2015广州强网杯-Crypto-小心猪圈

转载

weixin_30651273 于 2018-10-17 19:27:00 发布 206 收藏
原文链接：http://www.cnblogs.com/nldyy/p/9806474.html

注：本人纯小白，此题是看了很多writeup才明白并且复现的，只是为了巩固知识。

题目内容：

R29kIGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0I

分析：

一看就很迷，题说小心猪圈，首先想到猪圈密码。但这还有数字，所以貌似不能用。于是想到base64解码。

```
import base64
test="R29kIGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0NEY1MjUzNTg0MTQ5NDQ0MjRGMzU1MTU4NTM0RjUzNTI0NzQ5MzQ1ODRCNTc1MjU0NEE0QTU1NDc0OTUzNDM1NzRGNEU0RDU2NTE1NTU0NTE0RDQ5NUE0NDRCMzY1MzUwNEU1NTM0NTc1NTU5NEM0RjQ5NDkzMzU3NEIzMzRDNTU0RjQyNTI1NzMyMzQ0MjU0NEQ0QTRDNTQ1MTM1NDQ0MzQ3NEEzNDQ4NDc1OTRDNEE0NzQ2MzI1NzQ1NTYzMzU5NDc0RTQ3NDY0RjM0NDQ1NzRENTY0NDU3NTczNTQ0NDU0OTM0NTk1ODRENTk1MzQ4NDc1NjM0NTc0NTMzNEE1QTQ3NDI1MzQ3MzI0RDRDMzI0RDVBNDk1NDMyNTA0OTNE"
test=base64.b64decode(test)
print test
```

得到结果：

God
job:57656C6C20646F6E653A4A35584759364A414E3558474B4944544F525358414944424F355158534F535

发现的到一个比较靠谱的16进制数，于是转换成文本，用HxD，将16进制数保存到一个txt中，用HxD打开

得到如下结果：

Well
done:J5XGY6JAN5XGKIDTORSXAIDBO5QXSOSRGI4XKWRTJJUGISCWONMVQUTQMIZDK6SPNU4WUYL

一看还是和base有关呀。于是在上一个脚本里再base

```
import base64
test="R29kIGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0NEY1MjUzNTg0MTQ5NDQ0MjRGMzU1MTU4NTM0RjUzNTI0NzQ5MzQ1ODRCNTc1MjU0NEE0QTU1NDc0OTUzNDM1NzRGNEU0RDU2NTE1NTU0NTE0RDQ5NUE0NDRCMzY1MzUwNEU1NTM0NTc1NTU5NEM0RjQ5NDkzMzU3NEIzMzRDNTU0RjQyNTI1NzMyMzQ0MjU0NEQ0QTRDNTQ1MTM1NDQ0MzQ3NEEzNDQ4NDc1OTRDNEE0NzQ2MzI1NzQ1NTYzMzU5NDc0RTQ3NDY0RjM0NDQ1NzRENTY0NDU3NTczNTQ0NDU0OTM0NTk1ODRENTk1MzQ4NDc1NjM0NTc0NTMzNEE1QTQ3NDI1MzQ3MzI0RDRDMzI0RDVBNDk1NDMyNTA0OTNE"
test=base64.b64decode(test)
test2="J5XGY6JAN5XGKIDTORSXAIDBO5QXSOSRGI4XKWRTJJUGISCWONMVQUTQMIZDK6SPNU4WUYLOII3WK3LUOBRW24BTMJLTQ5DCGJ4HGYLJGF2WEV3YGNGFO4DWMVDWW5DEI4YXMYSHGV4WE3JZGBSG2ML2MZIT2PI="
test264=base64.b64decode(test2)
test232=base64.b32decode(test2)
print test264
print test232
```

结果是：

'ɹÆcᵀᵀ@7ɹÆ(ㄆÓ9ㄱ
Only one step
away:Q29uZ3JhdHVsYXRpb25zOm9janB7emtpcmp3bW8tb2xsai1ubWx3LWpveGktdG1vbG5ybm90dm1zfQ==

显然base32是可以的，但base64得不到正确结果。

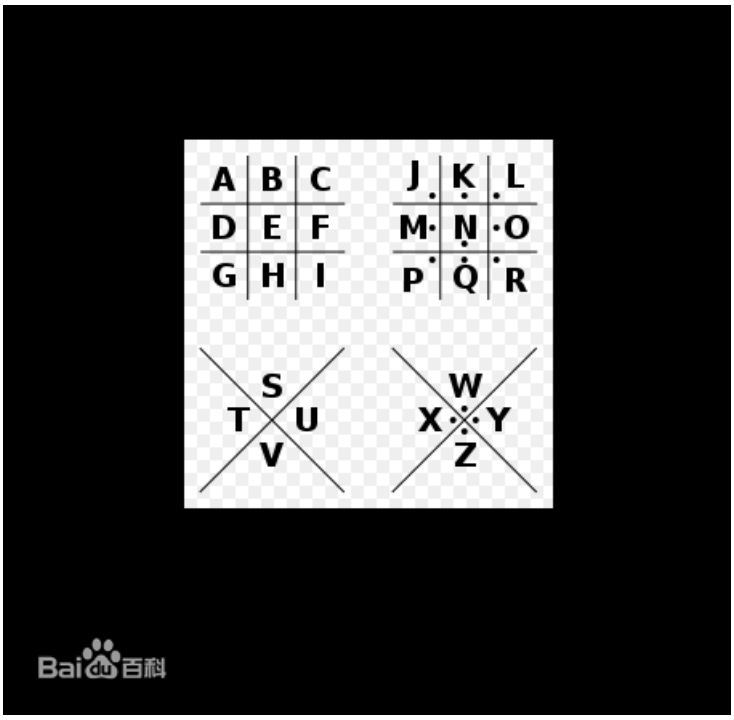
看结果，果断继续。

```
import base64
test="R29kIGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0NEY1MjUzNTg0MTQ5NDQ0MjRGMzU1MTU4NTM0RjUzNTI0NzQ5MzQ1ODRCNTc1MjU0NEE0QTU1NDc0OTUzNDM1NzRGNEU0RDU2NTE1NTU0NTE0RDQ5NUE0NDRCMzY1MzUwNEU1NTM0NTc1NTU5NEM0RjQ5NDkzMzU3NEIzMzRDNTU0RjQyNTI1NzMyMzQ0MjU0NEQ0QTRDNTQ1MTM1NDQ0MzQ3NEEzNDQ4NDc1OTRDNEE0NzQ2MzI1NzQ1NTYzMzU5NDc0RTQ3NDY0RjM0NDQ1NzRENTY0NDU3NTczNTQ0NDU0OTM0NTk1ODRENTk1MzQ4NDc1NjM0NTc0NTMzNEE1QTQ3NDI1MzQ3MzI0RDRDMzI0RDVBNDk1NDMyNTA0OTNE"
test=base64.b64decode(test)
test2="J5XGY6JAN5XGKIDTORSXAIDBO5QXSOSRGI4XKWRTJJUGISCWONMVQUTQMIZDK6SPNU4WUYLOII3WK3LUOBRW24BTMJLTQ5DCGJ4HGYLJGF2WEV3YGNGFO4DWMVDWW5DEI4YXMYSHGV4WE3JZGBSG2ML2MZIT2PI="
#test264=base64.b64decode(test2)
test232=base64.b32decode(test2)
test3="Q29uZ3JhdHVsYXRpb25zOm9janB7emtpcmp3bW8tb2xsai1ubWx3LWpveGktdG1vbG5ybm90dm1zfQ=="
test364=base64.b64decode(test3)
print test364
```

得到结果：Congratulations:ocjp{zkirjwmo-ollj-nmlw-joxi-tmolnrnotvms}

ocjp{zkirjwmo-ollj-nmlw-joxi-tmolnrnotvms}和明显的flag{}格式，于是想到题目的猪圈密码。

百度一波有一个图



应用上图，左右两两相对，ocjp正好可以对应flag。

最后

```
import base64
test="R29kIGpvYjo1NzY1NkM2QzIwNjQ2RjZFNjUzQTRBMzU1ODQ3NTkzNjRBNDE0RTM1NTg0NzRCNDk0NDU0NEY1MjUzNTg0MTQ5NDQ0MjRGMzU1MTU4NTM0RjUzNTI0NzQ5MzQ1ODRCNTc1MjU0NEE0QTU1NDc0OTUzNDM1NzRGNEU0RDU2NTE1NTU0NTE0RDQ5NUE0NDRCMzY1MzUwNEU1NTM0NTc1NTU5NEM0RjQ5NDkzMzU3NEIzMzRDNTU0RjQyNTI1NzMyMzQ0MjU0NEQ0QTRDNTQ1MTM1NDQ0MzQ3NEEzNDQ4NDc1OTRDNEE0NzQ2MzI1NzQ1NTYzMzU5NDc0RTQ3NDY0RjM0NDQ1NzRENTY0NDU3NTczNTQ0NDU0OTM0NTk1ODRENTk1MzQ4NDc1NjM0NTc0NTMzNEE1QTQ3NDI1MzQ3MzI0RDRDMzI0RDVBNDk1NDMyNTA0OTNE"
test=base64.b64decode(test)
test2="J5XGY6JAN5XGKIDTORSXAIDBO5QXSOSRGI4XKWRTJJUGISCWONMVQUTQMIZDK6SPNU4WUYLOII3WK3LUOBRW24BTMJLTQ5DCGJ4HGYLJGF2WEV3YGNGFO4DWMVDWW5DEI4YXMYSHGV4WE3JZGBSG2ML2MZIT2PI="
#test264=base64.b64decode(test2)
test232=base64.b32decode(test2)
test3="Q29uZ3JhdHVsYXRpb25zOm9janB7emtpcmp3bW8tb2xsai1ubWx3LWpveGktdG1vbG5ybm90dm1zfQ=="
test364=base64.b64decode(test3)
test4=test364[16:]
dic = {'a': 'j', 'b': 'k', 'c': 'l', 'd': 'm', 'e': 'n', 'f': 'o', 'g': 'p', 'h': 'q', 'i': 'r', 's': 'w', 'v': 'z',
          't': 'x', 'u': 'y', 'j': 'a', 'k': 'b', 'l': 'c', 'm': 'd', 'n': 'e', 'o': 'f', 'p': 'g', 'q': 'h', 'r': 'i',
          'w': 's', 'z': 'v', 'x': 't', 'y': 'u'}
flag=''
for i in test4:
    if i in dic:
        flag+=dic[i]
    else:
        flag+=i
print flag
```

运行得到结果。

转载于:https://www.cnblogs.com/nldyy/p/9806474.html