HGAME-Week2-WriteUp

1. Web

没基础的差距体现出来了，这周web本来一道都不会的，这道还是大🍗的教导和提醒下才做出的，得静下心来好好学习，不能继续混着了，选一个主方向来下功夫。

3. Cosmos的新语言

题目描述：

Cosmos 宣称他自主发明了一门新的编程语言。
但是大家发现原来是他拿 PHP 原封不动套的壳。那这就好办了，你来试试?
Challenge Address http://ad25388f64.php.hgame.n3ko.co/
Base Score 150
Now Score 150

点进链接，一开始我发现了网站的乱码是5秒一遍~~（无图）~~，也就是加密和时间有关系，大🍗让我一行行看代码，看懂代码后去到了mycode页面，看到了加密方式。共4种基本的加密手段，base64，strrev，rot13和移一位的凯撒加密。

一开始以为口令是随时间变的，加密方式不变（其实两者都变），就边学爬虫边写了个简单的，爬下代码然后按加密方式逆着解码，后面刷新一下发现加密方式变了，就再把加密方式爬下来写个循环进行解码。

题目的判断条件是提交的POST表单里的'token'与$_SERVER['token']相等（===）当然，逆着解出来的肯定与token===了。

用表单提交解出的token，但界面一直没有什么变化，最后大🍗指出了我没把返回值用上。。。。所以echo出结果。

害，好好学习，不要混迹于crypto和misc了。

2. Reverse

这一周的Re以学习为主，所以做出来大部分题

1. unpack

题目描述：

看起来是upx呢，但是怎么办呢?
Challenge Address http://q4f83ppqy.bkt.clouddn.com/unpack_00b2bb661b
Base Score 150
Now Score 150

就像幼稚园学长说的，这题放了学习资料后就和签到题没什么区别了。按照教程手动脱壳，结构都是一模一样的，然后脱出程序进行逆向。

一开始拖进IDA一看，我的妈呀，六百多函数，吓死。想着week1有人说IDA7.2会好很多，特意找了7.2，发现然并卵。于是把程序扔进Linux跑一下，发现输入了错误的flag有错误提示，就在IDA里搜索即发现关键函数，大致看了下逻辑，就是将输入的字符串用循环逐个加上在其数组中的值与内存上的一个区域进行比较。那么双击便看到加过的flag了，写个脚本减值就得出flag。

2. Classic_CrackMe

这好像是我做出分最高的题（其实不难23333）

题目描述：

是时候来一道1860年的经典——Crackme了！

Challenge Address http://q4f83ppqy.bkt.clouddn.com/Classic_CrackMe_b2d9e761dd.exe

Base Score 200

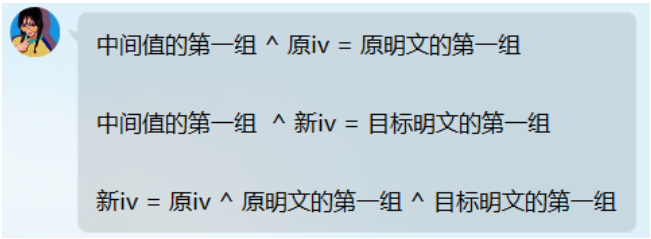
Now Score 200

一开始拖进IDA只能看到个大概运行逻辑，完全看不懂什么函数，搜索了一下，下了个工具分析语言，是C#，于是下Reflector，拖进去，仔细看看逻辑，边看边搜各个函数的作用

~~看代码自己动手~~，其逻辑是先判断输入是否头为"hgame{" 尾为 "}"，而且判断尾的方式是检测其所在的位置是否为某个数，这样就得出里面的长度为39。

接着将里面的内容分成两段，前一段长24，将它进行Aes解密，可以很容易的看到它作为偏移向量IV，然后解密密文得到另一组字符串。

当然，根据题目的意思，这个IV也是base64编码的，那么怎么求它呢？我一开始的思路是先将密文与密钥进行解密，然后再与明文进行异或，确实可以，但幼稚园学长提供了一个更简单的解法：



中间值指的是我将密文与密钥解密出的结果，这道题看起来只有一个明文，但它的逻辑实际上还有个明文，且那个才是原明文，现在题目里的"Same_ciphertext_"是目标明文的，也就是这个IV还是个新IV，题目原本给出了一个IV，用那个能解出原明文，也是一个hint"learn principle"（这个hint只有在前一半对或后一半对且前一半为base64才出现），当然，拿题目的密钥，IV，和密文也能解出这个hint（一开始我从IDA里看到的编码里解出这个还以为这是flag里的XD）

这样得到这个新IV后，就是flag的前半段。后半段就是str3

```
Array.Copy(aes.EncryptToByte(str4 + str3), 0x10, destinationArray, 0, 0x10);
if (Convert.ToBase64String(destinationArray).Equals("dJntSWSPWbWocAq4yjBP5Q=="))
{
    MessageBox.Show("注册成功！");
    this.Text = "已激活，欢迎使用！";
    this.status = 1;
}
```

str4是已知的，而且长度为16，所以用str4，密钥和题目的IV进行加密得到str3加密用的IV，那么已知IV，密钥和密文还有中间有次base64编码，就得出str3了。

其实不难对吧，主要就是加密而已（逃

3. babyPy

题目描述：

这道题可能出题人觉得过于简单，都没让我们下载，直接在线看。

CPython uses a stack-based virtual machine.

Challenge Address http://q432pxpwq.bkt.clouddn.com/week2/babyPy_task_e011896c39.log

Base Score 150

Now Score 150

点进去，python的字节码，没学过，百度着边学边看。看懂后题目思路还是很简单的，先将flag倒过来，再循环将字符和后面那个字符异或后存入，所以倒着解题就出来了（当然还有一些解码）。（吐槽一下Lurkrul学长的变量命名，这可能是这道题150分的原因XD）

4. babyPyc

题目描述：

听说上一题不够难?

sth about pyc header:

https://www.python.org/dev/peps/pep-0552/#id15

Challenge Address http://q432pxpwq.bkt.clouddn.com/week2/babyPyc_task_2441ab393b.cpython-37.pyc

Base Score 250

Now Score 250

啊啊啊啊，原来这个才是我做出来分最多的题。

作为一个放寒假才学python的人，做这道题前我还不知道什么是pyc呢。。。。

一开始搜着相关资料，试着在线反编译，果然不行，然后看了看学习资料里的博客，郑博学姐的博客还是挺正经的，我试着改头，发现不行，又自己编译了一些pyc对比着看，修改一些地方，但在线工具发现也只能出来很少的一部分源码（学长也说改着出源码不就成misc了嘛，很有道理），用dis库，也一直报错，后面找了工具反编译，但只出来字节码，字节码就字节码嘛，慢慢看就是了（中间还做了些其他的题目），后面发现，看不懂啊？？？？

问了下学长，是不完整，然后学长让我用dis和mashal库，但我这边一直报错，后面发现是版本问题，3.8搞3.7的有问题。终于弄出完整的字节码了，那就慢慢看呗（还学会了一些python的用法）

弄清楚逻辑后还是不难，~~难的是弄清楚~~，有些很经典的用法都是自己再编一个来看框架是不是一样。好，下面概述逻辑：

先输入flag，是一个自定义函数，这里有个坑，前面虽然给O0o这个储存密文的全局变量进行了赋值，但是在自定义函数里对O0o重新赋值，当然，前面那个也是能解出的，解出来的结果就告诉你不是真flag。

获取到用户输入的flag后，先判断了头尾，符合就取出括号内内容，再判断长度是否为36，是就将字符串倒序一次，然后用列表推导式（最复杂的部分，这里发现了列表推导式后也好做）将字符串进行重排列，排列的规则是：**栅栏密码，6栏的**（~~简洁明了~~逃。

从变量命名和数据就可以看出来一些端倪，36=6*6，col和row就是列和行，联想矩阵的c和r就是了，然后它还加了次密，将同一列的元素变为自身与下面那个元素相加，最后一排不做处理。

虽然它还模256，但这是没用的，两个ASCII上的元素加起来 LE 256,所以是用来混淆的。最后再编个码与O0o这个变量进行比较，所以我们逆着做题即可，写个脚本就可以得到flag。

下面是脚本：

```
from Lurkrul import flag
print(flag)
#不存在的，回文串学长上周说了看思路，脚本就不放啦
```

总结：emmm，这周re以教学性质为主，所以学习一些就能做出大部分的，而**Y姐姐的题**，week1和week2都做不出，遂弃之。

3. Crypto

目前来说，Crypto的题都是有难度，但想做出都是能做出的，毕竟是~~hgame最佳出题人~~Lurkul学长出的。

1. Verification_code

题目描述：

本周的签到题 XP

nc 47.98.192.231 25678

Challenge Address http://q432pxpwq.bkt.clouddn.com/week2/Veri

Base Score 125

Now Score 125

确实很签到的。。。。我感觉都没认真看代码，直接爆破的(p≥w≤q)

```
sha256(XXXX+0QDoETl0tJEYF3DL) == 50f65de9031b10716adad7c16fdd614ee036b9417ddb58a
722f81a69e7e2c2c8
Give me XXXX:
```

nc后出来一串，题意就是找到XXXX使得sha256加密后等于后面那个，由于看了下代码给了我们60秒，时间太充裕！！！而且才4位，于是暴力4层循环，而且当时大年初一爸妈喊着吃午饭了，题目里的编码都是手动复制粘贴的（逃，而且当时运气还挺好，第4个就爆出来了

```
a
b
c
d
eAA2
```

然后手动复制进去，然后让我输code，自然是从源码里再复制一下就可以了。我觉得Lurkrul学长~~看到会打大~~温柔善良不会怎么样的。

2. Remainder

啊，为什么要烤孙子，孙子做错了什么。

题目描述：

烤个孙子

Challenge Address http://q432pxpwq.bkt.clouddn.com/week2/Rem

Base Score 150

Now Score 150

一看题目，哇，这怕又是RSA的题了，搜了下资料，应该是考中国剩余定理（又名孙子定理），那么根据CRT，我可以求出m的e次方。

一开始一直想着开根开出来，后面问了下Lurkrul学长，学长说这就是个RSA的题，RSA不是用开根的，那这个也不是。一开始我想着RSA那就求私钥呗，但这里都是直接将质数作为模数，怎么会有非0的欧拉函数呢？后面突然想到那我再加密一次呗，反正m的e次方知道，质数也知道，然后就拿两个去做，但这样长度就爆掉了，后面没法求d，又问了下学长，学长说3个质数也是一样的求：

因为

$$d*e=1mod(phi(n)),phi(n)=(p-1)*(q-1)*(r-1)$$

求出d后，解密时：

$$令n=p*q*r,则c^d\ mod\, n=m,$$

这样子算的出，但我当时没注意到源码有个long_to_bytes，这样算出的长度远大于msg的范围（这是当然）所以后面找到一个优化长度的算法：

$$将c^d\ mod\, n=m拆为三个式子\begin{cases}m_1=c^d\ mod\, p\\m_2=c^d\ mod\, q\\m_3=c^d\ mod\, r\end{cases}$$

这里虽然降了模数，但d还是很大，于是继续，以第一个式子为例

$$设k满足d=k(p-1)+dp,dp=c\,mod\,(p-1)$$

$$那么c^d=c^{k(p-1)+dp}=c^{k(p-1)}*c^{dp}$$

$$由欧拉定理得：c^{p-1}\ mod\, p=1$$

$$则c^d\ mod\, p=m1\quad 根据模运算的规则，乘法符合分配律，得到$$

$$c^a\ mod\, p=m1$$

至此模数和次方都降了

$$dp=d\,mod\,(p-1)或者也可以算dp*e\equiv 1\,mod\,(p-1)$$

dq，dr同理，

现在算m：先拿dp,dq算出m1,m2,再算出q对p的逆元qI,

$$h_1=(qI*((m_1-m_2)mod\, p))mod\, p\,,m_{12}=m_2+h_1*q$$

照上式可解出1，2的通用解：

$$m_{12}+k(p*q),即显然可视为p*q为新p，r为新q$$

接着拿dr算出m3,以及r对新p的逆rI

$$则有：h_2=(rI*((m_{12}-m_3)mod(p*q)))mod(p*q)$$

$$m=m_3+h_2*rI$$

公式真难打。。。（没时间检查了，有错勿怪）

所以最后再bytes_to_long可得出一长串。我因为把0和o搞混了，一直没提交起，然后把花框上的字符按中国剩余定理搞了好久。。。蠢哭了

4. Misc

Cosmos的午餐

题目描述：

Cosmos做梦都想吃一次芽衣亲手做的午餐，边吃饭边左拥八重樱右抱希儿这种。

他在屏幕前对着图片做白日梦的样子恰巧被路过的ObjectNotFound看到了。

“唔...好香呀！”

“Cosmos！醒醒！别睡了！！起来做PWN了！！！”

PS: Cosmos经常往图片备注里塞东西。

Challenge Address http://oss-east.zhouweitong.site/hgame2020/week2/MeisLunch_

Base Score 200

Now Score 200

下载压缩包，打开一看就是流量分析题，但还多了一个ssl_log.log文件，一开始直接看，http直接只有一个文件，TCP追踪也一堆乱码，查了下，发现要把那个ssl_log.log导入即可（怎么导入自己查），导入后重新加载发现http里文件都显示出来了，先按大小排列，发现有个文件格外大，导出后拖进winhex一看，是PK，zip头文件，改后缀为zip，解压出一张图片，图片名为Outguess with the key，联想到题目提示的，就从图片备注里取出了key，但这个key怎么使用一直没有头绪，不是flag，让我猜，我用各种古典加密都不行，后面问了ObjectNotFound学长，学长提醒我文件名，所以这个文件名不是拿来翻译的，是某个工具的名字。。。。

所以key是提取密码，下载输入提取得到flag

2. 所见即所假

题目描述：

真亦假，假亦真，真真假假，假假真真；

实亦虚，虚亦实，实实虚虚，虚虚实实。

ObjectNotFound给了你一个压缩包和一副对子，转身离开了。

Challenge Address http://oss-east.zhouweitong.site/hgame2020/week2/Al

Base Score 100

Now Score 100

这道题提示挺明显的，下载后是一个加密的压缩包，压缩包备注：

百度下载了f5工具，可这工具是对图片用的，和压缩包密码没关系，想到题目名字，可能是伪加密，7z成功解压出图片，然后用f5工具就顺利提出flag

```
F5 key: NllD7CQon6dBsFLr
```

3. 地球上最后的夜晚

题目描述：

农历一年中最后的夜晚马上就要来临了。

唔... “最后的夜晚” ...这让我想起了去年春节前夕。

一个“上”字，区分开了名著《地球上最后的夜晚》，和毕赣导演的《地球最后的夜晚》。

一年了，ObjectNotFound手里的那本《地球上最后的夜晚》，还没有看完...

Challenge Address http://oss-east.zhouweitong.site/hgame2020/week2/LastEveningsOnEarth_p

Base Score 150

Now Score 150

这道题挺坑的，打开下载的压缩包，一个加密的压缩包，和一个名为No Password的pdf文件，我理解为了压缩包密码不在pdf里，一直对着这个题目扣字眼，一直无果。

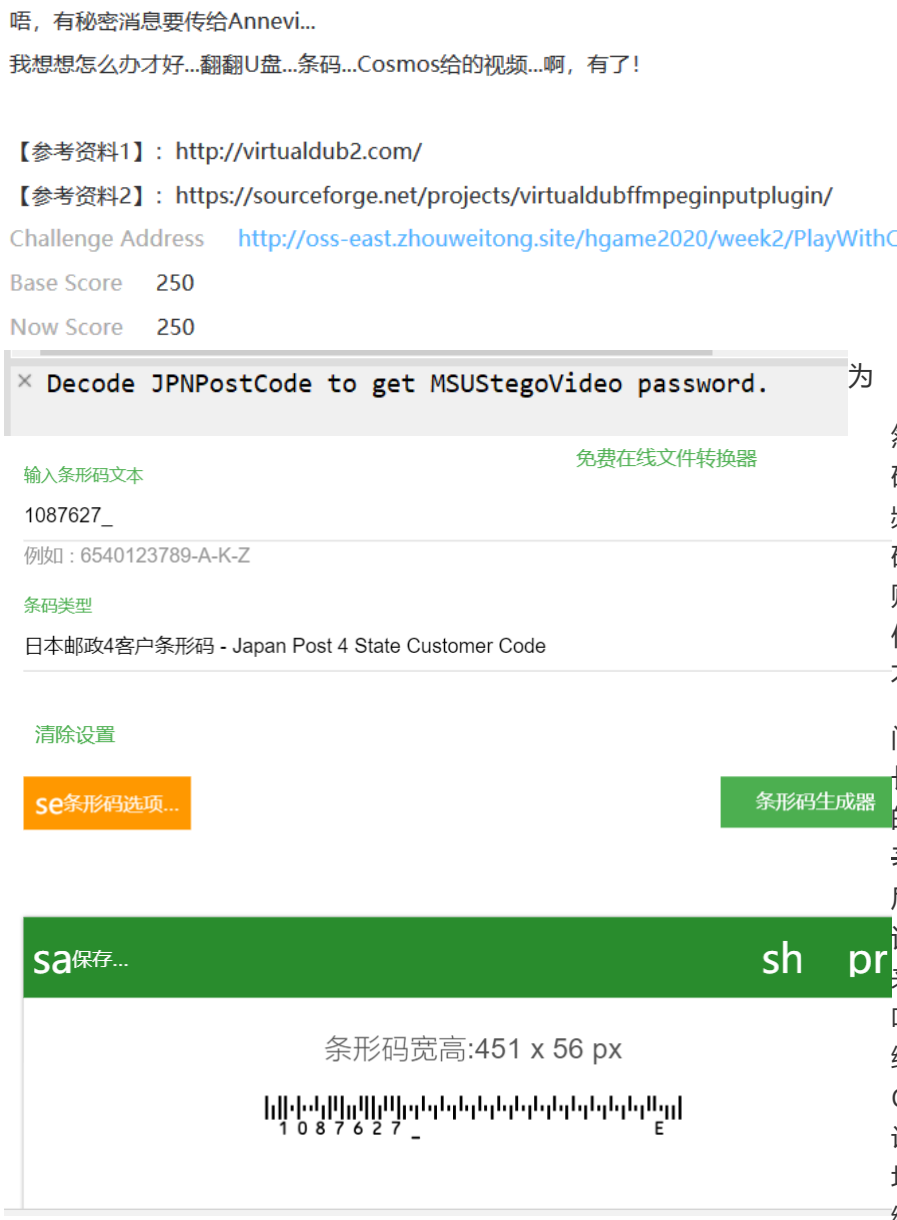
直到后面问了ObjectNotFound学长，学长说不是这个意思，是指pdf加密没设密码。我。。。。

找了下pdf加密工具，对应后解出压缩包密码，得到了《地球上最后的夜晚》的docx，没有隐藏文字，没有什么奇怪的特征，拖进Winhex一看，哈，PK头，改后缀，在word文件夹里看到里面有一个secret，打开即得flag

4. 玩玩条码

题目描述：

下载压缩包，压缩包注释：



出结果。

真•玩条码

打开JPNPostCode，是个条形码，查了下，是日本邮政条形码，找了一圈没得识别工具，只有生成工具，观察了一下，密码不长，于是手动试出密码为

然而这不是压缩包的密码。。。。看注释是将视频解出的某个工具的密码，下载工具后还是失败？这个工具要avi的文件，我用Pr导出为avi并不行

问了ObjectNotFound学长，学长说让我看题目给的学习资料，~~啊，还有学习资料啊，没看见~~，下载后转为avi文件，开始忘记设置了，这个视频转出来有10G，10G就10G呗，还是能用的，得到压缩包密码后，解出Code128.png，这个在线识别出一个网址，打开网址下载到一个压缩包，压缩包内一个二维码，扫描