

2018“百越杯”第四届福建省高校网络空间安全大赛部分题目

writeup

原创

听说名字太长了会很不好记  于 2018-12-02 18:05:32 发布  4740  收藏 2

分类专栏: [2018百越杯writeup](#) 文章标签: [CTF writeup](#) [百越杯](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/zfzdbdr1250/article/details/84724196>

版权



[2018百越杯writeup](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

2018“百越杯”第四届福建省高校网络空间安全大赛writeup

0x00题目存档:

链接: <https://pan.baidu.com/s/1v59VfheEC5XY8vyKvgEX3Q>

提取码: bbfj

0x01题目名称: 签到

操作内容:

Step 0: 题目信息

□

Step 1: 九乘九矩阵加密分析

莫名其妙就想到了矩阵加密, 百度搜了半天的解密方法也没找到...还好队友做出来了, 不然肯定会在这个题目上浪费很多时间。

Step 2: 求解数独

队友是直接搜了数独求解, 找到了在线求解数独的网站。

□

Step 3: md5加密

将解密后的81位数字按照从左到右、从上到下的顺序记录并进行md5加密即为flag。

□

FLAG值:

flag{cee3860fb3f4a52e615fa8aaf3c91f2b}

0x02题目名称：马男波杰克

操作内容：

Step 0: 题目信息

□

附件：

atool.png

Step 1: atool-图片隐写解密

□

FLAG值：

flag{jioiuojoi666}

0x03题目名称：血小板天下第一可爱

操作内容：

Step 0: 题目信息

□

附件：

atool.png

And:

□

Step 1: 二维码分析

直接用snipaste截左下角来补齐上边两个角，扫出信息后解码即可得到key

atool.png

Step 2: LSB解密

2.1 百度一番后可以找到相关的文章：

□

2.2 下载相应脚本并解密，需要注意的是lsb.py需要和crypt.py的脚本放在一个目录下才不会报错

□

2.3 解密过程

□

2.4 解密出即为flag

□

FLAG值:

```
flag{1_l0ve_LSB~}
```

0x04题目名称: flag_universe

操作内容:

Step 0: 题目信息

□

附件:

链接: <https://pan.baidu.com/s/1MHXgReLAHIOMbOYI-b-e-g>

提取码: 9uxv

Step 1: 分析tcp流

分析数据流，可以发现第十四个png图片也就是new_universe.png有点异常

Step 2: 导出图片，图片隐写分析

2.1 复制原始数据存到一个txt文档中，用010编辑器导入十六进制在存为png图片即可

```
atool.png
```

2.2 LSB隐写，zsteg直接分析比较快

□

FLAG值:

```
flag{Plate_err_klaus_Mail_Life}
```

0x05题目名称: warmup

操作内容:

Step 0: 题目信息

□

题目代码:

□

Step 1: 代码审计

1.1 分析代码

□

1.2 assert函数是可以执行代码的，功能有点类似于eval。由于echo flag已经被注释掉了，所以需要自己去构造assert执行输出flag.php的内容

□

1.3 这道题目应该跟Hack.lu-CTF 2018的一道题目有点神似...之前刚好有看过

□

Step 2: 构造相应URL

□

FLAG值:

```
flag{567b182c-c698-4a3f-8eb4-bde9795425fd}
```

比赛总结:

菜的抠脚QAQ