

# i春秋ctf夺旗赛（第四季）wirteup——misc

原创

jammy 于 2020-01-03 15:21:05 发布 2140 收藏 9

分类专栏: [CTF](#) 文章标签: [CTF MISC](#)

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/qq\\_41832837/article/details/103821095](https://blog.csdn.net/qq_41832837/article/details/103821095)

版权



[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

前言: 这次参加了i春秋ctf夺旗赛, misc类型一共有两道题。在这里跟大家分享一下解题步骤以及思路。

第一道题, Xlmg

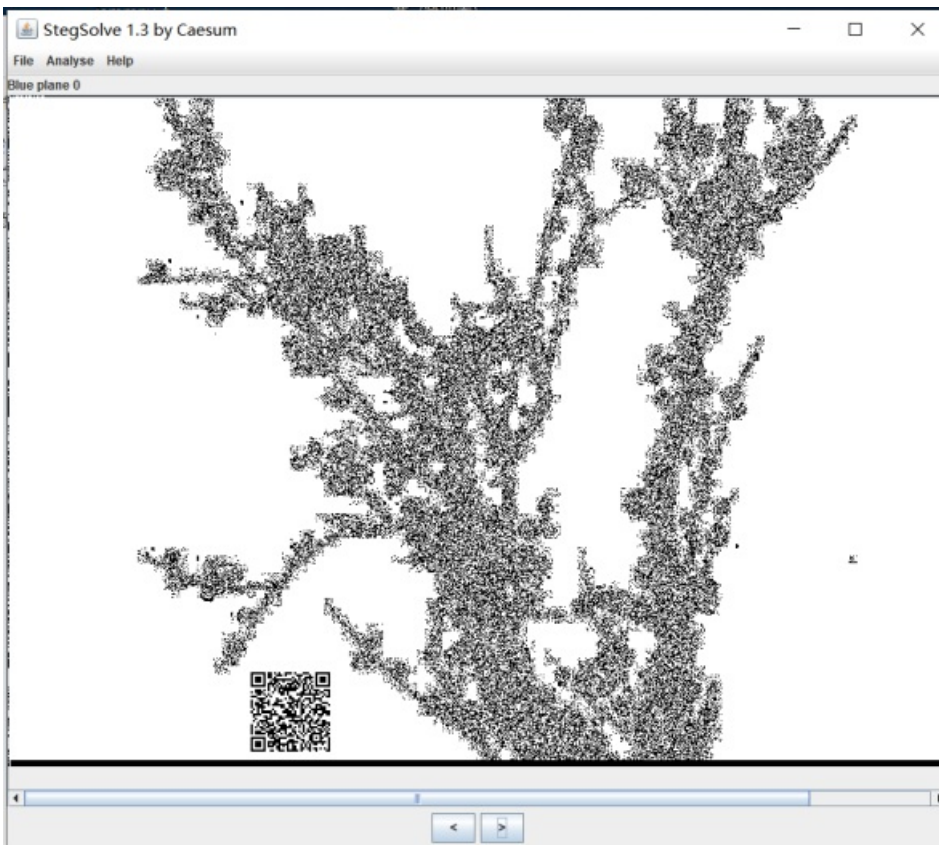
下载文件解压后, 得到一张png图片



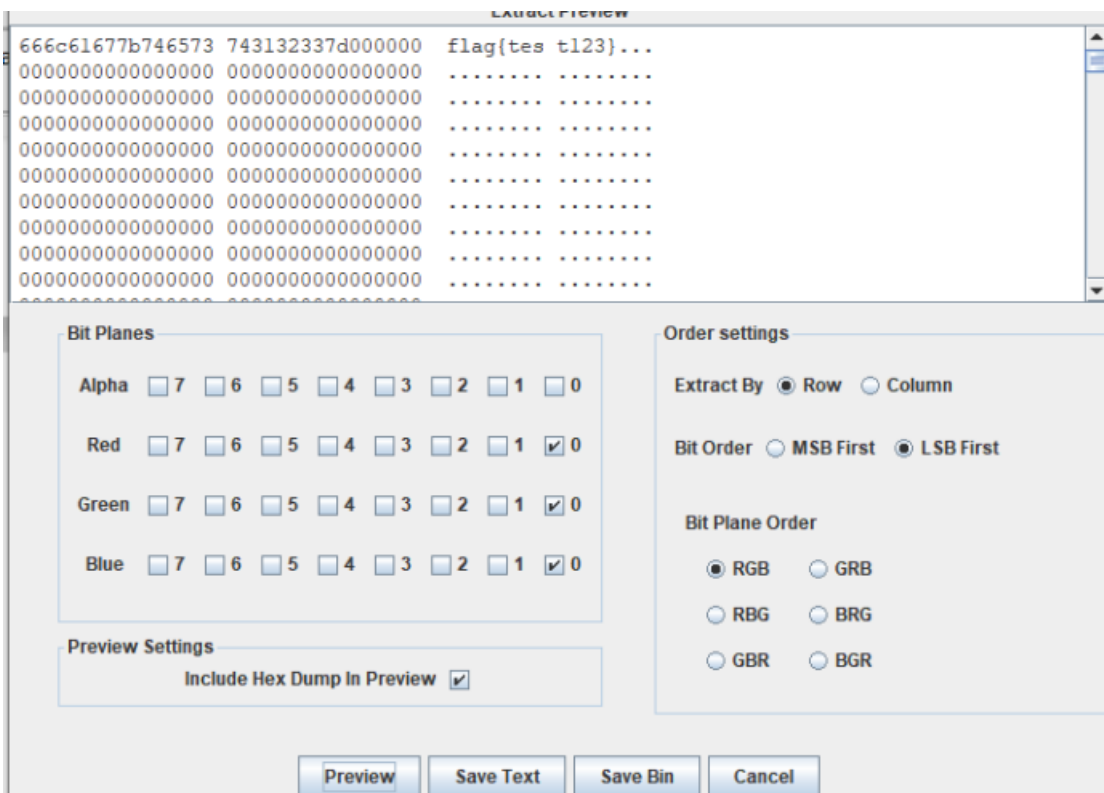
这道题考察是图片隐写。图片隐写是misc常见的题型之一, 接下来我会详细讲解一下解题步骤。

工具: stegsovlle

1、把图片放到stegsovlle分析, 程序最下面有两个小按钮, 不断点击直到得到一个被隐藏的二维码。



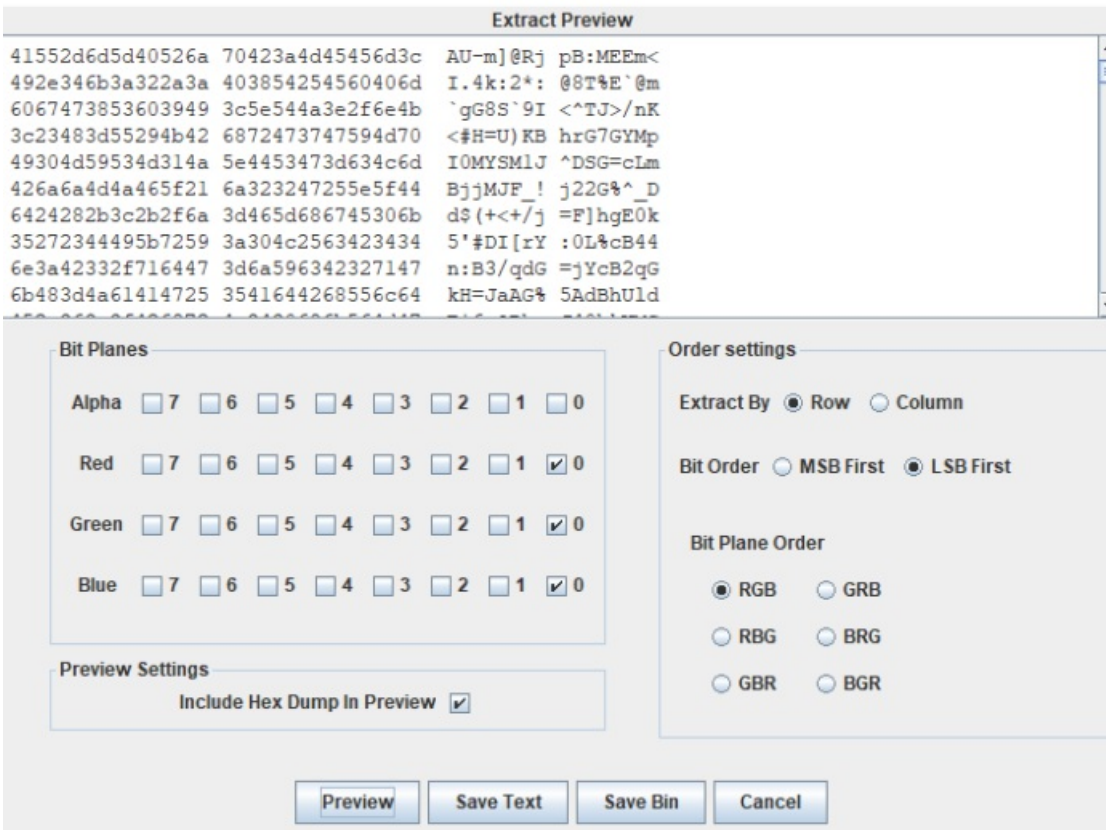
2、按照以往的题型，扫这个二维码就可以得到flag。但是这里有个坑，解码后的flag是假的。真的flag通过LBS隐写藏起来了。那怎么看是否存在LBS隐写呢？还是使用我们stegsolve隐写神器。点击程序最上面的Analyse，选择Data Extract。然后如图所示勾选功能，Preview一下。得到flag。



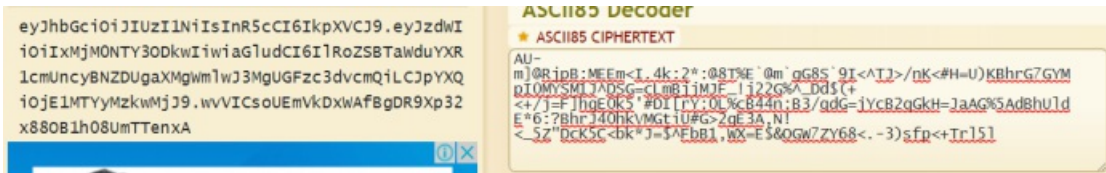
第二道题，pypi

首先我们要知道PyPI是什么？PyPI(Python Package Index)是python官方的第三方库的仓库

1、下载文件解压，我们会得到一个图片，还有一个需要输入密码才能解压的txt文件。遇到这种题型，图片中可能会找到我们需要的密码。一开始的解题步骤和上一题类似，通过stegsolve找到被隐写的信息。只不过，这里被隐写的信息不是明文，而是通过base85加密后的信息。



2、点击SaveBin保存下来。然后把密文拿到在线base85解密网站去破译：



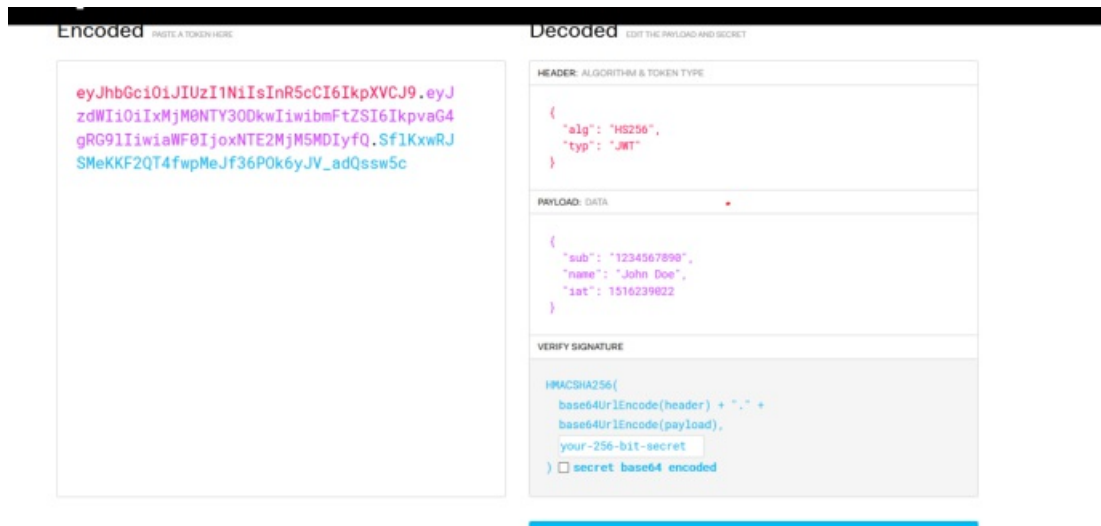
可以得到：

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwiaGludCI6IiRoZSBTaWduYXR1cmU

3、我们发现解密后的信息，是eyJ开头的。如果对jwt有所了解的，就该知道这里其实是加密后的jwt信息。不了解的也没关系，把它再进行一次base64解码。会得到以下结果：



4、可以看到“JWT”，所以我们JWT官网网站分析一下：



这里有个提示：签名的MD5就是解压缩的密码

5、对JWT进行爆破攻击，得到我们secret。使用的工具：c-jwt-cracker；

使用c-jwt-cracker需要我们在我们linux里安装好openssl头文件。

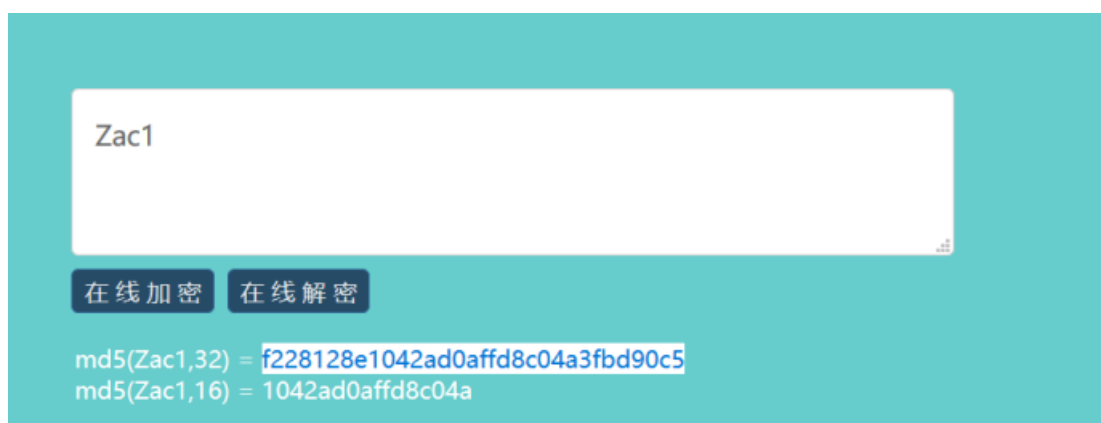
在linux的配置命令是：apt-get install libssl-dev

下载好c-jwt-cracker，还需要我么在工具所在目录执行make命令。目的是让文件makefile运行起来。编译完后会生成一个jwtcrack文件。

6、我们把解密后的base85信息放进去就可以得到签名了，如下图所示：

```
root@kali:~/Desktop/tools/c-jwt-cracker-master# ./jwtcrack eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiaWF0IjoxNTE2MzkwMjY5LWVVICsoUEmVkdXWAfBgDR9Xp32x880B1h08UmTTenxA
Secret is "Zac1"
root@kali:~/Desktop/tools/c-jwt-cracker-master#
```

7、再把Zac1进行MD5加密：



得到密码：f228128e1042ad0affd8c04a3fbd90c5

8、打开文本输入密码得到信息：Gameforflag，结合题目“pypi”，需要我们在pypi网站找到“Gameforflag”这个项目

gameforflag 0.0.1 ✓ Latest version

```
pip install gameforflag
```

Last released: Dec 4, 2019

Just a joke

**Navigation**

- Project description
- Release history
- Download files**

**Download files**

Download the file for your platform. If you're not sure which to choose, learn more about [installing packages](#).

Filename, size	File type	Python version	Upload date	Hashes
<a href="#">gameforflag-0.0.1.tar.gz</a> (1.2 kB)	Source	None	Dec 4, 2019	<a href="#">View</a>

9、下载下来，里面有个flag.py。打开得到flag{a70483c2fa93f9bd54c4fcf3cca0b484}

END:

笔者也是个小白，在不断学习和成长中。以后会不断更新各类CTF的writeup，以供更多的读者学习和积累知识，共同学习和探讨。