题目编号:ISCC-20XX-XX

第13届（2016）

**信息安全与对抗技术竞赛**

**题目设计说明书**

【！严格保密！请将所有资料打包加密传输！】

|  |  |
| --- | --- |
| 题目名称： | 试试看 |
| 题目类型： | Web |
| 题目作者： | 孙硕超 |
| 出题组织： | 杭州电子科技大学 |
| 出题日期： | 2017年08月10日 |

文档变更记录

（A：增加、M：修改、D：删除）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 版本 | 状态 | 参与者 | 日期 | 描述 |
| V1.0 | A | 孙硕超 | 2017.08.10 | 初稿 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1 引言 3](#_Toc454214768)

[1.1 编写目的 3](#_Toc454214769)

[1.2 缩写定义 3](#_Toc454214770)

[2 关卡设计 3](#_Toc454214771)

[2.1 出题要求 3](#_Toc454214772)

[2.2 设计思路 4](#_Toc454214773)

[2.3 关键技术及解决方案 4](#_Toc454214774)

[2.3.1 关键技术 4](#_Toc454214775)

[2.3.2 解决方案 4](#_Toc454214776)

[2.4 题目名称及描述 4](#_Toc454214777)

[2.4.1 题目名称 4](#_Toc454214778)

[2.4.2 题目描述 4](#_Toc454214779)

[2.5 题目部署方法 5](#_Toc454214780)

[2.6 过关流程及过关标志 5](#_Toc454214781)

[2.7 硬件使用及网络拓补 5](#_Toc454214782)

[3 相关问题 5](#_Toc454214783)

[3.1 题目分值 5](#_Toc454214784)

[3.2 题目Flag 5](#_Toc454214785)

[3.3 竞赛阶段服务器端监控方法 5](#_Toc454214786)

[3.4 须注意的问题 6](#_Toc454214787)

[4 附件 6](#_Toc454214788)

[4.1 附件1：题目源代码 6](#_Toc454214789)

[4.2 附件2：解题工具 6](#_Toc454214790)

[4.3 附件2：选手下载附件 6](#_Toc454214791)

# 引言

## 编写目的

本文档为第XX届信息安全与对抗技术竞赛(ISCC20XX)关卡类题目的详细设计文档。本文档面向竞赛组织者，用于说明此关卡的设计思路和搭建配置方法，本文档也可作为参赛者竞赛后的学习资料。

## 缩写定义

【文档中所用到的缩写定义】

|  |  |  |
| --- | --- | --- |
| 编号 | 缩写 | 定义 |
| 1 | DHCP | 动态主机配置协议 |
| 2 |  |  |

# 关卡设计

## 出题要求

1. 请严格按照模版详细撰写《ISCC分组对抗赛-对抗题-设计说明书》（必须严格按照文档模板要求写，不按照要求写的选手一律给分不超过2分，满分5分）；
2. 请严格按照模版填写《ISCC20XX对抗题-信息简表》；
3. 选手出题需要注意每一道题目放在一个文件夹中，文件夹以“ISCC20XX-编号”命名（例如ISCC2016-01），每人至少出两道题目；
4. 题目文件夹中包含一个题目设计报告和三个子文件夹：选手下载附件、解题工具和题目源代码；
5. 题目源代码做成压缩包统一放在“题目源代码”文件夹中；
6. 解题工具（便于主办方测试题目、如果工具较大可以只提供工具清单，写在一个txt文件中即可）做成压缩包统一放在“解题工具”文件夹中；
7. 提供给选手的附件做成压缩包统一放在“选手下载附件”文件夹中；
8. 服务器类题目环境不能因为选手做题而被破坏。限制选手的权限，尤其是写权限。比如随意修改题目服务器内部文件，修改数据库内容和控制题目服务器进行内网扫描等；
9. 修复题目服务器中操作系统的已知漏洞，降低选手利用这些漏洞得分的可能性；
10. 做到一个题目服务器中一个或者多个题目，而不是一个题目多个题目服务器；
11. 赛时的网络环境中会使用网络代理，题目不应与该环境要求有所冲突；
12. 保证题目flag的唯一性，不能出现一题多解的情况；
13. 出题过程中有疑问请联系我们，邮箱：[iscc2016@163.com](mailto:iscc2016@163.com)。

## 设计思路

考察本地文件包含(LFI)以及PHP 正则匹配的最大贪婪原则

## 关键技术及解决方案

### 关键技术

LFI的相关知识

贪婪模式匹配的原则是:在可匹配也可不匹配的情况下, 优先匹配，直到不能匹配成功的情况下，记录备选状态，并把匹配控制交给[正则表达式](http://www.111cn.net/list-10/" \t "http://www.111cn.net/phper/210/_blank)的下一个匹配字符，当之后的匹配失败的时候，再回溯，进行匹配。  
它会匹配尽可能多的字符。它首先看整个字符串，如果不匹配，对字符串进行收缩；遇到可能匹配的文本，停止收缩，对文本进行扩展，当发现匹配的文本时，它不着急将该匹配保存到匹配集合中，而是对文本继续扩展，直到无法继续匹配 或者 扩展完整个字符串，然后将前面最后一个符合匹配的文本(也是最长的)保存起来到匹配集合中。所以说它是贪婪的。

### 解决方案

要拿到 flag，必须有 resource=../flag.php，还必须有 resource=jpg，这里就是利用了 php 正则匹配的最大贪婪原则，如果我们这样构造

img=php://filter/resource=jpg/resource=../flag.php

php 的正则在匹配到 resource=jpg 的时候并没有停下，而是继续向前，直到匹配不到，就返回原来的匹配，如名，返回的是最大长度的匹配

GET FLAG

## 题目名称及描述

### 题目名称

试试看

### 题目描述

随意开火

## 题目部署方法

采用docker，运行dockerfile即可，端口任意

## 过关流程及过关标志

img=php://filter/resource=jpg/resource=../flag.php

## 硬件使用及网络拓补

【如果题目需要其他硬件支持，请在这里列出硬件配置及数量；如果题目网络存在多个节点，请给出题目的网络拓扑图】

# 相关问题

## 题目分值

200

## 题目Flag

flag{1ntere5ting\_PHP\_Regu1ar\_express1onssssss}

修改flag.php 文件即可

## 竞赛阶段服务器端监控方法

【如果需要监控服务器，请给出监控方法】

## 须注意的问题

【介绍部署题目、解题过程需要注意的一些问题】

# 附件

## 附件1：题目源代码

## 附件2：解题工具

## 附件2：选手下载附件