

# [攻防世界]base64stego(misc)

原创

yeh629 于 2019-10-10 11:08:35 发布 1090 收藏 1

分类专栏: [ctf](#) 文章标签: [攻防世界](#) [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/qq619337301/article/details/102476989>

版权



[ctf](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

题目:

给定一个stego.txt, 打开发现里面是很多行base64加密后的密文

思路:

尝试base64解码, 发现是隐写术的介绍, 没有任何发现。于是看了别人的writeup, 才知道base64隐写这个东西。

base64原理:

base64 是一种编码方式, 是一种可逆的编码方式。

编码后的数据是一个字符串, 包含的字符为: A-Za-z0-9+/  
共 64 个字符:  $26 + 26 + 10 + 1 + 1 = 64$  其实是 65 个字符, “=”是填充字符。

64个字符需要用6位来表示, 表示成数值为0~63。

编码时如果字符串字节数不是3的倍数, 则位数就不是6的倍数, 就不能划分成6位一组, 此时需要在原数据二进制值后添加0, 然后在编码后的字符串后加上一个或两个“=”, 表示添加的0的个数。

解码时先去掉等号, 转为二进制数, 多余位扔掉, 转为对应的ASCII码, 扔掉多余的0, 恢复成原字符串。

隐写原理:

解码时丢弃的0可以隐藏信息。

代码:

```
import base64
bin_str=''
b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
with open('stego.txt','r') as f:
    for line in f.readlines():
        stegb64="".join(line.split())
        rowb64="".join(str(base64.b64encode(base64.b64decode(stegb64)), 'utf-8').split())
        offset=abs(b64chars.index(stegb64.replace('=','')[-1])-b64chars.index(rowb64.replace('=','')[-1]))
        equalnum=line.count('=')
        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)
print(''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0,len(bin_str),8)]))
```

引用链接: [https://blog.csdn.net/m0\\_37442062/article/details/90517209](https://blog.csdn.net/m0_37442062/article/details/90517209)