VNCTF2021 misc wp

原创

Pois0n# 于 2021-03-16 18:49:52 发布 664 收藏 4

分类专栏： misc web

本文链接：https://blog.csdn.net/qq_49354488/article/details/114893872

Misc

这次比赛排名在25，还可以。

[VNCTF 2021]Check_In

签到

打开题目底下就是

```
vnctf{Have_a_good_time!}
```

[VNCTF 2021]Questionnaire

问卷，做完就给

> 比赛时候没做这个问卷，导致排名往后掉了几名

```
vnctf{See_you_next_time}
```

[VNCTF 2021]冰冰好像藏着秘密

解压出来得到一个png图片，

文件名是`FFT`我们搜索一下

搜到`博里叶变换`，我们继续搜一下博里叶变换脚本

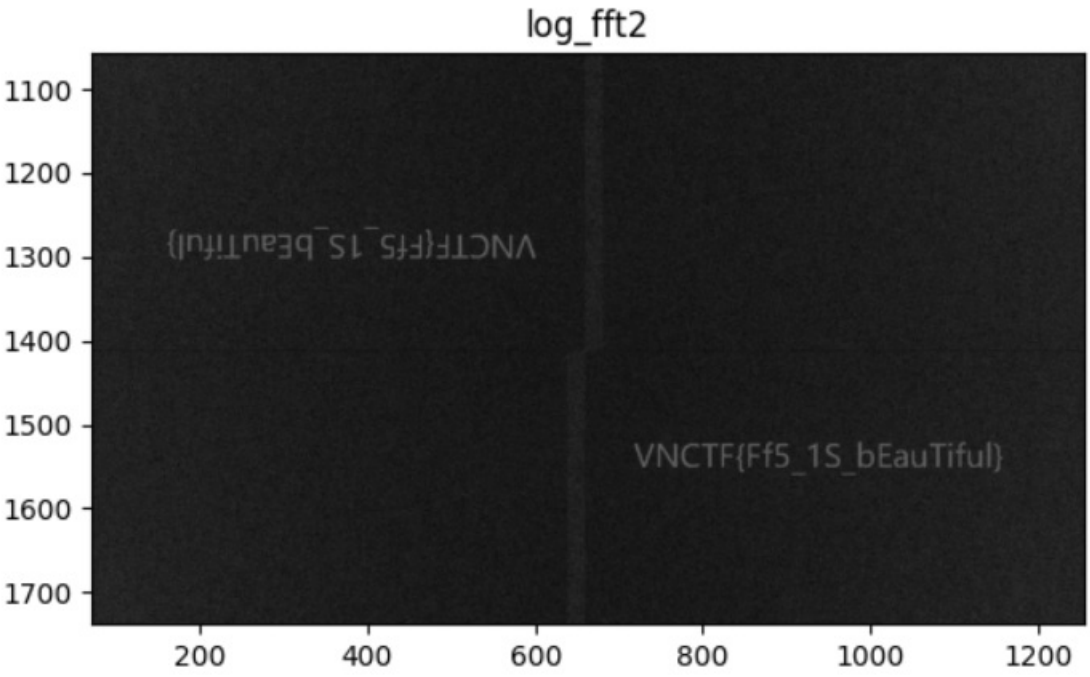
> 因为之前的附件可能存在问题，并没有跑出来，群里出题人重新发了一个附件才解出来的

参考文献：

https://blog.csdn.net/yemeinanhai/article/details/109550549?spm=1001.2014.3001.5501

```
import numpy as np
import cv2 as cv
from matplotlib import pyplot as plt
img = cv.imread('1.bmp', 0)
f = np.fft.fft2(img)
logf = 20*np.log(np.abs(f))
plt.imshow(logf, 'gray')
plt.show()
```

得到flag

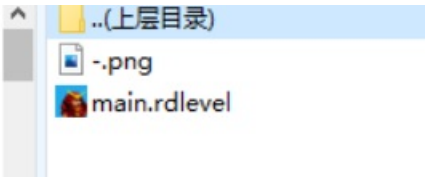



```
VNCTF{Ff5_1S_bEauTiful}
```

[VNCTF 2021]Do_you_like_Rhythm_Doctor

我们下载附件，发现文件后缀不对，改成zip

打开发现里面有两个文件



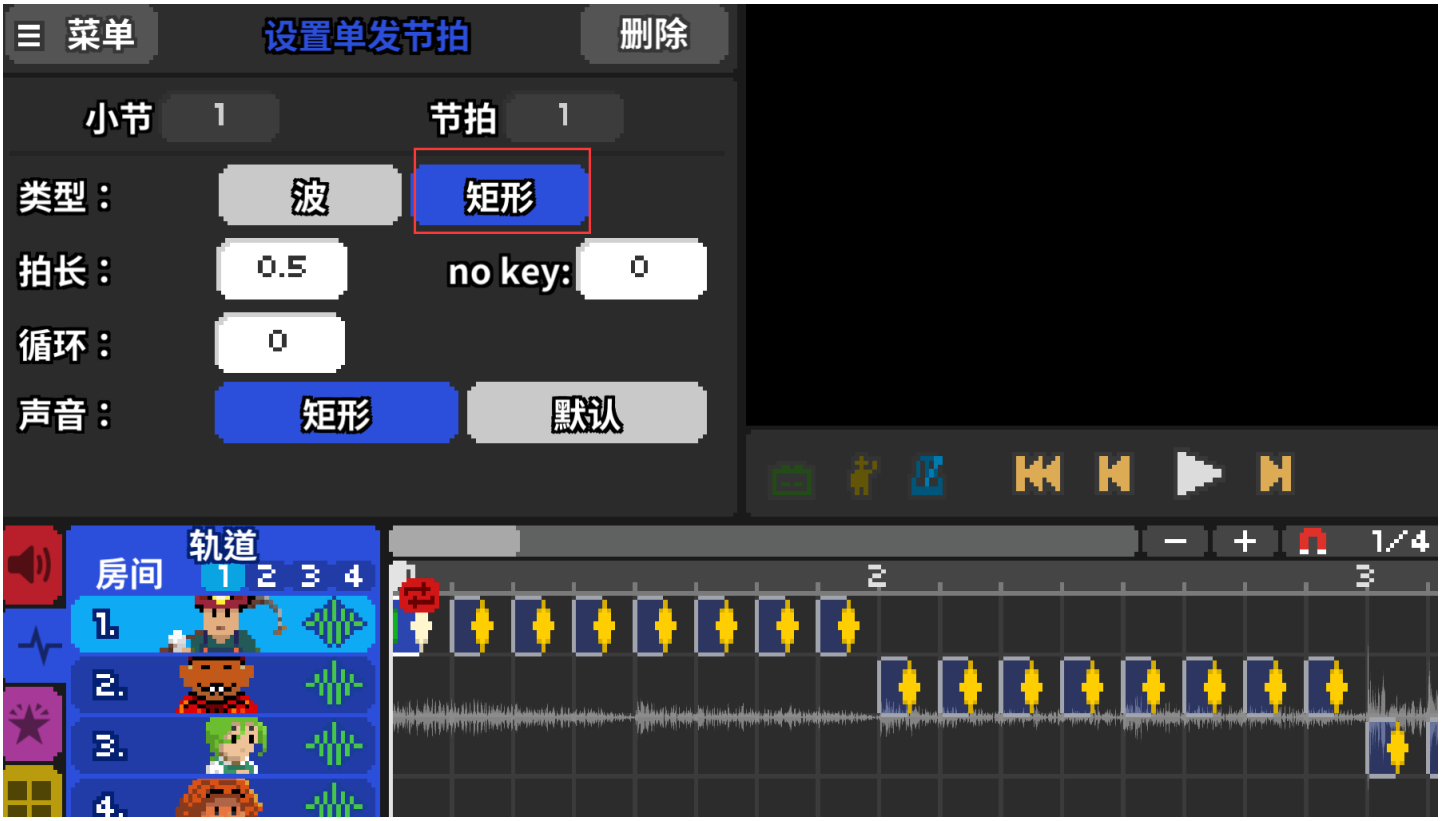
解压一下，

> 图片没有什么隐写，应该，反正我没找到

我们根据题目，搜了一下节奏医生，找到了编辑器，下载下来并打开文件

> 之前失败的步骤不写了，

我们看到第一个节拍是`矩形`


菜单
设置单发节拍
删除
小节
1
节拍
1
类型：
波
矩形
拍长：
0.5
no key:
0
循环：
0
声音：
矩形
默认
轨道
房间
1
2
3
4
1.
2.
3.
4.
1/4

第二个是波形

而且节拍正好是`8`个一组，我们猜测是二进制，并且矩形是零，波形是1，然后一行一行的进行

> 不要问为什么矩形是0，波形是1，试出来的

得到以下内容，

```
01100110   01101100 01100001 01100111 1111011
01010111   00110011 00110001 01100011 01101111
01101101   01100101 01011111 01010110 00100110
01001110   01011111 01000011 01010100 01000110 01111101
```

> 需要注意的是，在这四行结尾紧凑的那四段节拍，解密出来都是}，所以这里我只加了一个

转换一下即可

```
flag{W31come_V&N_CTF}
```

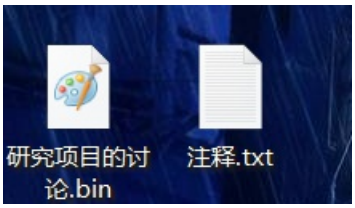
[VNCTF 2021]interesting_fishing

题目

```
crazyman_army是某安全公司的研究人员

这天他的其邮箱里发现了一封奇怪的邮件

你能帮助他找到其隐藏的信息吗

附件是第一部分的flag

图片是第二部分的flag

最后flag为 第一部分+第二部分(vnctf{*})
```

我们可以看到附件是第一部分，图片是第二部分

解压附件给了两个文件



我们查看注释一下

```
# 并无卵用

crazyman_army是某安全公司的研究人员
这天他的其邮箱里发现了一封奇怪的邮件
你能帮助他找到其隐藏的信息吗

注意:
附件是第一部分的flag
图片是第二部分的flag
最后flag为 第一部分+第二部分

hint:powershell解码后的字符可能存在不可读的情况 那并不是解码错误
```

我们先将`bin`改为`eml`后缀

然后，我们用工具`foxemil`打开这个附件。会得到一个图片和一个压缩包

研究项目的介绍

crazyman

发给 crazyman

myproject.rar (17 MB)

您好,crazyman_army
我是一个正在学习安全的大一学生,目前看过您关于其的很多分析报告以及漏洞复现的文章
最近我正在开发一个项目用于自动化样本分析 同时这是我对某国黑客的研究
希望您能够抽出您的宝贵时间给予我的目前研究一些宝贵的建议
谢谢

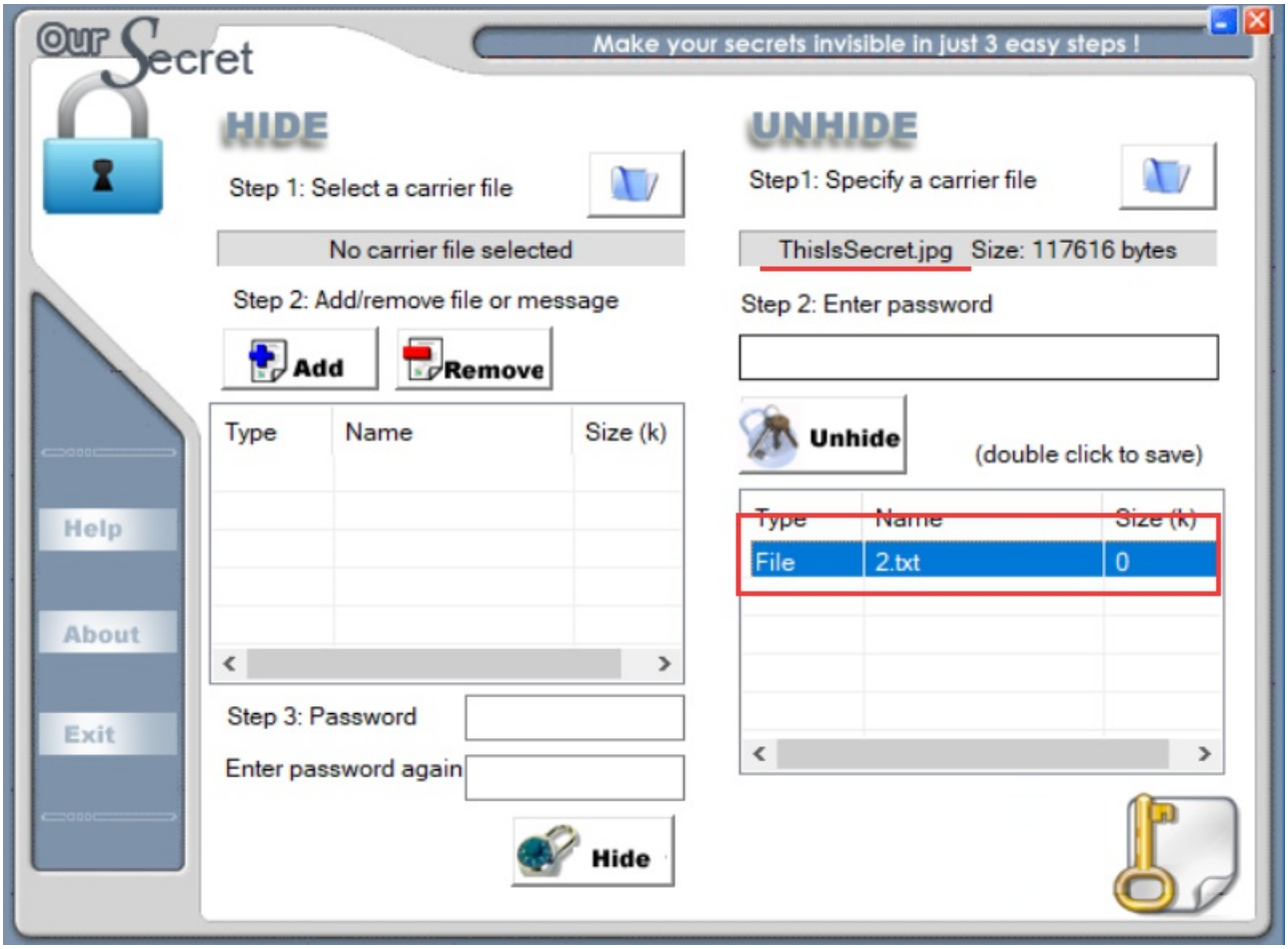
此致
敬礼

这两个文件都给扒下来

> 之前解题失败步骤不重复。

图片用`OurSecret`打开

> 根据文件名称，猜测是Secret



打开文件会得到后半部分flag

我们在查看压缩包

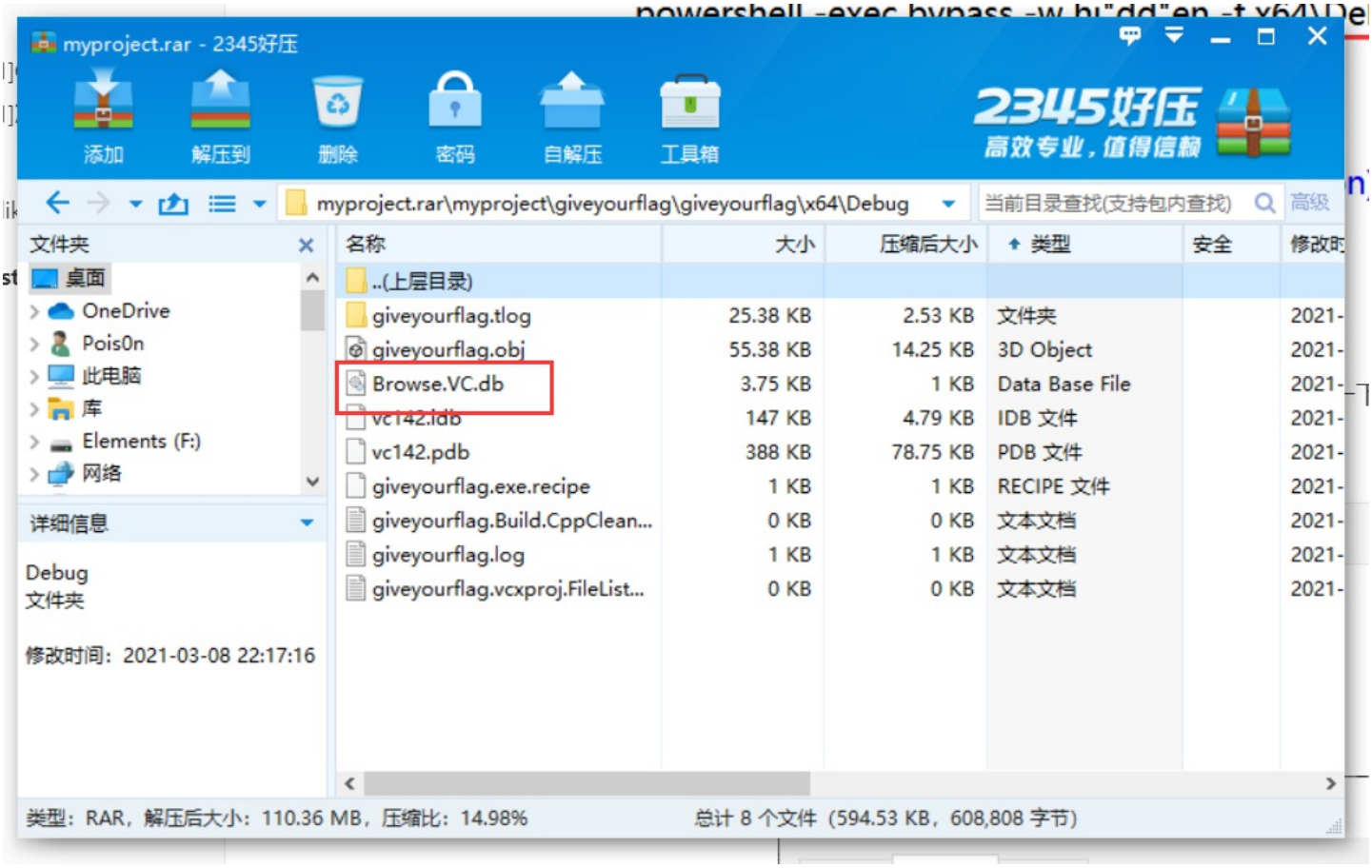
将文件解压出来，因为没有提示，我们挨个文件看

```
  -<Link>
     <SubSystem>Console</SubSystem>
     <EnableCOMDATFolding>true</EnableCOMDATFolding>
     <OptimizeReferences>true</OptimizeReferences>
     <GenerateDebugInformation>true</GenerateDebugInformation>
   </Link>
  -<PostBuildEvent>
    -<Command>
       powershell -exec bypass -w hi"dd"en -f x64\Debug\Browse.VC.db
     </Command>
   </PostBuildEvent>
 </ItemDefinitionGroup>
-<ItemDefinitionGroup Condition="'$(Configuration)|$(Platform)'=='Debug|x64'">
  -<ClCompile>
     <WarningLevel>Level3</WarningLevel>
```

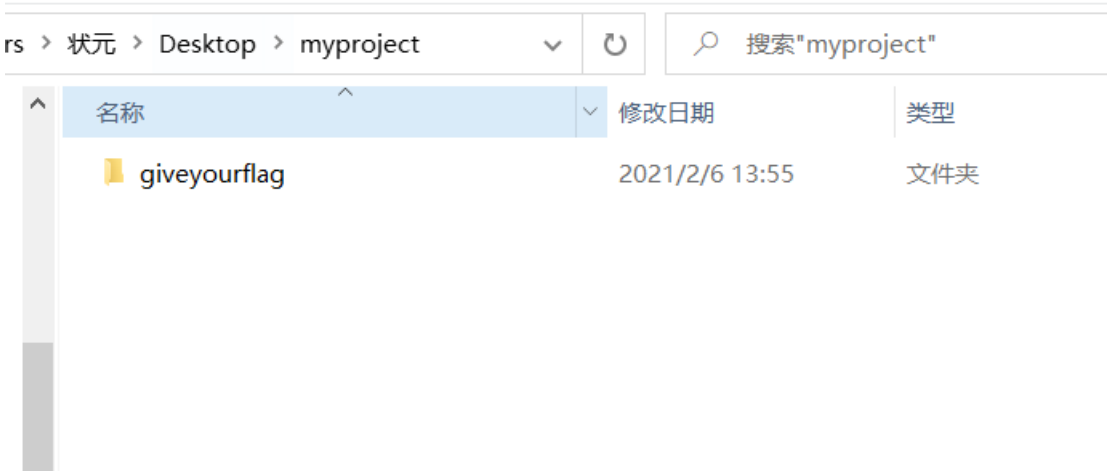
被我们找到了这个文件，我们发现文件中并没有该文件，我们返回rar中查找一下

发现在一下路径中有`Browse.VC.db`

```
myproject\giveyourflag\giveyourflag\x64\Debug
```

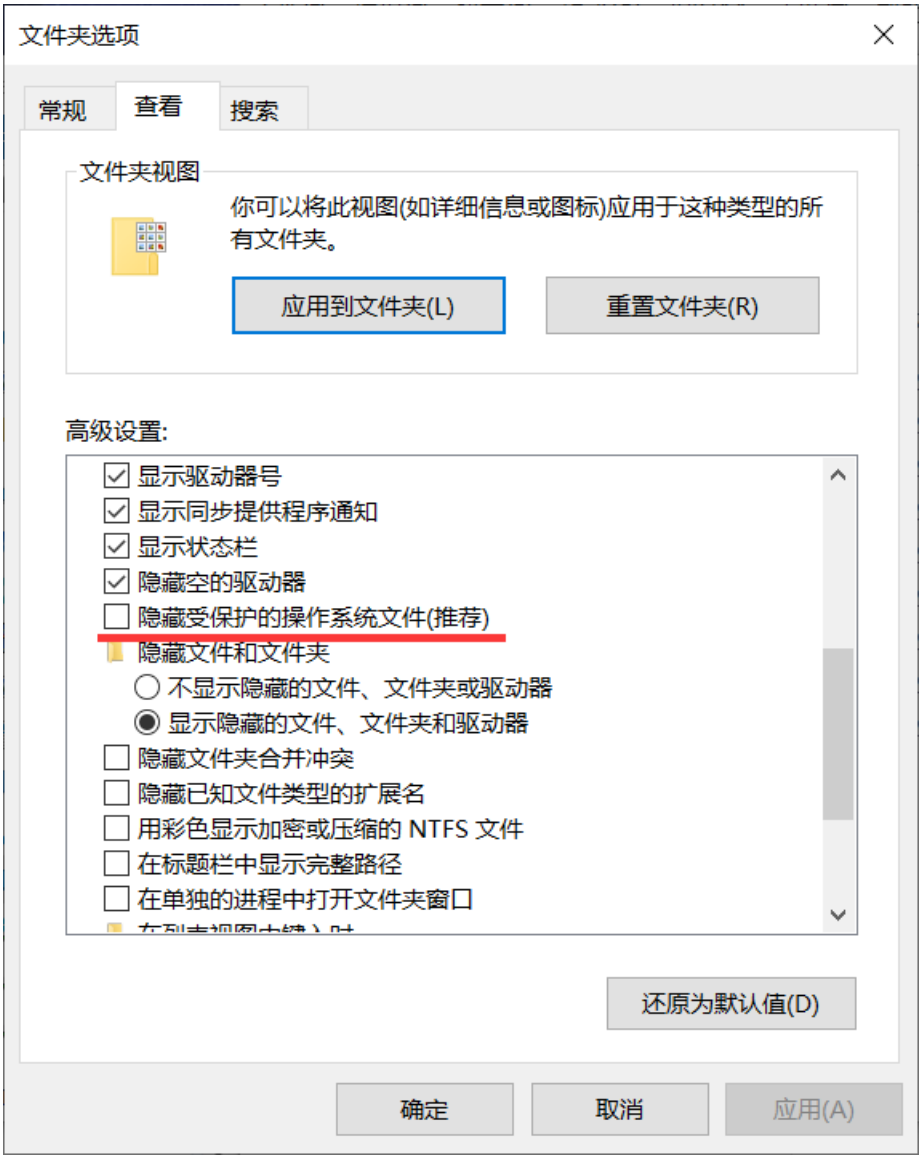


继续返回文件中查看，发现就是没有，我们单独将这个文件解压出来，解压出来发现还是没有这个文件。

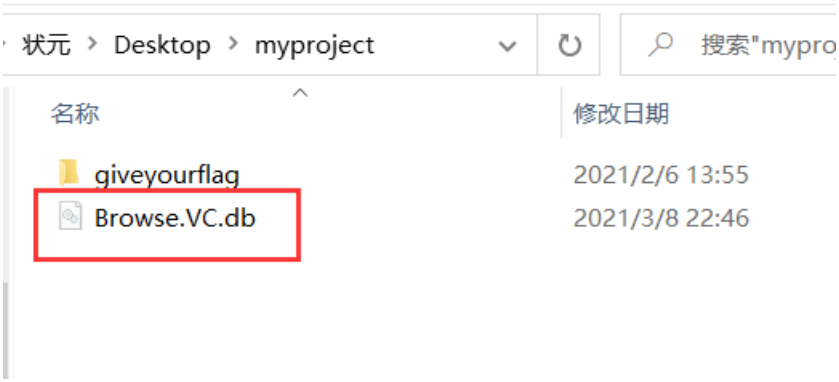


我们猜测进行了文件隐藏。

找到文件夹选项，把红线标记处取消勾选



会发现目录下多出一个文件



用记事本打开

得到以下信息

```
$encodestring = "XAB1AC0ANgA1ADQAMwAyAD8AXAB1AC0ANgA1ADQAMgAwAD8AXAB1AC0ANgA1ADQAMgAwAD8AXAB1AC0ANgA1ADQAMgA0AD8
AXAB1AC0ANgA1ADQAMgAxAD8AXAB1AC0ANgA1ADQANwA4AD8AXAB1AC0ANgA1ADQAOAA5AD8AXAB1AC0ANgA1ADQAOAA5AD8AXAB1AC0ANgA1ADQ
AMQA4AD8AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAMwA3AD8AXAB1AC0ANgA1ADQAMgAwAD8AXAB1AC0ANgA1ADQAMwA0AD8AXAB1AC0
ANgA1ADQAOQAxAD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAA3AD8AXAB1AC0ANgA1ADQAOAA1AD8AXAB1AC0ANgA1ADQAOQAxAD8
AXAB1AC0ANgA1ADQAOAA3AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAAzAD8AXAB1AC0ANgA1ADQAOAAxAD8AXAB1AC0ANgA1ADQ
AOAA4AD8AXAB1AC0ANgA1ADQAOAAyAD8AXAB1AC0ANgA1ADQAOAA3AD8AXAB1AC0ANgA1ADQAOAA3AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0
ANgA1ADQAOAA1AD8AXAB1AC0ANgA1ADQAOQAwAD8AXAB1AC0ANgA1ADQAMwA3AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMgAxAD8
AXAB1AC0ANgA1ADQAOQAwAD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQAMgA0AD8AXAB1AC0ANgA1ADQAOQAxAD8AXAB1AC0ANgA1ADQ
AMgA2AD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAMwAwAD8AXAB1AC0ANgA1ADQAMwAxAD8AXAB1AC0
ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAMwAzAD8AXAB1AC0ANgA1ADQAOQAwAD8AXAB1AC0ANgA1ADQAMgA3AD8AXAB1AC0ANgA1ADQAMQA1AD8
AXAB1AC0ANgA1ADQAMgAzAD8AXAB1AC0ANgA1ADQAMwA3AD8AXAB1AC0ANgA1ADQAMgA4AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQ
AMQA5AD8AXAB1AC0ANgA1ADQAMwA2AD8AXAB1AC0ANgA1ADQAOQAwAD8AXAB1AC0ANgA1ADQAMwA3AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0
ANgA1ADQAMgA3AD8AXAB1AC0ANgA1ADQAOAA5AD8AXAB1AC0ANgA1ADQANQA2AD8AXAB1AC0ANgA1ADQAMQA1AD8AXAB1AC0ANgA1ADQAMgA1AD8
AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAMwAzAD8AXAB1AC0ANgA1ADQAMQA1AD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQ
AMgA2AD8AXAB1AC0ANgA1ADQAMwAzAD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0
ANgA1ADQAMgAxAD8AXAB1AC0ANgA1ADQAMgAwAD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMgAyAD8AXAB1AC0ANgA1ADQAMwA1AD8
AXAB1AC0ANgA1ADQAMgAxAD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQ
AMgA4AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMQA3AD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0
ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8
AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQAMwA0AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMgAyAD8AXAB1AC0ANgA1ADQ
AMwA1AD8AXAB1AC0ANgA1ADQAMwAxAD8AXAB1AC0ANgA1ADQAMwAzAD8AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0
ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQAMwAzAD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMgA1AD8
AXAB1AC0ANgA1ADQAMwA2AD8AXAB1AC0ANgA1ADQAMgAxAD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQ
AOAA4AD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQAMgA3AD8AXAB1AC0ANgA1ADQAMwAxAD8AXAB1AC0ANgA1ADQAMwA2AD8AXAB1AC0
ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQANQA4AD8AXAB1AC0ANgA1ADQAMgA1AD8
AXAB1AC0ANgA1ADQAMgAyAD8AXAB1AC0ANgA1ADQAMgAwAD8AXAB1AC0ANgA1ADQAMwAyAD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQ
AOAA2AD8AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQANgAxAD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQAMgAyAD8AXAB1AC0
ANgA1ADQAMwA1AD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8
AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQANgA5AD8AXAB1AC0ANgA1ADQANQA3AD8AXAB1AC0ANgA1ADQANQAwAD8AXAB1AC0ANgA1ADQ
ANgAzAD8AXAB1AC0ANgA1ADQANgA4AD8AXAB1AC0ANgA1ADQAOQAxAD8AXAB1AC0ANgA1ADQAOAA3AD8AXAB1AC0ANgA1ADQANwA5AD8AXAB1AC0
ANgA1ADQAOQA5AD8AXAB1AC0ANgA1ADQAOAA2AD8AXAB1AC0ANgA1ADQAOAA4AD8AXAB1AC0ANgA1ADQAMgA0AD8AXAB1AC0ANgA1ADQAMwA5AD8
AXAB1AC0ANgA1ADQAMgAyAD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQAMgA2AD8AXAB1AC0ANgA1ADQAMgA1AD8AXAB1AC0ANgA1ADQ
AMwAxAD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0ANgA1ADQAOQAwAD8AXAB1AC0ANgA1ADQAMgAyAD8AXAB1AC0ANgA1ADQAMwA5AD8AXAB1AC0
ANgA1ADQAMgAyAD8A"
$bytes  = [System.Convert]::FromBase64String($string);
$decoded = [System.Text.Encoding]::UTF8.GetString($bytes);
echo $decoded
```

将中间部分内容进行base64解密

得到以下内容

\u-65432?\u-65420?\u-65420?\u-65424?\u-65421?\u-65478?\u-65489?\u-65489?\u-65418?\u-65426?\u-65437?\u-65420?\u-65434?\u-65491?\u-65486?\u-65487?\u-65485?\u-65491?\u-65487?\u-65486?\u-65483?\u-65481?\u-65488?\u-65482?\u-65487?\u-65487?\u-65486?\u-65485?\u-65490?\u-65437?\u-65425?\u-65421?\u-65490?\u-65439?\u-65424?\u-65491?\u-65426?\u-65439?\u-65426?\u-65430?\u-65431?\u-65426?\u-65433?\u-65490?\u-65427?\u-65415?\u-65423?\u-65437?\u-65428?\u-65425?\u-65419?\u-65436?\u-65490?\u-65437?\u-65425?\u-65427?\u-65489?\u-65456?\u-65415?\u-65425?\u-65426?\u-65433?\u-65415?\u-65439?\u-65426?\u-65433?\u-65499?\u-65486?\u-65488?\u-65421?\u-65420?\u-65425?\u-65422?\u-65435?\u-65421?\u-65499?\u-65486?\u-65488?\u-65428?\u-65425?\u-65417?\u-65499?\u-65486?\u-65488?\u-65425?\u-65426?\u-65499?\u-65486?\u-65488?\u-65434?\u-65425?\u-65422?\u-65435?\u-65431?\u-65433?\u-65426?\u-65499?\u-65486?\u-65488?\u-65433?\u-65425?\u-65425?\u-65436?\u-65421?\u-65499?\u-65486?\u-65488?\u-65439?\u-65427?\u-65431?\u-65436?\u-65499?\u-65486?\u-65488?\u-65458?\u-65425?\u-65422?\u-65420?\u-65432?\u-65499?\u-65486?\u-65488?\u-65461?\u-65425?\u-65422?\u-65435?\u-65439?\u-65426?\u-65499?\u-65486?\u-65488?\u-65469?\u-65457?\u-65450?\u-65463?\u-65468?\u-65491?\u-65487?\u-65479?\u-65499?\u-65486?\u-65488?\u-65424?\u-65439?\u-65422?\u-65439?\u-65426?\u-65425?\u-65431?\u-65439?\u-65490?\u-65422?\u-65439?\u-65422?

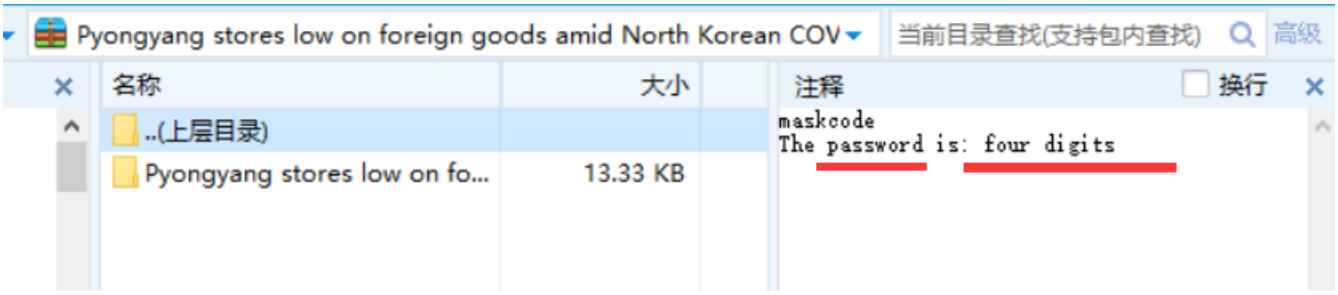
RTF格式

用65536减去之后，进行数据转换，获得网址

https://vnctf-213-1257061123.cos.ap-nanjing-myqcloud.com/Pyongyang%20stores%20low%20on%20foreign%20goods%20amid%20North%20Korean%20COVID-19%20paranoia.rar

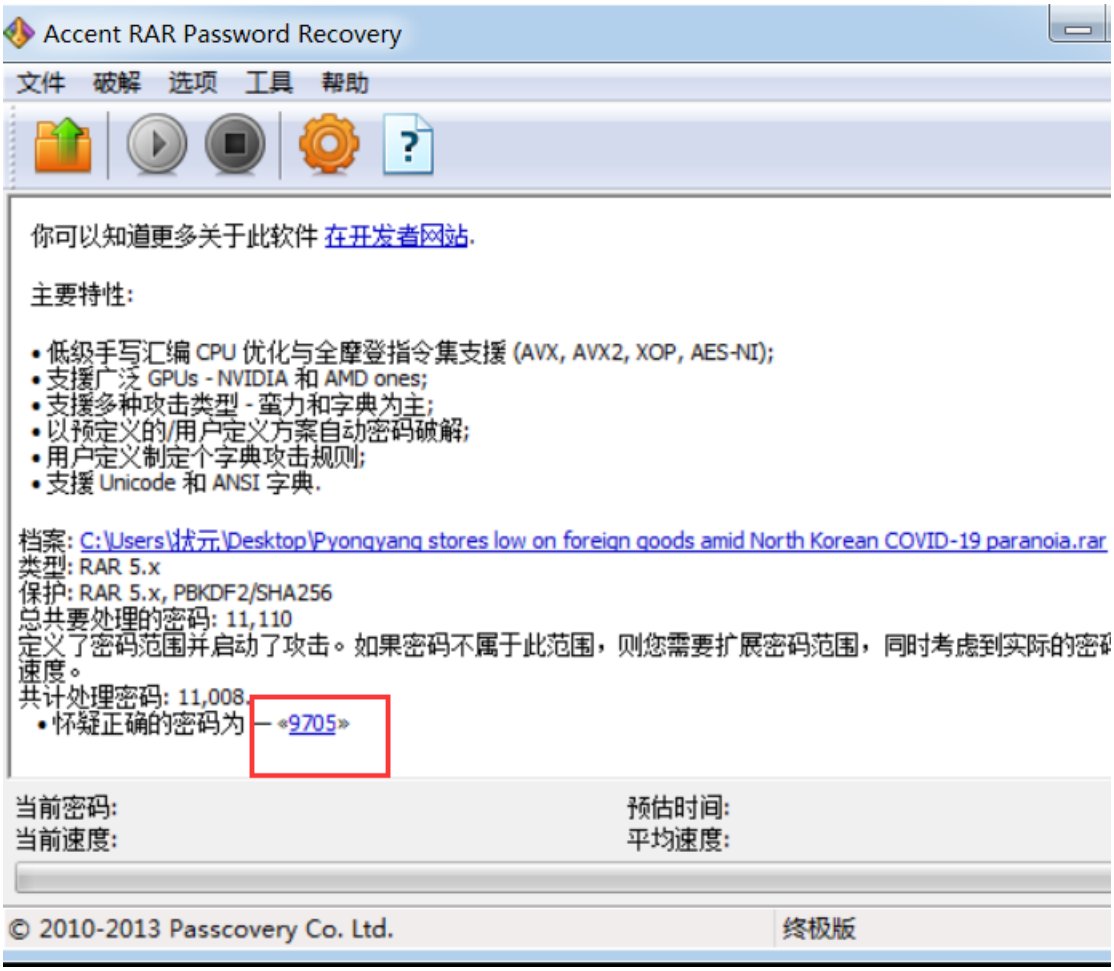
下载下来

提示密码是四位数



我们进行RAR爆破，使用工具`Accent RAR Password Recovery`

得到密码`9705`



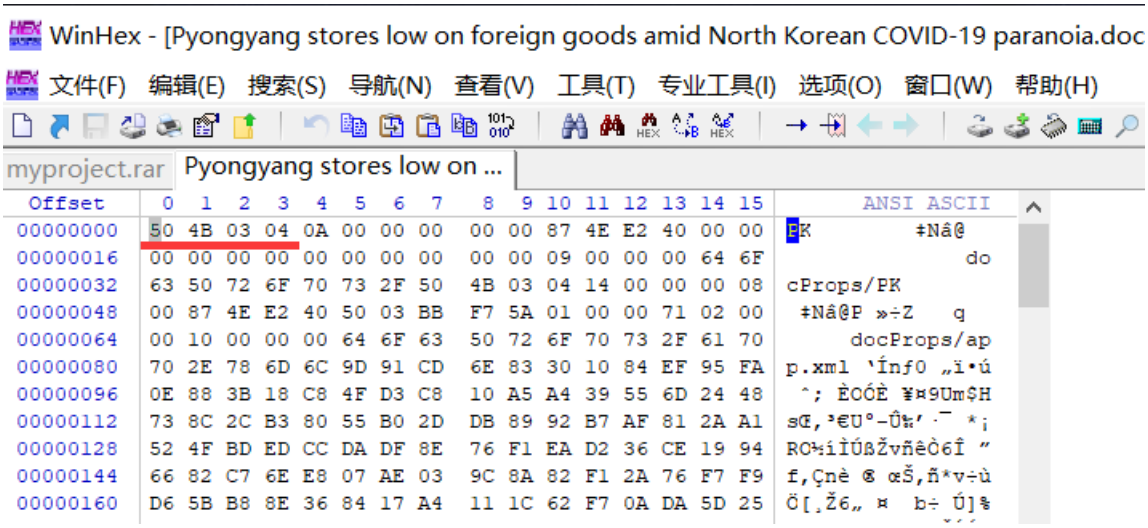
解压出来word文件

打开得到以下内容

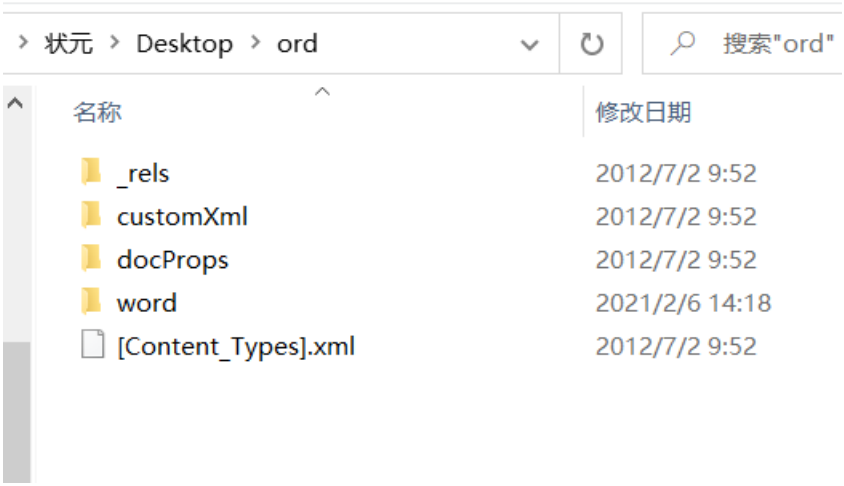
```
Pyongyang stores low on foreign goods amid North Korean COVID-19 paranoia
Amid an ongoing, full-scale border lockdown against COVID-19, North Korea on Tuesday warned its citizens against
 relying on imported foreign goods — calling the habit a dangerous “disease” that could spread the virus from ab
road.
Pyongyang’s warning against bringing in foreign goods is not just empty words, either: On Monday, sources told V
OA that supermarkets and shops in Pyongyang have lacked foreign-sourced staples for months, including coffee, co
coa and chocolate. This appears to be out of paranoia that foreign goods could carry traces of COVID-19 — which
is possible, according to the United Nations, though not the most common way the virus has been transmitted worl
dwide.
Sources also told VOA that there’s currently no evidence that food items are coming across the border from China
, with only locally produced items available on Pyongyang store shelves.
INTENSE BORDER CONTROL
Tuesday’s state-run Rodong Sinmun newspaper cautioned against the country’s long-standing “importation fever” (
수입병), which comes as the North continues a strict border control. The DPRK even set up “shoot on sight” zones
 along its border with China for fear that travelers could carry the virus. Meanwhile, the country is operating
under the contested premise that items, air and even yellow dust pollution could carry COVID-19 across borders.
“The most entangling issue today on [the DPRK] demon
```

> 有点难受，看不懂

我们将文件放到`winhex`中发现文件是zip文件头



改一下后缀，解压



经过尝试进入`word`目录找到，`hideinfo.xml`

放到winhex查看一下

oject.rar | hideinfo.xml

set	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
0000	50	79	6F	6E	67	79	61	6E	67	20	73	74	6F	72	65	73	Pyongyang stores
0016	20	6C	6F	77	20	6F	6E	20	66	6F	72	65	69	67	6E	20	low on foreign
0032	67	6F	6F	64	73	20	61	6D	69	64	20	4E	6F	72	74	68	goods amid North
0048	20	4B	6F	72	65	61	6E	20	43	4F	56	49	44	2D	31	39	Korean COVID-19
0064	20	70	61	72	61	6E	6F	69	61	0A	41	6D	69	64	20	61	paranoia Amid a
0080	6E	20	6F	6E	67	6F	69	6E	67	2C	20	66	75	6C	6C	2D	n ongoing, full-
0096	73	63	61	6C	65	20	62	6F	72	64	65	72	E2	80	8C	E2	scale borderâ€Câ
0112	80	8C	E2	80	8C	E2	80	8C	E2	80	8D	EF	BB	BF	E2	80	€Câ€Câ€Câ€ ï»¿â€
0128	8D	E2	80	AC	20	6C	6F	63	6B	64	6F	77	6E	20	61	67	â€¬ lockdown ag
0144	61	69	6E	73	74	20	43	4F	56	49	44	2D	31	39	2C	20	ainst COVID-19,
0160	4E	6F	72	74	68	20	4B	6F	72	65	61	20	6F	6E	20	54	North Korea on T
0176	75	65	73	64	61	79	20	77	61	72	6E	65	64	20	69	74	uesday warned it
0192	73	20	63	69	74	69	7A	65	6E	73	20	61	67	61	69	6E	s citizens again
0208	73	74	20	72	65	6C	79	69	6E	67	20	6F	6E	20	69	6D	st relying on im
0224	70	6F	72	74	65	64	E2	80	8C	E2	80	8C	E2	80	8C	E2	portedâ€Câ€Câ€Câ
0240	80	8C	E2	80	8D	E2	80	AC	EF	BB	BF	E2	80	AC	20	66	€Câ€ â€¬ï»¿â€¬ f
0256	6F	72	65	69	67	6E	20	67	6F	6F	64	73	20	E2	80	94	oreign goods â€”
0272	20	63	61	6C	6C	69	6E	67	20	74	68	65	20	68	61	62	calling the hab
0288	69	74	20	61	20	64	61	6E	67	65	72	6F	75	73	20	E2	it a dangerous â
0304	80	9C	64	69	73	65	61	73	65	E2	80	9D	20	74	68	61	€œdiseaseâ€ tha
0320	74	20	63	6F	75	6C	64	20	73	70	72	65	61	64	20	74	t could spread t
0336	68	65	20	76	69	72	75	73	20	66	72	6F	6D	20	61	62	he virus from ab
0352	72	6F	61	64	2E	0A	50	79	6F	6E	67	79	61	6E	67	E2	road. Pyongyangâ
0368	80	99	73	20	77	61	72	6E	69	6E	67	20	61	67	61	69	€™s warning agai
0384	6E	73	74	20	62	72	69	6E	67	69	6E	67	20	69	6E	E2	nst bringing inâ
0400	80	8C	E2	80	8C	E2	80	8C	E2	80	8C	E2	80	8D	E2	80	€Câ€Câ€Câ€Câ€ â€
0416	AC	E2	80	8C	EF	BB	BF	20	66	6F	72	65	69	67	6E	20	¬â€Cï»¿ foreign
0432	67	6F	6F	64	73	20	69	73	20	6E	6F	74	20	6A	75	73	goods is not jus
0448	74	20	65	6D	70	74	79	20	77	6F	72	64	73	2C	20	65	t empty words, e
0464	69	74	68	65	72	3A	20	4F	6E	20	4D	6F	6E	64	61	79	ither: On Monday
0480	2C	20	73	6F	75	72	63	65	73	20	74	6F	6C	64	C2	A0	, sources toldÂ
0496	56	4F	41	C2	A0	74	68	61	74	20	73	75	70	65	72	6D	VOAÂ that superm
0512	61	72	6B	65	74	73	20	61	6E	64	20	73	68	6F	70	73	arkets and shops
0528	20	69	6E	20	50	79	6F	6E	67	79	61	6E	67	20	68	61	in Pyongyang ha
0544	76	65	20	6C	61	63	6B	65	64	20	66	6F	72	65	69	67	ve lacked foreig
0560	6E	2D	73	6F	75	72	63	65	64	20	73	74	61	70	6C	65	n-sourced staple
0576	73	20	66	6F	72	20	6D	6F	6E	74	68	73	2C	20	E2	80	s for months, â€
0592	8C	E2	80	8C	E2	80	8C	E2	80	8C	E2	80	8D	EF	BB	BF	Câ€Câ€Câ€Câ€ ï»¿
0608	E2	80	8D	E2	80	8C	69	6E	63	6C	75	64	69	6E	67	20	â€ â€Cincluding
0624	63	6F	66	66	65	65	2C	20	63	6F	63	6F	61	20	61	6E	coffee, cocoa an
0640	64	20	63	68	6F	63	6F	6C	61	74	65	2E	20	54	68	69	d chocolate. Thi
0656	73	20	61	70	70	65	61	72	73	20	74	6F	20	62	65	20	s appears to be
0672	6F	75	74	20	6F	66	20	70	61	72	61	6E	6F	69	61	E2	out of paranoiaâ
0688	80	8C	E2	80	8C	E2	80	8C	E2	80	8C	E2	80	8D	E2	80	€Câ€Câ€Câ€Câ€ â€
0704	AC	E2	80	8D	E2	80	AC	20	74	68	61	74	20	66	6F	72	¬â€ â€¬ that for
0720	65	69	67	6E	20	67	6F	6F	64	73	20	63	6F	75	6C	64	eign goods could
0736	20	63	61	72	72	79	20	74	72	61	63	65	73	20	6F	66	carry traces of
0752	20	43	4F	56	49	44	2D	31	39	20	E2	80	94	20	77	68	COVID-19 â€” wh
0768	69	63	68	20	69	73	E2	80	8C	E2	80	8C	E2	80	8C	E2	ich isâ€Câ€Câ€Câ
0784	80	8C	E2	80	8D	EF	BB	BF	E2	80	AC	EF	BB	BF	20	70	€Câ€ ï»¿â€¬ï»¿ p
0800	6F	73	73	69	62	6C	65	2C	C2	A0	61	63	63	6F	72	64	ossible,Â accord

发现是零宽隐写

用记事本打开，得到以下内容

```
Pyongyang stores low on foreign goods amid North Korean COVID-19 paranoia
Amid an ongoing, full-scale border         lockdown against COVID-19, North Korea on Tuesday warned its citizens
 against relying on imported         foreign goods — calling the habit a dangerous “disease” that could spread t
he virus from abroad.
Pyongyang’s warning against bringing in         foreign goods is not just empty words, either: On Monday, source
s told VOA that supermarkets and shops in Pyongyang have lacked foreign-sourced staples for months,         incl
uding coffee, cocoa and chocolate. This appears to be out of paranoia         that foreign goods could carry tra
ces of COVID-19 — which is         possible, according to the United Nations, though not the most common
 way the virus has been transmitted worldwide.
Sources also         told VOA that there’s currently no evidence that food items are coming across the border fr
om China, with only locally produced items available on Pyongyang store shelves.
INTENSE BORDER CONTROL
Tuesday’s state        -run Rodong Sinmun newspaper cautioned against the country’s long-standing “importation f
ever” (수입병), which comes         as the         North continues a strict border control. The DPRK even set up
 “shoot on sight” zones along its border with China for fear that         travelers could carry the virus. Meanw
hile, the country is operating under         the contested premise that items, air and even yellow dust pollutio
n         could carry COVID-19 across borders.
“The         most entangling issue today         on [the DPRK] demon
```

零宽隐写

[外链图片转存失败,源站可能有防盗链机制,建议将图片保存下来直接上传(img-VipUW8VY-1615891305446)(VNCTF2021.assets/image-20210316181154455.png)]

```
vncWthfe{APre T_1Sa_mc0 M1nGI?_fr0m_l@z@RuS}
```

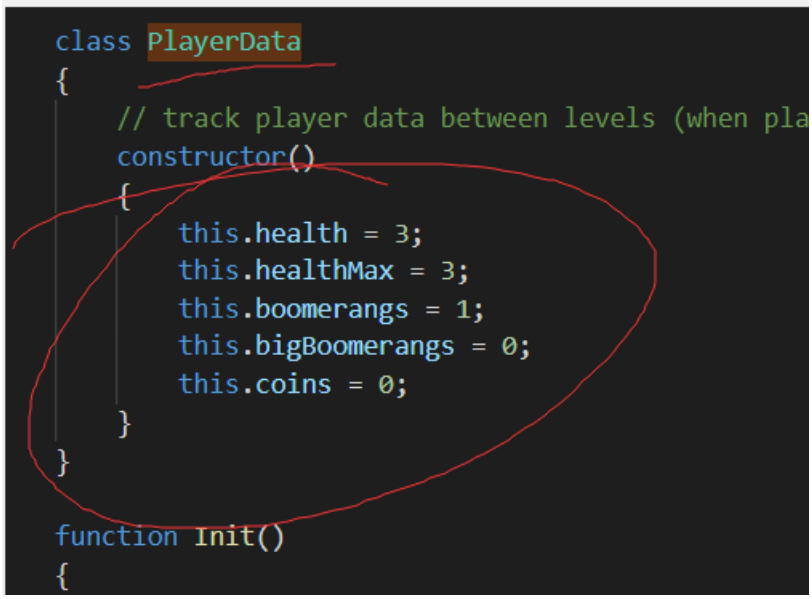
Web

[VNCTF 2021]Ez_game

JS泄露

F12一下可以看到game.js等三个js文件

我们查看一下，发现`game.js`开头是实例化，玩家信息我们在页面`Ctrl+Shift+F`搜索一下



更改一下参数，改为`999999`即可，改的太大，会卡死

然后F12在控制台跳一下关`NextLevel()`，一直跳就得到了flag。

> 一开始是跳到第九关然后打死的。后面才知道这个方法
> 如果一直跳关的话，也可以不改上面参数


```
flag{this_game_is_funny!}
```