WEEK2

web（die)

reverse(keep-alive)

本来打算写第一题的，结果第二题开始之后直接上瘾。一边玩一边写出来。[手动保命]（多亏了幼稚园学姐对我的鼓励[doge]） 

由于我只写了一题，我还是写长点保命，好歹还能看看。sad]

面对一道所谓经典的crackme。第一步打开IDA发现什么都看不懂！！！难道真要我看汇编嘛，我表示深深的拒绝，然后试试odb打开，虽然调试起来熟悉了很多，但是由于不知道什么原因，下断点还有注释第二遍调试就没了，在不知道什么的情况下。在幼稚园的一点点hint下，在吾爱破解上发现了入口。

有一个软件Exeinfo，可以查壳，（虽然我没用）查壳后发现是一个C#语言写的（我当场陷入了懵逼），好在发现了一个软件可以调试C#，我索性试了试dnSpy-x86.exe。跟着别人的教程试了试dnSpy，入口下断点，发现别人的教程对我好像没什么帮助，于是乎我用odb的思想开始调试，遇到函数用逐过程f10，如果弹出crackme框框的话，那那个就是进入crackme的函数，由于第一次调试都是对象的程序，我满脑子的拒绝导致我懈怠了很多。

```
1  using System;
2  using System.Windows.Forms;
3
4  namespace CrackMe
5  {
6      // Token: 0x02000004 RID: 4
7      internal static class Program
8      {
9          // Token: 0x0600000F RID: 15 RVA: 0x000027C7 File Offset: 0x000009
10         [STAThread]
11         private static void Main()
12         {
13             Application.EnableVisualStyles();
14             Application.SetCompatibleTextRenderingDefault(false);
15             Application.Run(new Form1());
16         }
17     }
18 }
```

进过不懈的调试发现我下断点的地方是crackme的入口。

到了断点，使用逐语句f9进入函数，果然是的。

```
private void button1_Click(object sender, EventArgs e)
{
    if (this.status == 1)
    {
        MessageBox.Show("你已经激活成功啦，快去提交flag吧~~~");
        return;
    }
    string text = this.textBox1.Text;
    if (text.Length != 46 || text.IndexOf("hgame{") != 0 || text.IndexOf("}") != 45)
    {
        MessageBox.Show("Illegal format");
        return;
    }
    string base64iv = text.Substring(6, 24);
    string str = text.Substring(30, 15);
    try
    {
        Aes aes = new Aes("SGc0bTNfMm8yMF9XZWVLMg==", base64iv);
        Aes aes2 = new Aes("SGc0bTNfMm8yMF9XZWVLMg==", "MFB1T2g5SWxYMDU0SWN0cw==");
        string text2 = aes.DecryptFromBase64String("mjdRqH4d1O8nbUYJk+wVu3AeE7ZtE9rtT/8BA8J897I=");
        if (text2.Equals("Same_ciphertext_"))
        {
            byte[] array = new byte[16];
            Array.Copy(aes2.EncryptToByte(text2 + str), 16, array, 0, 16);
            if (Convert.ToBase64String(array).Equals("dJntSWSPWbWocAq4yjBP5Q=="))
            {
                MessageBox.Show("注册成功！");
                this.Text = "已激活，欢迎使用！";
                this.status = 1;
            }
            else
            {
                MessageBox.Show("注册失败！\nhint: " + aes2.DecryptFromBase64String("mjdRqH4d1O8nbUYJk+wVu3AeE7ZtE9rtT/8BA8J897I="));
            }
        }
        else
        {
            MessageBox.Show("注册失败！\nhint: " + aes2.DecryptFromBase64String("mjdRqH4d1O8nbUYJk+wVu3AeE7ZtE9rtT/8BA8J897I="));
        }
    }
    catch
    {
        MessageBox.Show("注册失败！");
    }
}
```

仔细分析后发现我根本看不懂加密解密的东西，这里调用的函数库我表示看不懂，而且官方文档也没有表示这个具体时干什么的，见（.NET文档）。又过了好久，我发现问题应该是出在这是一个aes加密，如此明白的暗示我一开始居然没有get到。于是我开始了关于aes的学习。

以下两个网站我现在还没看明白

1.（AES入门教程）

2.（AES小白教程）

做个标记，以后继续看。

大概明白了原理我断言flag是以'hgame'{开头，以'}'结尾，然后中间密码分两段，第一段flag是求vi(cbc加密模式的偏移值)，第二段flag是求明文。

第一段flag

已知[明文，密文，key]求vi

由于偏移值只是一个和明文异或关系的事物，我试试在网上找脚本直接求解，果不其然，在花费大量时间之后，我啥也没找到。[泪奔]

在幼稚园的鼓励下，最后我试试能不能改造一个python脚本解出vi，思路是先反向解出明文和vi的异或值，然后再和明文异或可以得到vi。

```
import base64
from Crypto.Cipher import AES
# 密钥（key）, 密斯偏移量（iv） CBC模式加密

def AES_Encrypt(key, data):
    vi = '0PuOh9IlxO54Icts'
    pad = lambda s: s + (16 - len(s)%16) * chr(16 - len(s)%16)
    data = pad(data)
    # 字符串补位
    cipher = AES.new(key.encode('utf8'), AES.MODE_CBC, vi.encode('utf8'))
    encryptedbytes = cipher.encrypt(data.encode('utf8'))
```

```
    # 加密后得到的是bytes类型的数据
    encodestrs = base64.b64encode(encryptedbytes)
    # 使用Base64进行编码,返回byte字符串
    #print(encodestrs)
    enctext = encodestrs.decode('utf8')
    # 对byte字符串按utf-8进行解码
    return enctext


def AES_Decrypt(key, data):
##    vi = chr(0)*16
##    vi = '/TyXYzPnY;$)\we_'
    vi = '0PuOh9IlX054Icts'
    data = data.encode('utf8')
    encodebytes = base64.decodebytes(data)
    # 将加密数据转换位bytes类型数据
    cipher = AES.new(key.encode('utf8'), AES.MODE_CBC, vi.encode('utf8'))
    text_decrypted = cipher.decrypt(encodebytes)
    unpad = lambda s: s[0:-s[-1]]
    text_decrypted = unpad(text_decrypted)
    # 去补位
    text_decrypted = text_decrypted.decode('utf8')
    return text_decrypted


key = 'Hg4m3_2o2O_WeeK2'
##data = 'Learn principles'
###other = 'Learn principles'
##other = 'Same_ciphertext_'
###AES_Encrypt(key, data)
##enctext = AES_Encrypt(key, data)
##print(enctext)
##text_decrypted = AES_Decrypt(key, enctext)
##new_text = []
##for i in range(0,16):
##    new_text.append(chr(ord(other[i])^ord(text_decrypted[i])))
##
##print(new_text)
###print(text_decrypted)
##
##for i in range(0,16):
##    print(new_text[i],end = '')
##
##
##print('\n')


##enctext = 'dJntSWSPWbWocAq4yjBP5Q=='
##enctext = base64.decodebytes(enctext)
##print(enctext)
##text_decrypted = AES_Decrypt(key, enctext)
##print(text_decrypted)

code =
(b'\xc6\x52\x8a\x40\x0e\x51\x3e\x9c\xb2\x03\x56\x01\x8c\x37\x8b\xe4\x74\x99\xed\
x49\x64\x8f\x59\xb5'
b'\xa8\x70\x0a\xb8\xca\x30\x4f\xe5')
base64str = base64.b64encode(code)
```

```
print(base64str)
flag = hgame{L1R5WFl6UG5ZOyQpXHdlXw==DiFfer3Nt_w0r1d}
```

中间未加注释的是得到异或值得方法，后面则是下一段flag。

第二段

已知明文得前半段，密文的后半段，vi，key。求明文后半段。通过明文的加密可知，密文的前半段有一部分是固定的，中间有一个base64的字符‘5？？？’转换成一个字符串‘？\x74\x99’

再了解了一下base64的加密原理后，我可以猜测字符串中的？是由一个二进制111001？？组成的，所以就只有四种可能，我取了00试了一下，直接就成功了。得到base64的密文，再解码得到string明文，后半段及是我想要的falg后半段

FLAG = hgame{L1R5WFl6UG5ZOyQpXHdlXw==DiFfer3Nt_w0r1d}

pwn(die)

crypto(die)

misc(die)