Hgame --week 1 wp

----EkkoSonya

web

Hitchhiking_in_the_Galaxy

修改header

用burpsuite 点击 我要搭顺风车 1.要求 无限非概率引擎 (Infinite Improbability Drive) 访问 于是修改user-agent

2.要求本地访问 修改X-Forward-for:127.0.0.1

3.收到茄子的特别要求 修改refer为 https://cardinal.ink/

得到flag

watermelon

简单且上头的小游戏

查看网页的js文件，发现游戏主要规则存放在project.js中

ctrl+f 搜索gameover 发现一个

```
gameOverShowText: function (e, t) {
    if(e > 1999){
        alert(window.atob("aGdhbWV7ZG9feW91X2tub3dfY29jb3NfZ2FtZT99"))
    }
    // this.ajaxLoad("http://www.wesane.com/admin.php/Gamescore/saveGames
}
```

将其复制到base64解密 得到flag

智商检测鸡

100道定积分 直接上了 定积分计算器 ， 结束就得flag (可能有点不讲武德....)

看了资料后，感觉是用python爬虫去网页获取积分题目，然后自动帮算的思路...

RE

helloRe

拖入ida 没有显然的main 稍微找一下就可以找到 直接f5

主要目的就是我输入一个flag 然后循环 字符 异或 (FFh--) 要与给定的数据相等

直接

```c
#include <stdio.h>
int main (void)
{
    int ss[]={0x97,0x99,0x9C,0x91,0x9E,0x81,0x91,0x9D,0x9b,0x9a,0x9a,0xab,0x81,0x97,0xae,0x80,0x83,0x8f,0x94,0x89,0x99,0x97};
    char flag[25];
    int x = 0xff;
    for(int i = 0;i<22;i++)
    flag[i]=ss[i]^(x--);
    printf("%s",flag);
        return 0;

}
```

得到flag

pypy

打开一开始一脸懵 后来知道是python字节码

找到官网 硬着慢慢翻译

程序主要是对raw_flag后两次循环处理 第一次循环 类似于奇偶位交换 第二次循环 是每个字符与其的位置异或即可 末尾给出your_flag 就是反推即可

```python
myflag = '30466633346f59213b4139794520572b45514d61583151576638643a'
cipher = list(myflag.decode('hex'))
length = len(cipher)
for i in range(length):
    ch = chr(ord(cipher[i])^i)
    cipher[i]=ch
for i in range(length//2):
    t = cipher[2*i+1]
    cipher[2*i+1] = cipher[2*i]
    cipher[2*i] = t
print(cipher)
```

得到flag

pwn

whitegive

已经给了c源码 点进去查看 发现只要输对 passward的地址就可以得到flag

Crypto

まひと

用Editor打开 发现是摩斯密码 在线解密 得到一个个数字 是ascii码 再转换后得到 Vigenere-Liki:}VkmvJb!1XtAxe!hpM1{M+9xqzrTM_Nj~cRg4x 根据提示 维基利亚 搜索大概了解了一下编码过程

找了个在线解码 根据liki秘钥得到 }KccnYt!1NlPpu!zeE1{C+9pfrhLB_Fz~uGy4n

根据hint的提示 感觉还是需要栅栏凯撒

爆破解码后得到flag

Misc

Base全家福

隔着base64 32 16混合解码得到flag

不起眼压缩包的养成的方法

Editor打开拉到最底下发现有plain.zip 以及 Password is picture ID 改其后缀名.zip得到压缩包

上网搜索图片id，解压可得发现nopassword.txt 和 plain.zip

打开plain.zip 仍需要密码 根据no password提示 以及都存有no password.txt 其CRC32均相同

采用明文破解

不过在将no password压缩要注意 采用 storage压缩 不然不行 (在这卡了好久，问了Akira瞬间明白)

之后又有一个flag.zip

用Editor打开 是各个字符ascii的十六进制 复制解决得到flag

Galaxy

浏览了往年的题目 找到一些思路

首先收到.pcapng文件

用wireshark打开找到了galaxy.png

打开确实是单纯的星空壁纸

后来百度 了解可能改了实际的长宽显示不全(会导致在linux等打不开来检验) 确实这样 网络找了个python脚本算了实际的长 修改后得到flag

hgame{Wh4t_A_W0nderful_Wallpaper}

word：re

得到两个docx文档 根据第一个 先单纯的搜了一串 得到萦绕耳畔的美妙音乐

而后用Editor打开发现PK 修改后缀zip得到 password后根据brainfxxk解码 得到密码：DOYOUKNOWHIDDEN?

打开第二个文件 根据画面提示snow解码 去google搜到snow， 下载snow.exe 将下面空白与tab键的组合解码

得到flag