

HGAME 2021 WEEK 1 WRITE UP

Web

Hitchhiking_in_the_Galaxy

抓个包，可以看到：

请求

Raw 头 Hex

```
GET /HitchhikerGuide.php HTTP/1.1
Host: hitchhiker42.0727.site:42420
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4324.146
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange,v=b3;q=0.9
Referer: http://hitchhiker42.0727.site:42420/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

响应

Raw 头 Hex HTML Render

```
HTTP/1.1 302 Found
Date: Sat, 06 Feb 2021 02:50:35 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: index.php
Content-Length: 277
Connection: close
Content-Type: text/html; charset=UTF-8

<html><head><title>405 Method Not Allowed</title></head>
<body> bgcolor="white">
<center>
  <h1>405 Not Allowed</h1>
  <p>顺风车不是这么搭的</p>
</center>
<br>
<center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
```

改方式为post，再按题目提示依次修改头部内容得flag：

请求

Raw 头 Hex

```
POST /HitchhikerGuide.php HTTP/1.1
Host: hitchhiker42.0727.site:42420
Upgrade-Insecure-Requests: 1
User-Agent:Infinite Improbability Drive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange,v=b3;q=0.9
Referer: https://cardinal.ink
X-Forwarded-For:127.0.0.1
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

响应

Raw 头 Hex Render

```
HTTP/1.1 200 OK
Date: Sat, 06 Feb 2021 02:52:42 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 62
Connection: close
Content-Type: text/html; charset=UTF-8

hgame(s3Cret_0f_HitCHhiking_in_the_GAI@xy_i5_d0nT_p@nic!)
```

watermelon

f12打开控制台，看到主函数在project.js里，找了很久，在一个函数里发现这样一段：

singleColor.png share.jpg loading.gif project.js > 了解更多信息

要优质打印此缩小的文件吗? 优质打印 不再显示

```

2076     t = e.substring(0, e.lastIndexOf("//") + 2),
2077     n = window.location.host,
2078     o = t + n + "/Service/Share/index";
2079     this.gameAllHttp = o, cc.log("gameAll", this.gameAllHttp), this.s
2080     var c = document.URL,
2081         a = 0,
2082         i = c.substring(c.lastIndexOf("/game/") + 1, c.length).split(
2083         i.length >= 2 && (a = i[1]), this.gameHttpId = a, cc.log("gameId"
2084         e.substring(e.lastIndexOf("//") + 4, e.lastIndexOf("com") + 3));
2085     this.moreGameUrl = "http://m.wesane.com/"
2086   },
2087   gameOverShowText: function (e, t) {
2088     if(e > 1999){
2089       alert(window.atob("aGdhbWV7ZG9fFeW91X2tub3dfY29jb3NfZ2FtZT99"))
2090     }
2091     // this.ajaxLoad("http://www.wesane.com/admin.php/Gamescore/saveC
2092   },
2093   gamePV_load: function () {
2094     this.ajaxLoad("http://www.wesane.com/admin.php/Activityshow/gameI
2095   },
2096   ajaxOnLogoResult: function () {
2097

```

A B gameovershow 3 四配 取消

base64解码后得到flag

宝藏走私者/走私者的愤怒

按照题目给的资料，发现是http走私问题。

于是构造如下：

```

HTTP/1.1 200 OK
Server: ATS/7.1.2
Date: Sat, 06 Feb 2021 02:57:54 GMT
Content-Type: text/html; charset=UTF-8
Age: 0
Connection: keep-alive
Content-Length: 904

<!DOCTYPE html>
<html>
<head>
<title>SECRET SERVER</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0">
<link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
<!-- If It IE -->
<script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
<script src="https://oss.maxcdn.com/respond/1.4.0/respond.min.js"></script>
</head>
<body>
<script src="https://code.jquery.com/jquery.js"></script>
<script src="js/bootstrap.min.js"></script>

<br><div class="alert alert-success" style="width: 80%; max-width: 800px; min-width: 50px; max-height: 1600px; min-height: 50px; margin: 100px auto auto; display: block; float: none; text-align: center;">
>WELCOME LOCALHOST. HERE IS THE SECRET:<br>hgame(HTp+sMUG9HnG45-r3atty-d4nG3r0Us!)</div>

```

第二题与之前题构造一致，但开始不知道为什么得不到flag，后来突然又可以了。。。

智商检测鸡

看题目应该要写脚本，但仍存在以下问题：

- 1.在什么地方提交答案？ 后来学长提醒我抓包看一下，于是找到answer这个东西
- 2.提交answer的格式是什么？ 最后经学长提醒是json格式
- 3.如何更新数据？ 抓包发现是给了一个新cookie

最终python脚本：

```
newcookies='eyJzb2x2aw5nIjoxfQ.YBdjLA.XgHwU8KEynA3_wFM0NiOTHw_bAk'
while 1:
    import requests
    from requests.cookies import RequestsCookieJar
    import json
    url="http://r4u.top:5000/api/getQuestion"
    headers =
    {'Content-Type': 'application/json; charset=UTF-8',
     'User-Agent': 'Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/88.0.4324.104 Safari',
     'Cookie': 'session='+newcookies}
    r = requests.get(url,headers=headers)
    firstIndex = r.text.find('<math>')
    lastIndex = r.text.find('</math>')
    str1 = r.text[firstIndex:lastIndex]
    s=0
    t=[0]*10
    num=0
    while str1.find('<mn>',s)>=0:
        index1=str1.find('<mn>',s)
        for i in range(index1+3,index1+10):
            if (str1[i]>='0') and (str1[i]<='9'):
                t[num]=t[num]*10+int(str1[i])
        if (str1[index1-6]=='-'):
            t[num]=-t[num]
        num=num+1
        s=index1+1
    answer1=t[2]/2*t[1]*t[1]+t[3]*t[1]-t[2]/2*t[0]*t[0]-t[3]*t[0]
    answer = ('%.2f'%answer1)
    url="http://r4u.top:5000/api/verify"
    q = requests.post(url, headers=headers, data=json.dumps({'answer':answer}))
    for (name, cookie) in q.cookies.items():
        print (name, cookie)
    newcookies=cookie
    print(q)
    print(newcookies)
    print(answer)
```

Misc

Base全家福

签到题！感动=.=

拿编码去base64、32、16解码得flag

不起眼压缩包的养成的方法

下载图片，binwalk+foremost一波得到图片和压缩包。

记事本打开图片，发现提示：压缩包密码是pixiv ID。

上p站找一波后解压压缩包，发现NO Password.txt，并发现可以明文攻击。

用ARCHPR明文攻击，开始不成功，发现是没注意hint，应用储存方式加密txt。

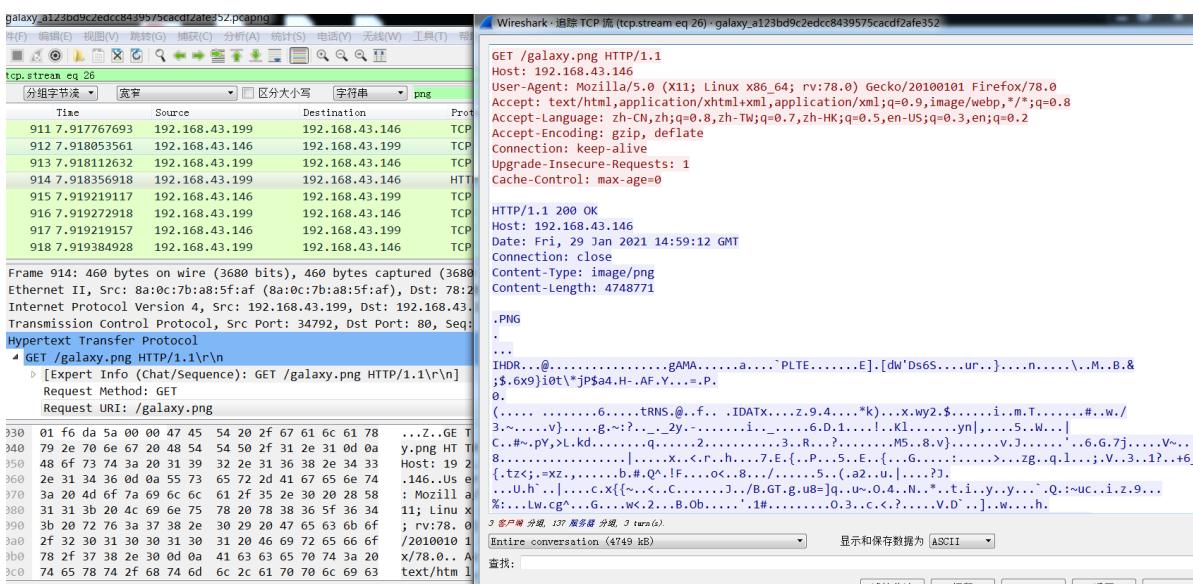
打开后发现还有压缩包，怀疑是伪加密，直接记事本打开，发现一串html编码。

解密得：

hgame{2IP_is_Useful_and_Me9umi_i5_W0r1d}

Galaxy

下载后用wireshark打开，并搜索png文件



以原始数据存储，并删掉头部得到png文件。

发现png文件用kali打不开，怀疑修改了图片大小。

在网上搜了脚本

```
import os
import binascii
import struct

crcbp = open("666.png", "rb").read()      # 打开图片
crc32frombp = int(crcbp[29:33].hex(), 16)  # 读取图片中的CRC校验值
print(crc32frombp)

for i in range(4000):                      # 宽度1-4000进行枚举
```

```
for j in range(4000):    #高度1-4000进行枚举
    data = crcbp[12:16] + \
        struct.pack('>i', i)+struct.pack('>i', j)+crcbp[24:29]
    crc32 = binascii.crc32(data) & 0xffffffff
    #print(crc32)
    if(crc32 == crc32frombp):      #计算当图片大小为i:j时的CRC校验值，与图片中的CRC比较，当相同，则图片大小已经确定
        print(i, j)
        print('hex:', hex(i), hex(j))
```

跑出实际大小，stegsolve修改得：



hgame{Wh4t_A_W0nderful_Wallpaper}

Word RE:MASTER

把first修改为zip格式，打开后发现password.xml，并将内容brainfuck解码

```
+++++ +++[- >++++ +++< ]>+++ +. <++ +[>+ ++<]> ++.  
<+ ++[> +++<] >+. <+ ++[> ---<] >-. ++ +++. <+++[ -  
>--- <]>-. ++++. + .++++ +++. <+++[ ->--- <]>-- ----.  
+. ---- --.. + .++++ +++++. <+++ [ ->-- -<]>-- ----- .<
```

code execute clear

input: DOYOUKNOWHIDDEN?

output clear

获得密码打开第二个docx，打开隐藏文字和字符，发现用tab和space写的内容。

开始以为是whitespace，后来学长提醒图片是hint，于是发现snow隐写，解密得flag。

Crypto

做不出，实在做不出:(

Transformer

水一道最简单的题。。

发现txt内容符合词频统计，解密得flag(在最后加入年份)