题目编号:ISCC-20XX-XX

第 1x届（201x）

**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： | Collide |
| 题目类型： | Basic |
| 题目作者： | 唐誉铭 |
| 出题组织： | NSC |
| 出题日期： | 2018-3-31 |

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 |
| 0.1 | A | 唐誉铭 | 2018-3-1 | 填写 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**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 |  |  |
| 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

在MD5广泛应用的今天，被视为安全高效的MD5任不能认为是百分之百安全，要求选手懂得MD5的算法实现，以及可能出现的漏洞。

## 关键技术及解决方案

### 关键技术

hash-extend attack

### 解决方案

MD5采用每64字节作为一个分组，每一组加密的得到的密文作为下一次加密的初始向量，我们虽然不知道$key的内容，但是知道$key.”guest”的MD5，和$key的长度，所以可以使用已知MD5作为初始向量，再往后拓展一组含有admin的分组，得出最终MD5。

在github上有现成的拓展攻击工具https://github.com/iagox86/hash\_extender，可以通过以下参数攻击得到正确的MD5。

./hash\_extender -d guest -f md5 -s 78cfc57d983b4a17e55828c001a3e781 -a admin -l 46 --out-data-format=html

## 题目名称及描述

### 题目名称

Collide

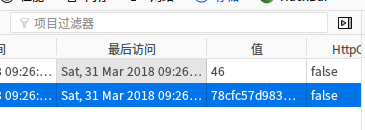
### 题目描述

那么长的秘钥，要爆破到什么时候啊

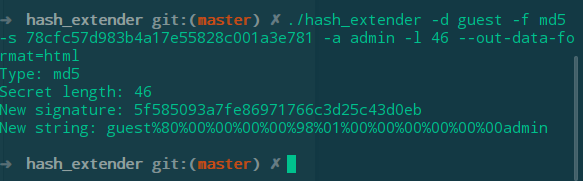
## 题目部署方法

部署在服务器上，需要php7.0或php5.0 + Apache环境，把index.php和secret.php部署在Web根目录即可。

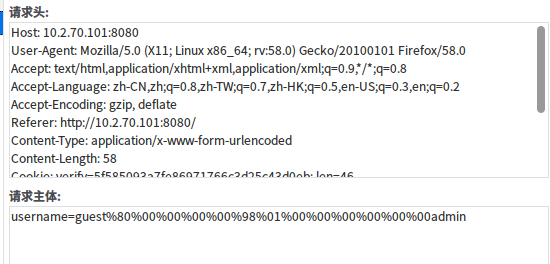
## 过关流程及过关标志

【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】

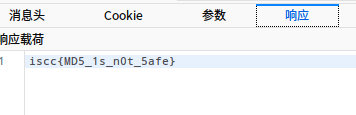
在cookie中获取原MD5值和key的长度。



构造新username和MD5.



抓包改包改变参数。



得到flag

## 硬件使用及网络拓补

不需要

# 相关问题

## 题目分值

250

## 题目Flag

iscc{MD5\_1s\_n0t\_5afe}

## 竞赛阶段服务器端监控方法

监控服务器负载，如果发现存在DDOS攻击，禁止该IP访问

## 须注意的问题

无

# 附件

## 附件1：题目源代码

见附件