

XCTF攻防世界：MISC新手题解（7~12）

原创

[CNwanku](#) 于 2019-12-18 11:29:34 发布 953 收藏 2

文章标签：[信息安全](#) [反编译](#) [jar](#) [python](#)

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_43233085/article/details/103594407

版权

XCTF攻防世界：MISC新手题解（7~12）

[坚持60s](#)

[gif](#)

[掀桌子](#)

[如来十三掌](#)

[base64stego](#)

[功夫再高也怕菜刀](#)

[坚持60s](#)

坚持60s 👍 5 最佳Writeup由 [不要让我起名提供](#)

难度系数: ★ 1.0

题目来源: [08067CTF](#)

题目描述: 菜狗发现最近菜猫不爱理他, 反而迷上了菜鸡

题目场景: 暂无

题目附件: [附件1](#)

https://blog.csdn.net/qq_43233085

下载是个打包的java程序, 打开是一个游戏文件



既然是程序会给出flag, 那么flag就在源代码中了, 用java反编译工具反编译, 在文件中可以找到PlaneGameFrame.class中找到flag(大括号中base64需要解码)。

```

class Explorer {
    ...
}

class PlaneGameFrame {
    ...
    case 6:
        println(g, "flag{RGFqaURhbG1f5mlud2FuQ2hpamk=}", 50, 150, 300);
        break;
}

```

得到 flag{DajiDali_JinwanChiji}

gif

gif 👍 8 最佳Writeup由 [不要让我起名提供](#)

难度系数: ★ 1.0

题目来源: 暂无

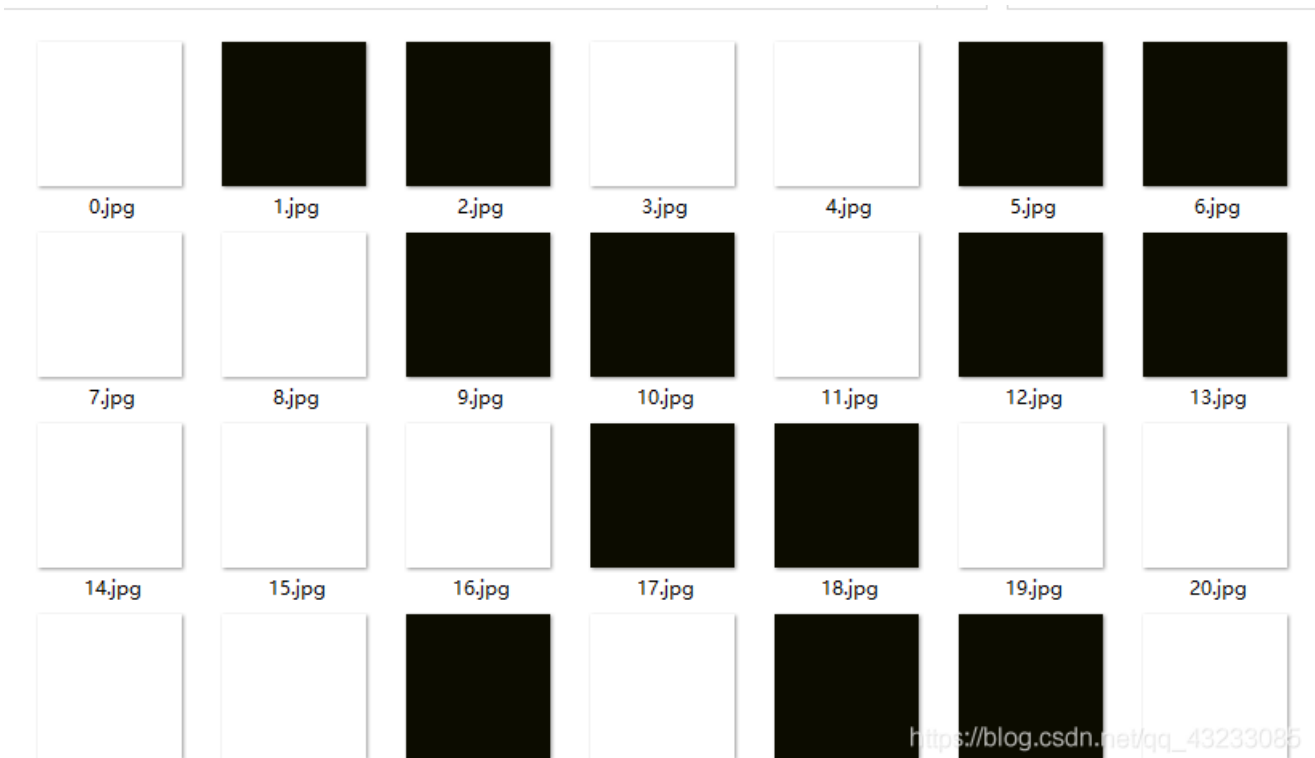
题目描述: 菜狗截获了一张菜鸡发给菜猫的动态图, 却发现另有玄机

题目场景: 暂无

题目附件: [附件1](#)

https://blog.csdn.net/qq_43233085

打开压缩包发现许多张黑白颜色的图片



将黑白图片分别记为1,0, 得到

```
01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101
```

转化为字符串形式即可

```
import re
a = '01100110011011000110000101100111011110110100011001110101010011100101111101100111011010010100011001111101'
b = re.findall(r'.{8}', a)
flag = ''
for i in b : flag += chr(int(i, 2))
print(flag)
```

得到flag{FuN_giF}

掀桌子

掀桌子 👍 12 最佳Writeup由渣渣再提供 WP 建议

难度系数: ★ 1.0

题目来源: DDCTF2018

题目描述: 菜狗截获了一份报文如下c8e9aca0c6f2e5f3e8c4efe7a1a0d4e8e5a0e6ece1e7a0e9f3baa0e8eafae3f9e4eafae2eae4e3eae bfaebe3f5e7e9f3e4e3e8eaf9eaf3e2e4e6f2, 生气地掀翻了桌子(°□°)ノノ

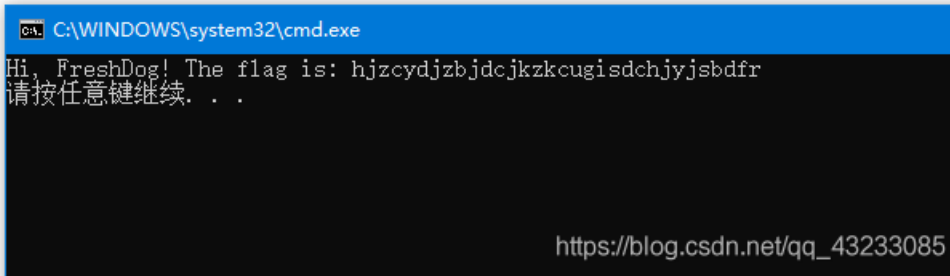
题目场景: 暂无

题目附件: 暂无

https://blog.csdn.net/qq_43233085

现题目中的字符串由0-9、a-f组成，我们知道2位十六进制可表示1个字节，写脚本将该字符串两两分组转换成字节，发现所有字节均大于128，我们又知道ASCII码表示范围是0-127，于是每一个字节都减去128，再转换成字符串，得到flag

```
1 cc = '\xc8\xe9\xac\xa0\xc6\xf2\xe5\xf3\xe8\x
2 cd = ""
3 for i in cc:
4     cd+=chr(ord(i) - 128)
5 print(cd)
```



得到flag{hjzcydjzbdcjzkcugisdchjyjsbdf}

如来十三掌

如来十三掌

8 最佳Writeup由渣渣禹提供

难度系数: ★ 1.0

题目来源: 暂无

题目描述: 菜狗为了打败菜猫, 学了一套如来十三掌。

题目场景: 暂无

题目附件: 附件1

https://blog.csdn.net/qq_43233085

下载后发现为一串看不懂的文字, 网上搜索发现有一个“与佛论禅”的网站, 应该可以解密

网站地址: <http://www.keyfc.net/bbs/tools/tudoucode.aspx>

开始直接粘贴进去, 好像解不了...

太深奥了, 参悟不出佛经的真意.....

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

人无善恶, 善恶存乎尔心

夜哆悉諳多苦奢陀奢諦冥神哆虛穆瞻三任三即諳諳即冥迦冥隸數顯耶迦奢若吉性陀諳佈奢智任諳若奢數菩奢集遠俱老竟寫明奢若梵等虛瞻豆蒙密離性婆瞻礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真性勝訥得俱沙罰婆是性遠得訥數罰輸哆遠薩得槃漫夢虛瞻亦聽訥娑瞻瑟輸諳尼摩罰薩具大倒參夢任阿心罰等奢大度地冥顯瞻沙蘇輸奢恐豆任得罰提哆伽諳沙楞鉢三死性摩大蘇奢數一遮

https://blog.csdn.net/qq_43233085

发现格式要在前面加上佛曰:

MzkuM3gyMUAwnzuvn3cgozMLMTuvqzAenJchMUAeqzWenzEmLJW9

听佛说宇宙的真谛

参悟佛所言的真意

普度众生

不可说,不可说,一说即是错

佛曰: 夜哆悉諳多苦奢陀奢諦冥神哆虛穆瞻三任三即諳諳即冥迦冥隸數顯耶迦奢若吉性陀諳佈奢智任諳若奢數菩奢集遠俱老竟寫明奢若梵等虛瞻豆蒙密離性婆瞻礙他哆提哆多鉢以南哆心曰姪罰蒙訥神。舍切真性勝訥得俱沙罰婆是性遠得訥數罰輸哆遠薩得槃漫夢虛瞻亦聽訥娑瞻瑟輸諳尼摩罰薩具大倒參夢任阿心罰等奢大度地冥顯瞻沙蘇輸奢恐豆任得罰提哆伽諳沙楞鉢三死性摩大蘇奢數一遮

https://blog.csdn.net/qq_43233085

第一反应将其进行BASE64解密, 但是解码失败, 据题意, 十三...ROT13编码。

将其先ROT13再加密一次即解密, 之后再行BASE64解码

得到flag值, flag{bdscjhbkmfrdhhvckijndskvbkjdsab}

base64stego

base64stego 26 最佳Writeup由zEr0_0提供

难度系数: 1.0

题目来源: [olympicCTF](#)

题目描述: 菜狗经过几天的学习, 终于发现了如来十三掌最后一步的精髓

题目场景: 暂无

题目附件: [附件1](#)

https://blog.csdn.net/qq_43233085

本来以为又要与佛论禅了, 结果发现它的加密是假的, 用WinRAR的修复功能直接修复解压, 发现了一个txt文件。打开文件, 进行base64解码, 结果如下:

Steganography is the art and science of writing hidden messages in such a way that no one

意思是说, 隐写是个很好的解决方法

马上上网查了查, 发现base64可以隐写的, 并发现了大佬们的脚本代码

```
#coding=utf-8
def get_base64_diff_value(s1, s2):
    base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
    res = 0
    for i in xrange(len(s2)):
        if s1[i] != s2[i]:
            return abs(base64chars.index(s1[i]) - base64chars.index(s2[i]))
    return res
def solve_stego():
    with open('D:\火狐下载\1.txt', 'rb') as f:
        file_lines = f.readlines()
        bin_str = ''
        for line in file_lines:
            steg_line = line.replace('\n', '')
            norm_line = line.replace('\n', '').decode('base64').encode('base64').replace('\n', '')
            diff = get_base64_diff_value(steg_line, norm_line)
            print diff
            pads_num = steg_line.count('=')
            if diff:
                bin_str += bin(diff)[2:].zfill(pads_num * 2)
            else:
                bin_str += '0' * pads_num * 2
            print goflag(bin_str)
def goflag(bin_str):
    res_str = ''
    for i in xrange(0, len(bin_str), 8):
        res_str += chr(int(bin_str[i:i + 8], 2))
    return res_str
if __name__ == '__main__':
    solve_stego()
```

这个是python2的脚本，所以运行要用python2来运行，否则出错这里无法解决，编码符设置我为ANSI
跑下脚本，得到flag，flag{Base_sixty_four_point_five}

功夫再高也怕菜刀

功夫再高也怕菜刀 👍 18 最佳Writeup由T1M·河东小伍提供

难度系数: ★ 1.0

题目来源: 安恒杯

题目描述: 菜狗决定用菜刀和菜鸡决一死战

题目场景: 暂无

题目附件: 附件1

https://blog.csdn.net/qq_43233085

下载附件，用foremost进行pcapng文件的分离，得到一个zip，打开zip，得到一份加密的flag.txt文件。然后用wireshark打开pcapng文件，查找flag.txt关键字

应用程序 ▾ 位置 ▾ Wireshark ▾ 星期六 15:58

a.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器... <Ctrl-/> 表达式... +

分组详情 ▾ 宽窄 ▾ 区分大小写 字符串 ▾ lag.txt 查找 取消

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|----------------|----------------|----------|--------|------|
| 1149 | 50.140816842 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 |
| 1150 | 50.147576455 | 192.168.43.83 | 192.168.25.128 | HTTP | 515 | HTT |
| 1151 | 50.189982026 | 192.168.25.128 | 192.168.43.83 | TCP | 54 | 478 |
| 1152 | 50.295304588 | 219.216.128.25 | 192.168.25.128 | TCP | 2814 | 80 |
| 1153 | 50.295383546 | 192.168.25.128 | 219.216.128.25 | TCP | 54 | 584 |
| 1154 | 50.332176266 | 219.216.128.25 | 192.168.25.128 | TCP | 4194 | 80 |
| 1155 | 50.332340670 | 192.168.25.128 | 219.216.128.25 | TCP | 54 | 584 |

Transmission Control Protocol, Src Port: 80, Dst Port: 47856, Seq: 247, Ack: 206198,

Hypertext Transfer Protocol

Line-based text data: text/html (7 lines)

```
->|./\t2017-12-08 11:42:11\t0\t0777\n..\t2017-12-08 11:39:10\t4096\t0777\n1.php\t2017-12-08 11:33:16\t33\t0666\n6666.jpg\t2017-12-08 11:42:11\t102226\t0666\nflag.txt\t2017-12-08 11:35:29\t17\t0666\nhello.zip\t2017-12-08 09:32:36\t224\t0666\n
```

0190 6a 70 67 09 32 30 31 37 2d 31 32 2d 30 38 20 31 jpg·2017 -12-08 1

01a0 31 3a 34 32 3a 31 31 09 31 30 32 32 32 36 09 30 1:42:11· 102226·0

01b0 36 36 36 0a 66 6c 61 67 2e 74 78 74 09 32 30 31 666:flag.txt:201

01c0 37 2d 31 32 2d 30 38 20 31 31 3a 33 35 3a 32 39 7-12-08 11:35:29

发现有个6666.jpg，右键第1150个数据包，追踪TCP流，复制从FFD8开始到FFD9的内容，到winHex里新建文件粘贴，注意粘贴格式是ASCII Hex。

Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · a.pcapng

Content-type: application/x-www-form-urlencoded

Content-Length: 204999

```

aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImR
pc3BsYXlfZXJyb3JzIiwic19yZXBsYWNlKCIJccIIsIiIsJGMpOyRjP
kZj1iYXNlNjRfZGVjb2RlKCRFUE9TVFsiejEiXSk7JGM9JF9QT1NUWy
J6MiJdOyRjPjY2RlKCRFUE9TVFsiejEiXSk7JGM9JF9QT1NUWy
XBSyYWNlKCIJccIIsIiIsJGMpOyRjPjY2RlKCRFUE9TVFsiejEiXSk7
bGVuKCRjKTskaSs9MikkYnVmLj11cmxkZWVZGUoIiUiLnN1YnN0cig
kYyYwkaSwyKSk7ZWVZGUoIiUiLnN1YnN0cigkYyYwkaSwyKSk7ZWVZ
k%2FIjEiOiwIik702VjaG8oInw8LSIp02RpZSgp0w%3D%3D&z1=RDp
cd2FtcDY0XHd3d1x1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FFE00010
4A46494600010101007800780000FFDB004300010101010101010101
1010101010101010101010101010101010101010101010101010101
010101010101010101010101010101010101010101010101010101
010101010101010101010101010101010101010101010101010101
1FFDB00430101010101010101010101010101010101010101010101
010101010101010101010101010101010101010101010101010101
1010101010101010101010101010101010101010101010101010101
021101031101FFC4001F000001050101010101010101010101010101
00102030405060708090A0BFFC400B5100002010303020403050504

```

53 客户端 分组, 2 服务器 分组, 3 turn(s).

整个对话 (206 kB) 显示和保存数据为 ASCII 流 7

查找: 查找下一个(N)

Wireshark · 追踪 TCP 流 (tcp.stream eq 7) · a.pcapng

```

1E99E32319C999F681B7A90C6156C60609DD73276E31F2E7B8183F2
F37EE7EFDCFFD7383F9C758F77D65FF00AF78FF00F408EBC6C4DD4A
DE4F5F4EDBD97BBA2E9A7F2A3E830EB45E89F7DD41EBD5FC7AF7F7B
AC9B59E658327293B9CF2E1BEF7FB5FF02EBF8D15763FF571FF00B8
BFFA08A2B86DFE1FFC05797F93FBFEFE9E65DA5FF81BFF002F5FE96
BFFD9HTTP/1.1 200 OK
Date: Fri, 08 Dec 2017 11:42:07 GMT
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Content-Length: 7
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

->|1|<-POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*;
q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 723

```

53 客户端 分组, 2 服务器 分组, 3 turn(s).

整个对话 (206 kB) 显示和保存数据为 ASCII 流 7

查找: 查找下一个(N)

保存为jpg格式，可以得到图片，





图片里的文字就是密码，输入密码，得到flag。

flag{3OpWdJ-JP6FzK-koCMAK-VkfWBq-75Un2z}