

# Hackme-Crypto-wp

原创

[iReverse](#) 于 2019-09-13 18:36:12 发布 356 收藏

分类专栏: [Hackme-Misc-wp](#) 文章标签: [Hackme-Misc-wp](#)

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\\_41509200/article/details/100808093](https://blog.csdn.net/qq_41509200/article/details/100808093)

版权



[Hackme-Misc-wp](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

## Hackme-Crypto-wp

背景:

这几天老师要求我们把hackme的题目做出来, 于是便开始了新的征程, 一定把全部flag找出来, fighting...

### 题目及解题思路

#### 1、easy

```
526b78425233745561476c7a49476c7a4947566863336b7349484a705a3268305033303d
```

利用经验觉得像16进制转字符串，于是找个在线网站试试



还真有点线索，发现有点像base64的加密格式，然后再找个在线转换网站，解密后得到了flag



## 2、r u kidding

EKZF{Hs'r snnn dzrx, itrs bzdrzq bhogdq}

题目描述为EKZF{Hs'r snnn dzrx, itrs bzdrzq bhogdq}, 与FLAG{}的格式非常接近, 于是便想到是凯撒加密, 找个凯撒加解密的在线网站, 当位移是25时出现了flag

qqxiuzi.cn/bianma/kaisamima.php

题目练习平台 CTF在线工具 Chrome+ 墙外媒体 视听资料 视频站

学生优惠套餐 云数据库 /元/月

立即抢购

促销

云服务  
元/3月  
培养,助

百度智能云

EKZF{Hs'r snnn dzrx, itrs bzdrzq bhogdq}

位移 25 加密 解密

FLAG{It's tooo easy, just caesar cipher}

[https://blog.csdn.net/qq\\_41509200](https://blog.csdn.net/qq_41509200)

本文在参考下面各位大佬的博客的得到的部分wp, 谢谢各位朋友

[https://www.aloxaf.com/2018/07/hackme\\_inndy/](https://www.aloxaf.com/2018/07/hackme_inndy/)

<https://sp4rta.github.io/2018/12/01/inndy-writeup/>

<https://sp4rta.github.io/2018/12/01/inndy-writeup/>

### 3、not hard

Nm@rmLsBy{Nm5u-K{iZKPgPMzS2IIPc%\_SMOjQ#O;uV{MM?PPFhk|Hd;hVPFhq{HaAH<

Tips: pydoc3 base64

题目提示我们在python3的手册中查找base64的用法, 上面的字符串先base85解密, 再base32解密即得flag

下面是用python3实现得到flag的代码

```
import base64
base85_str = b'Nm@rmlsBy{Nm5u-K{iZKPgPMzS2I*1Pc%_SMOjQ#0;uV{MM*?PPFhk|Hd;hVPFhq{HaAH<'
print(base85_str)
base32_str = base64.b85decode(base85_str)
print(base32_str)
flag = base64.b32decode(base32_str)
print(flag)
```



The screenshot shows a Python IDE with a file named 'flag.py' containing the following code:

```
1 import base64
2 base85_str = b'Nm@rmlsBy{Nm5u-K{iZKPgPMzS2I*1Pc%_SMOjQ#0;uV{MM*?PPFhk|Hd;hVPFhq{HaAH<'
3 print(base85_str)
4 base32_str = base64.b85decode(base85_str)
5 print(base32_str)
6 flag = base64.b32decode(base32_str)
7 print(flag)
```

The Run console shows the following output:

```
Run: flag x
b'IZGECR33IRXSA6LPOUQGW3TP04QGEYLTMUZTEIDFNZRW6ZDJNZTT67I='
b'FLAG{Do you know base32 encoding?}'
Process finished with exit code 0
```

[https://blog.csdn.net/qq\\_41509200](https://blog.csdn.net/qq_41509200)

## 知识扩展

- python3中base64模块的使用  
<https://docs.python.org/zh-cn/3/library/base64.html?highlight=base64>

## 4、 classic cipher 1

MTHJ{CWTNXRJCUBCGXGUGXWREXIPOYAOEYFIGXWRXCHTKHFCOHCDFDUCGTZXOHIXOEOWMEHZO}  
Solve this substitution cipher

提示说要用替换加密，于是找到了一个在线网站解密即得flag

quipquip is a fast and automated cryptogram solver by [Edwin Olson](#). It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor aboun darie saren t).

**Puzzle:**  
MTHJ {CWTNXRJCUBCGXGUGXWREXIPOTAOEYFYGXWRXCHTKHFCOHCDFDUGGTXZOHIXOEBOWMEHZO}

**Clues:** For example G=R QVW=THE  
MTHJ=FLAG

auto

Solve

0	-1.700	FLAG { SOLVING SUBSTITUTION CIPHER DECRYPTION IS ALWAYS EASY JUST LIKE A PIECE OF CAKE}
1	-1.826	FLAG { SOLDING SUBSTITUTION CIPHER ME CRYPTION IS ALWAYS EASY JUST LIKE A PIECE OF CAKE}
2	-2.244	FLAG { SOLDING SUBSTITUTION RICHEMPER MYCTION IS ALWAYS EASY JUST LIKE A CIERE OF RAKE}
3	-2.357	FLAG { SOLDING SUBSTITUTION RIC JEPHER PYCTION IS ALWAYS EASY MUST LIKE A CIERE OF RAKE}
4	-2.575	FLAG { SOLVING SUBSTITUTION KIRD CHECK HYRTION IS ALWAYS CASY JUST LIMCA RICK C OF KAMC}
5	-2.693	FLAG { SOLVING SUBSTITUTION HIP WE D MEHD OPTION IS ALZAC SEAS CRUST LIKE A PIE HE OF HAKE}
6	-2.887	FLAG { SULZING SONS DID ODIUM CIPRE THE C TYPDUM IS ALWAYS EASY VO S D LIKE A PIECE UFC AKE}
7	-2.898	FLAG { TOLVING TRUTH I H R H ION CIP WEB DE CBS PHI ON ITALY AS TEATS M RTH LIKE A PIECE OF CAKE}

[https://blog.ssdn.net/pw\\_41509200](https://blog.ssdn.net/pw_41509200)

真正的flag其实是单词之间是没有空格的

## 5、 classic cipher 2

Solve this vigenere cipher

题目是一堆大写英文字母，提示说用维吉尼亚解密来做，于是找个在线网站来解密，得到红框中的内容

input

Cipher Text:

```
V KGIFEI WCTPK MJ C SNMEF FF TYQDJLJ CIJNYPG YNQ CCMMBGNL
WRGCNMJ AVXY TCZBLWRP CUFIUV LGWSQ KSNTI EFMIG MIY ERE
OWJXCXLGTGBNPOVR WRYEM VHVCKC NOH DCAEU THQNJ I MJ CW
GTYDVTTFIDLR IRGZVZKH GESPGAXKI YKSGPVA KHG CEOB BX
TVUUXVQL IF GPLWZSLER AVDMQHYGIU XQ ZTZXRWRNUIWI CCOWDS
AFIHYHM NP GTNLTYF QEMBZRCXO ENS BTVVCBTK VVUTNVV CETU SR
PFVNTS QHH GJC UAIECV ALAMXS EKMLORV ARW NQKPRX KN FBR
FZEIY FXU FJ NEI UPFQ UOEKTL Y QF TBCUCXV ENIEI YI CDDPHVF
TUF VGJTTS GWJMSJ SV JVB JGBVTTMF PAS WTUIROMX VBWR
VCKDRKCD GIEV YET DEWICW ZPL YRGR THE OCKR OHY G A HYRZZI
```

Cipher Variant: Classical Vigenere ▾

Language: English ▾

Key Length: 3-100 (e.g. 8 or a range e.g. 6-10)

Break Cipher Clear Cipher Text

Result

Clear text [\[hide\]](#)

Clear text using key "vigenereciphercanbecrackedbyfrequencyanalysisattack":

clear text using key - vigenere cipher can be cracked by frequency analysis attack .

A CAESAR SALAD IS A SALAD OF ROMAINE LETTUCE AND CROUTONS DRESSED WITH PARMESAN CHEESE LEMON JUICE OLIVE OIL EGG WORCESTERSHIRE SAUCE GARLIC AND BLACK PEPPER IT IS TRADITIONALLY PREPARED TABLESIDE HISTORY THE SALADS CREATION IS GENERALLY ATTRIBUTED TO RESTAURATEUR CAESAR CARDINI AN ITALIAN IMMIGRANT WHO OPERATED RESTAURANTS IN MEXICO AND THE UNITED STATES CARDINI WAS LIVING IN SAN DIEGO BUT HE WAS ALSO WORKING IN TIJUANA WHERE HE AVOIDED THE RESTRICTIONS OF PROHIBITION HIS DAUGHTER ROSA RECOUNTED THAT HER FATHER INVENTED THE DISH WHEN A FOURTH OF JULY RUSH DEPLETED THE KITCHENS SUPPLIES CARDINI MADE DO WITH WHAT HE HAD ADDING THE

[https://blog.csdn.net/qq\\_41509200](https://blog.csdn.net/qq_41509200)

在wps中寻找FLAG字符，结果发现FLAG

SEARCHING RESTAURANT WHEN SHE WAS VISITED BY THE CUBAN REVOLUTIONARY COLONEL DONALD KILGALLEN WROTE OF A CAESAR CONTAINING ANCHOVIES DIFFERING FROM CARDINIS VERSION THE FLAG HAS NINE WORDS AND YOU NEED TO ADD CURLY BRACES TO FLAG AND FLAG HAS SPACES AND ALL IN UPPERCASE THE BIG FOOD RAGE IN HOLLYWOOD THE CAESAR SALAD WILL BE INTRODUCED TO NEW YORKERS BY GILMORES STEAK HOUSE ITS AN INTRICATE CONCOCTION THAT TAKES AGES TO PREPARE AND CONTAINS ZOWIE LOTS OF GARLIC RAW OR SLIGHTLY CODDLED EGGS CROUTONS ROMAINE ANCHOVIES PARMEASAN SIC CHEESE OLIVE OIL VINEGAR AND PLENTY OF BLACK PEPPER RECIPE EDIT THE FLAG IS VIGENERE CIPHER CAN BE CRACKED BY FREQUENCY ANALYSIS ATTACK ACCORDING TO ROSA CARDINI THE ORIGINAL CAESAR SALAD UNLIKE HIS BROTHER ALEXS AVIATORS SALAD DID NOT CONTAIN PIECES OF ANCHOVY THE SLIGHT ANCHOVY FLAVOR COMES FROM THE WORCESTERSHIRE SAUCE CARDINI WAS OBLIGED TO

[https://blog.csdn.net/qq\\_41509200](https://blog.csdn.net/qq_41509200)

FLAG{VIGENERE CIPHER CAN BE CRACKED BY FREQUENCY ANALYSIS ATTACK}