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： | Only Admin |
| 题目类型： | WEB |
| 题目作者： | 秦凯 |
| 出题组织： | Wpsec\_1战队 |
| 出题日期： | 2017年06月20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 | 秦凯 | 2017.06.20 | 初稿 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目 录**

[1 引言 3](#_Toc454094894)

[1.1 编写目的 3](#_Toc454094895)

[1.2 缩写定义 3](#_Toc454094896)

[2 关卡设计 3](#_Toc454094897)

[2.1 出题要求 3](#_Toc454094898)

[2.1.1 服务器类题目 3](#_Toc454094899)

[2.1.2 附件下载类题目 3](#_Toc454094900)

[2.2 设计思路 4](#_Toc454094901)

[2.2.1 题目背景 4](#_Toc454094902)

[2.2.2 题目特点 4](#_Toc454094903)

[2.2.3 题目考察点 4](#_Toc454094904)

[2.3 关键技术及解决方案 4](#_Toc454094905)

[2.3.1 关键技术 4](#_Toc454094906)

[2.3.2 解决方案 4](#_Toc454094907)

[2.4 题目名称及描述 4](#_Toc454094908)

[2.4.1 题目名称 4](#_Toc454094909)

[2.4.2 题目描述 4](#_Toc454094910)

[2.5 题目部署方法 4](#_Toc454094911)

[2.6 过关流程及过关标志 5](#_Toc454094912)

[2.7 硬件使用及网络拓补 5](#_Toc454094913)

[3 相关问题 5](#_Toc454094914)

[3.1 题目分值 5](#_Toc454094915)

[3.2 题目Flag 5](#_Toc454094916)

[3.3 竞赛阶段服务器端监控方法 5](#_Toc454094917)

[3.4 须注意的问题 5](#_Toc454094918)

[4 附件 5](#_Toc454094919)

[4.1 相关附件 6](#_Toc454094920)

# 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

【介绍题目的背景、特点、考察选手哪些方面的能力】

考察代码审计能力，在过滤方案中找出缺陷，发现并利用反序列化登入任意用户账号。

## 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

【介绍题目的解题思路】

1. 首先扫描发现有web.tar.gz 源码泄露
2. 源代码审计后发现escape函数对参数类型判断有缺陷，没有判断参数是类的情况
3. 记住密码功能处存在反序列化漏洞，构造反序列化，登陆时代入cookie，造成注入

## 题目名称及描述

### 题目名称

【给题目设定一个名称，尽量控制在10个字（word）以内，中英文不限】

Only Admin

### 题目描述

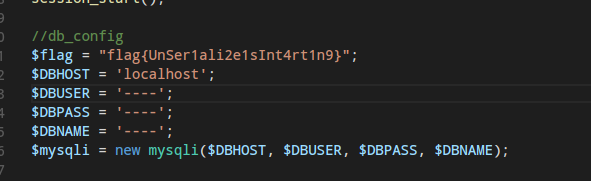
【题目描述作为给参赛选手的提示，文字风格可以幽默点（可以参照其他CTF比赛的题目描述风格）】

听说只有admin可以看到flag？

## 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】

1. 部署在服务器上
2. 安装apache/nginx
3. 安装php、mysql
4. 解压题目到web根目录，导入数据库install.sql
5. 修改config.php中相关变量

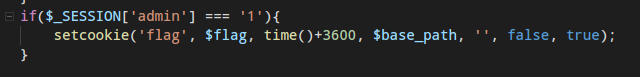


5. 访问测试

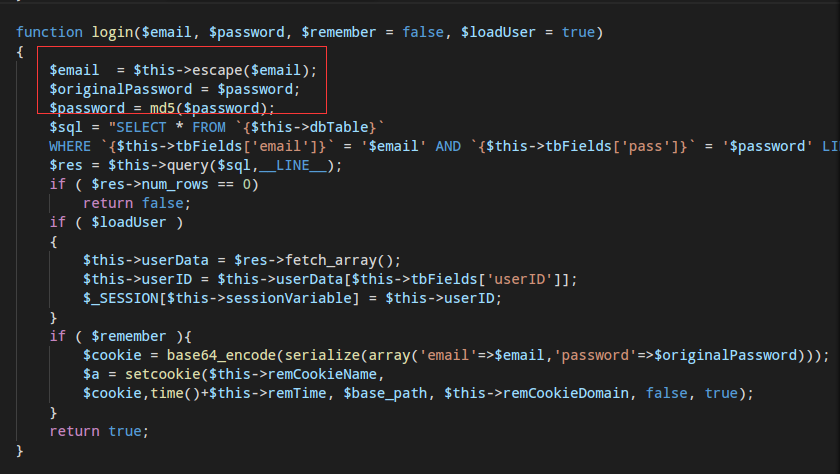
## 过关流程及过关标志

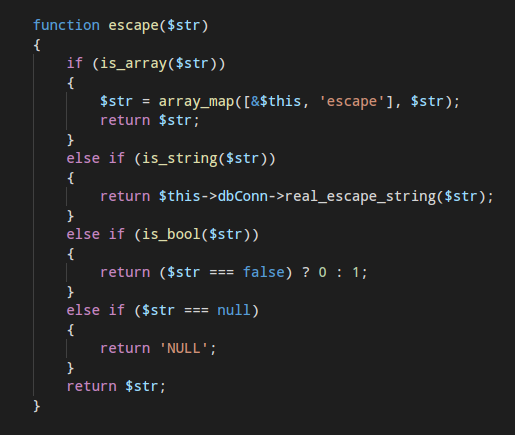
【分步骤详细说明解题过程，附带每一步的截图，题目测试人员能够按照本小节所提供的解题过程成功复现解题】

1. 扫描web根目录，发现有web.tar.gz
2. 下载源代码审计，发现只要以管理员身份登陆即可获取flag

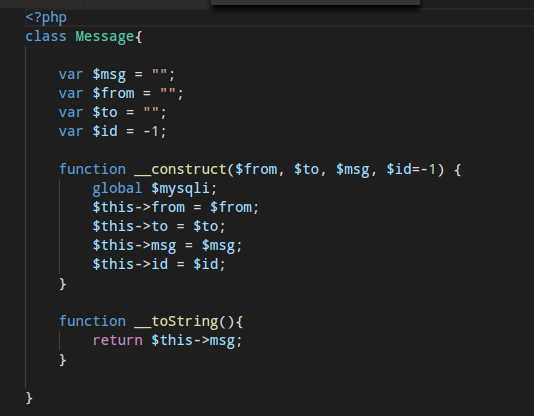


1. 发现阅读消息处有xss，但是cookie是Httponly，xss无法利用。
2. 登陆函数，和过滤函数如下



  
 4. 发现过滤函数没有判断参数是类，记住密码功能存在注入

1. 通读代码，找到可利用的类Message



1. 构造注入语句，' union select 1,'admin',1,1#，构造反序列化字符串
2. 构造payload YToyOntzOjg6InBhc3N3b3JkIjtzOjExOiJ0ZXN0QHFxLmNvbSI7czo1OiJlbWFpbCI7Tzo3OiJNZXNzYWdlIjo0OntzOjM6Im1zZyI7czoyOToiJyB1bmlvbiBzZWxlY3QgMSwnYWRtaW4nLDEsMSMiO3M6NDoiZnJvbSI7czoxOiIxIjtzOjI6InRvIjtzOjE6IjIiO3M6MjoiaWQiO2k6LTE7fX0=
3. Cookie打过去获取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】

350分

## 题目Flag

【给出题目的flag及修改flag的方法】

在config.php里修改。



flag{UnSer1ali2e1sInt4rt1n9}

## 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】

Web根目录的源码打包文件请勿删除，是给解题者用以审计的。

# 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