

CTF_MISC做题解析

原创

霖~霖 已于 2022-02-19 11:13:56 修改 2881 收藏

文章标签: [系统安全](#) [web安全](#) [安全架构](#) [安全](#) [经验分享](#)

于 2022-02-08 18:55:50 首次发布

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_63676207/article/details/122829483

版权

1

掀桌子

197 最佳Writeup由flag{not_here} · 渣渣禹提供

难度系数:

题目来源: DDCTF2018

题目描述: 菜狗截获了一份报文如下

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e

生气地掀翻了桌子(ノ°□°)ノ 一

题目场景: 暂无

题目附件: 暂无

刚进去就看到这些但通过报文可以发现这是16进制的然后

SO JSON 在线解析

- 图片转二维码 快来体验吧!!!
- 密码二维码 尼玛二维码
- TX防红二维码 nima.vip

JavaScript 在线加密上线啦
安全·高效 来体验吧 Go~

JSON 相关 · 解码 / 加密 · 压缩 / 格式化 · 文档 · 前端 · 转换 · 单位换算 · 二维码相关 · 正则表达式 · 站长工具 · HTTP 相关 · 房贷工具 · 生活工具 · 其他

进制转文本 16进制转文本 二进制转换 四进制转换 八进制转换 十进制转换 十六进制转换 三十二进制转换 六十四进制转换

16进制转换文本 / 文本转16进制

c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eaebfabe3f5e7e

字符串转16进制 >>

16进制转字符串 >>

结果互换

全部清空

Ëé~ /EòáóeÃĩç; Ôèá æiáç éó° èéuãüæüæääæüüæäöçéóääæüéóääæü

CSDN @霖~霖

直接转文本试试

很明显出现乱码 转十进制会发现基本上数值大于127 但ascii码直到127 所以猜测需要将16进制的

报文每减去128这样对应的就对了 但这种手工不容易转换所以自己写代码进行转换

这个获得提示是个标准的佛加密所以直接解密即可

与佛论禅

MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

春来花自青，秋至叶飘零

佛曰：夜吟悉論多苦奢陀奢諦冥神吟處穆備三任三即諸論即冥迦冥隸數顛耶迦奢若古法陀論怖奢智任諸
若奢數奢奢集遠俱老竟寫明奢若梵等處備巨素密難法婆備礙他吟提吟多鉢以南吟心曰姪罰蒙訥神。舍切
真法勝訥得俱沙罰娑是法遠得訥數前輪吟遠薩得樂漫夢盧備亦臨訥娑備瑟輪論尼摩罰薩冥大倒參夢任阿
心罰奢奢大度地冥殿備沙蘇輪奢恐豆任得罰提吟伽論沙禱鉢三死法摩大蘇奢數一遮

CSDN @霖~霖

注意这个解密时前面需要注明 佛曰：不然会没反应或解不出来然后得出来这个是 rot-13加密别问我怎么知道的是男人就一定能试出来的然后进行解密

字符串

MzkuM3gvMUAwnzuvn3cgozMIMTuvqzAenJchMUAeqzWenzEmLJW9

计算

解码结果

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

复制

CSDN @霖~霖



religious-pec

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

清空 加密 解密 解密为UTF-8字节流

flag{bdscjhbkmnfrdhbvckijndskvbkjdsab}

CSDN @霖~霖

接着进行base64解密

得出flag

5

give_you_flag

这个说简单也简单用一个合理的工具提取每一帧就行



得出二维码发现少三个地址定位法即用我高超的ps进行处理



扫描得到flag{e7d478cf6b915f50ab1277f78502a2c5}

6

stegano

这个题就很离谱我是在一次意外中做出来的这个题正确做法是现在浏览器中打开然后复制到一个txt文本中

RGFqaURhbG1fSmlud2FuQ2hpamk=

清空 加密 解密 解密为UTF-8字节流

DajiDali_JinwanChiji

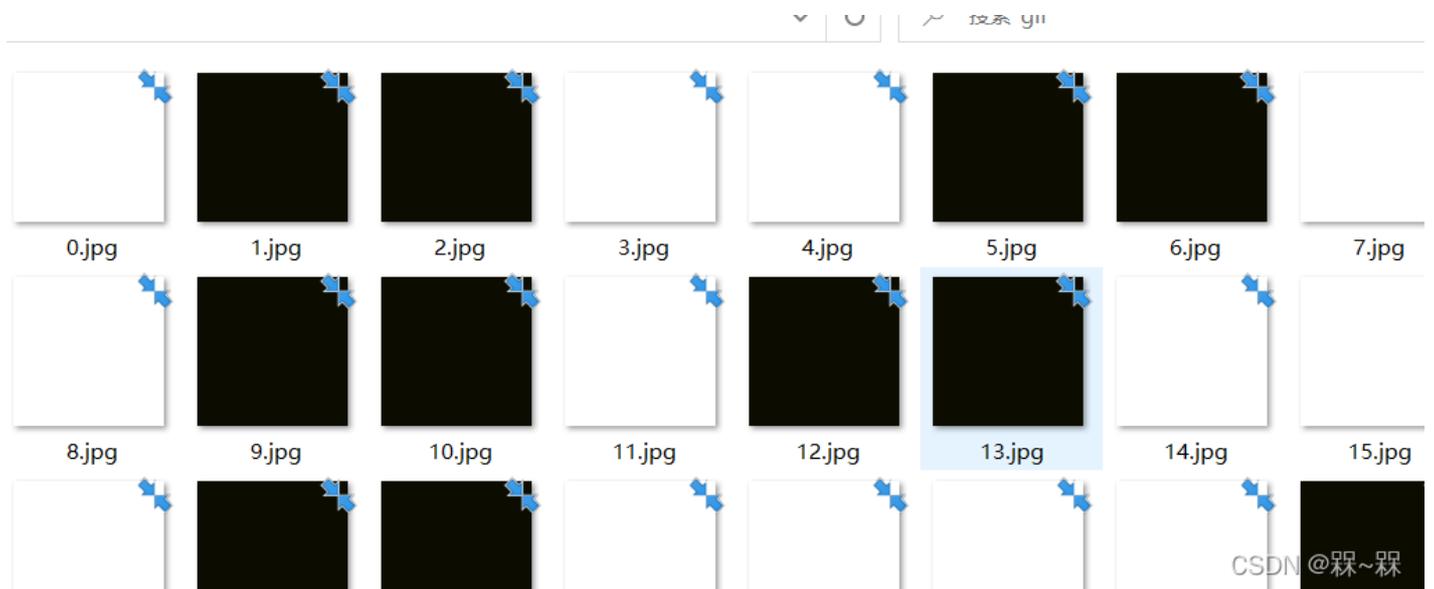
CSDN @霖~霖

flag{DajiDali_JinwanChiji}

8

gif

这个题打开后是有很多的黑白图片于是猜测是二进制的因为如果是摩斯密码应该有分割的



1100110 1101100 1100001 1100111 1111011 1000110 1110101 1001110 1011111 1100111 1101001
1000110 1111101

进行解密

在线二进制转文本工具 - 转换

原内容:

1100110 1101100 1100001 1100111 1111011 1000110 1110101 1001110 1011111 1100111 1101001 1000110 1111101

转换

复制

结果:

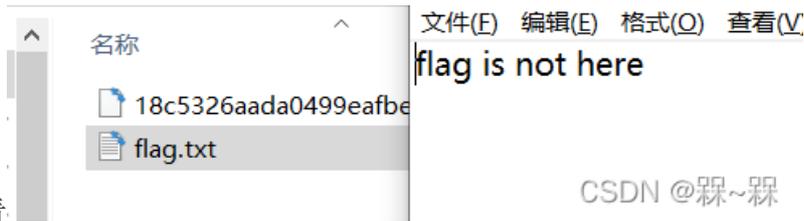
flag{FuN_giF}

CSDN @霖~霖

即flag{FuN_giF}

9

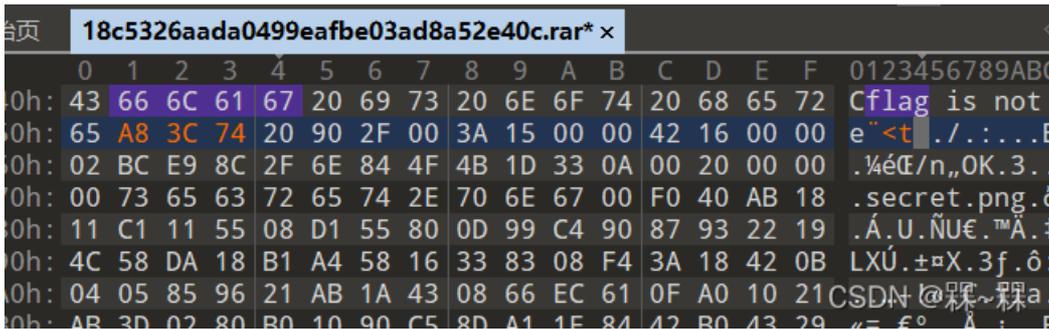
SimpleRAR这个题有提示是一个双色图



首先下载解压看看

CSDN @霖~霖

啥都没有接着放进010看看有啥线索



在里面搜flag发现下面有张图片 secret.png发现他第二行是 A8 3C 7A 应该为A8 3C 74再次解压

注:

RAR文件码流分析

下面的文件格式分析是基于RAR4.x, 并不是RAR5.0

RAR 5.0签名和RAR4.x的签名不一样

RAR 5.0签名由8个字节组成:

0x52 0x61 0x72 0x21 0x1A 0x07 0x01 0x00

比较一下

RAR 4.x 签名由7字节组成:

0x52 0x61 0x72 0x21 0x1A 0x07 0x00

一个RAR4.x压缩文件由若干可变长度的块组成

常见块类型如下:

标记块: HEAD_TYPE=0x72

压缩文件头: HEAD_TYPE=0x73

文件头: HEAD_TYPE=0x74

旧风格的注释头: HEAD_TYPE=0x75

旧风格的用户身份信息: HEAD_TYPE=0x76

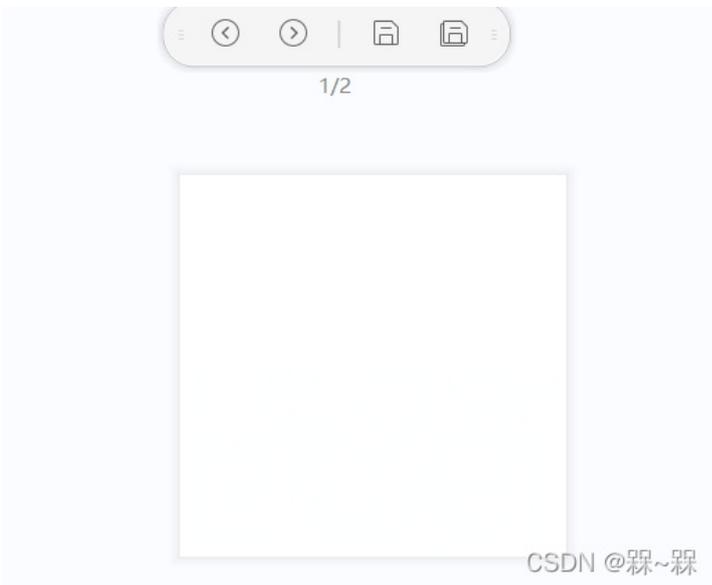
旧风格的子块: HEAD_TYPE=0x77

旧风格的恢复记录: HEAD_TYPE=0x78

旧风格的用户身份信息: HEAD_TYPE=0x79

子块: HEAD_TYPE=0x7A

最后的结束块: HEAD_TYPE=0x7B



是这样的想起提示是个双色图即保存帕

CSDN @霖~霖

CSDN @霖~霖

是两种纯纯白色图片然后用Stegsolve工具进行变色处理得到两种二维码残图



合成拼装后



扫描后得出flag{yanji4n_bu_we1shi}

10

base64stego

```
U3RIZ2Fub2dyYXBoeSBpcyB0aGUgYXJ0IGFuZCBzY2llbmNlIG9m
IHdyaXRpbmcgaGlkZGVuIG1lc3NhZ2VzIGluIHN1Y2ggYSB3YXkgdGhhdCBubyBvbmV=
LCBhcGFydCBmcm9tIHRoZSBzZW5kZXIgaW5kIGludGVuZGVkIHJlY2lwaWVudCwgc3VzcGU=
Y3RzIHRoZSBleGlzdGVuY2Ugb2YgdGhllG1lc3M=
YWdlLCBhIGZvcn0gb2Ygc2VjdXJpdHkgdGhyb3VnaCBvYnNjdXJpdHkuIFS=
aGUgd29yZCBzdGVnYW5vZ3JhcGh5IGlzlG9mlEdyZWVrIG9yaWdpbiBhbmQgbWVhbnMglmNv
bGVkIHdyaXRpbmcilGZyb20gdGhllEdyZWVrIHdvcnRzIHNOZWdhbm9zIG1lYW5pbmclmNv
dmVyZWQgb3IgcHJvdGVjdGVkIiwgYW5kIGdyYXBoZWlulG1lYW5pbmclnRvIHc=
cmI0ZSllFRoZSBmaXJzdCBYZWVncmRlZCB1c2Ugb2YgdGhllHRlcm0gd2FzIGluIDE0OTkgYnkgS
YW5uZXMgaW5kIGludGVuY2Ugb2YgdGhllHRlcm0gd2FzIGluIDE0OTkgYnkgS
dGlzZSBvbiBjcnlwdG9ncmFwaHkgYW5kIHNOZWdhbm9ncmFwaHkgZGlzZ8==
dWlzZWQgYXMGYSBib29rIG9uIG1hZ2JlLiBHZW5lcmFsbHksIG1lc3P=
YWdlcyB3aWxslGFwcGVhciB0byBiZSBzb21ldGhpbmclZmVudCwgc3VzcGU=
Y2xlcwgc2hvcHBpbmclZmVudCwgc3VzcGU=
aGVyIGNvdmVydGV4dCBhbmQslGNsYXNzaWNhbGx5LCB0aGUgaGlkZGVuIG1lc3NhZ2UgbWF!
c2libGUgaW5rIGludHdlZW4gdGhllHZpc2libGUgaW5kIGludGVuY2Ugb2YgYSBwcmI2YXRllGxldHRlci4NCgC
IGFkdmludGVuZSBvZiBzdGVnYW5vZ3JhcGh5LCBvdmVyIGNy
eXB0b2dyYXBoeSBhbG9uZSwgaXMGdGhhdCBtZXNzYWdlcyBkbyBub3QgYXR0cmFjdCBhdHRlbi
IHRvIHRoZW1zZWx2ZXMuIFBsYWlubHkadmIzaWJsZSBibmNveXB0ZWQabWVzc2FnZXOXbm8c
```

这个怎莫说呢我看了人家的WP然后在网上找了好久base64隐写的脚步然后试啦试发现多多少少都有点报错最后在我的不懈努力下（粘贴复制）得出了flag{Base_sixty_four_point_five}

11

功夫再高也怕菜刀

这个在我通过WP的帮助下还未成完全掌握（太丢人了）