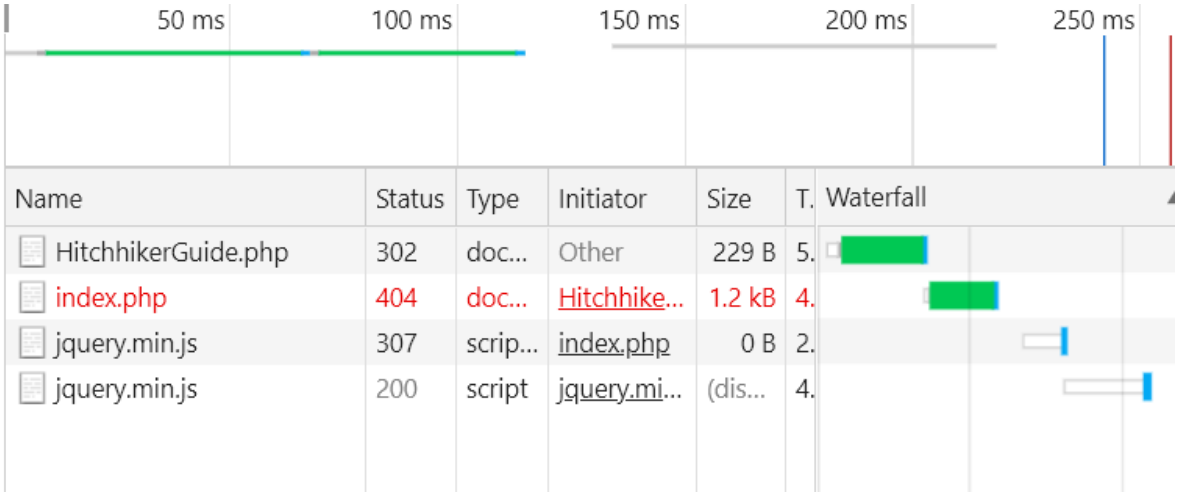
HGAME 2021 Week 1 Writeup

Web

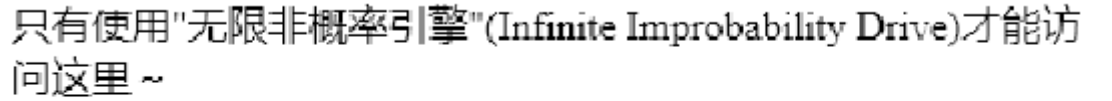
Hitchhiking_in_the_Galaxy

打开界面后发现出现404字样以及一个链接，点击链接后发现 URL 改变但是页面显示信息并没有变化，按照惯例打开 Network 发现跳转的 302 状态的文件。



使用 Burp suite 抓包后发现出现新界面。

405 代码应该是请求方法不对，于是改用 POST 方法再次尝试。



提示使用无限非概率引擎才能访问，于是改变 User-Agent 再次访问 。

```
HTTP/1.1 200 OK
Date: Sat, 06 Feb 2021 16:01:16 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 148
Connection: close
Content-Type: text/html; charset=UTF-8

□□□□□<a href="https://github.com/wuhan005">□□</a>
□□□□□□□□□□<a href="https://cardinal.ink/">Cardinal</a>
□□
```

你知道吗？茄子特别要求：你得从他的Cardinal过来

得到两个网址，做题的时候误以为需要使用第二个网址作为 Referer 访问第一个网址，但是并没有发现有关 flag 的任何信息，最后尝试用第二个网址作为 Referer 访问之前的界面。

flag仅能通过本地访问获得

成功进入下一步，使用 fakeIp 伪造本地访问，最终成功得到 flag。

watermelon

没什么思路，利用大西瓜的特性，修改长宽，玩到2000分得到 flag。

MISC

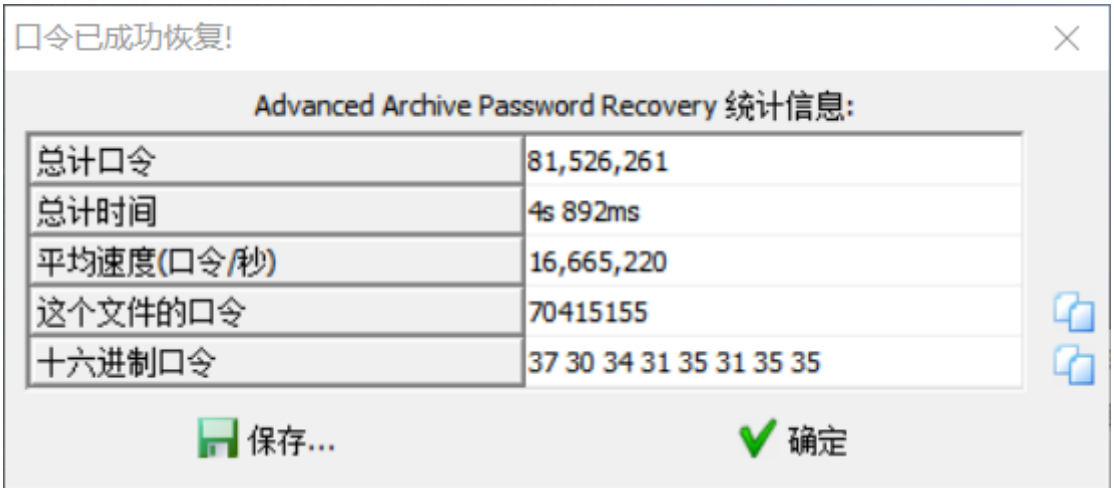
Base 全家福

题目提示是 Base 全家福，那就是 base 编码，观察字符后决定使用 Base64 来解码，同理再经过 Base32 、Base16 解码，得到 flag（可能是给我们这样的菜菜一条活路吧，不至于第一周就被踢出去的题目）。

不起眼压缩包的养成的方法

题目首先给了一张图，题目又提示压缩包养成方法，于是猜测是图片中藏了个压缩包，使用 binwalk 检测后发现确实如此，使用 dd 分离得到加密的压缩包文件。

使用暴力破解



得到文件的密码解密后，得到一个一个名为 NO PASSWORD 的 txt 文件和一个 plain.zip 文件，上网查了一下 plain 的意思发现是直白的。打开 txt 显示 " 有时候我们不需要在意密码，因为它太强或是为空 XD 顺便一提我使用存储 "。

一开始没有什么头绪，于是乎打开 plain 查看内容，发现内部也有一个 NO PASSWORD 文件，于是瞬间顿悟，plain 提示使用明文解密，直接压缩后明文解密报错，想起提到的意义不明的存储，于是使用存储压缩后明文攻击，成功解密，得到了一个名为 flag.zip 的压缩包。

想起后半句话 " 密码为空 " 于是先猜测使用的是伪加密，解密失败。但是在修改过程中发现大段格式相同的字符，使用 unicode 解码后得到 flag。

Galaxy

题目给出了一个流量包，提示一张藏着秘密的星空壁纸，于是过滤 http 请求，发现 Galaxy 的 png 图片，还原得到星空壁纸。感觉长宽比例极其难受，使用 CRC 校验，发现问题，修改长宽得到 flag。

结语

一周的时间没有做什么题目出来，作为一名大二的参赛选手可以说是非常的不应该了，Web实际上只做出来了一道题，高数曾经想用爬虫解决但是 MathML 结点爬取上出现了问题，杂项的最后一道题因为知道 word 文档的本质就直接转换成 zip 解压得到了 password.xml 文件，打开后得到一堆字符，感觉像是 brainfuck 但是无法解码陷入僵局，个人还是很期待能够见到解题过程。Cyrpto 方向也做过一些尝试，但是在 まひと 第一层摩斯电码解码之后就没有什么想法了。

本周的学习没有什么进展，但是感觉好像能感受到 hgame 的乐趣，在希望在接下来的几周之内能够继续这样学到许多知识。