXXXXXXXXXXXXXXXX}

4. 例：curl -k -d "answer=xxx" -X POST -v --user user:pwd https://172.20.1.11/api/sub_answer

5. 返回格式：JSON

6. 频率限制：1 秒

7. 内容：

```
成功：
{
    "status":1,
    "msg":"success",
    "questionScore":128,  //得分
    "questionRank":1      //本次提交题目排名
}
```

```
失败：
{
    "status":0,
    "msg":"提示信息"
}
```

（四） 重置题目接口

1. 地址：https://172.20.1.11/api/reset_question
2. 请求方式：POST
3. 参数：

参数	答案
ChallengeID	1

4.
5. 例：curl -k -d "ChallengeID=1" -X POST -v --user user:pwd https://172.20.1.11/api/reset_question
6. 返回格式：JSON
7. 频率限制：60 秒（60 秒内只能重置一次）
8. 内容：

```
成功：{"status":1,"msg":"success"}

失败：{"status":0,"msg":"提示信息"}
```

（五） 获取机器信息接口

1. 地址：https://172.20.1.11/api/get_machines_info
2. 请求方式：GET
3. 例：curl -k -X GET --user user:pwd https://172.20.1.11/api/get_machines_info
4. 返回格式：JSON
5. 频率限制：60 秒（60 秒内只能获取一次）
6. 内容：

```
[
    {
        "name":"test1", //机器名称
        "questions":[
            {
                "challengeID":18,//题目 id
                "is_running":true,//赛题端口状
```

```
态
                    "connection_number":2//  进程连
接数
                }
            ],
            "virtual_memory":{// 服务器内存信息
                "available":428322816,//  已获取内
存
                "used":450215936,// 已使用内存
                "cached":194371584, // 缓存
                "percent":58.5, // 百分比
                "free":387031040,// 剩余内存
                "shared":9244672,// 共享内存
                "total":1032589312// 总物理内存
            },
            "cpu":{// CPU 信息
                "physical_count":1,// 物理数量
                "logical_count":1,// 逻辑数量
```

```
            "percent":21.9 // 资源百分比 0.1/s
        },
        "swap_memory":{// 交换内存信息
            "used":0,// 已使用
            "total":2147479552,// 总量
            "percent":0,// 百分比
            "free":2147479552 // 剩余
        },
        "process_number":130// 服务器进程数
    }
]
```

（六） 获取排行榜数据接口

1. 地址：https://172.20.1.11/api/get_ranking
2. 请求方式：GET
3. 例 ： curl -k -X GET --user user:pwd https://172.20.1.11/api/get_ranking
4. 返回格式：JSON
5. 频率限制：1 秒
6. 内容：

```
[
    {
        "rank": 1,//排名
        "team_name": "name",//战队名称
        "total_score": 128,//队伍总分
        "first_blood_num": 1,//一血数量
        "answer_count": 2,//答题数量
    }
]
```

六、 比赛纪律

（一）参赛队不得以任何形式破坏比赛秩序，包括但不限于攻击平台，破坏比赛设施或干扰他人正常比赛；

（二）参赛队所用机器人应有自主知识产权，不得损害他人知识产权；

（三）裁判有权根据现场情况对违规、违纪战队进行减分、中止比赛、禁赛、通告等处理；

（四）比赛过程中请随时关注答题页面的公告栏，所有执行规则及判罚以最新公告为准；

（五）比赛过程中对平台或题目有问题，可以在答题

页面端点击“呼叫裁判”按钮反馈问题，请描述清楚遇到的问题，否则不予回应；

（六）禁止在场内随意走动，避免跨战队交流。