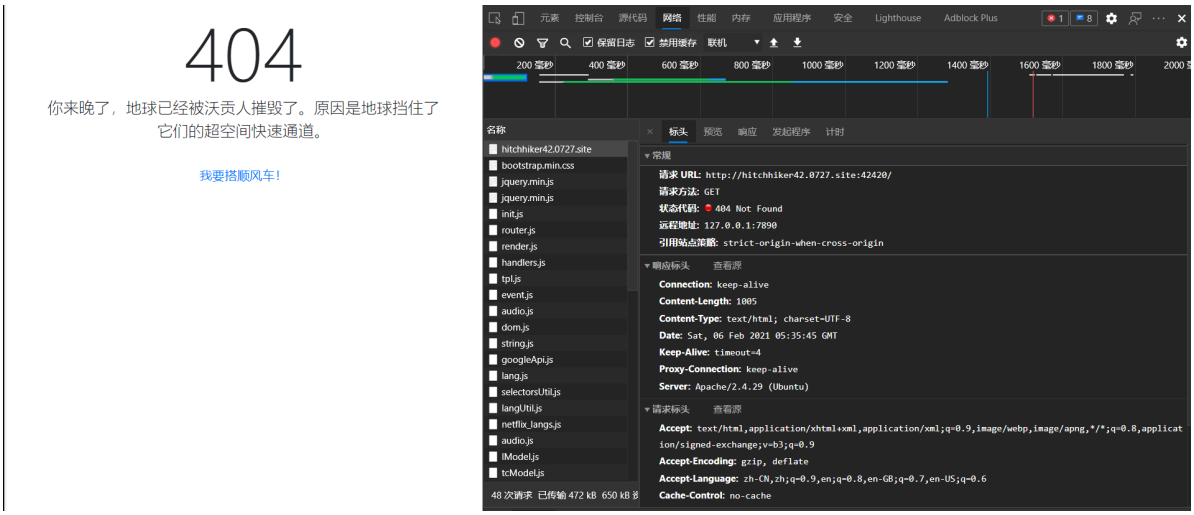
# Week 1 WP

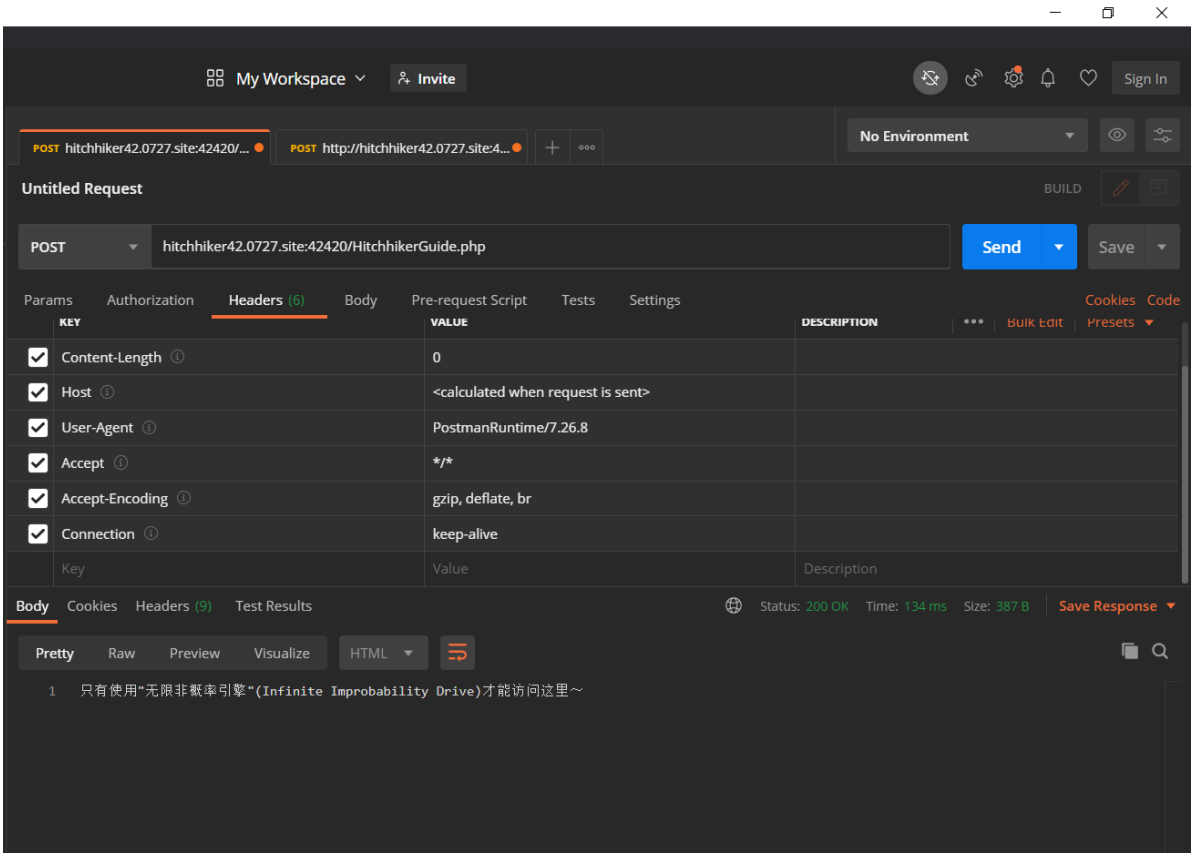
## Web

## Hitchhiking_in_the_Galaxy

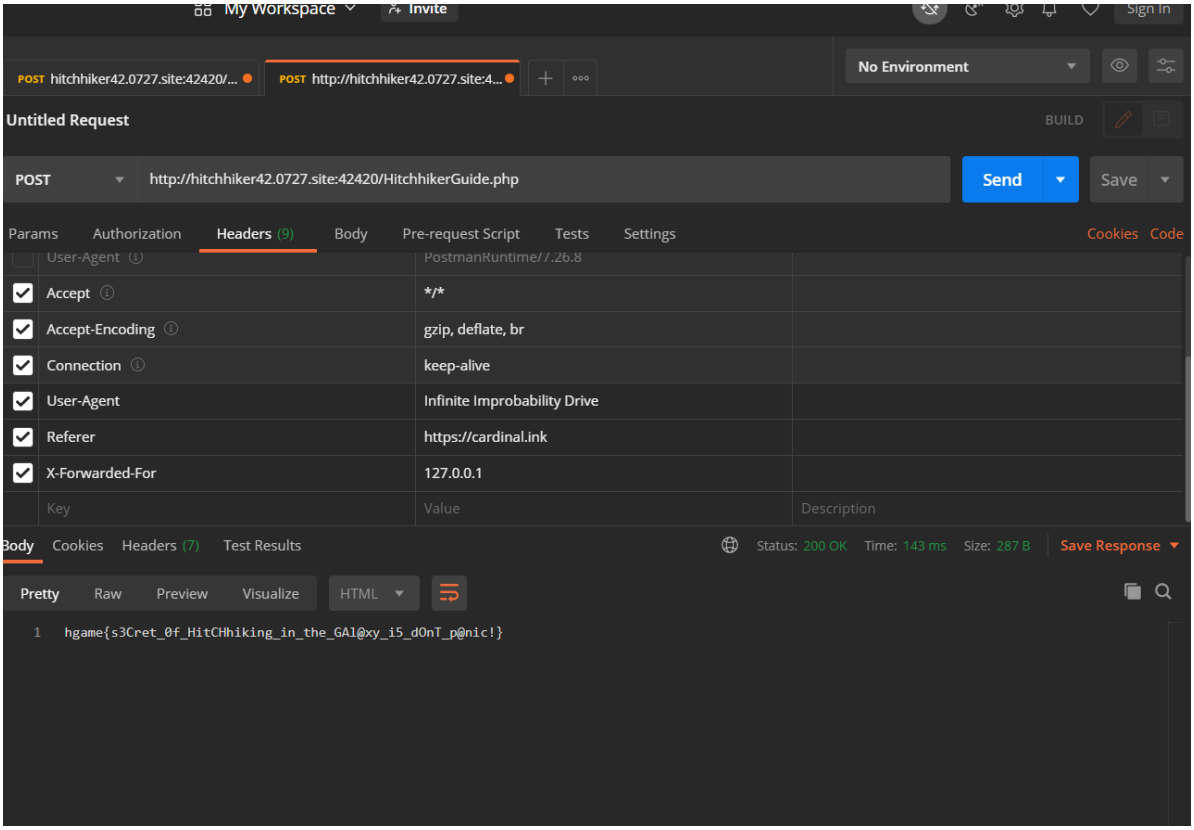



打开题目，发现使用get请求方式404，想到本题考点在于http请求和headers。

然后我们前往源代码中看，发现分隔符上有提示headers，bingo( 明确了 然后下面有一个“HitchhikerGuide.php”的地址，想到将其复制至原url后方 使用postman用POST进行请求，效果如下




提示要使用唯一指定搜索agent，将headers进行修改，进入到下一步（后面的图片就不放上了，发现提示要使用localhost才能进行访问，并且要从大茄子🍆的cardinal.link进行访问，修改X-Forwarded-For和Referer:



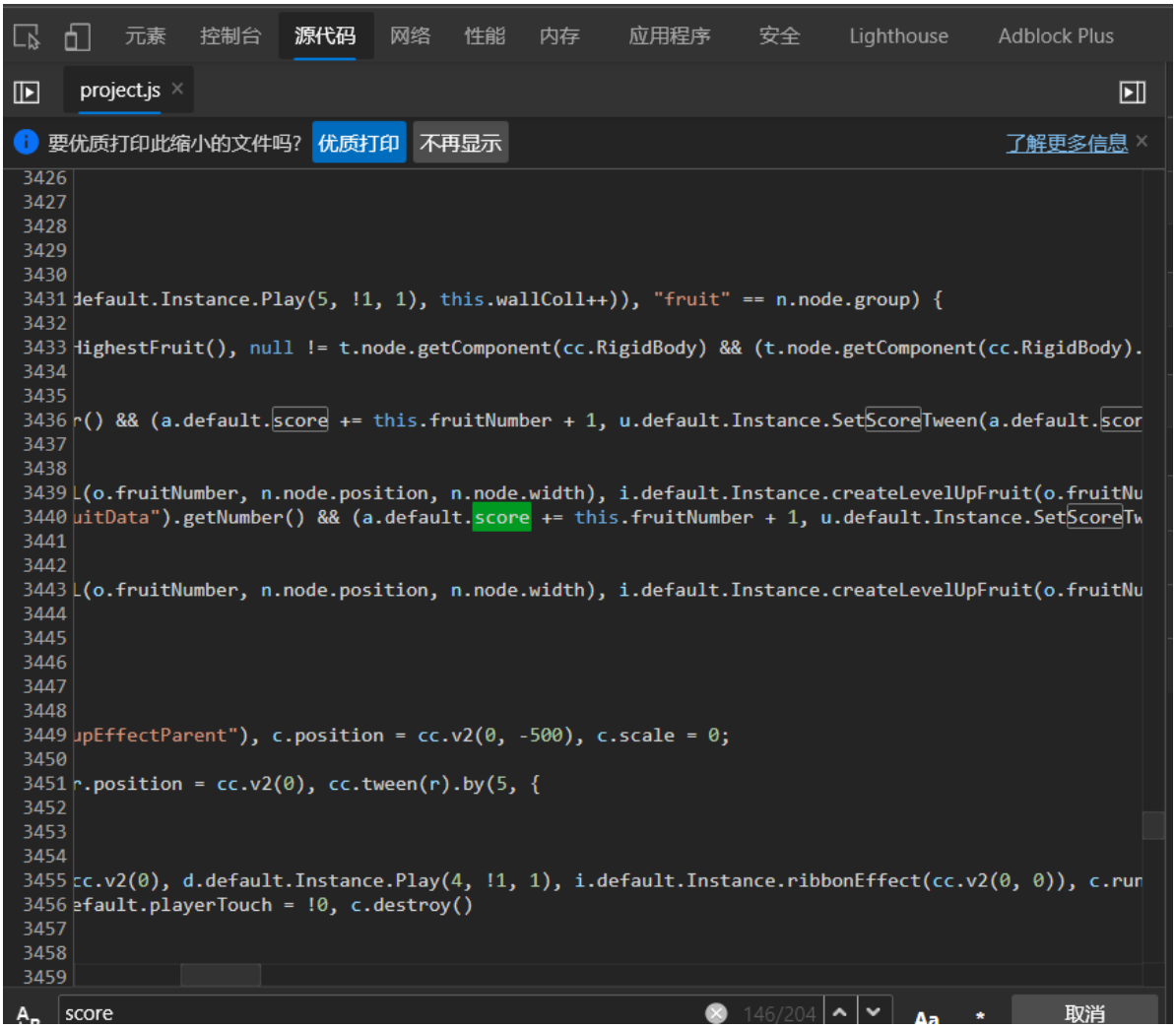

得到flag！ ^_^

# watermelon

这道题是一道非常有意思的题目，而且他的解法也非常多样。

首先，先开始玩，玩着玩着发现死了 eiii~~~，看到提示，超过2000分就可以活得flag。

同样，我们打开控制台，找到源代码，仔细一看，发现控制主算法的程序，名为project.js，随后使用search功能直接搜索"score":




显然，这行代码非常容易理解，将this.fruitNumber + 1改为+2000即可得到flag

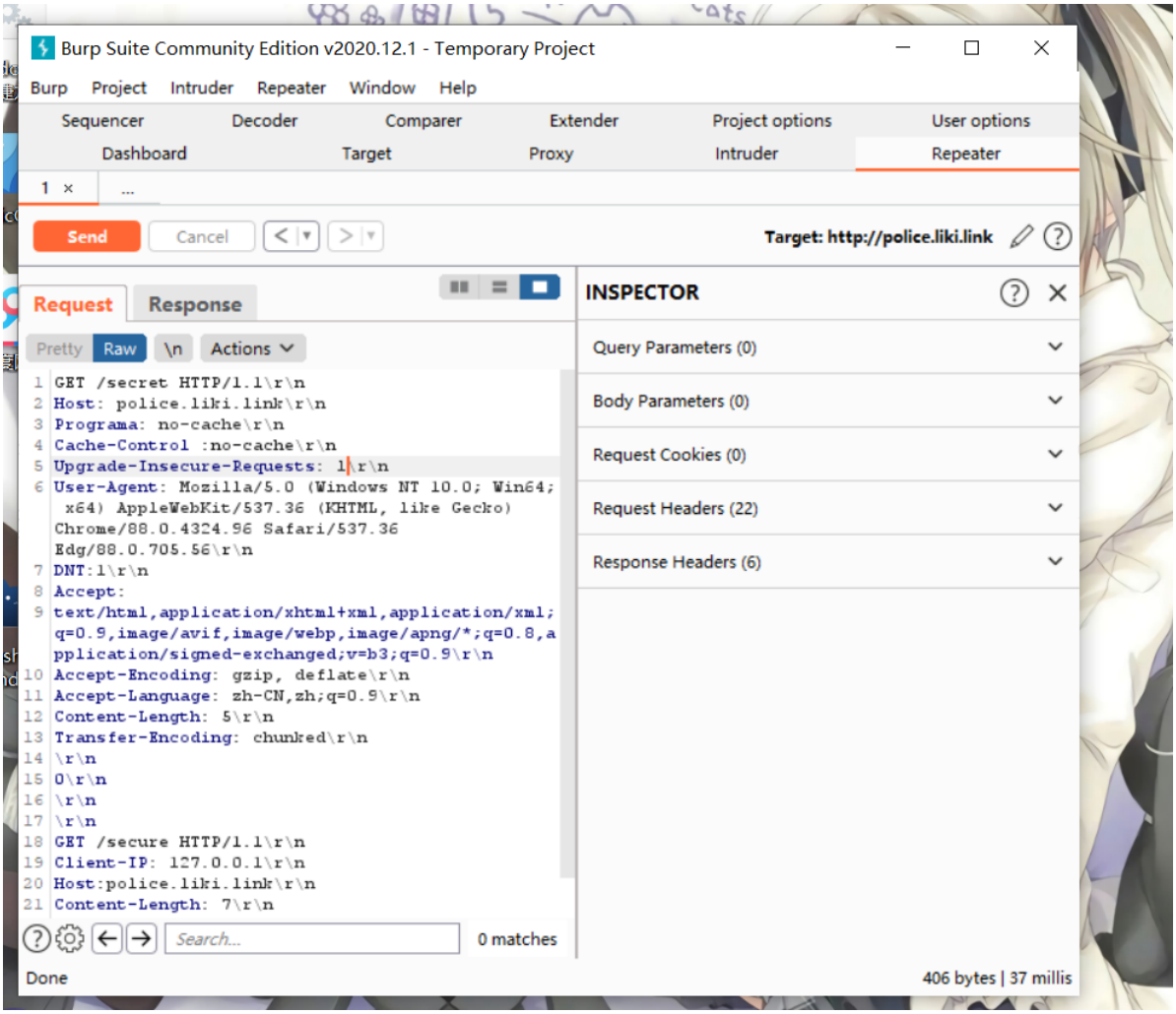
# 宝藏走私者

YOU CAN ONLY VISIT THE SECRET_DATA AS LOCALHOST!

第一眼，以为改个ip就好了，于是还是postman直接冲，发现不太行，后来看了看liki补充的资料，才发现要请求走私两步，于是，使用burp，先构造请求，然后再正常发送request。就得到了flag

# 走私者的愤怒

·本题为《宝藏走私者》的升级版，还是一样，直接打开 burp开冲，




最终在response中得到flag hgame{Fe3l^tHe~4N9eR+oF_5mu9gl3r!!}

# MISC

## Base全家幅

看到题目中给了一串密码 仔细一看 有128位 再看题目 base全家福，结合base密码规律 合理猜测为两个base64密码结合，对其进行base64→base32→base16的迭代操作，两串密码一结合，即为flag

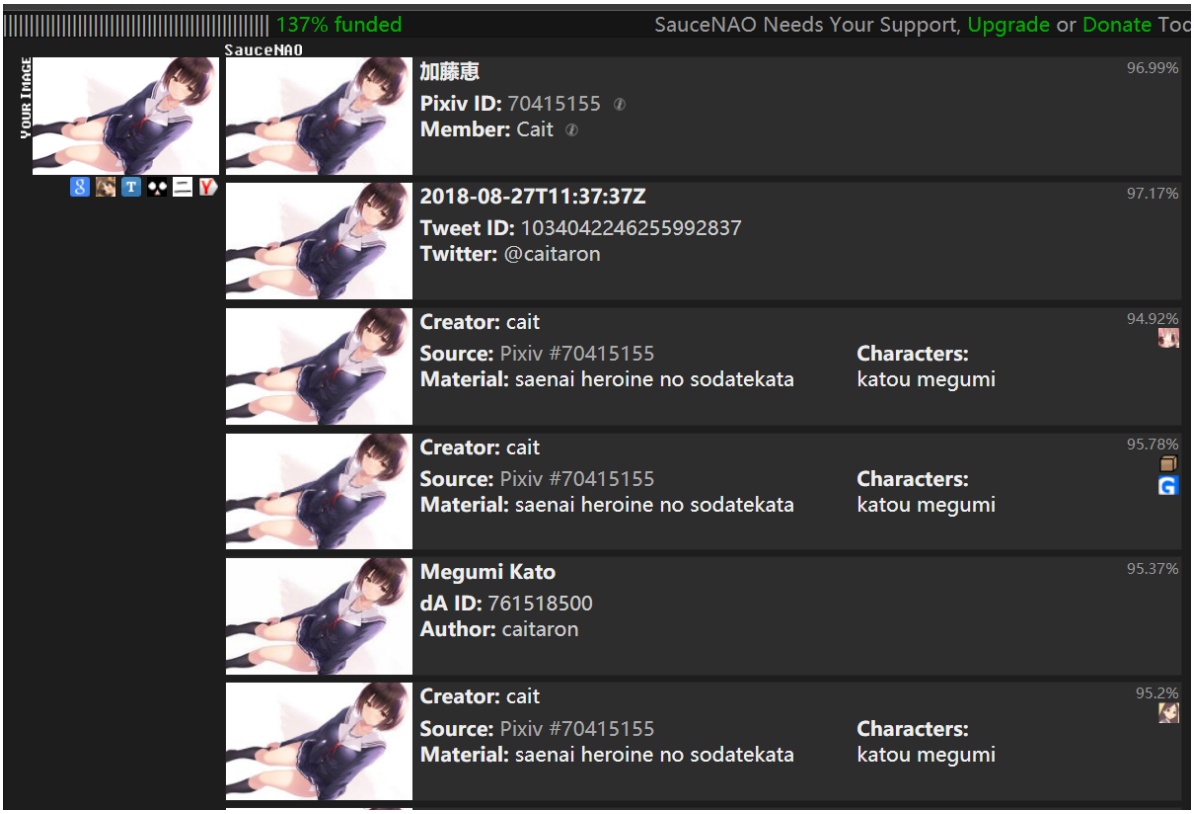
# 不起眼的压缩包的养成的方式

打开图片，发现是一个可爱的小姐姐，立马想到图片其实是拼接了一个压缩包在里面。

利用foremost发现图片中包含了一个压缩包

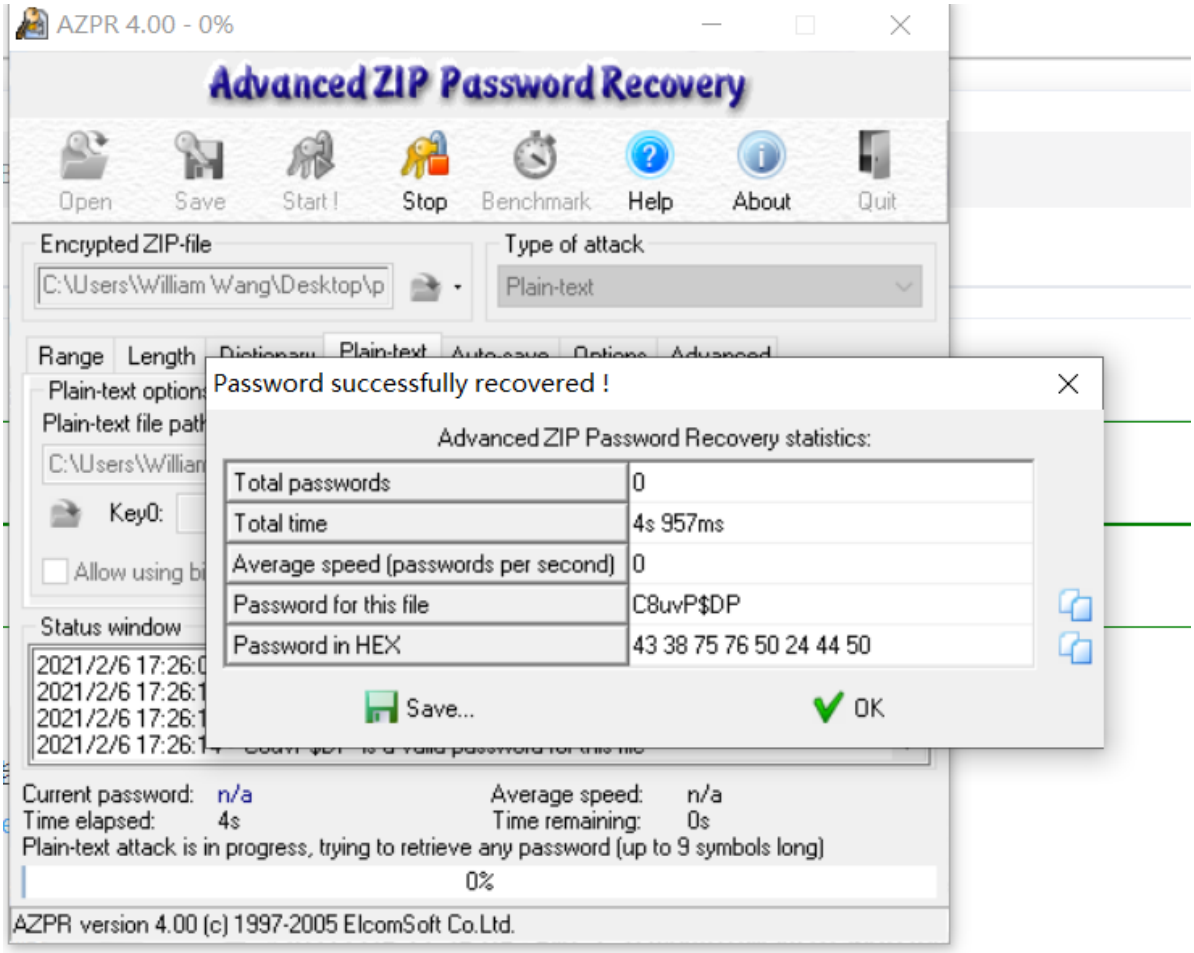
后缀改成7zip，并结合2020年的wp，想到 第一个zip包的密码是这张图片在某个奇特的图片网站的id

使用SauceNAO， 不难发现她的id为70415155，带进第一个zip，果不其然 解开了




打开第二个压缩包

发现里面也有一个叫NOPASSWORD.txt,想到可以使用明文攻击，遵循明文攻击的request 1kbの原则，我们选择仅储存的压缩方式，然后 使用AZPR对其进行攻击，得出密钥



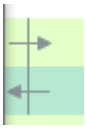

带入下一层，然后进入终想关，结果 还要密码555~

于是乎，将整个flag.zip拉入notepad++中进行分析。不看不知道，一看吓一跳

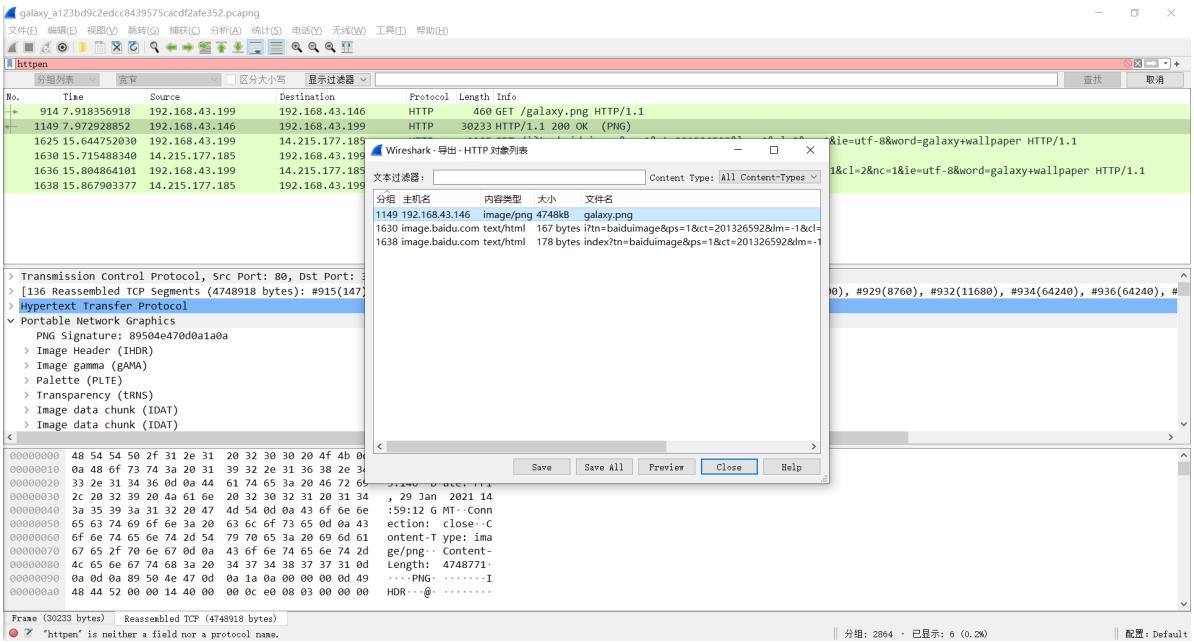

这好像就是ascaii码呢，我们写个小脚本，将&#x;去掉，转成base64即可得到结论 附当时过程 （忘记去掉/）了……(虽然VSCODE可以直接替换掉。。主要用来展示flag)

# Galaxy

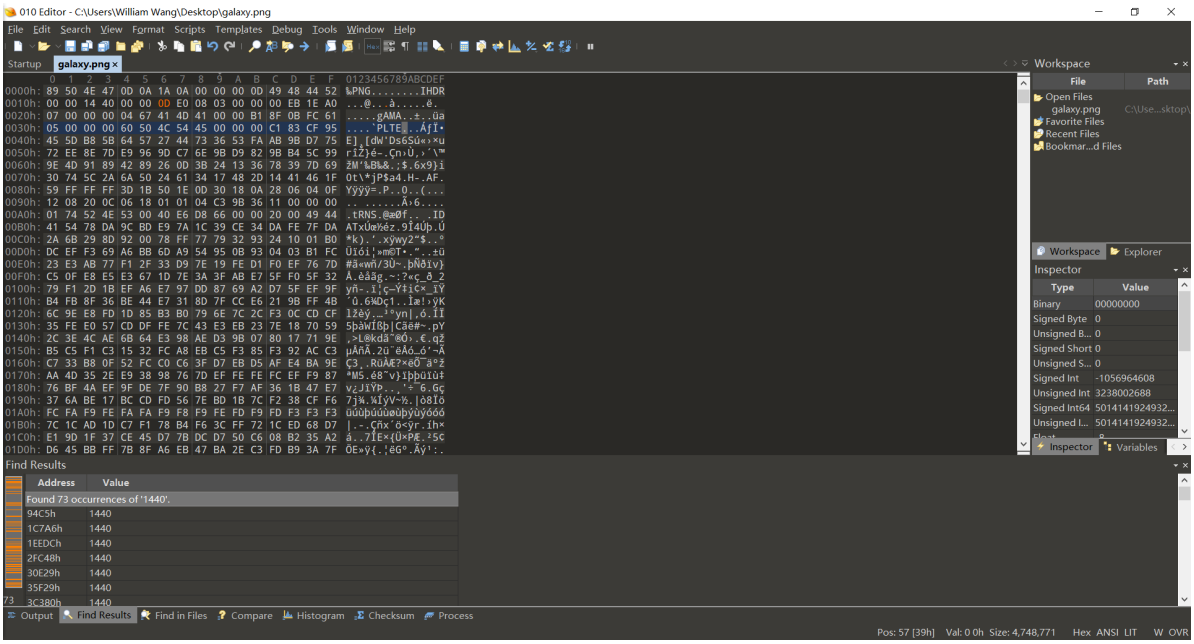
pcapng 数据包捕获格式包,我们将其下载后使用WireShark将其打开，过滤出http包



发现 有两个 source在交互，不难发现192.168.43.146的response状态是200 OK的 而且是一张png，将她导出




发现是一张星空的图片，没什么特点，有事无事打开010editor




，再右键打开原图片属性 发现原图片分辨率为8184*3296 想到会不会是图片没有显示完整呢，将3296换算成十六进制，为CE0。google了一下，发现这一类型的题目大部分都是修改第二行第六位的数字，对照了一下发现正好是原图片的长度所对应的值，将C改为D 保存 查看，flag浮出水面。


# Conclusion

第一次打网络安全方面的比赛，又能学到东西，感觉比赛也很有意思；这次因为太菜了555和还有一场同时进行的比赛的缘故 只做了这么几道题，希望后面再接再厉！！