Week1 WriteUp —— NightChampagne

总结：在hgame的第一周里，我只做出了四道题ε=(´ο｀*)))唉~（准确来说是三道。。。），虽然很多题有思路，但却因为在中间某个位置卡住而不了了之。还是简单说一下做出来的和有点思路的题目吧。

Web

Hitchhiking_in_the_Galaxy

web 的第一题，最开始按 F12 之后完全不知道从何下手

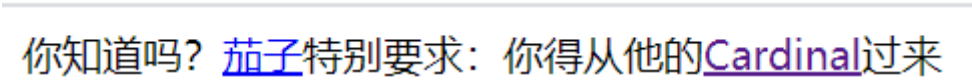
```
<html>
    <head>
        <link href="//maxcdn.bootstrapcdn.com/bootstrap/4.1.1/css/bootstrap.min.css" rel="stylesheet" id="bootstrap-css">
        <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/3.2.1/jquery.min.js"></script>
        <title>Don't Panic!</title>
        <!------ Include the above in your HEAD tag ---------->
    </head>
    <body>
        <div class="page-wrap d-flex flex-row align-items-center">
            <div class="container">
                <div class="row justify-content-center">
                    <div class="col-md-12 text-center">
                        <span class="display-1 d-block">404</span>
                        <div class="mb-4 lead">你来晚了，地球已经被沃贡人摧毁了。原因是地球挡住了它们的超空间快速通道。</div>
                        <a href="HitchhikerGuide.php" class="btn btn-link">我要搭顺风车！ </a>
                    </div>
                </div>
            </div>
        </div>
    </body>
</html>

```

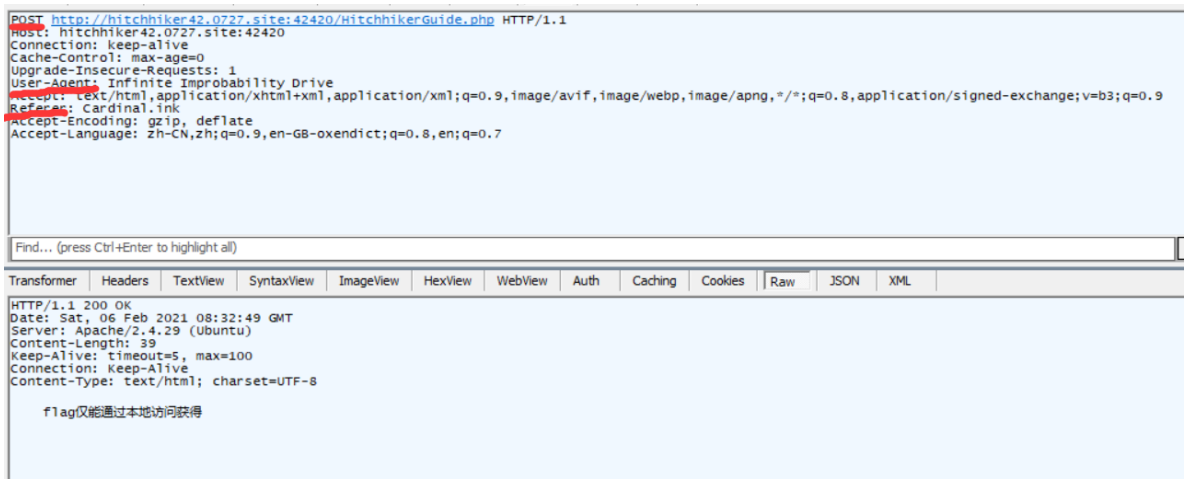
找了 Web 方面的题看了下，在网上下载了一个抓包工具 Fiddler 。学习了一下之后进行抓包。

之后也是没什么思路，后来我注意到返回值是 302，说明被转换了，联系到下面的 405，上网查看了一下是请求方式不对。不过也不知道具体应该怎么改。按照例题上把 GET 改成了 POST，竟然误打误撞对了。

看到只有用所谓的“无限非概率引擎才能访问”，想了下应该是更改报文头的 User-Agent 部分（毕竟是搜索引擎嘛），而后又有了新的要求：



点击 Cardinal，进入一个网站，将网址复制下来，替换掉 Referer 部分。还有最后一个要求：flag仅能通过本地访问。



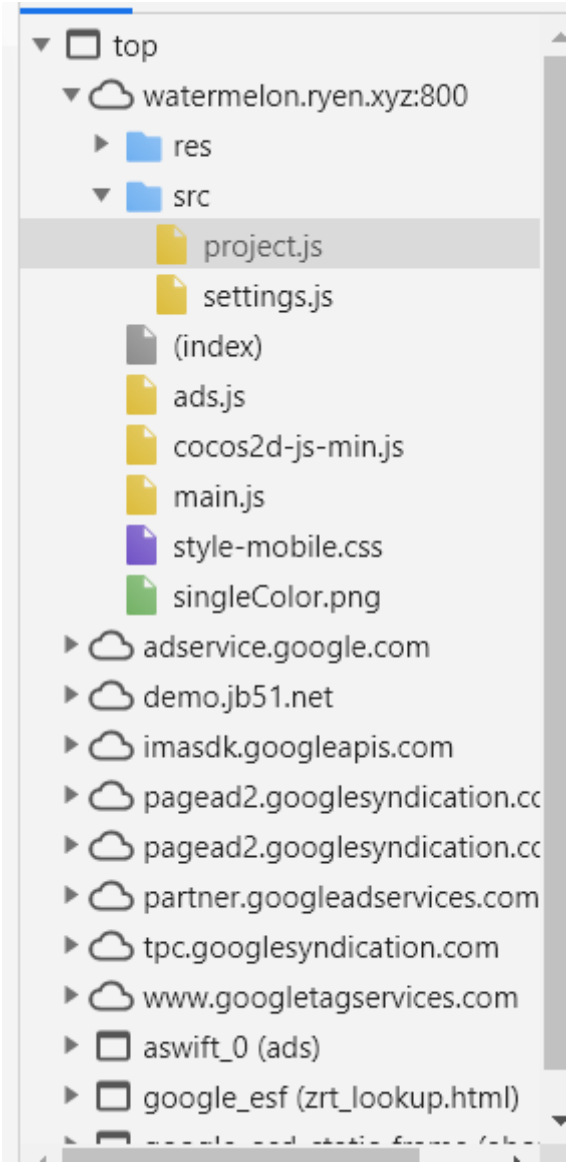
在百度上搜索一番可以知道用 Client-IP 或者 X-Forwarded-For 进行伪装。不过我一直以为是要拿到服务器那边的 IP 地址，被 0x4qE 学长指点之后重新看了一下本地访问的定义，又看了看类似的题目，应该是直接跟 127.0.0.1。重新更改报文之后，拿到 flag。

watermelon

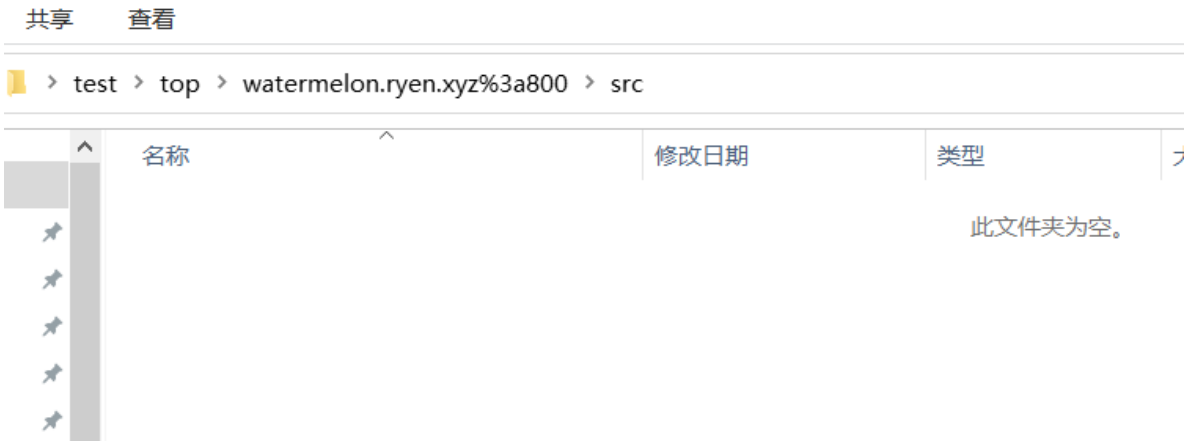
合成大西瓜是一道游戏题，打到 2000 分就可以拿到 flag 。试了几次，发现很困难，大概要两个西瓜多一点才行。于是想到能否更改游戏呢？经过多次尝试和网上搜索之后，发现大西瓜的核心程序在 project.js 里面，在谷歌浏览器中打开 F12，在Sources -> Page里面进行查看，之后经过一番查找在 3436 和 3440行找到了想要的代码

```
a.default.score += this.fruitNumber + 1;
```

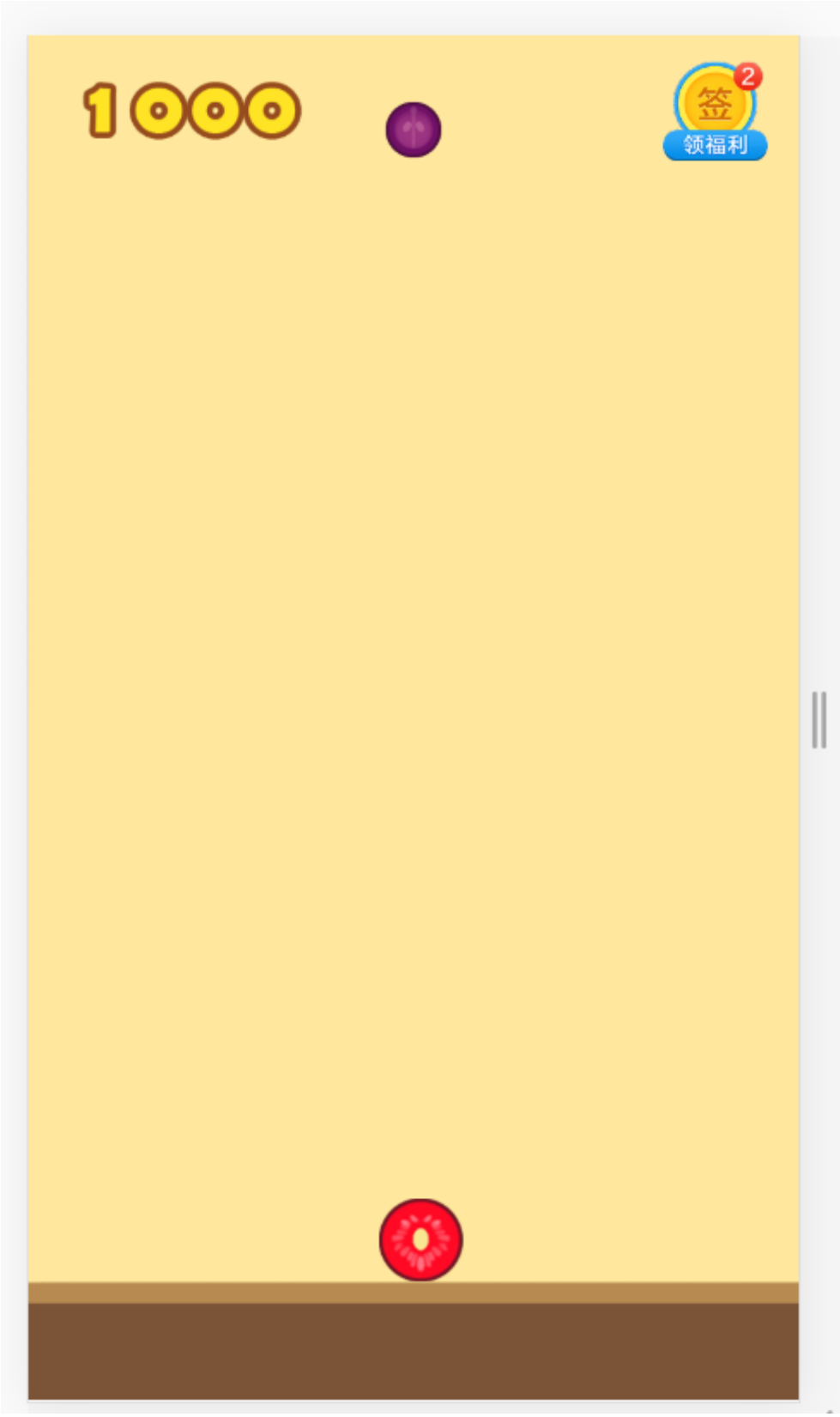
然后只要将 1 改成大一点的数字就可以轻松过关了。有一个方法是在桌面创建一个文件夹，里面按照Sources里面的路径：



创建对应的文件夹（top 外面一层文件名任意；创建文件夹时:为不可用字符，使用 %3a 代替）：



然后在 F12 界面右击 project.js,选择 save for overrides 即可发现我们创建的文件夹对应的目录下有了一个名为 project.js 的 JavaScript 文件，这时便可以对网页进行修改了。修改完成后 Ctrl + S保存之后刷新页面就可以~~来一局轻松的大西瓜~~拿到flag了。



宝藏走私者

这道题我最开始没有看到资料导致弄了半天不知道为什么不能伪造IP地址。不过看了资料也没什么帮助。。。大致明白了HTTP走私攻击的意思，但实际操作起来总是不对。。。ε=(´ο｀*))唉，等着看看其他人的 WriteUp 吧。

智商检测鸡

这道题严格意义上我并没有做出来，现在想起来应该跟第一，第二题有相似的地方吧？（纯属猜测）不过区区 100 道定积分而已，拿出计算器十来分钟就算完了，拿到 flag。

走私者的愤怒

第三题都没做出来第五题作为第三题的升级版更是没戏了，ε=(´ο｀*)))唉。

Reverse

没怎么看 Reverse 的题，而且我下载 IDA 时好像出现了什么问题，看 CSDN 上面的文章也不是很懂，IDA 也不会用，看着这些题只能一声长叹(╥╯^╰╥)

Pwn

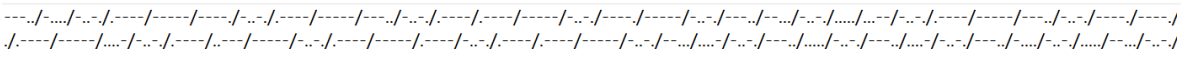
Pwn 的处境比 Reverse 更糟糕，我看了语神的博客，却好像根本看不懂，连一些相关的环境和工具也不知道，似乎完全没有进步。

Crypto

まひと

这道题做了一些步骤吧，题目的意思不是很懂，没看过咒术回战。缝合怪的话，或许最后是好几种加密方式混合的?

首先打开文件，肯定是摩斯电码



将其放到在线翻译器下面进行翻译：

这次应该是大致看一下可以确定应该是 ASCII 编码（因为其对应大部分的字符也落到了英文字母区，加深了我的判断）//这里的图找不到了，我记得我是手写转换的

大部分都是英文字母，唯独最后两位是'='，联想到可能是 base64 编码，试了一下，得到：

Vigenere-Liki:}VkmvJb!1XtAxe!hpM1{M+9xqzrTM_Nj~cRg4x

因为出题人是Liki姐姐，Vigenere 又是另一种密码，应该没问题。

因为最后的形式是 hgame{xxxx} 的形式，我把第一位的 } 移到了最后。Vigenere 密码需要秘钥，我输入了 Liki，得到了我的最终结果，但之后没有什么头绪了，可能是}不应该移位而用其它方法？还是没问题要把密文拆成几部分分别解密？'!','_','~'和数字是什么意思，是密文的一部分还是暗示？（我还想过数字是凯撒密码的暗示）暂时就不得而知了，放出我的最后结果：

对称之美

这道题看题面应该是对称加密，但我下载的Python好像有点问题，加上我没有Python的基础，看了一下注释里的 cipher 好像也是一种编码方式。暂时没有做了。

Transformer

这道题看完成人数应该是比较简单的一道题，但我确实觉得没有头绪，附件上的字符串应该是md5的编码形式，但我没有解出来，网上的在线转换器也没给出答案。

Misc

base全家福

应该是最简单的一道题了，将密文按照 base64，base32，base16 依次解密便可得到明文，不多赘述了。

不起眼的压缩包的养成方法

这道题应该是图片隐写术的题，奈何不知怎么回事，我的电脑就是下载不了 binwalk，Windows 和 Ubuntu 都不行，ε=(´ο｀*))唉~，用 winhex 看到图片最后有 PASSWORD IS ID 的提醒，又用 Stegsolve 里面的 Data Extract 功能试了一下。后来上网看了下类似的题，我的感觉是这道题用 binwalk 分出一个需要密码的文件，然后在网络上（有人说的 P 站是啥(⊙_⊙)?）找到这张图片出处的 ID 打开可得 flag。

Galaxy

这道题没有看过，不过我想还是图片隐写一类的题。

Word RE：MASTER

这道题给了两个 word 文件，其中一个有密码。最开始我以为应该是第一个文件里的那串我看不懂的字符串应该是密文一类的东西，后来感觉好像又不是（音游是啥啊(⊙_⊙)?）。既然如此呢便想到能否暴力破解或者是绕过第二个文件的密码？网上下载的 Fastreader 和 Advanced Office Password Recovery 效果都不是很理想，说实话我也不清楚到底怎么做了。。。