

## WEEK1——Write up

### 一、Web

#### 1. Hitchhiking\_in\_the\_Galaxy

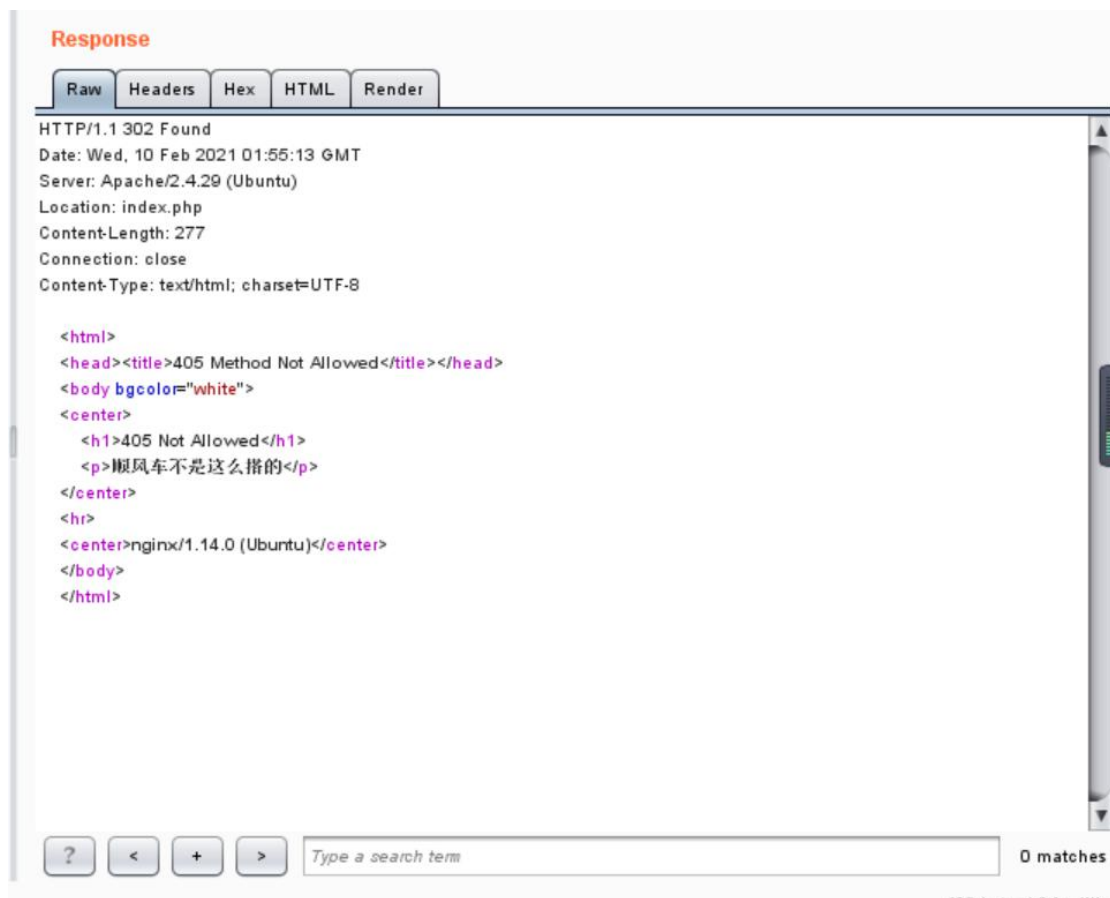
打开链接，界面中要求要搭顺风车。

404

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。

[我要搭顺风车！](#)

但是点击“我要搭顺风车！”没有反应。于是用 burp 抓包。



捕捉到关键信息“405 Not Allowed”，应该是请求头出现了问题，将 GET 改成了 POST，成功跳转到下个界面。



只有使用“无限非概率引擎”才能访问？意思是访问者得用这个“无限非概率引擎”才能访问，于是在 User-Agent 后面加上“Infinite Improbability Drive”，跳转到下个界面。

```
HTTP/1.1 200 OK
Date: Wed, 10 Feb 2021 02:07:31 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 148
Connection: close
Content-Type: text/html; charset=UTF-8
```

你知道吗？<a href="https://github.com/wuhan005">茄子</a>特别要求：你得从他的<a href="https://cardinal.ink">Cardinal</a>过来

一开始看到这个提示的时候，没有任何思路，在看了 http 的知识后，在 Referer，把原来的网址改成了 <https://cardinal.ink/>，来到最后的界面，要求只能本地访问。小 case，只要伪造 ip 就行了，加上 X-Forwarded-For: 127.0.0.1，成功得到 flag。

## 2. Watermelon

用 chrome 浏览器打开大西瓜，进行玩游戏。奈何太菜了，玩不到 2000（得到 flag 的分数）。便打开了 chrome 的开发者工具，在痛苦的浏览了代码后，找到核心 project.js 中的大西瓜碰撞得分的函数，将+1 改成了+2000，分分钟玩到了 80 多万的分数，成功拿到 flag。

## 3. 宝藏走私者

幸运地搭“顺风车”，拿到了 flag。

## 4. 智商检测鸡

观察到定积分“ $ax+b$ ”的规律，因为不会用 python 写脚本，就用 C 语言写了个程序来刷题，

痛苦地输入了差不多 30 分钟的数据，拿到了 flag。

附上 C 语言的代码

```
#include<stdio.h>
int main(void)
{
    double y;
    int x,x1,x2,a,b;
    scanf("%d%d%d%d",&a,&b,&x1,&x2);
    y=(0.5*a*x1*x1+b*x1)-(0.5*a*x2*x2+b*x2);
    printf("%.2f",y);
    return 0;
}
```

## 二、Misc

### Base 全家福

看到题目提供的乱码有大写字母，小写字母和数字，再结合“base 全家福”，明白这是个 base64。于是用 base 解码器依次解码，最终得到 flag。