

宁波市第三届网络安全大赛-WriteUp（Misc）



水星Sur 于 2020-07-07 18:29:52 发布 2731 收藏 5

分类专栏: [Python Misc CTF](#) 文章标签: [信息安全 CTF CTF 夺旗赛](#)

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/pone2233/article/details/107187497>

版权



[Python 同时被 3 个专栏收录](#)

5 篇文章 0 订阅

订阅专栏



[Misc](#)

22 篇文章 0 订阅

订阅专栏



[CTF](#)

20 篇文章 0 订阅

订阅专栏

文章目录

[友情链接](#)

[内心OS](#)

[Misc | 完成 | 第一](#)

[Misc | 完成 | BBQ](#)

[Misc | 完成 | 看图说话](#)

[Misc | 未完成 | 等等我](#)

[Misc | 未完成 | 抓我把](#)

最后十分感谢各位观看~谢谢, 在下给大家比一个☺

友情链接

Web师傅: [skyxmao师傅](#)

内心OS



第一次参加这种大型比赛, 实力较菜, 请师傅们多多指点

[Misc | 完成 | 第一](#)

下载文件，看一下doc没有任何问题，



图片已做防盗链处理
请在原文件中访问该图片

没有发现任何隐写，然后修改文件后缀名docx为zip，解压

将所有解压后的文件打开，用notepad++ 在此全部文件中搜索flag字段，即可找到flag



图片已做防盗链处理
请在原文件中访问该图片

Misc | 完成 | BBQ



图片已做防盗链处理
请在原文件中访问该图片

庞大的base64，使用Notepad++



图片已做防盗链处理
请在原文件中访问该图片



图片已做防盗链处理
请在原文件中访问该图片

相信大家一眼就能看到是base64文件隐写流（可能不准确）

这里推荐一手脚本

```

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('BBQ.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()

```



图片已做防盗链处理
请在原文件中访问该图片

Misc | 完成 | 看图说话



使用了N多JPG隐写，最后使用到了这个软件SilentEye

由于是弱密码，一跑就出来了

以下都是弱口令

```
"123456", "123456789", "111111", "5201314", "12345678", "123123", "password", "1314520", "123321", "7758521", "1
234567", "5211314", "666666", "520520", "woaini", "520131", "11111111", "888888", "hotmail.com", "112233", "1236
54", "654321", "1234567890", "a123456", "88888888", "163.com", "000000", "yahoo.com.cn", "sohu.com", "yahoo.cn",
"111222tianya", "163.COM", "tom.com", "139.com", "wangyut2", "pp.com", "yahoo.com", "147258369", "123123123", "
147258", "987654321", "100200", "zxcvbnm", "123456a", "521521", "7758258", "111222", "110110", "1314521", "11111
111", "12345678", "a321654", "111111", "123123", "5201314", "00000000", "q123456", "123123123", "aaaaaa", "a1234
56789", "qq123456", "11112222", "woaini1314", "a123123", "a111111", "123321", "a5201314", "z123456", "liuchang",
"a000000", "1314520", "asd123", "88888888", "1234567890", "7758521", "1234567", "woaini520", "147258369", "1234
56789a", "woaini123", "q1q1q1q1", "a12345678", "qwe123", "123456q", "121212", "asdasd", "999999", "1111111", "12
3698745", "137900", "159357", "iloveyou", "222222", "31415926", "123456", "111111", "123456789", "123123", "9958
123", "woaini521", "5201314", "18n28n24a5", "abc123", "password", "123qwe", "123456789", "12345678", "11111111",
"dearbook", "00000000", "123123123", "1234567890", "88888888", "11111111", "147258369", "987654321", "aaaaaaaa
", "1111111111", "66666666", "a123456789", "11223344", "1qaz2wsx", "xiazhili", "789456123", "password", "8765432
1", "qqqqqqqq", "000000000", "qwertyuiop", "qq123456", "iloveyou", "31415926", "12344321", "0000000000", "asdfgh
jkl", "1q2w3e4r", "123456abc", "0123456789", "123654789", "12121212", "qazwsxedc", "abcd1234", "12341234", "1101
10110", "asdasdasd", "123456", "22222222", "123321123", "abc123456", "a12345678", "123456123", "a1234567", "1234
qwer", "qwertyui", "123456789a", "qq.com", "369369", "163.com", "ohwe1zvw", "xiekai1121", "19860210", "1984130",
"81251310", "502058", "162534", "690929", "601445", "1814325", "as1230", "zz123456", "280213676", "198773", "48
61111", "328658", "19890608", "198428", "880126", "6516415", "111213", "195561", "780525", "6586123", "caonima99
", "168816", "123654987", "qq776491", "hahabao", "198541", "540707", "leqing123", "5403693", "123456", "12345
6789", "111111", "5201314", "123123", "12345678", "1314520", "123321", "7758521", "1234567", "5211314", "520520",
"woaini", "520131", "666666", "RAND#a#8", "hotmail.com", "112233", "123654", "888888", "654321", "1234567890",
"a123456"
```



Misc | 未完成 | 等等我

由于比赛结束，看不了题目。题目就发不了了。

不过我经过脚本跑出了这些不知道有没有用

```
12, 235, 05, 0125, 01234, 035, 0145, 01234, 3, 25, 05, 4, 023, 25, 25, 015, 013, 05, 4, 015, 23, 05, 023, 0123, 023, 4, 015, 15, 012, 0123, 12
5, 123, 025, 023, 4, 0123, 125, 125, 125, 13
```

不好意思了，这里我也卡住了

Misc | 未完成 | 抓我把

下载数据流，在数据流，在4 和 5 中看到了一堆的数字，一看就知道504B 是zip，把他复制出来放入txt中



图片已做防盗链处理
请在原文件中访问该图片



图片已做防盗链处理
请在原文件中访问该图片

同样使用插件



图片已做防盗链处理
请在原文件中访问该图片

获得zip，打开下载是一个加密的word，然后使用软件跑一下得到密码

123321（又是一个弱密码）



图片已做防盗链处理
请在原文件中访问该图片

然后我就呆住，请各位大师师傅赐教，我真不会惹。（PS：师傅们吃草莓嘛？）



最后十分感谢各位观看～谢谢，在下给大家比一个☐

