INVIN HGAME 2019 week-1 writeup

WEB

谁吃了我的flag

看到vim，知道是vim临时文件，尝试下载`.index.html.swp`，然后用`vim -r`命令恢复。

换头大作战

post一下，把UA、referer、cookies都改一遍。

very easy web

双重url编码。

can u find me?

先看源代码，发现`f12.php`，访问后在回复头中发现password，post后发现`iamflag.php`，访问发现被重定向，开bp拿到flag。

MISC

Hidden Image in LSB

拿stegsolve点几下就出来了。

打字机

紫罗兰永恒花园里的字母，替换一下就好了。

Broken Chest

先把zip头改了，解压发现有密码，看到压缩包后面有密码，然后解压出flag

Try

用wireshark打开流量包，提取出zip文件，有密码，但是给了掩码，尝试纯数字爆破出来了。解压出一个jpg，看到里面有zip文件头，改后缀为zip，解压出一个docx文件。又发现里面有zip文件头，再改后缀解压，解压出一堆xml，不是专业misc，不太懂这方面。在一个document文件里面看到有flag，不太清楚正确的解法。

CRYPTO

Mix

先摩斯电码解一下，然后是ASCII HEX，栅栏加凯撒就出来了。

perfect_secrecy!

一看到感觉是标准的异或密码学题，可以看到key的长度非常长，足以保证明文和flag在异或的过程中没有信息丢失。所以将异或后的flag和异或后的明文异或就能把key消掉。之后就是比较标准的流密码加密类型，用固定的密钥加密大量文本。这题还有就是知道了flag的长度是33，更好爆破出flag。综合一下通过脚本爆破出flag。

Base全家

一直base64或者base32或者base16，然后最后一个base58。

RE

brainfxxker

brainfuck这个语言还是蛮有名的，以前早有耳闻，但是没研究过，刚好借此机会弄懂了。给的那一串代码中，核心就是循环里其实是实现一个乘法，然后再加几或者减几最后输出。

HelloRe

扔到IDA中F5。

Pro的Python教室(一)

就一个base64。

PWN

aaaaaaaaaa

输入大于99个a就行了

PS:web选手内心苦啊，二进制一点都不会。。。