

南京邮电大学CTF隐写术部分Writeup

转载

[weixin_30399797](#) 于 2017-01-08 00:42:00 发布 125 收藏 1

文章标签: [php](#)

原文链接: http://www.cnblogs.com/Chesky/p/nuptzj_Steganography_Writeup.html

版权

女神

听说这是女神的私房照，里面藏着flag哦

<http://115.28.150.176/misc1.jpg>

这个链接居然打不开，摔！万念俱灰！主办方可否给力点！

P.S.为了方便日后学习，暂时列下原题。

PP.S.我承认我只是想看图。

图种

将 gif 图片拉进 HexEditXP，拉到底，看到文件结尾有个 2333.gif，说明该文件包含其他的东西。

结合题目标题，猜测为 zip 或 rar 隐藏，其中：

RAR Archive (rar) 文件头: 52617221

ZIP Archive (zip) 文件头: 504B0304 文件尾: 50 4B

通过查找后发现没有 RAR 格式的特征码。符合 ZIP 格式。

重命名为 zip，解压后得到 gif 文件。

结合题目 hit:

flag是动态图最后一句话的拼音首字母

得到flag为

nctf{dssdcmlw}

丘比龙De女神

flag是照片文件的md5值(小写)

所以有那么多女神吗.....

按照第二题步骤查看。

查找后发现文件头没有对应上，手动修改为 0304。

然而打开后发现文件损坏.....

再次查找发现文件总共有 3 个值为 504B，并且查看到 gif 文件尾。

改文件头即可。解压密码为提示中的 love.

参考资料

文件头特征码 <http://blog.csdn.net/guoguo1980/article/details/5317665>

压缩文件格式 <http://www.joychou.org/index.php/Misc/ZIP-File-Format.html>

隐写术总结 <http://bobao.360.cn/learning/detail/243.html>

图片隐写自动化工具 <https://github.com/devttys0/binwalk/blob/master/INSTALL.md>

转载于:https://www.cnblogs.com/Chesky/p/nuptzj_Steganography_Writeup.html