JLUCTF

原创

Ni9htMar3 于 2016-12-26 22:00:21 发布 797 收藏

分类专栏： WriteUp 文章标签： writeup

本文链接：https://blog.csdn.net/Ni9htMar3/article/details/53889649

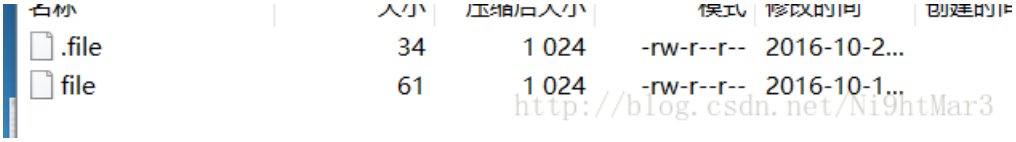
比较早的一次比赛，一直没有上传writeup，那次比赛挺基础的，基本上全部AK，部分提由于关系统的原因没有保留下writeup

签到题

明显就是凯撒加密，解密即得

文件

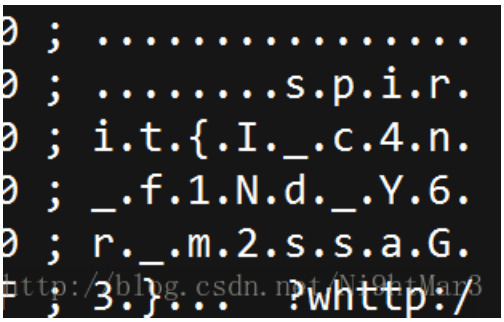
是一个.7z的压缩包，若是用其他解压软件会发现没有东西，若是用7z软件打开，会发现其他格式的（7z软件），



直接打开第一个文件，由**txt**访问，即得

大家想要的入门题b1

直接用UE查看



得到flag

PPAP

用Stg分析，打开**File Format**最下面发现疑似*base64*加密的字符串

```
Ascii:
V2UxYzBt ZXRvc3Bp
cml0Q1RG IQ==PK
        RIW
```

解密即得

This is Flag

发现一串疑似*md5*加密的字符，直接解密即得

110m

`slpFiernicte{CAiHpahReari}`明显就是栅栏加密，分析即得12栏`spirit{AHaRai lFenceCipher}`

买一送一

打开网站，发现有一张图片，下载下来，用**Stg**分析，打开**File Format**发现

```
Ascii:
KUZUE4DD NVWDAZJS
JF5GGMSV GJHEMOLI
MJWVEZSO NVDHUWSU
JV4WMUJ5 HU======
```

用*base64*解密两次即得flag

就要求底数

已知K ^ N = P, 给定N为7,和P为437104634676747795452235896466702336，求K

K= 提交查询

直接写一个简单的python脚本跑出即得

```
print 437104634676747795452235896466702336 ** (1.0/7)
```

流量分析

直接wireshark分析，找到

```
658 GET /su?wd=Spirit%7BBaii_ddU_ju4t_e45y%7D&action=opensearch&ie=UTF-8 HTTP/1.1
```

发现与flag很像，转码即得

这得多少？！

打开发现是求解N的阶乘末尾0的数量，写一个脚本即得

```
def zeros(n):
    x = n // 5
    return x + zeros(x) if x else 0 # 最短: return n // 5 + zeros(n // 5) if n // 5 else 0
a = 56789
print zeros(a)
```

decrypt2

打开txt发现一长短字符，说了是加密，还有密钥，猜测是维吉尼亚加密。`http://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx`在这个网站字段破解

```
— MESSAGE w/Key #29 = 'applepin' ——————————
the viganère ciphar is a metdod of encnypting ahphabetiy text by uoing a serees of difberent caasar
ciphars based kn the letpers of a kayword. it es a simpla form of pklyalphaxetic subotitutioj.the
vigejère ciphen has been neinventad many tiies. the mephod was oniginallu describad by giovwm battispa
bellask in his 1553 bokk la cifrw del. sig. geovan batpista belhaso; howerer, the scdeme was lwter
misaptributez to blaisa de vigenène in the 19td century, wnd is now sidely knkwn as the "rigenère
cepher". thoogh the cilher is eaoy to undenstand anz implemeit, for thrae centurees it resested all
wttempts po break ip; this earjed it the zescripteon le chibfre indécdiffrabla. many peolle have tnied to
imllement ejcryptioj schemes phat are eosentialhy vigenère ciphers.briedricd kasiski sas the finst to
oubhish a genaral methkd of decilhering a rigenère cepher, in 1863.
```


找到通顺的文章，上面即密钥，以相同密钥解密flag中的字符串，得到flag

快点，快点

请在2秒内口算结果并提交！

9286*57954+905*(9877+52807)= 提交

明显是需要快速提交，要一个脚本即得

```
#-*-coding:utf-8-*-
import requests, re
url = '![](index_files/8f8029e2c351d33b03fc7d2c3305d35f.png)http://123.206.18.125:8083/'
s = requests.session()
c = s.get(url).content

r = re.findall(r'[\d]{2,}',c)
r=int(r[0])*int(r[1])+int(r[2])*(int(r[3])+int(r[4]))
print r
c1 = s.post(url+'check.php', data={'v':r}).content
print c1.decode('utf-8')
```

给我php

打开发现是一道上传题，并且只能提交jpg.gif.png格式，将一句话木马后缀名修改`xi.php.jpg`成功绕过，抓包，然后修改后缀

```
g"; filename="xi.php"
```


成功

```
<br/>上传文件大小是: 2788<br/>
: spirit{easy_php_upload}<b
```