# Hgame Final Writeup


## 0x03 Crypto

### Response

这的确是签到题。。不过感觉AES的题都蛮好玩的。。
知道CBC的工作方式就OK了，有`range(3)`次机会，其中IV不变，不停伪造密文/明文来异或就行了。。

直接上exp（时间原因没写自动脚本，60s的时间，手慢就要重来了。。）

```python
import binascii

def _print(promot, msg):
    print('\n'+binascii.hexlify(msg).decode()+'\n')

xor = lambda p, q: bytes(x^y for x,y in zip(p,q))

# >>> b'0000000000'
plaintext_0_suffix = b'0'*10
_print('>>>', plaintext_0_suffix)

#### first respones in hex
r0 = input('>>> ').encode()
r0 = binascii.unhexlify(r0)

_print('>>>', r0)
```

```
17
18  iv = r0[:16]
19
20  text = b'Alice'+b'\x00'*11
21  x1 = xor(iv, text)
22
23  r0c0 = r0[16:32]
24  plaintext_1 = xor(r0c0, x1)
25
26  # >>>
27  _print('>>>', plaintext_0_suffix + plaintext_1 + b'')
28
29  ##### second reponses in hex
30  r1 = input('>>> ').encode()
31  r1 = binascii.unhexlify(r1)
32
33  _print('>>>', iv + r1[32:48])
34
35  ##### third challenge
36  challenge2 = input('>>> ').encode()
37  challenge2 = binascii.unhexlify(challenge2)
38
39  _print('>>>', iv + r1[32:48] + xor(x1, challenge2) + r1[32:48])
```

代码写的很乱，跟着走拿到flag

`hgame{RefL3cti0n_@tt4ck_wiTh_c8C~B1t-fLiPpiNg}`

# 0x04 Misc

## Good Video

解压，是hevc编码的视频，看着75的分值应该是签到题不用想太复杂
看了一遍之后发现有几个快速闪过的画面，于是考虑有内容夹在帧内

先试了用ffmpeg提取出所有frame，结果发现提取不完整，于是用py临时写了个脚本

```
1  import cv2
2
3  cap = cv2.VideoCapture('GoodVideo.mp4')
4
5  i = 0
6  while(cap.isOpened()):
7      ret, frame = cap.read()
```

```
    if ret:
        i += 1

        name = "img2/frame%s.jpg"%str(i).rjust(10, '0')
        cv2.imwrite(name, frame)

        print(f'\rframe={i}', end='')
        #cv2.imshow('Frame',frame)
        if cv2.waitKey(1) & 0xFF == ord('q'):
            break
    else:
        break

cap.release()
cv2.destroyAllWindows()
```

所有frame提取出来后发现有二维码的片段，于是开始慢慢找。。
找完再用PS拼上。。思路简单，操作其实有点耗时。。

拼完之后就是

扫出二维码拿到flag

`hgame{gO0D_vId3O_EESvLoEPyC$zHlOJEHc0h&14}`