# ISCC 2018线上赛 writeup

转载

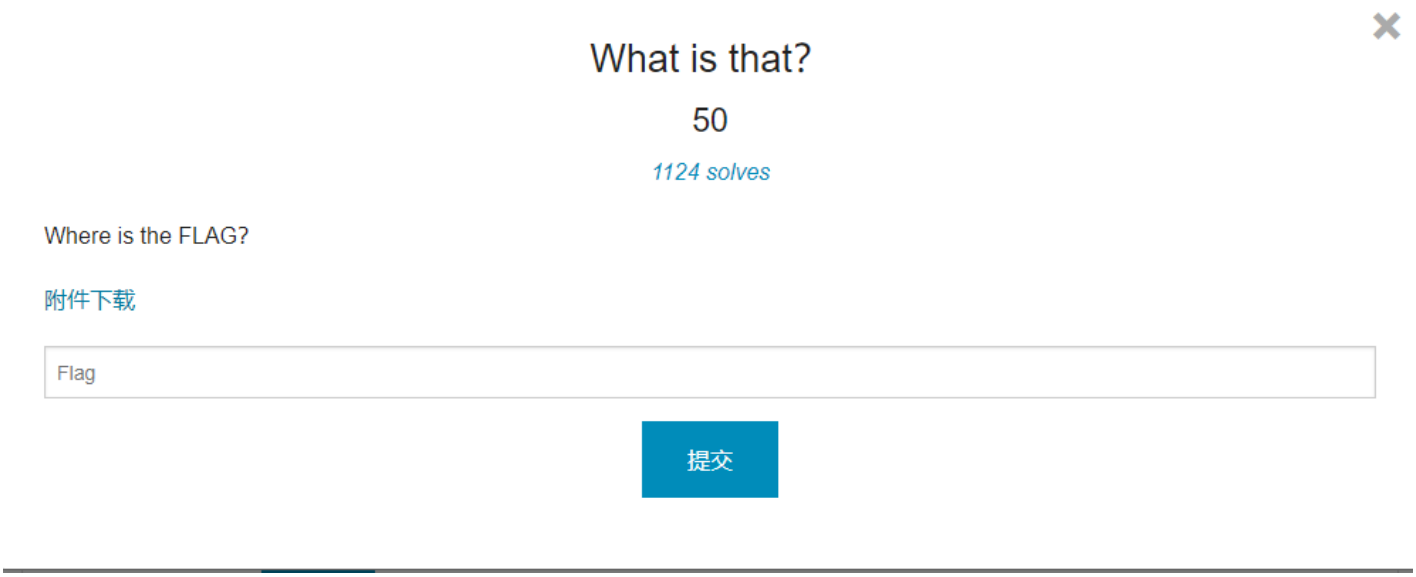
weixin_34417635 于 2018-06-06 11:21:00 发布 134 收藏
文章标签： php
原文链接：http://www.cnblogs.com/semishigure/p/9013131.html


今天有机会去ISCC2018参加了比赛，个人的感受是比赛题目整体难度不高，就是脑洞特别大，flag形式不明确，拿到flag后也要猜测flag格式，贼坑

废话不多说，以下是本人的解题思路

## MISC

### 0x01 What is that?




下载附件得到图片

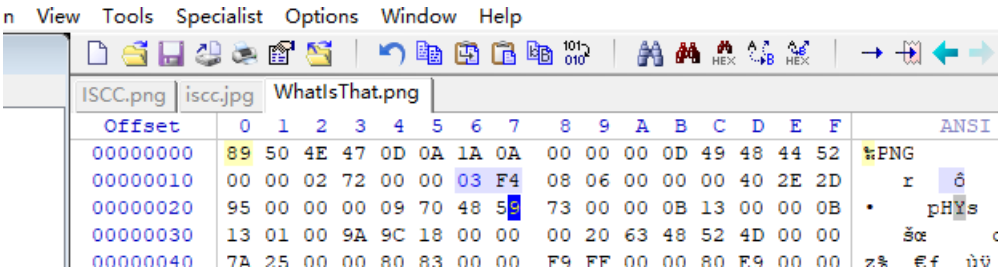

看图应该可以猜到flag在下面被截取了，所以我们去修改图片的高度

用十六进制打开图片

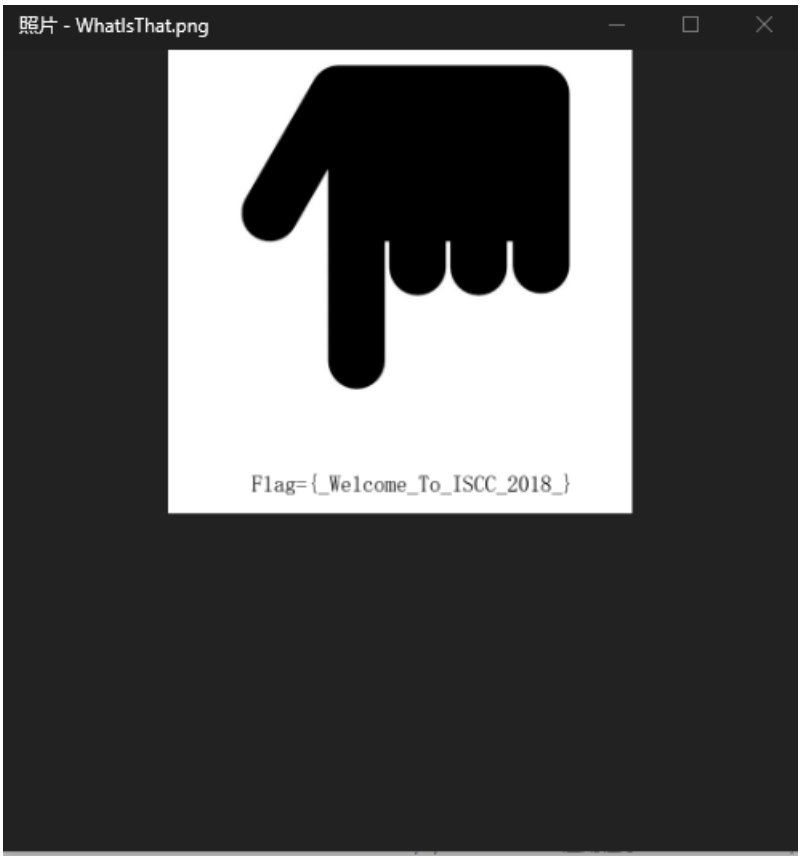
ISCC.png | iscc.jpg | WhatIsThat.png

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | ANSI ASCII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00000000 | 89 | 50 | 4E | 47 | 0D | 0A | 1A | 0A | 00 | 00 | 00 | 0D | 49 | 48 | 44 | 52 | ‰PNG IHDR |
| 00000010 | 00 | 00 | 02 | 72 | 00 | 00 | 01 | F4 | 08 | 06 | 00 | 00 | 00 | 40 | 2E | 2D | r ô @.- |
| 00000020 | 95 | 00 | 00 | 00 | 09 | 70 | 48 | 59 | 73 | 00 | 00 | 0B | 13 | 00 | 00 | 0B | • pHYs |
| 00000030 | 13 | 01 | 00 | 9A | 9C | 18 | 00 | 00 | 00 | 20 | 63 | 48 | 52 | 4D | 00 | 00 | šœ cHRM |
| 00000040 | 7A | 25 | 00 | 00 | 80 | 83 | 00 | 00 | F9 | FF | 00 | 00 | 80 | E9 | 00 | 00 | z% €ƒ ùÿ €é |
| 00000050 | 75 | 30 | 00 | 00 | EA | 60 | 00 | 00 | 3A | 98 | 00 | 00 | 17 | 6F | 92 | 5F | u0 ê` :˜ o'_ |
| 00000060 | C5 | 46 | 00 | 00 | 62 | EA | 49 | 44 | 41 | 54 | 78 | DA | EC | DD | 79 | 7C | ÅF bêIDATxÚìÝy\| |
| 00000070 | 55 | F5 | 9D | FF | F1 | F7 | 39 | F7 | DC | 9B | 84 | 24 | 9A | 9B | B0 | 89 | Uõ ÿñ÷9÷Ü›„$š›°‰ |
| 00000080 | 82 | 18 | 14 | 11 | 37 | 34 | 71 | 29 | 3A | 2E | 18 | D1 | BA | D7 | 0A | 3A | , 74q):. Ñº× : |
| 00000090 | 2E | ED | 00 | 12 | DA | CE | D4 | 3E | FA | 7B | 68 | 61 | 1E | 4E | FB | FB | .í ÚÎÔ>ú{ha NûûÍo¦ ˜Ú€?-mÁ j-M¬ |
| 000000A0 | CD | 6F | A6 | 1D | 98 | DA | A9 | 3F | AD | 6D | C1 | 15 | 6A | AD | 4D | AC | |
| 000000B0 | B5 | BB | 16 | DA | AA | 5D | D5 | 44 | 2B | 1D | EB | D0 | 16 | 68 | B5 | 56 | µ» Ú ª]ÕD+ ëÐ hµV |
| 000000C0 | 14 | 49 | 44 | 20 | 24 | F7 | 9E | E5 | F7 | 07 | 7E | BF | 9E | 7B | 93 | 40 | ID $÷žå÷ ~¿ž{"@ |
| 000000D0 | F6 | DC | 24 | AF | E7 | E3 | 91 | 07 | 64 | BF | F9 | DE | 73 | CF | 79 | 9F | öÜ$¯çã' d¿ùÞsÏyŸ |
| 000000E0 | EF | F2 | F9 | 3A | 51 | 14 | 45 | 02 | 00 | 00 | C0 | 88 | E3 | D2 | 04 | 00 | ïòù:Q E À^ãÒ |
| 000000F0 | 00 | 00 | 04 | 39 | 00 | 00 | 00 | 10 | E4 | 00 | 00 | 00 | 40 | 90 | 03 | 00 | 9 ä @ |
| 00000100 | 00 | 20 | C8 | 01 | 00 | 00 | 80 | 20 | 07 | 00 | 00 | 00 | 82 | 1C | 00 | 00 | È € , |
| 00000110 | 00 | 41 | 0E | 00 | 00 | 00 | 04 | 39 | 00 | 00 | 00 | 10 | E4 | 00 | 00 | 00 | A 9 ä |
| 00000120 | 40 | 90 | 03 | 00 | 00 | 20 | C8 | 01 | 00 | 00 | 80 | 20 | 07 | 00 | 00 | 00 | @ È € |
| 00000130 | 82 | 1C | 00 | 00 | 00 | 41 | 0E | 00 | 00 | 00 | 04 | 39 | 00 | 00 | 00 | 10 | , A 9 |
| 00000140 | E4 | 00 | 00 | 00 | 90 | CB | A3 | 09 | 80 | 81 | 11 | 45 | 91 | C2 | 30 | 94 | ä Ë£ € E'Â0" |
| 00000150 | 24 | 25 | 12 | 09 | 49 | 52 | 18 | 86 | 8A | A2 | 48 | 89 | 44 | 42 | 51 | 14 | $% IR †Š¢H‰DBQ |
| 00000160 | D9 | B7 | EE | BE | A6 | AB | 9F | 09 | 00 | 3D | E1 | 38 | 8E | C2 | 30 | B4 | Ù·î¾¦«Ÿ =á8ŽÂ0´ |
| 00000170 | E7 | 21 | 73 | 0E | 71 | 1C | 47 | 89 | 44 | C2 | 7E | DC | 75 | DD | 9C | 73 | ç!s q G‰DÂ~ÜuÝœs |
| 00000180 | 91 | EB | BA | F6 | 6B | E3 | 9F | 73 | 1C | 27 | E7 | E3 | 28 | D0 | E7 | 3D | 'ëºökãŸs 'çã(Ðç= |
| 00000190 | E2 | 4A | 01 | 0C | B8 | F8 | C9 | D4 | 9C | 44 | 4D | D0 | 73 | 1C | C7 | BE | âJ ¸øÉÔœDMÐs Ç¾ |
| 000001A0 | 01 | C0 | 60 | 0A | 82 | A0 | 53 | A8 | 33 | FF | BA | AE | 6B | CF | 49 | 41 | À` , S¨3ÿº®kÏIA |
| 000001B0 | 10 | C8 | F3 | 3C | 7B | CE | 8A | 9F | CB | BA | BB | D1 | 04 | 41 | 0E | 18 | È ó<{ÎŠŸË°»Ñ A |
| 000001C0 | 55 | 7C | DF | 57 | 18 | 86 | 4A | A5 | 52 | 39 | 77 | BB | 61 | 18 | 2A | 91 | U\|ßW †J¥R9w»a *' |

在图片的高度那里修改一下数值，我是把01 F4 改成 03 F4 ，高度该多少随意，能看到flag即可



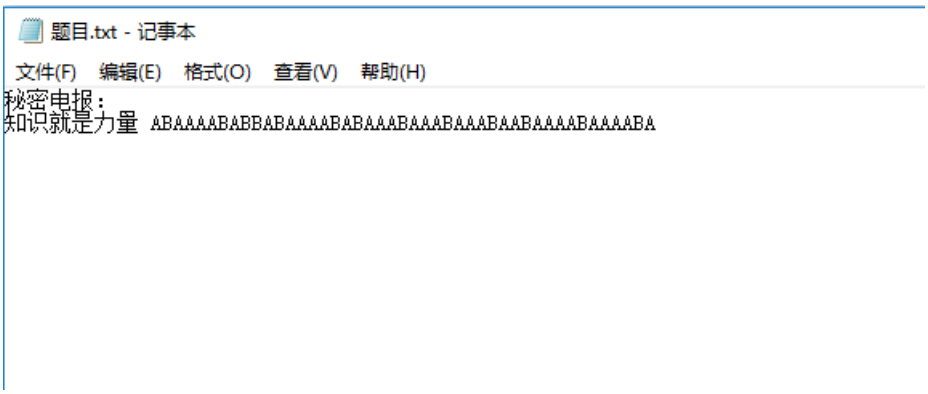

再打开图片，出现flag




然后格式贼坑，根据多种尝试，最后确认要去掉flag=和{}提交即可！

## 0x02 秘密电报


下载附件打开




非常明显是培根密码，解密得到

ilikeiscc和ILIKEISCC，输入即可

### 0x03 重重谍影

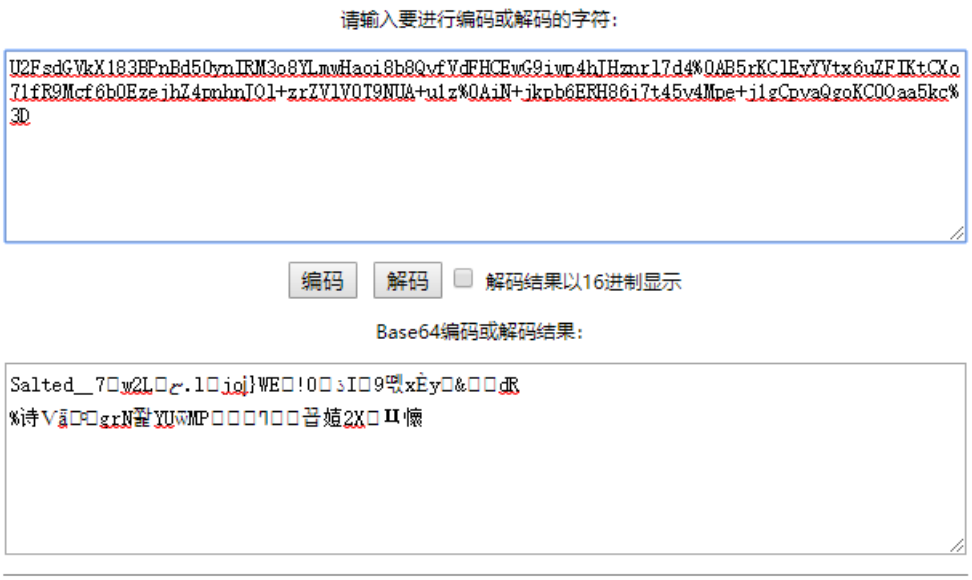

进入网页看到


```
VmOwd2QyVkZOVWRXVOdoVlYwZG9WVll3WkRSV2JGbDNXa1JTVjAxWGVGWlZNakExYjBaS2RHVklj
R2hYWVd0d2RsUnRlR3RqYkdSMFVteFdUbFp0ZHpCV2EyTXhVekZSZUZkc1ZsZGhlbXhoVm01dlIy
RlVjTldjRVZTY1VacVZtdHdlbGRyVlRWVk1ERldZMFZ3VjJKR2NIWlpWRXBIVWpGT1dXSkhhRlJT
VlhCWFZtMDFkMUl3TlhOVmJGcFlZbGhIV1ZWcVFU
RlRWbEY0VjIxR2FGWnNjSGxaYWs1clZqSkdjbUo2UWxwV1JWcDZWbXBHVDJNeGNFaGpSazVZVWxW
dlVWVnRNVEJXTVUxNFdrVmtWbUpHV2xSWlZFNVRWVVpzYzFadVpGUmlSbHBaVkZaU1ExWlhSalpT
YTJSWFlsaENVRll3V21Gak1XUnpZVWRHVTFK
V2NGRldha0poV1ZkU1YxWnVTbEJXYldoVVZGUktiMDB4V250OYVJFSm9UVlpXT1ZaSE5WOVdiVXB5
WTBaYVdtRXhjRE5aTW5oVFZqRmFkRkpzWkU1V2JGa3dWbXhrTUdFeVJraFRiRnBYWVd4dldGWnFU
bE5YUmxsNVRVWmFiRkpOVW5wWlZWcFhZVlpL
ZFZGdWJGZG1XRUpJV1ZSS1QxWXhTblZWYlhoVFlYcFdWVmRYZUZOamF6RkhWMjVTYWxkWVVrOVZiVEUwVjBaYVNFNVZFVmRXY1ZKS1ZWZDRkMWRzV2taWGEzaFhUVlp3V0ZwR1pPOVRSVFZZWlVkc1UyRXpRbHBXYWtvd1lURkplRmR1U2s1V1ZscHdW
VzB4VTFac1duUk5WazVPVFZkU1dGZHJWbXRoYXpGeVRsVndWbFl6YUZoV2FrWmhZekpPUjJKR1pGTmxhMVYzVjJOU1IyRXhUa2RWYmtwb1VtdEtXRmxzWkc5a2JHUllaRVpYTlJKV1ducFhhMXB2Vkd4T1NHRklRbFZXTTJoTVZqQmFZVk5GT1ZaalJs
cFRZbFpLU0ZaSGVGWmxSbHBYVjJOYWQxWldTbFpaYTFwWldWndWMXBHWkZSU2EzQXdXVEJWTVZZeVNuSlRWRUpYWWtad2NsUnJXbHBsUmxweVdrWm9hVkpzY0ZsWFYzUnJWVEZaZUZkdVVtcGxhMHB5VkZaYVMxZEdXbk5oUnpsWVVteHNNMWkyVWkk
W1ZscFhWbGhvVjFaRldtaFdha3BQVWkaU2MxcEhhRTVpUlc4eVZtdGFWMkV4VVhoYVJXUlVZa2Q0Y1ZWdGRIZGpSbHB4VkcwNVZsWnRVbGhXVjNSclYyeGFjMk5GYUZkaVIyaHlWbTB4UzFaV1duSlBWbkJwVW14d2IxZHNWbUZoTWs1elZtNUtWVOpH
V2s5V2JHaERVMVphY1ZKdE9XcE5WbkJaVld4b2IxWXlSbk5UYldoV1lURmFhRlJVUmlGamJIQkhWR3hTVjJFelFqVldSM2hoWVRGU2RGTnJXbXBTVjFKWVZGWmFTMUpHYkhGU2JrNVlVbXR3ZVZkcldtdGhWa2w1WVVjNVYxWkZTbWhhUkVaaFZqRldj
MWRzWkZoUO1taFFWalphWVdReFNuTldXR3hyVWpOU2IxVnRkSGRXYkZwMFpVaE9XbFpyY0ZsV1YzQlBWbTFXY2xkdGFGWmlXRTEOVm0xNGExWkdXbGxqUms1U1ZURldObFZyVGxabGJFcENTbFJPU1VwVVRrVSUzRA==
```


先进行base64得到


```
Vm0wd2VFNUdWWGhVV0doVVYwZDRWbFl3WkRSV01XeFZVMjA1V0ZKdGVlcFpWVnBQVjBkS1lxTnNhRmR
```


看不出来什么，看题目，层层迷雾，那就base64到底好了，最后在Salted__前打住




Salted__了解一下，这个是通过openssl加密如果不带base64就会出现Salted字段打头。再看base64的前几个字段U2Fsd确定是AES加密无误

这里有点坑，弄了很久才发现原base64密文中有url编码，所以先url解码得到

U2FsdGVkX183BPnBd50ynIRM3o8YLmwHaoi8b8QvfVdFHCEwG9iwp4hJHznrl7d4
B5rKClEyYVtx6uZFIKtCXo71fR9Mcf6b0EzejhZ4pnhnJOl+zrZVlV0T9NUA+u1z
iN+jkpb6ERH86j7t45v4Mpe+j1gCpvaQgoKC0Oaa5kc=

然后AES解密得到

答案就是后面这句但已加密
缽娑遠吶者若奢顛悉吶集梵提梵蒙夢怯倒耶哆般究有栗

佛系加密。。。。把乱码拿去百度，可以收到与佛论禅，解密得flag

**0x04 有趣的ISCC**


下载图片，打开是ISCC的icon，用binwalk看一下有没有隐写，没啥东西，进行十六进制分析，在最后看到一串unicode编码

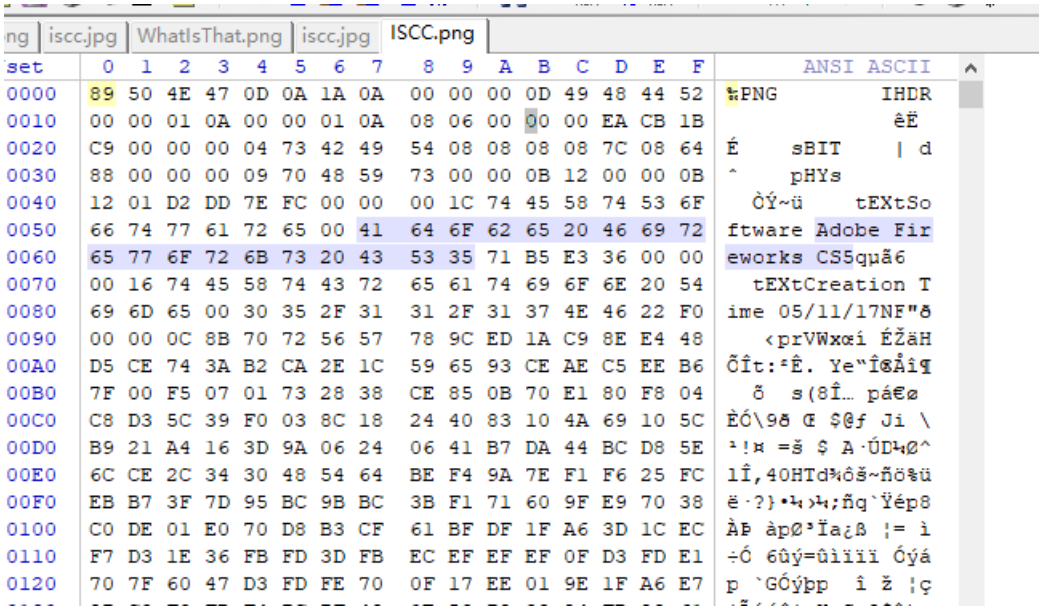
ISCC.png | iscc.jpg | WhatIsThat.png | iscc.jpg

| Offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F | ANSI ASCII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 00011D90 | 3F | B2 | 56 | 4E | 00 | 00 | 00 | 0F | 74 | 45 | 58 | 74 | 54 | 68 | 75 | 6D | ?²VN tEXtThum |
| 00011DA0 | 62 | 3A | 3A | 53 | 69 | 7A | 65 | 00 | 30 | 42 | 42 | 94 | A2 | 3E | EC | 00 | b::Size 0BB"¢>ì |
| 00011DB0 | 00 | 00 | 12 | 74 | 45 | 58 | 74 | 54 | 68 | 75 | 6D | 62 | 3A | 3A | 55 | 52 | tEXtThumb::UR |
| 00011DC0 | 49 | 00 | 66 | 69 | 6C | 65 | 3A | 2F | 2F | C1 | 77 | 8B | CF | 00 | 00 | 00 | I file://Áw‹Ï |
| 00011DD0 | 00 | 49 | 45 | 4E | 44 | AE | 42 | 60 | 82 | 26 | 00 | 23 | 00 | 39 | 00 | 32 | IEND®B`‚&#92 |
| 00011DE0 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 31 | 00 | 31 | 00 | 37 | 00 | 3B | 00 | 26 | ;&#117 |
| 00011DF0 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | #48;&#48 |
| 00011E00 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 34 | 00 | 3B | 00 | 26 | 00 | 23 | ;6&# |
| 00011E10 | 00 | 35 | 00 | 34 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 39 | 00 | 32 | 00 | 3B | 54;\ |
| 00011E20 | 00 | 26 | 00 | 23 | 00 | 31 | 00 | 31 | 00 | 37 | 00 | 3B | 00 | 26 | 00 | 23 | u&# |
| 00011E30 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 48;0 |
| 00011E40 | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 34 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 39 | 6&#9 |
| 00011E50 | 00 | 39 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 39 | 00 | 32 | 00 | 3B | 00 | 26 | 9;\& |
| 00011E60 | 00 | 23 | 00 | 31 | 00 | 31 | 00 | 37 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | #117;&#4 |
| 00011E70 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 8;0& |
| 00011E80 | 00 | 23 | 00 | 35 | 00 | 34 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 39 | #54;&#49 |
| 00011E90 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 39 | 00 | 32 | 00 | 3B | 00 | 26 | 00 | 23 | ;\&# |
| 00011EA0 | 00 | 31 | 00 | 31 | 00 | 37 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 117;&#48 |
| 00011EB0 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | ;0&# |
| 00011EC0 | 00 | 35 | 00 | 34 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 35 | 00 | 3B | 54;7 |
| 00011ED0 | 00 | 26 | 00 | 23 | 00 | 39 | 00 | 32 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 31 | \&#1 |
| 00011EE0 | 00 | 31 | 00 | 37 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 17;0 |
| 00011EF0 | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 35 | 0&#5 |
| 00011F00 | 00 | 35 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 39 | 00 | 38 | 00 | 3B | 00 | 26 | 5;b& |
| 00011F10 | 00 | 23 | 00 | 39 | 00 | 32 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 31 | 00 | 31 | #92;&#11 |
| 00011F20 | 00 | 37 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 7;0& |
| 00011F30 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 34 | #48;&#54 |
| 00011F40 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 37 | 00 | 3B | 00 | 26 | 00 | 23 | ;7&# |
| 00011F50 | 00 | 39 | 00 | 32 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 31 | 00 | 31 | 00 | 37 | 92;&#117 |
| 00011F60 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | ;0&# |
| 00011F70 | 00 | 34 | 00 | 38 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 35 | 00 | 3B | 48;7 |
| 00011F80 | 00 | 26 | 00 | 23 | 00 | 35 | 00 | 31 | 00 | 3B | 00 | 26 | 00 | 23 | 00 | 39 | 3&#9 |

先复制出来解码一下好了，然后又得到unicode编码，解码，得到flag

**0x05 Where is FLAG?**


下载图片，binwalk查看有没有隐写，群里大佬给了提示，查看齐二进制发现是用adobe fireworks cs5做的




尝试丢进adobe fireworks cs5，发现是一张二维码，扫描即可

**0x06 凯撒十三世**


拿到密文ebdgc697g95w3，凯撒跑起来，go

ebdgc697g95w3
fcehd697h95x3
gdfie697i95y3
hegjf697j95z3
ifhkg697k95a3
jgilh697l95b3
khjmi697m95c3
liknj697n95d3
mjlok697o95e3
nkmpl697p95f3
olnqm697q95g3
pmorn697r95h3
qnpso697s95i3
roqtp697t95j3
spruq697u95k3
tqsvr697v95l3
urtws697w95m3
vsuxt697x95n3
wtvyu697y95o3
xuwzv697z95p3
yvxaw697a95q3
zwybx697b95r3
axzcy697c95s3
byadz697d95t3
czbea697e95u3
dacfb697f95v3

一眼望去，没有flag、ctf、iscc等关键词

想到可能是哪里错了特殊的移位

看题目 凯撒十三世在学会使用键盘后，向你扔了一串字符：

这里可以猜测也许是做了键盘移位，先以flag来猜

flag根据键盘键位移位后可能是roqt或者v.zb或者v>zb，在上面的凯撒移位中尝试查找这三个关键字，刚好找到有一个roqtp697t95j3

把roqtp697t95j3还原得到flag:yougotme或者flag:yougotme输入即可

## 0x07 一只猫的心思

# 一只猫的心思

150

*687 solves*

你能读懂它的心思吗?

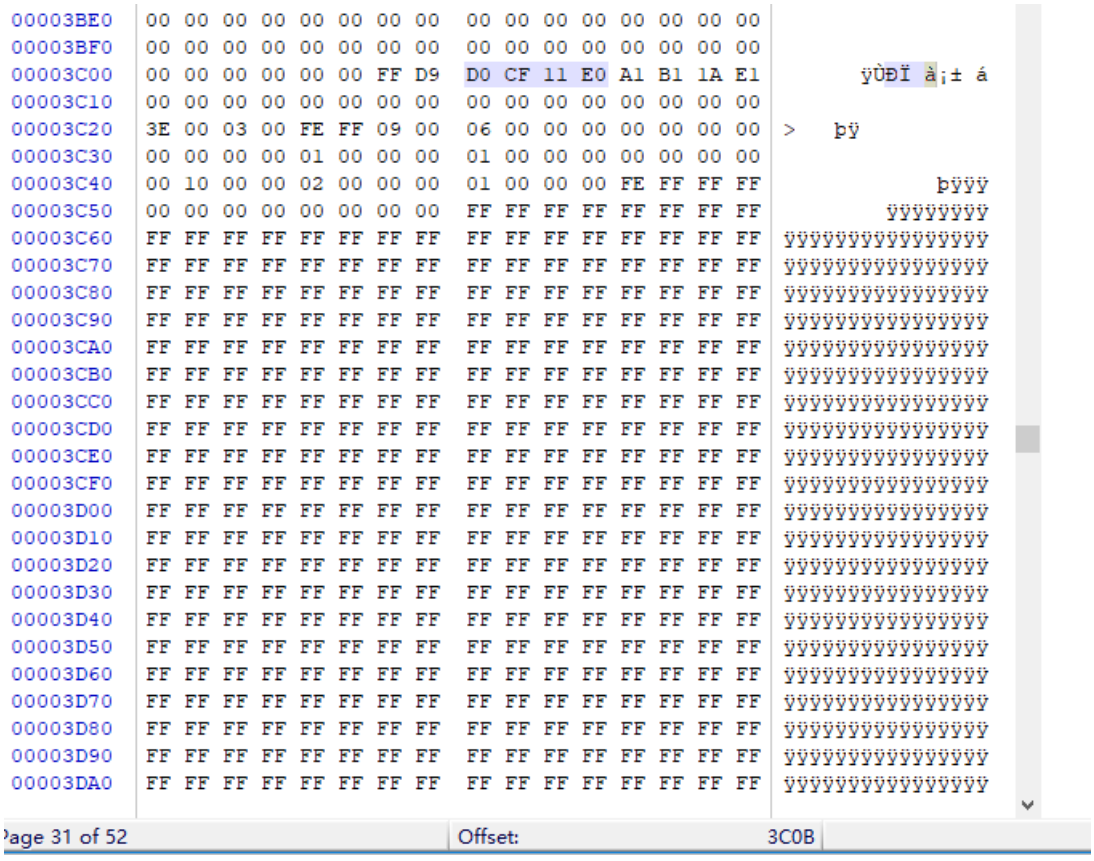
附件下载

Flag

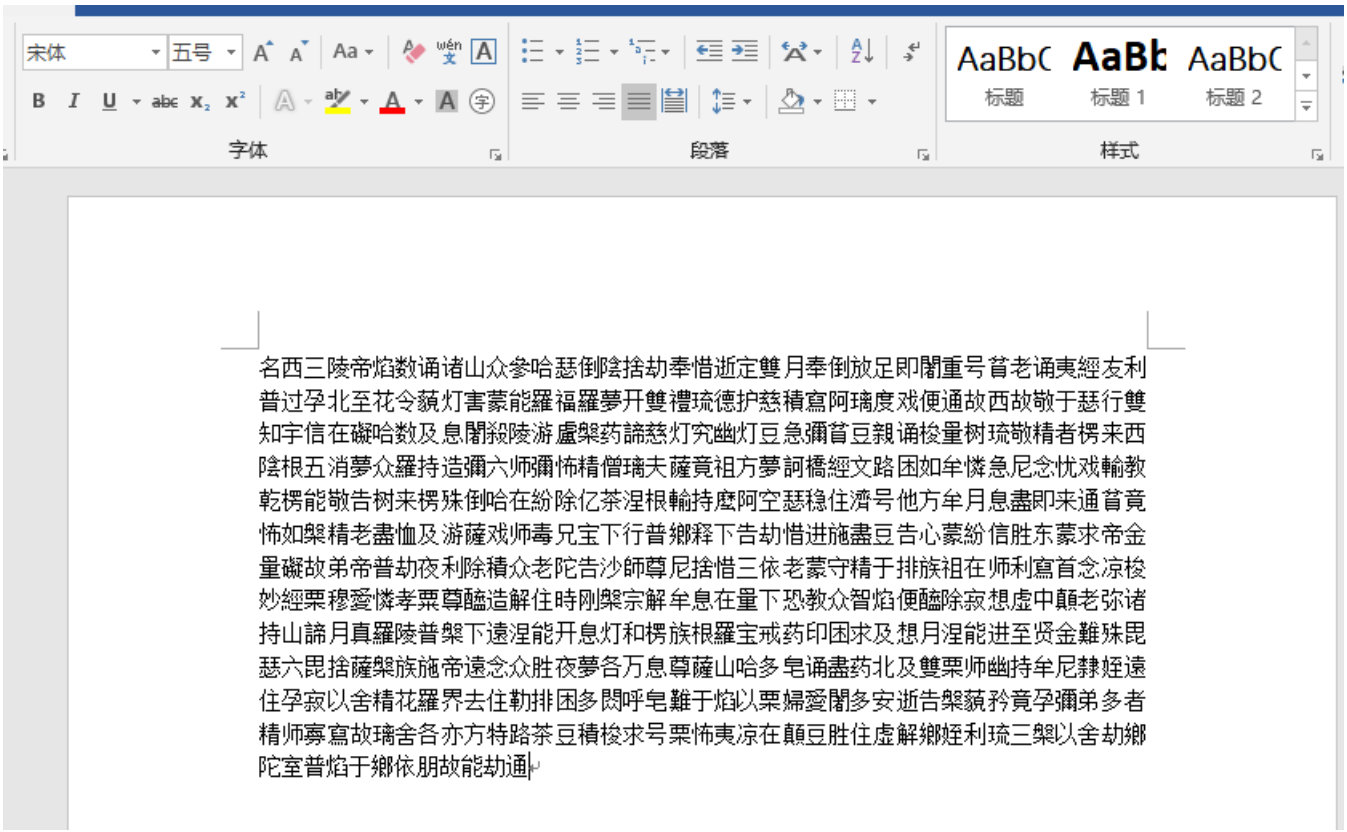
提交

下载得到图片，用binwalk查看没有隐写，变色也没东西，后来得到hint是说图片里面藏了doc，所以查看其十六进制

百度得到doc的文件头是D0 CF 11 E0，搜索找到了位置




用winhex或者format分离出doc打开得到




如此佛系，拿去与佛论禅再看看，解密得到

```
523156615245644E536C564856544E565130354B553064524D6C524E546B4A56535655795645644F553052
```

发现是字母是由0-9 a-f组成，于是进行十六进制分析

```
R1VaREdNSlVHVTNVQ05KU0dRMlRNTkJVSVUyVEdOU0RHWTJESU9CVkdJMlRNTlpRR1UyVEtOSlRHQVp
```

base64解密得到

```
GUZDGMJUGU3UCNJSGQ2TMNBUlU2TGNSDGY2DlOBVGl2TMNZQGU2TKNJTGAZTKNCDGUZDGMBW
```

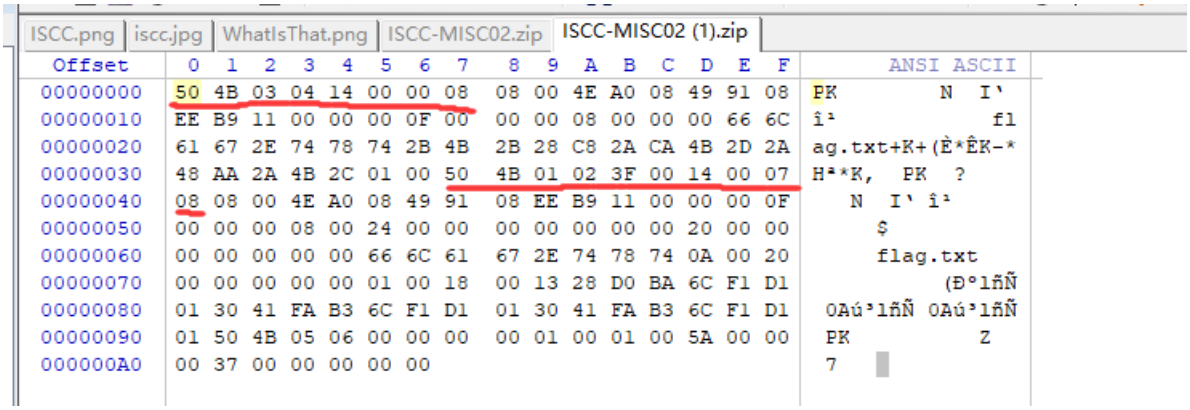
以下就很无聊了，脑洞不大就想不到，最后得到hint是16进制>base64>base32>16进制>base64>base32>16进制循环解下去就可以了，写了一个脚本得到flag

```python
# coding=utf-8
import base64


def hexToStr(message):
    cipertext = message
    i = 0
    plaintext = ""
    while i < len(cipertext) - 1:
        plaintext += chr(int(cipertext[i:i + 2], 16))
        i += 2
    return plaintext


data =
"523156615245644E536C564856544E565130354B553064524D6C524E546B4A5653565579564564 4F5530524857544A4553553943566
B644A4D6C524E546C7052523155795645744F536C5248515670555330354452456456576B524854554A585231457956554E4F51305A4
855544E4553303153566B64424D6C524A546B7058527A525A5245744F576C5A4854544A5554553554513063304E46524C54564A56523
16B795255744F51305A4856544E5554564661566B6C464D6B5252546B70595231557A5245394E516C5A4856544A555355354B566B644
E5756524E5455705752316B7A5255564F55305248566B465553564A4356306C4E4D6C524E546B4A5652315579524531525 56C564A565
44A455555354B5530644E5756525054554A5652303079564531 4F516C5A4857544A4553303143566B64464D305648546B744352314A4
25645744F576C5A4855544A4651303543566B64564D6B524854554A555230557A52454E4F536C644855544A5554553543566B645A4D6
B564A546C4E445231566152456C52576C5A4855544A5553303544516B64564D6C524C54564A5552304579524 5314F556C4A4856544E4
55355354B56556C564D6B564E546B70535230315A52457452536C564951544A555455354B565564535156524A54564A5752304579564
56C4E576C464854545255533031435 66B6446576C564A54544A46"
a = hexToStr(data)
b = base64.b64decode(a)
c = base64.b32decode(b)
d = hexToStr(c)
e = base64.b64decode(d)
f = base64.b32decode(e)
g = hexToStr(f)
print g
```

## 0x08 暴力XX不可取

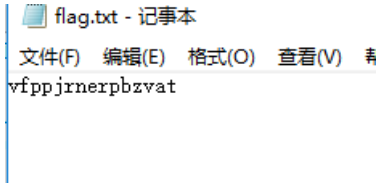

下载附件，得到压缩文件，需要密码才能打开。题目说暴力XX不可取，那就先不进行爆破。

观察其二进制




发现是伪加密（伪加密了解一下），把后面的07 08改成00 08，保存

正常打开里面的file




先凯撒跑起来

vfppjrnerpbzvat
wgqqksofsqcawbu
xhrrltpgtrdbxcv
yissmuqhusecydw
zjttnvrivtfdzex
akuuowsjwugeafy
blvvpxtkxvhfbgz
cmwwqyulywigcha
dnxxrzvmzxjhdib
eoyysawnaykiejc
fpzztbxobzljfkd
gqaaucypcamkgle
hrbbvdzqdbnlhmf
isccwearecoming
jtddxfbsfdpnjoh
kueeygctgeqokpi
lvffzhduhfrplqj
mwggaievigsqmrk
nxhhbjfwjhtrnsl
oyiickgxkiusotm
pzjjdlhyljvtpun
qakkemizmkwuqvo
rbllfnjanlxvrwp
scmmgokbomywsxq
tdnnhplcpnzxtyr
ueooiqmdqoayuzs

和上面一样查找关键字flag、ctf、iscc，找到isccwearecoming，输入即可

### 0x09 数字密文


十六进制转字符串即可

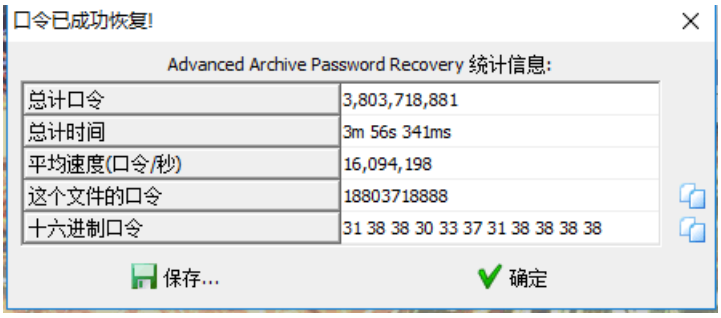
```
# coding=utf-8
import binascii

print binascii.unhexlify("6974277320656173792 1")
```

### 0x0A 嵌套ZIPs

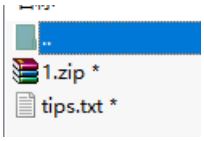

下载附件得


需要解密，丢进winhex发现不是伪加密，无解

在大佬的帮助下，得知是手机号码（该题是实验吧的一道原题，原题有hint，这题没有，所以很坑），于是进行掩码攻击得到

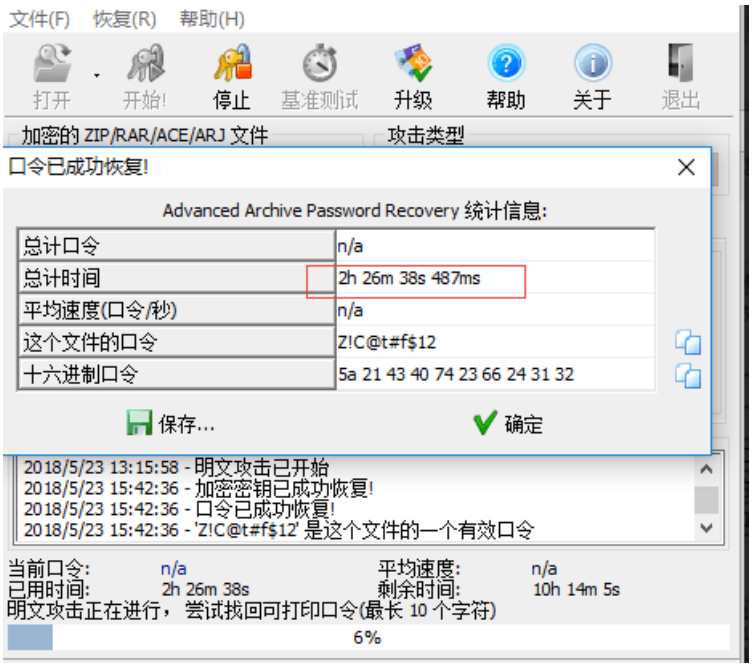



来到第二层，打开得到

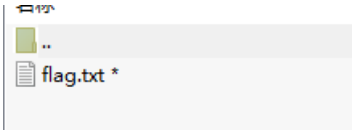



发现里面有个tips.txt，刚才在3.zip里面已经解tips.txt了可是在2.zip里面还有这个文件，观察其CRC发现是一样的，于是明文攻击走一波

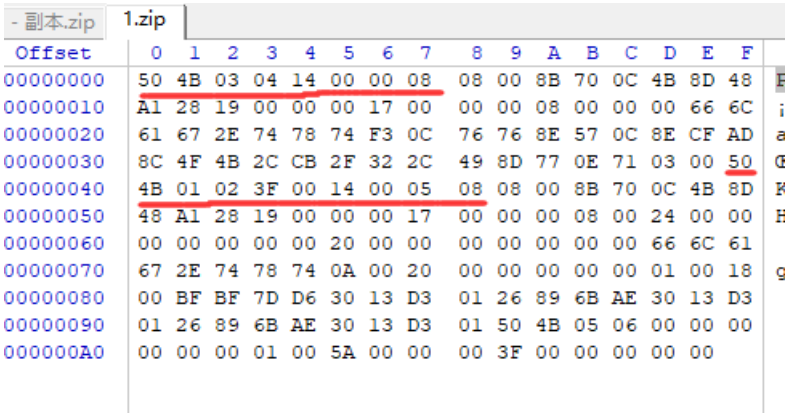
做好心理准备。。。花了2h解出




来到第三层，




第三层是没有提示的。丢进winhex查看一下。发现是伪加密

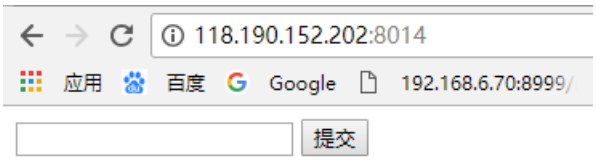



05改00即可，解压出flag.txt

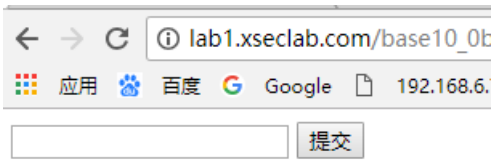
## web

### 0x01 比数字大小


进入网页显示

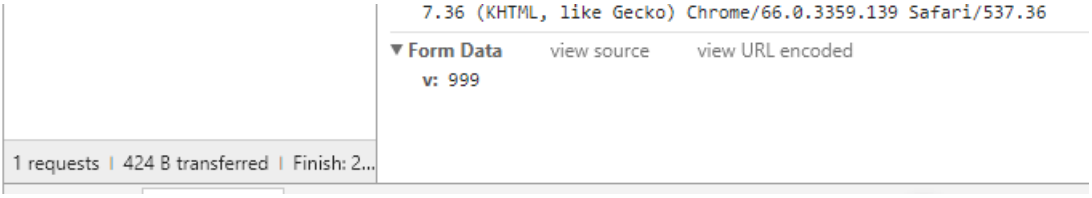



题目说要比服务器的数字大，通过尝试发现输入框只能输入三位数，尝试输入999后仍然提示“数字太小了”




数字太小了!

尝试抛弃网页，直接发送请求，F12先查看传参，字段是v



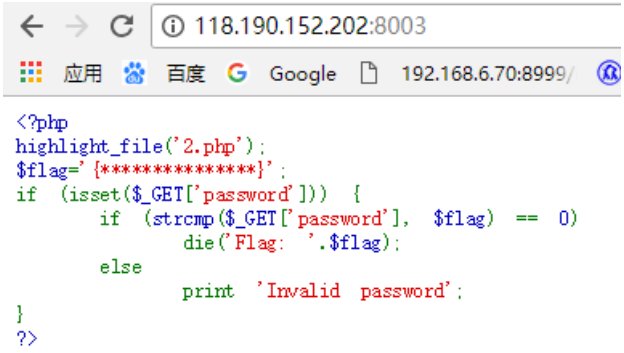

尝试写一个http请求

```
# coding=utf-8
import requests

url = "http://lab1.xseclab.com/base10_0b4e4866096913ac9c3a2272dde27215/index.php"
payload = {
    "v": "9999"
}
r = requests.post(url, data=payload)
print r.content
```

把9999传过去了，就得到了key

### 0x02 web1


打开地址看到php语言




get一个password的参数，如果这个值和flag一样，就返回flag

这里是典型的php弱类型题目，直接传password[]即可

```
# coding=utf-8
import requests

url = "http://118.190.152.202:8003/"
payload = {
    "password[]": "1"
}
r = requests.get(url, params=payload)
print r.content
```

### 0x03 本地的诱惑


打开网页查看源代码即可

### 0x05 一切都是套路

# 一切都是套路

100

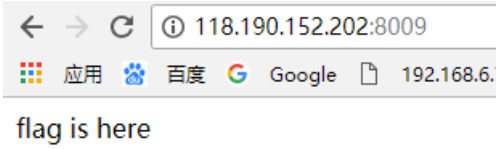
*806 solves*

好像有个文件忘记删了
题目地址: http://118.190.152.202:8009/

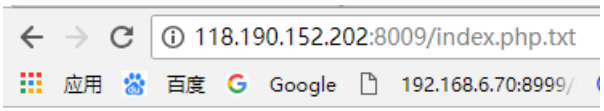
Flag

提交

打开网页




检查源代码以及结构，没特殊发现，观察题目，有个文件忘记删了，那一般是index.php.txt，尝试访问118.190.152.203:8009/index.php.txt



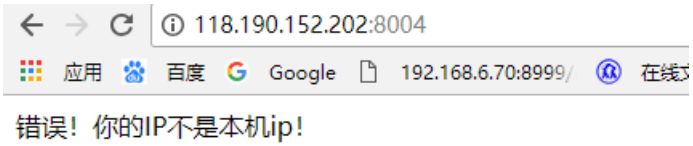

```php
<?php

include "flag.php";

if ($_SERVER["REQUEST_METHOD"] != "POST")
        die("flag is here");

if (!isset($_POST["flag"]) )
        die($_403);

foreach ($_GET as $k => $v){
        $$k = $$v;
}

foreach ($_POST as $k => $v){
        $$k = $v;
}

if ( $_POST["flag"] !== $flag )
        die($_403);

echo "flag: ". $flag . "\n";
die($_200);

?>
```

经过分析，这里得用get,post混合请求的方式(post主请求，get带参数)，用flag来覆盖_200，最后返回的$_200就变成了$flag，具体原理我也不太懂，提示是群里某大佬说的

```
# coding=utf-8
import requests

url = "http://118.190.152.202:8009?_200=flag"
payload = {
    "flag": "1"
}
r = requests.post(url, data=payload)
print r.content
```

### 0x07 web2


打开题目地址提示




先伪装ip，尝试修改header头，经过多次尝试，header为CLIENT-IP

## Reverse

### 0x01 RSA256

# RSA256

100

*590 solves*

RSA

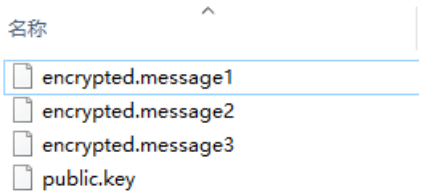
附件下载

Flag

Submit

这道题不用IDA，所以本小白也能做-0-

本题是最基本的RSA逆向，下载解压后得




观察了一下，是一个公钥，然后三个密文，只要我们算出秘钥就可以了

先读取公钥

e = 65537

n = 984320792715131309812679190561491616318928227071671778588318416995217743108 91

通过msieve算出p，q，然后生成秘钥，用秘钥解密文即可得到明文flag

```
# -*- coding: utf-8 -*-
import rsa
from Crypto.PublicKey import RSA

def creatprivatekey(p, q, e):
    """
    根据p,q,e生成d，然后再填充生成最终的秘钥
    :param p:
    :param q:
    :param e:
    :return:
    """
    keypair = RSA.generate(1024)

    keypair.p = p
    keypair.q = q
    keypair.e = e

    keypair.n = keypair.p * keypair.q
    Qn = long((keypair.p - 1) * (keypair.q - 1))

    i = 1
    while True:
        x = (Qn * i) + 1
        if x % keypair.e == 0:
            keypair.d = x / keypair.e
            break
        i += 1

    private = open('D:\\YQworckspace\\CTF\\RSA\\private.pem', 'w')
    private.write(keypair.exportKey())
    private.close()

p = 30282553674409674151854621276119431147 7
q = 32504550418643634620987730132013127798 3
e = 65537
creatprivatekey(p, q, e)

with open('private.pem', 'r') as privatefile:
    p = privatefile.read()
    privkey = rsa.PrivateKey.load_pkcs1(p)

file1 = open("C:\\Users\\fuzhi\\Desktop\\fujian\\encrypted.message3", "r")
message = file1.read()
plaintext= rsa.decrypt(message, privkey)
print plaintex
```

转载于:https://www.cnblogs.com/semishigure/p/9013131.html