

Web-Hitchhiking_in_the_Galaxy

题目进去显示404错误，F12查看源代码并没有发现什么，那就抓个包看看。

The screenshot shows the Burp Suite Professional v2.0beta interface. The top menu bar includes Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The main window is divided into two panes. The top pane, titled 'Filter: Hiding CSS, image and general binary content', displays a table of intercepted HTTP requests. The bottom pane shows the details of the selected request (index 1).

#	Host	Method	URL	Params	Edited	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP
1	http://hitchhiker42.0727.si...	GET	/HitchhikerGuide.php			302	469	HTML	php	405 Method Not Allo...			159.75.113.183
2	http://hitchhiker42.0727.si...	GET	/index.php			404	1181	HTML	php	Don't Panic!			159.75.113.183
3	https://incoming.telemetry...	POST	/submit/telemetry/0af79865-25fa...		✓							✓	52.34.254.140

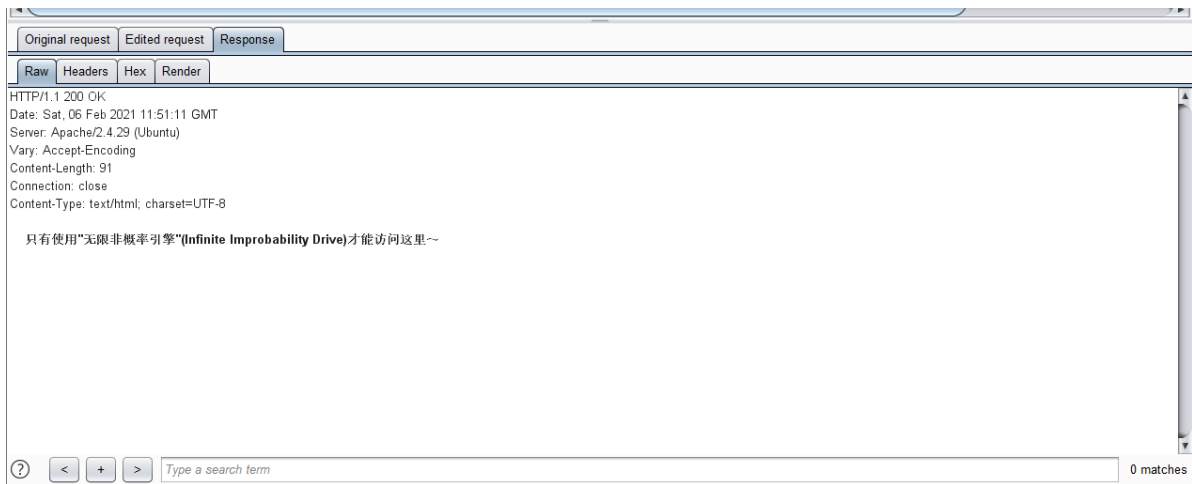
The selected request (index 1) is a GET request to `http://hitchhiker42.0727.si.../HitchhikerGuide.php`. The response is an HTTP/1.1 302 Found status. The response body is HTML, and the content type is `text/html; charset=UTF-8`. The response body contains the following HTML code:

```
<html>
<head><title>405 Method Not Allowed</title></head>
<body bgcolor="white">
<center>
<h1>405 Not Allowed</h1>
<p>顺风车不是这么搭的</p>
</center>
<hr>
<center>nginx/1.14.0 (Ubuntu)</center>
</body>
</html>
```

响应中显示“405 Methon Not Allowed”,考虑换一种请求方式试试看。

The screenshot shows the Burp Suite Professional v2.0beta interface with the 'Original request' tab selected. The request is a POST to `/HitchhikerGuide.php` on `http://hitchhiker42.0727.si.../HitchhikerGuide.php`. The request body is empty. The request headers are as follows:

```
POST /HitchhikerGuide.php HTTP/1.1
Host: hitchhiker42.0727.si...:42420
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://hitchhiker42.0727.si...:42420/
Upgrade-Insecure-Requests: 1
```



然后又提示要使用“无限非频率引擎”才能访问。改请求头加上"User-Agent"中将"Firefox/B5.0"换成"Infinite Improbability Drive"。之后又提示：茄子特别要求得从他的Cardinal过来。在请求头中添加"Referer: <https://cardinal.ink/>",又提示：flag仅能通过本地访问。在请求头中加"X-Forwarded-For: 127.0.0.1"。最后得到flag: hgame{s3Cret_of_HitCHhiking_in_the_GAI@xy_i5_dOnT_p@nic!}。

Web-宝藏走私者

对于我这个纯正的萌新小白来讲，题目有提示和给资料是最友好的。要不然根本没思路。学习了题目给出的资料，我就有了大致的思路——http走私。因为题目说我不是localhost不能访问，所以我构造一个http走私。通过抓包可以知道这个flag就在/secret里



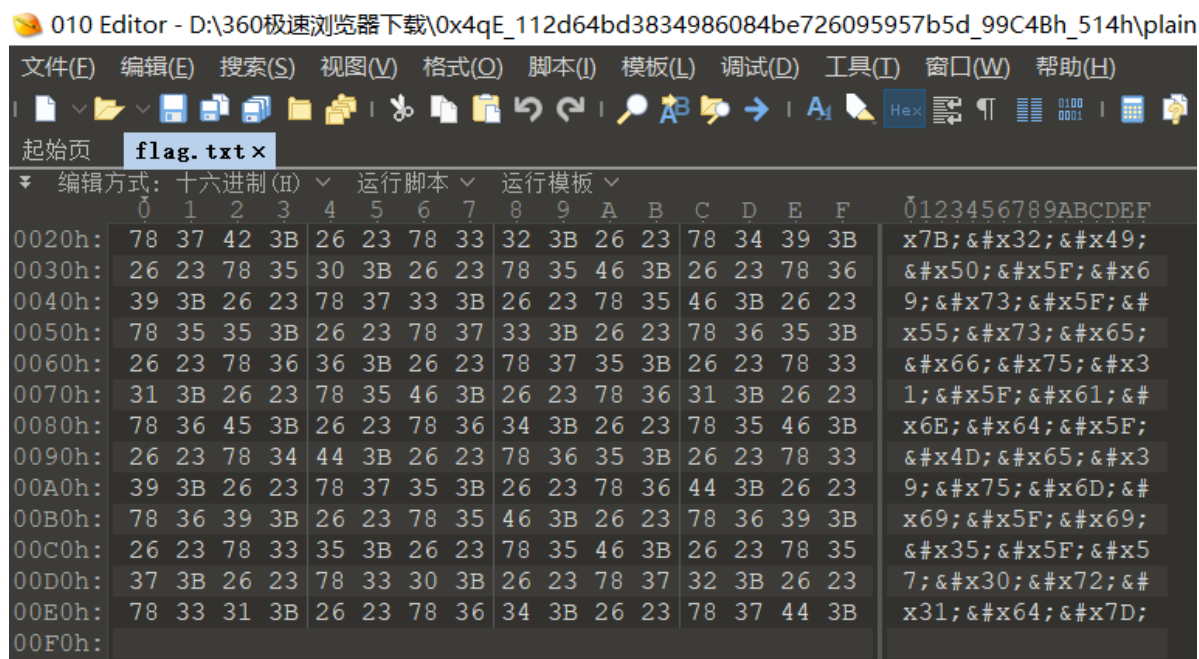
我记得我之前做的时候就是这么构造的，但是我现在再写一遍的时候怎么都不行（心态崩了）所以求学长原谅，flag我就不写了，当时做出就只关心flag没留意别的，这次长教训了，下次一定边做边写wp

MISC-Base全家福

这道题应该是签到题吧，复制粘贴去百度上依次进行base64解码base32解码和base16解码之后得到flag:hgame{We1c0me_t0_HG4M3_2021}.

MISC-不起眼压缩包的养成的方法

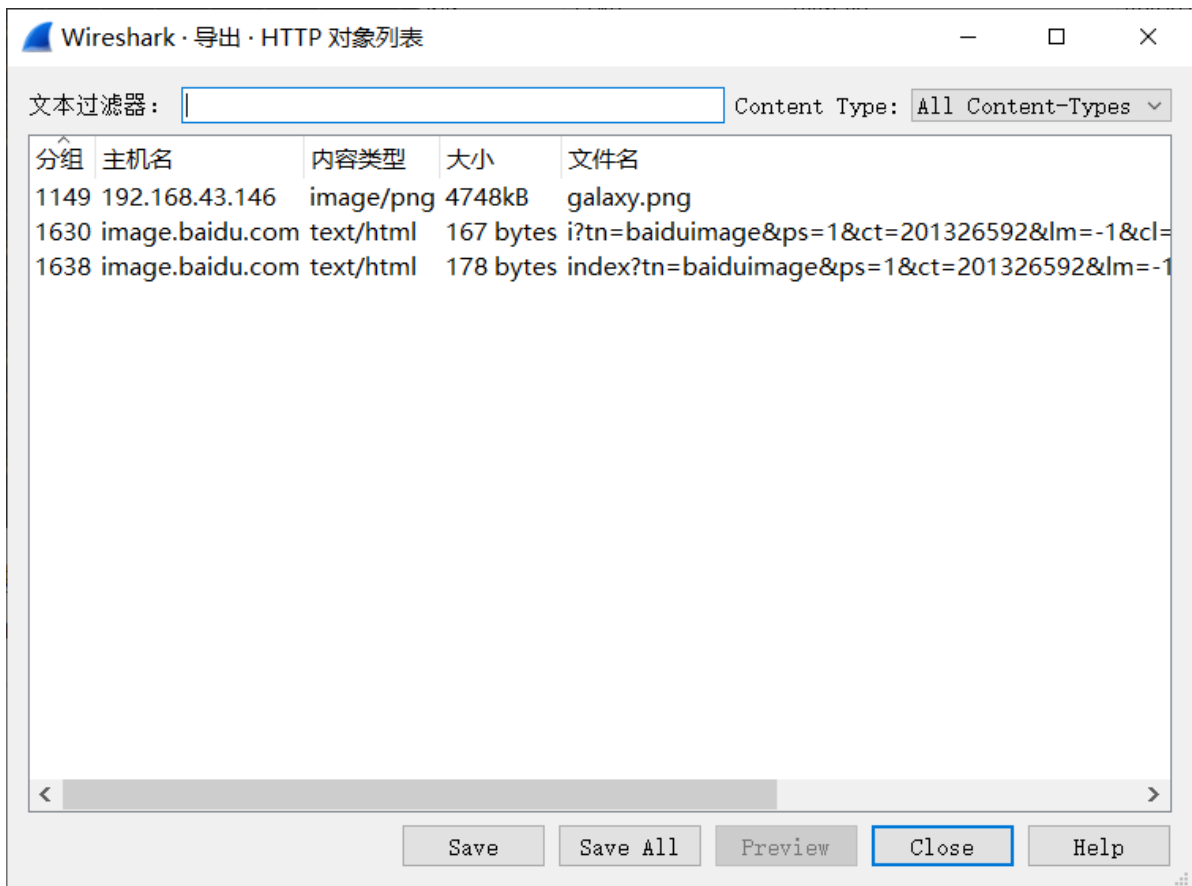
题目进去给了一张图，把它下载后，根据提示猜测做法应该是直接改后缀。将它放到010 Editor中，果然是图片隐写，前边是一张jpg后面是一个压缩包，选中压缩包部分直接另存为.zip文件后得到一个压缩包，解压。但是它有密码，果然没有这么简单。将它放到010 Editor中，发现是一个真加密压缩包，emmm。猜测密码应该有提示，选中压缩包右键查看属性，果然发现了秘密。注释中写着：password is picture ID (up to 8 digits)。去百度图片搜索，知道ID为70415155，之后输入密码果然是这个（也可以直接暴力破解）。解压后是一个txt文件和一个压缩文件，txt文件提示有时候不需要密码emmm。打开压缩文件，又是有密码（刚开始我是想直接暴力破解的，但是没成功。。。）后来上网搜索后知道了明文攻击，给的txt文件正好和压缩包里的txt文件相同，把txt文件压缩后进行明文攻击得到密码：C8uvP\$DP（好家伙，我直接好家伙，难怪暴力破解不了）。之后又是相同的情况，一个压缩包有密码，一个txt文件，但是压缩包里没有相同的txt文件，而是一个flag.txt文件（终于无限循环要结束了）虽然不能进行明文攻击，但是将压缩包放入010 Editor中发现它是伪加密，直接修改，将“00 01”改成“00 00”保存。然后直接解压得到flag.txt。点开后发现是乱码的，直接上Editor查看



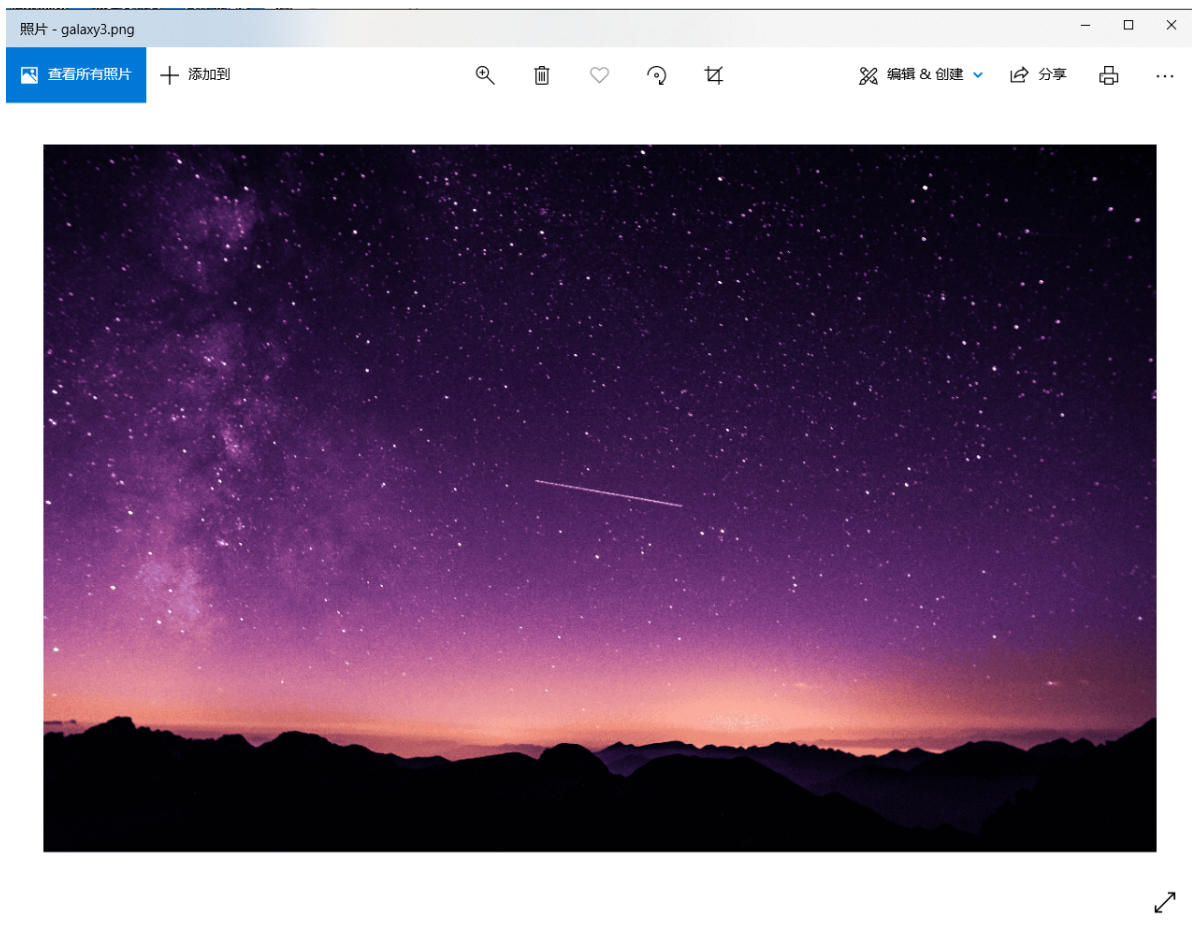
发现右边是十六进制的字符串，然后就是将十六进制转十进制，十进制转ascii码，ascii码转字符，最后得到flag: hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}

MISC-Galaxy

题目点开下载了一个流量包，wireshark打开导出对象hppt，可以得到



保存图片可以看到一张图



好像没啥，放到010 Editor中，发现问题

好，去网上百度学习一下，了解一些解题的工具，耐心一点还是能把一些简单的题目解出来的。综上，我得好好学习。。。现在好像我有点危险week2的题我还一题未解。