题目编号:ISCC-20XX-XX

第XX届（20XX）

**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： | Web |
| 题目作者： | 韦仲祖 |
| 出题组织： |  |
| 出题日期： | 20XX年XX月XX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 | 韦仲祖 | 2017.08.11 | 初稿 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1 引言 3](#_Toc454215007)

[1.1 编写目的 3](#_Toc454215008)

[1.2 缩写定义 3](#_Toc454215009)

[2 题目设计 3](#_Toc454215010)

[2.1 出题要求 3](#_Toc454215011)

[2.2 考察知识点和设计思路 4](#_Toc454215012)

[2.3 题目难度和分值估计 4](#_Toc454215013)

[2.4 题目部署方法 4](#_Toc454215014)

[2.4.1 题目运行环境 4](#_Toc454215015)

[2.4.2 题目部署详细过程 4](#_Toc454215016)

[2.4.3 其他说明 4](#_Toc454215017)

[2.5 关键技术及解决方案 5](#_Toc454215018)

[2.5.1 关键技术 5](#_Toc454215019)

[2.5.2 解题思路 5](#_Toc454215020)

[2.5.3 解题步骤 5](#_Toc454215021)

[2.5.4 竞赛结果提交 5](#_Toc454215022)

[2.6 题目监控 5](#_Toc454215023)

[3 附件 5](#_Toc454215024)

[3.1 附件1：题目部署相关 5](#_Toc454215025)

[3.2 附件2：题目解题相关 5](#_Toc454215026)

[3.3 附件2：题目虚拟机 6](#_Toc454215027)

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)分组对抗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 |  |  |

题目设计

## 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》；
2. 请严格按照模版填写《ISCC20XX对抗题-信息简表》；
3. 请尽量使用较新的CVE漏洞、并在漏洞基础上做适当改动；
4. 选手可以利用题目本身漏洞获取题目所在服务器的一定权限，必须注明权限所属的用户或用户组；
5. 题目统一编号为：ISCC20XX-编号，并以编号给题目文件夹命名，例如ISCC2016-1；
6. 题目部署所需要的附件统一放在“题目部署附件”文件夹中；
7. 题目解答所需要的附件统一放在“题目解答附件”文件夹中；
8. 在VMware虚拟机中部署好题目，使用VMware导出功能（文件 - 导出），将虚拟机导出为\*.ovf、\*.ova格式文件，导出文件放在“题目虚拟机”文件夹中，并在备注中注明虚拟机的操作系统类型，系统或部分应用的用户名/密码，以便于直接部署；
9. 出题过程中有疑问请联系我们，邮箱：[iscc2004@163.com](mailto:iscc2004@163.com)。

## 考察知识点和设计思路

【详细描述题目的设计思路、考察选手哪些方面的能力等】

很基础的web以及php代码审计

## 题目难度和分值估计

【最高分1000分，100分为一档，共10档】

## 题目部署方法

**把源文件放到apache+php环境即可**

### 题目运行环境

**apache+php**

#### 操作系统

【如果题目对操作系统类型及版本没有特殊要求，请填写Linux、Windows均可；如果题目对操作系统类型或版本有特殊要求，请详细填写操作系统类型及其版本号，例如：ubuntu-14.04.1-server-amd64】

linux 或者windows

#### 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】

### 题目部署详细过程

【详细记录部署题目的过程，包括安装软件、设置权限等（必须精确到每一个步骤，最好能提供一个**一键安装脚本**）例如：第一步：安装mysql ，执行命令sudo apt-get install mysql-server，第二步：设置\*\*文件为可执行权限，……】

**把源文件放到apache+php环境即可**

### 其他说明

【部署题目过程需要特别注意的一些问题】

## 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】

很基础的web以及php代码审计

### 解题思路

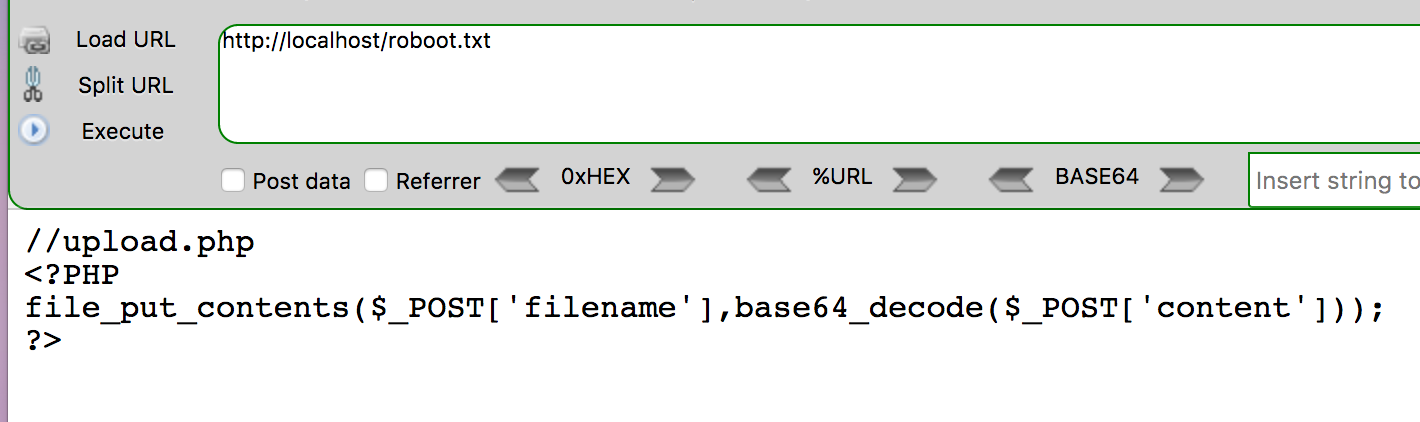
【介绍题目的解题思路】

先找到后门漏洞然后利用

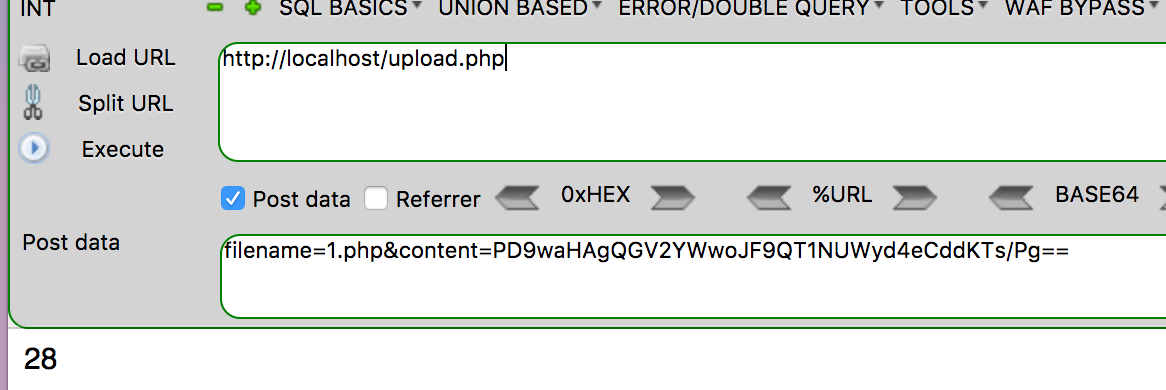
### 解题步骤

【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。最好能提供一个**一键解题脚本**】

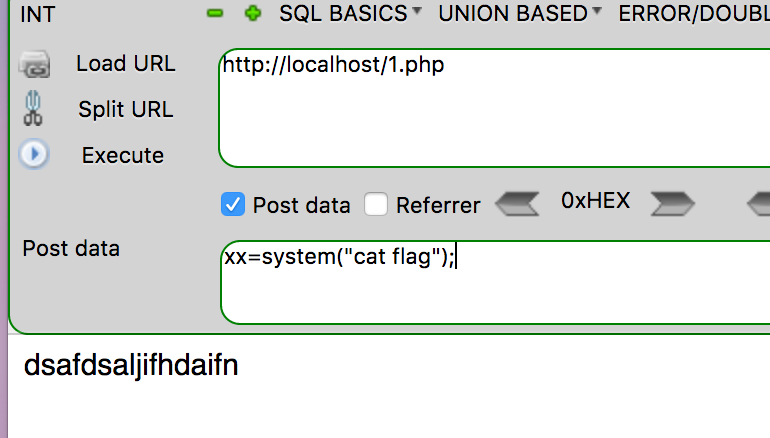
1.做web题套路看看roboot.txt



2.然后可以上传一句话



3.查看flag



### 竞赛结果提交

【获取题目服务器系统权限后，在shell中执行flag请求命令，获取Flag，然后在竞赛管理系统提交】

## 题目监控

【如果需要监控服务器，请给出保障服务器稳定运行的方法、服务器监控方式等】

附件

## 附件1：题目部署相关

【附件包括题目部署附件，建立独立文件夹“题目部署附件”】

## 附件2：题目解题相关

【附件包括题目解题附件，建立独立文件夹“题目解答附件”】

## 附件2：题目虚拟机

【附件包括题目虚拟机导出文件（\*.mf、\*.ovf、\*.vmdk），建立独立文件夹“题目虚拟机”】