题目编号:ISCC-20XX-XX

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： | 请ping我的ip 看你能Ping通吗？ |
| 题目类型： | Web |
| 题目作者： | 张孟奇 |
| 出题组织： | 河南牧业经济学院 |
| 出题日期： | 2017年06月24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 | 张孟奇 | 2017.06.24 | 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14届信息安全与对抗技术竞赛(ISCC2017)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 |  |  |
| 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

【介绍题目的背景、特点、考察选手哪些方面的能力】

考察php的命令执行漏洞的使用和绕过。

## 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】

掌握Php命令执行漏洞的使用和绕过。

### 解决方案

【介绍题目的解题思路】

1、通过php命令执行来执行linux命令 然后查看当前网站目录下的flag.txt。 这道题需要熟悉常见的命令执行需要的一些符号。

## 题目名称及描述

### 题目名称

请ping我的ip 看你能Ping通吗？

### 题目描述

【题目描述作为给参赛选手的提示，文字风格可以幽默点（可以参照其他CTF比赛的题目描述风格）】

我都过滤了，看你怎么绕。

## 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】

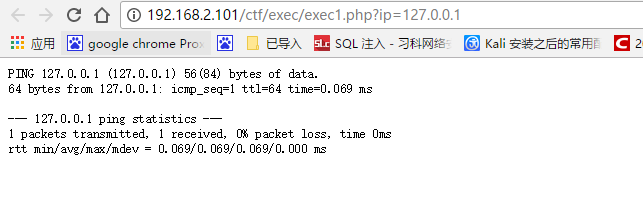
环境要求：php5以上包括5 系统： linux。

直接把源代码传到服务器上即可

## 过关流程及过关标志

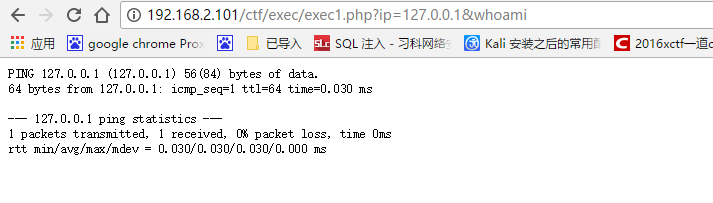
【分步骤详细说明解题过程，附带每一步的截图，题目测试人员能够按照本小节所提供的解题过程成功复现解题】

1. 看到网站上提示“请Ping通我的ip 看你会ping通吗“，由此可以想到是远程命令执行利用。
2. 然后开始在url后面加上？ip=127.0.0.1 然后出现了东西

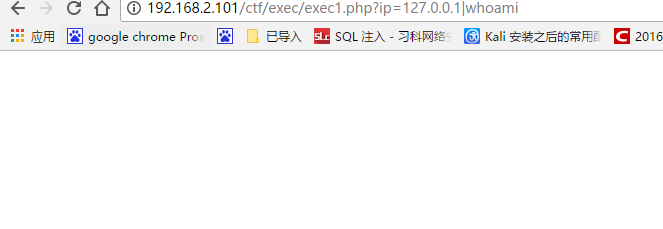


3、然后尝试在127.0.0.1后面加一些命令执行的符号“&、；、|；- $ < > ` ||“可以发现仍然没有变化

符号&



符号|



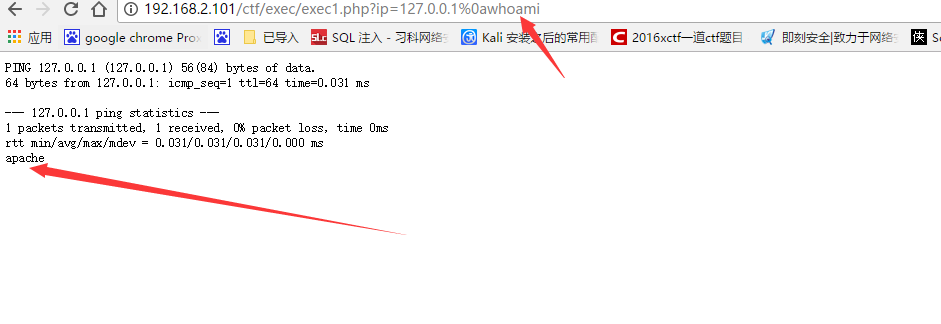
符号；



符号 $



* 1. 可以发现他们都没执行成功，但是却没有过滤%0a



* 1. 直接cat flag.txt 就可以查看到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

【题目难度满分为500分，每50分一档、共10档。请给出你对题目难度的评分】

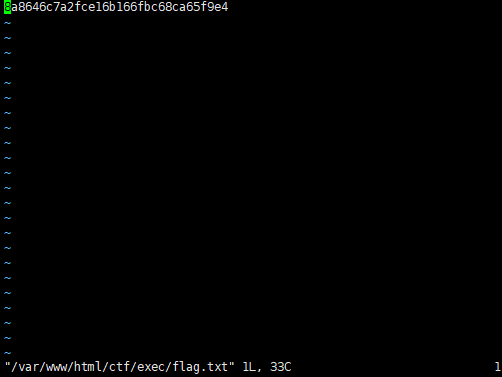
150分

## 题目Flag

【给出题目的flag及修改flag的方法】

Flag: 8a8646c7a2fce16b166fbc68ca65f9e4

修改flag的方法：找到当前目录下的flag.txt 文件里面的值



## 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】

收

1. 请保证php.ini 里面的disable\_functions 这个里面没有禁用shell\_exec函数
2. 请将flag.txt 的文件属性用root设置为只读不能写 以保证flag不被修改，同时部署web题目时需要将用户设为普通用户，低权限。

# 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