题目编号:ISCC-2017-01

第14届（2017）

**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： | php是世界上最好的语言 |
| 题目类型： | Web |
| 题目作者： | dogboy |
| 出题组织： | 南京邮电大学 |
| 出题日期： | 2017年8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 | 朱帅 | 2016.06.20 | 初稿 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

1. 引言 3
   1. 编写目的 3
   2. 缩写定义 3
2. 关卡设计 3
   1. 出题要求 3
   2. 设计思路 4
   3. 关键技术及解决方案 4
      1. 关键技术 4
      2. 解决方案 4
      3. 题目名称 4
      4. 题目描述 5
   4. 题目部署方法 5
   5. 过关流程及过关标志 5
3. 相关问题 5
   1. 题目分值 5
   2. 题目Flag 5
   3. 竞赛阶段服务器端监控方法 6
   4. 须注意的问题 6
4. 附件 6
   1. 附件1：题目源代码 6
   2. 附件2：解题工具 6
   3. 附件2：选手下载附件 6

# 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

php弱类型语言的漏洞点

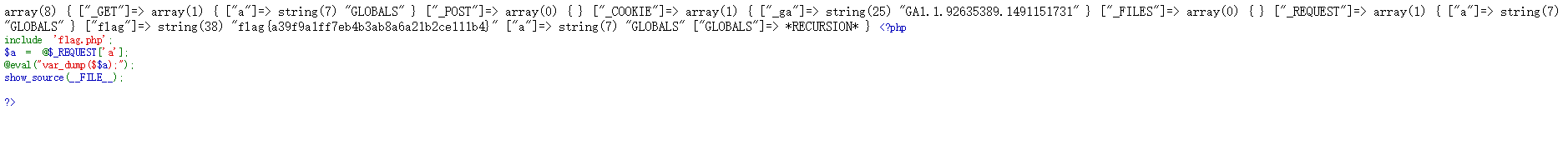
## 关键技术及解决方案

### 关键技术

【介绍解答题目需要掌握哪些技术，以及这些技术的时代背景】

### 解决方案

打开页面，发现有源代码作为提示，判断一下运行逻辑，突破口是使password的md5值等于0，使用md5的php弱类型缺陷，把md5为0e开头的字符串赋值给password，绕过第一个判断，页面跳转，得到一个新的页面no\_md5.php，发现有源码提示，阅读代码后发现存在eval函数，突破口就在双美元符号处，$$a可以拆分成$ $a，即我们输入的变量a的值是作为另一个变量的名，使用超全局变量，输出所有变量，payload为: ?a=GLOBALE，得到flag。

题目名称及描述

### 题目名称

php是世界上最好的语言

### 题目描述

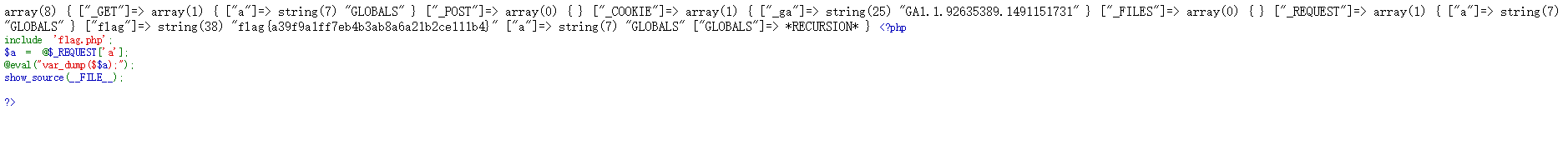
听说你用php？

## 题目部署方法

【分三种题型：1、提供附件给选手下载；2、部署在服务器上，分步骤给出题目的部署过程，附带每一步的截图和详细的文字说明；3、不需要附件或服务器】

## 过关流程及过关标志

打开页面，发现有源代码作为提示，判断一下运行逻辑，突破口是使password的md5值等于0，使用md5的php弱类型缺陷，把md5为0e开头的字符串赋值给password，绕过第一个判断，页面跳转，得到一个新的页面no\_md5.php，发现有源码提示，阅读代码后发现存在eval函数，突破口就在双美元符号处，$$a可以拆分成$ $a，即我们输入的变量a的值是作为另一个变量的名，使用超全局变量，输出所有变量，payload为: ?a=GLOBALE，得到flag。

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

150

## 题目Flag

flag{a39f9a1ff7eb4b3ab8a6a21b2ce111b4}

修改flag.php

## 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