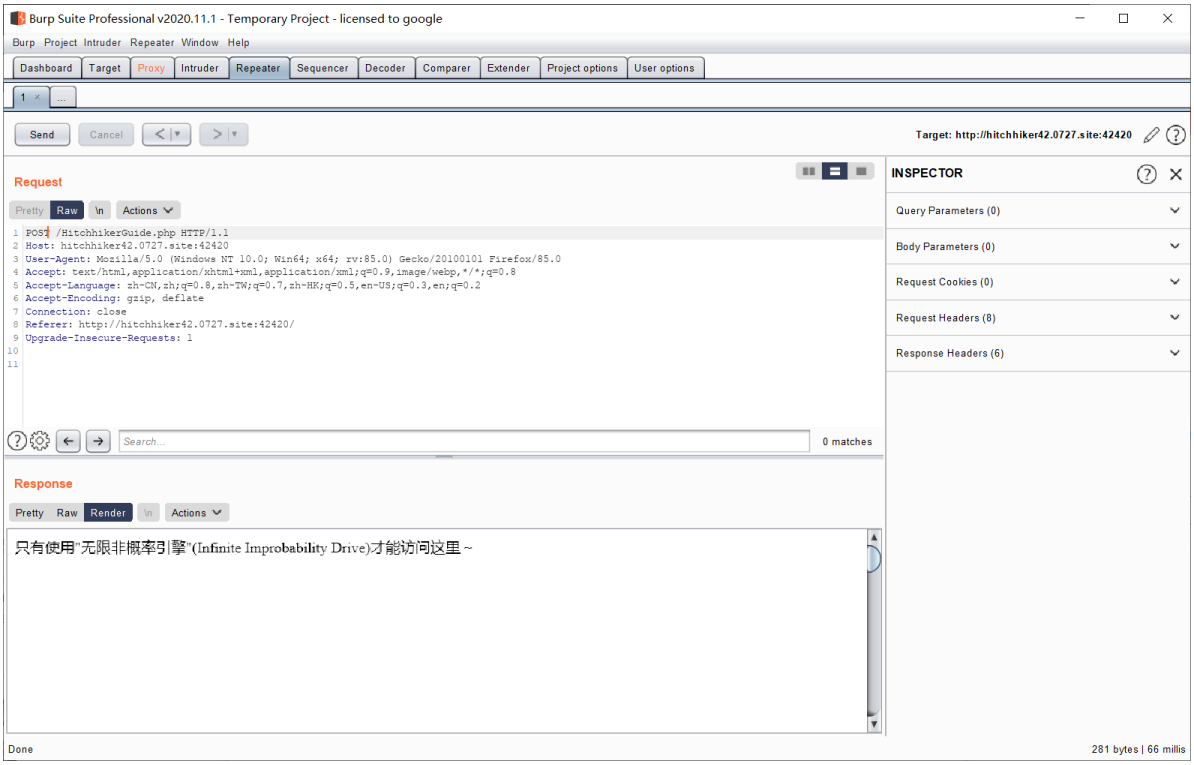
学长们好呀，这里是弱鸡 web 手第一周的 writeup，由于忘记了有 wp，所以没截图，以下全是复现，很多摸索过程有省略和缺失。做题不规范，wp两行泪（哭

一、顺风车

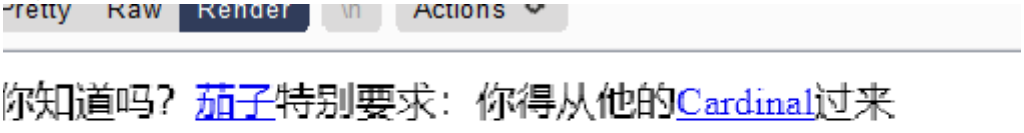
这一题，我先用 Burp Suite 抓包，报文扔进 Repeater send 了一下， response 出来如下

，查了一下 405 错误是 GET 请求错误，将 请求 GET 改为 POST 后，果然出现了下一个提示



看了一下翻译，完全一脸懵逼，不能说是非常有用吧，可以说是与题目毫无关系，看来是玩梗。于是猜测是访问的引擎指的是浏览器不对。查了一下怎么改浏览器来源，找到了这篇文章

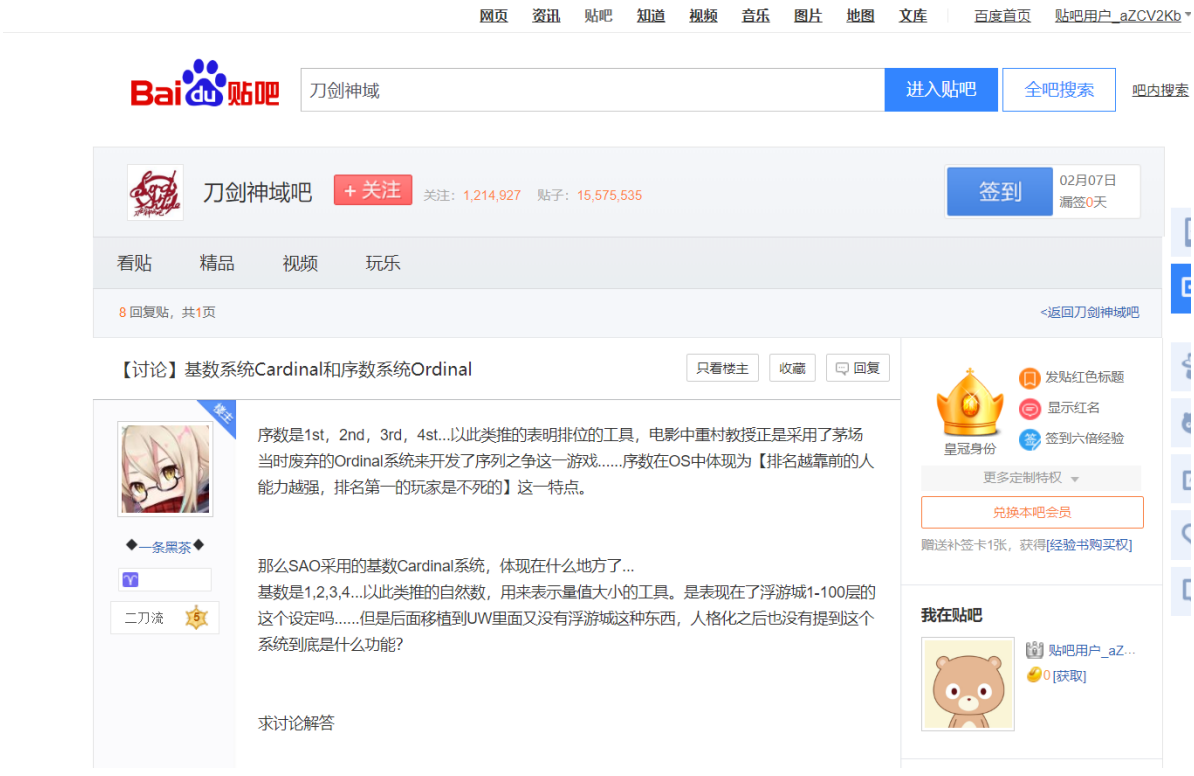
于是找了一下 User-Agent 的用法，将报文中的 User-Agent 那一行改为 User-Agent: Infinite Improbability Drive ,竟然还有

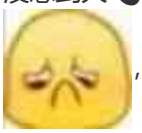


，茄子大大的

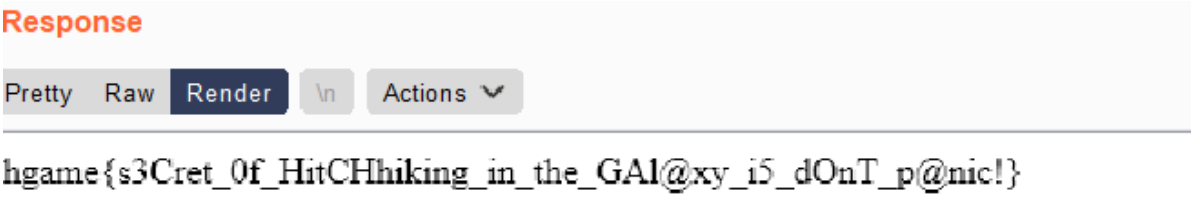
吩咐自然要照做，查了一下 Cardinal 有框架、枢机的意思，但是还是不懂，但突然看到词条下面有这么个东西

然后找到了这个



没想到大🐦是刀剑粉。看来是访问来源不对，于是又去查怎么改访问来源（此步花了我一个下午  ，最后用了手机科学上网 Google 了一下），找到了 Referer 头的用法，然后加上了一个 Referer 头，从 https://cardinal.ink/ 访问，然后发现竟然还有，提示 flag 仅能本地访问获得，于是继续 Google，是访问 IP 不是本地，使用 X-Forwarded-For 可以伪造IP，加上 X-Forwarded-For: 127.0.0.1

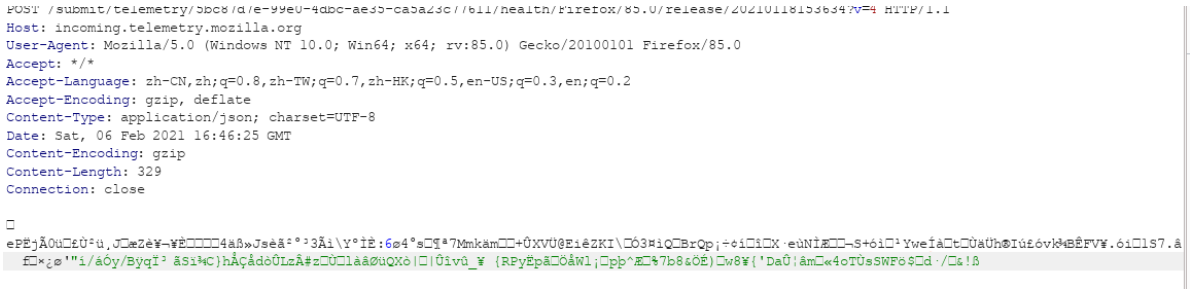
,完美搞定，获得flag一份



二、合成大西瓜

先玩一会大西瓜，随便摆

得出分数然后抓包。本来我觉得这题目就是改一下分数就行了，结果还是加密的



完全找不到分数是哪个，一头雾水。然后完全没办法没思路，知识盲区，只能去看看审查元素，试图找到线索。最后好像找到了一个 score ，但是复现不了了，忘记在哪找到的了，哭。最后刷新网页得到 flag 。

三、求 100 道积分

这一题真的不会写，算完了100道题，写了一个c程序输入参数计算的，得到答案。

四、Base 家族

查了一下 Base 家族，是一种加密方式，于是先丢进 Base 64 解码，然后 Base 32 ，依次往下，最终得出 flag 。