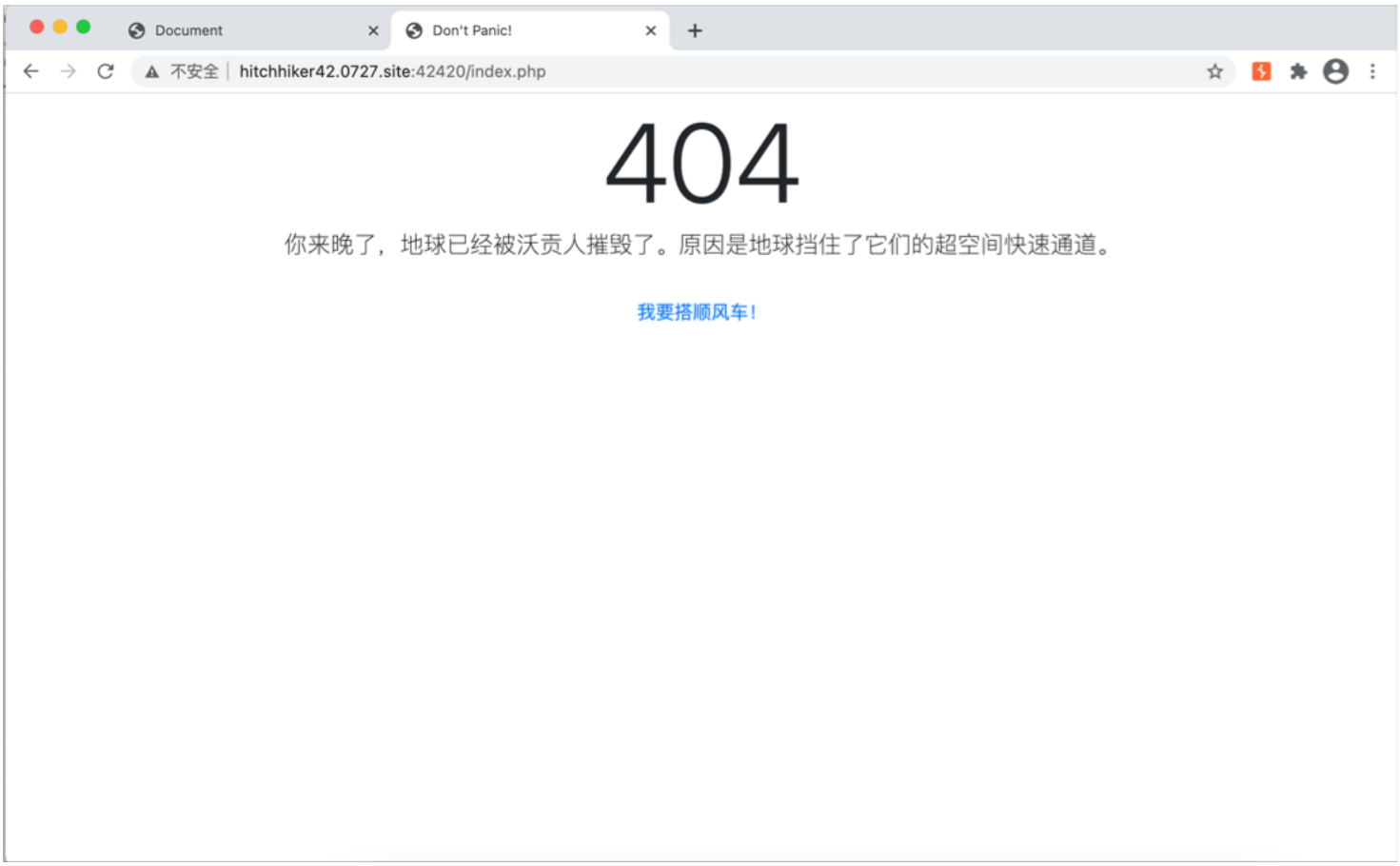
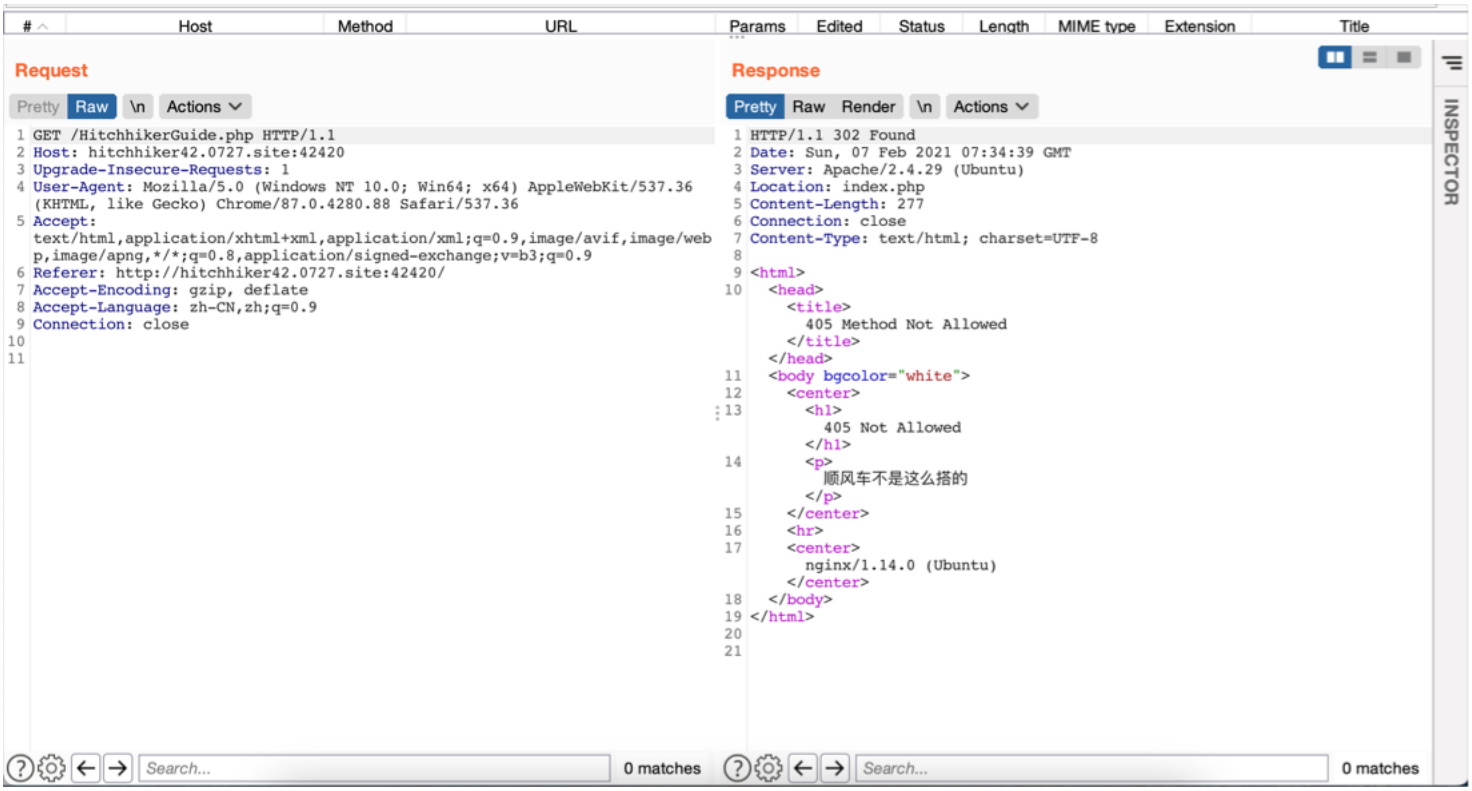
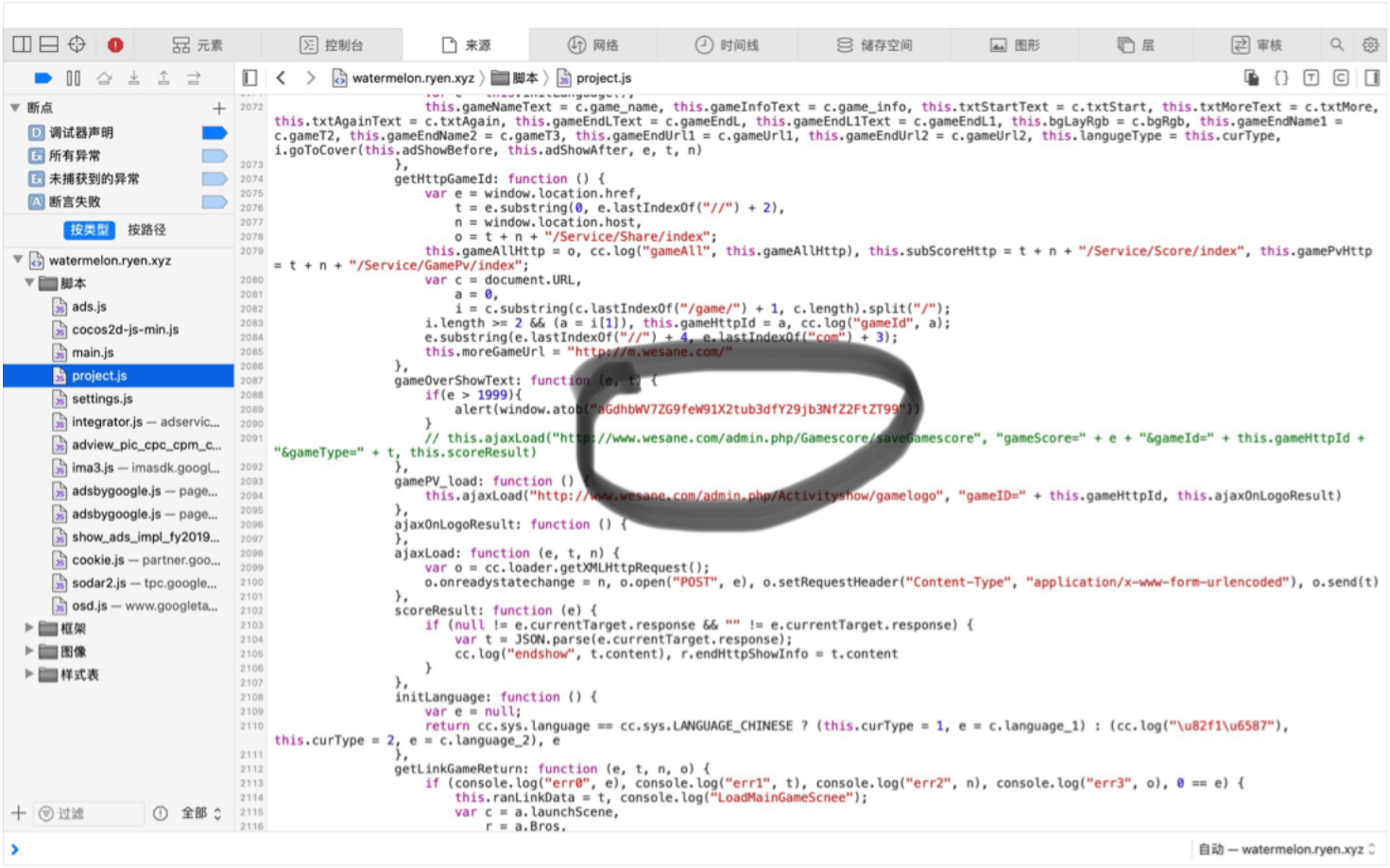
WEB

第一题，访问得到该页面。点超链接没反应，打开 bp 发现是 302 临时重定向，改为 post，加 referer 头，一波操作得到 flag。





第二题，是一个js写的小游戏，玩游戏过程中没有任何拦到任何http请求，那么flag一定在js代码中，仔细阅读得到。经base64解码得到flag。

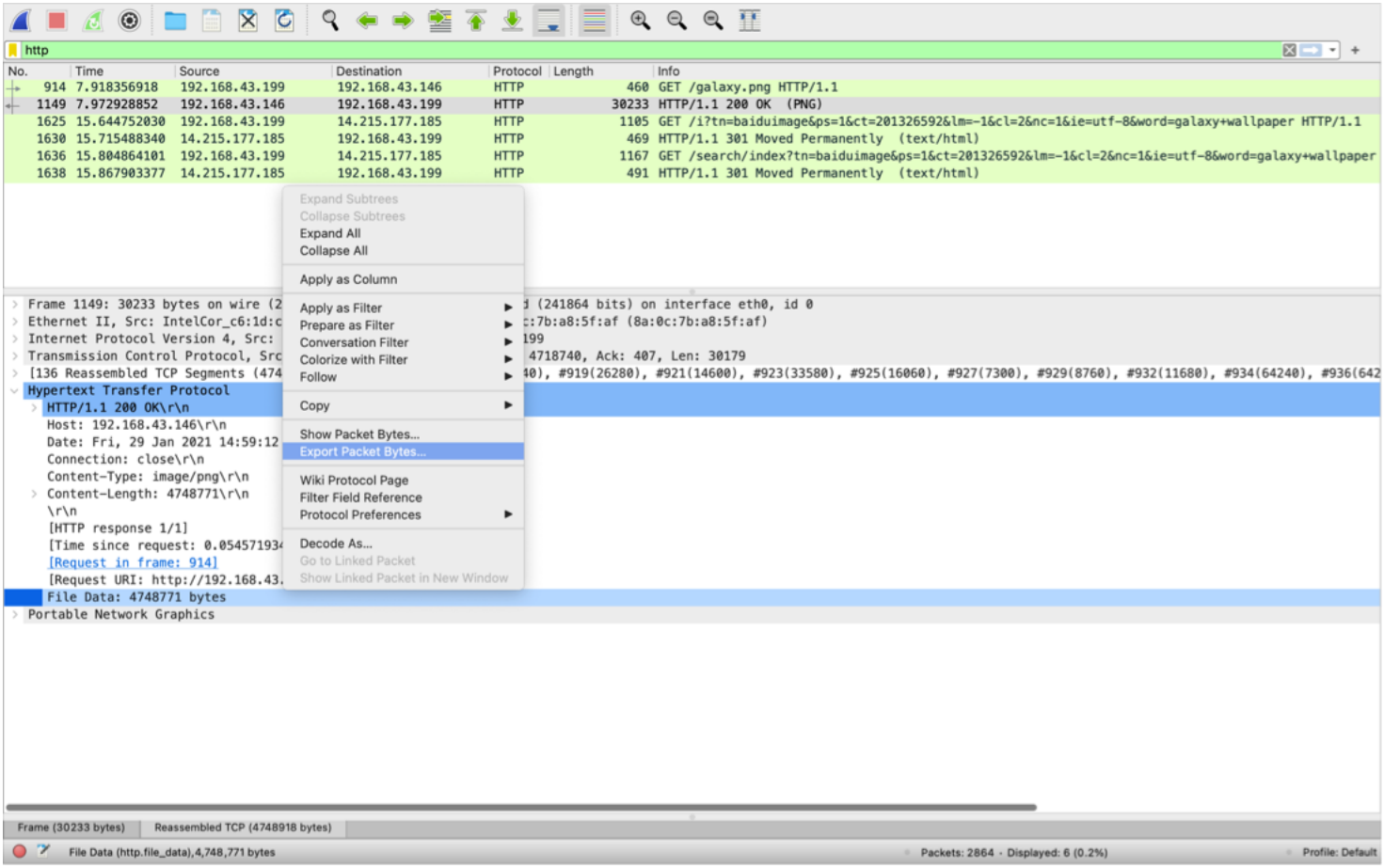


第四题，做完了一百道高数题得道flag。考点应该是cookie伪造，只知道前面一段是base64码，后面的加密手段没有解出来，不影响拿flag。

MISC

第一题，依次经过base64，base32，base16解码，得到flag。

第三题，从wireshark导出目标文件，发现打不开，用pngcheck，得知crc32不正确，应该是图片的大小被改了，用一个python程序算出原图的实际大小，修改，图片打开成功，flag就在最下面，可是1和l竟然分不清，提交的时候出了问题。


http
No. Time Source Destination Protocol Length Info
914 7.918356918 192.168.43.199 192.168.43.146 HTTP 460 GET /galaxy.png HTTP/1.1
1149 7.972928852 192.168.43.146 192.168.43.199 HTTP 30233 HTTP/1.1 200 OK (PNG)
1625 15.644752030 192.168.43.199 14.215.177.185 HTTP 1105 GET /i?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=galaxy+wallpaper HTTP/1.1
1630 15.715488340 14.215.177.185 192.168.43.199 HTTP 469 HTTP/1.1 301 Moved Permanently (text/html)
1636 15.804864101 192.168.43.199 14.215.177.185 HTTP 1167 GET /search/index?tn=baiduimage&ps=1&ct=201326592&lm=-1&cl=2&nc=1&ie=utf-8&word=galaxy+wallpaper
1638 15.867903377 14.215.177.185 192.168.43.199 HTTP 491 HTTP/1.1 301 Moved Permanently (text/html)
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes...
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Frame 1149: 30233 bytes on wire (2
Ethernet II, Src: IntelCor_c6:1d:c
Internet Protocol Version 4, Src:
Transmission Control Protocol, Src
[136 Reassembled TCP Segments (474
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
Host: 192.168.43.146\r\n
Date: Fri, 29 Jan 2021 14:59:12
Connection: close\r\n
Content-Type: image/png\r\n
Content-Length: 4748771\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.05457193
[Request in frame: 914]
[Request URI: http://192.168.43.
File Data: 4748771 bytes
Portable Network Graphics
Frame (30233 bytes)
Reassembled TCP (4748918 bytes)
File Data (http.file_data),4,748,771 bytes
Packets: 2864 · Displayed: 6 (0.2%)
Profile: Default

通过crc32算图片尺寸.py

使用 Xcode 打开

```
import os
import binascii
import struct

crcbp = open("/Users/tianyuzhan/Downloads/asqw.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(10000):    #宽度1-4000进行枚举
    for j in range(10000):   #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))
```