Hgame 2021 WEEK4——容熙

Web

macguffin

打开查看网页源代码，发现提示 `/static/www.zip` ，下载得到源码。

查询代码，发现是nodejs的题目

搜索相关的题目，发现可能是原型链污染。

根据文章

https://nikoeurus.github.io/2019/12/18/D%5E3ctf-ezts/#js%E5%8E%9F%E5%9E%8B%E9%93%BE%E6%B1%A1%E6%9F%93

得知原型链污染有两种条件，一个是merge操作，一个是json解析。

而app.js里

```
const app = express()
app.use(bodyParser.urlencoded({ extended: true })).use(bodyParser.json())
app.use('/static', express.static('static'))
```

这里恰好启用了json解析。

在如下代码里发现需要使用让crying=true才能访问/wish

```
app.all('/wish', (req, res) => {
    if (!req.session.crying) {
        return res.send("forbidden.")
    }

    if (req.method == 'POST') {
        let wishes = req.body.wishes
        console.log(wishes);
        req.session.wishes = ejs.render(`<div class="wishes">${wishes}</div>`);
        return res.redirect(302, '/show');
    }

    return res.render('wish');
})
```

而对req.session.crying的赋值在

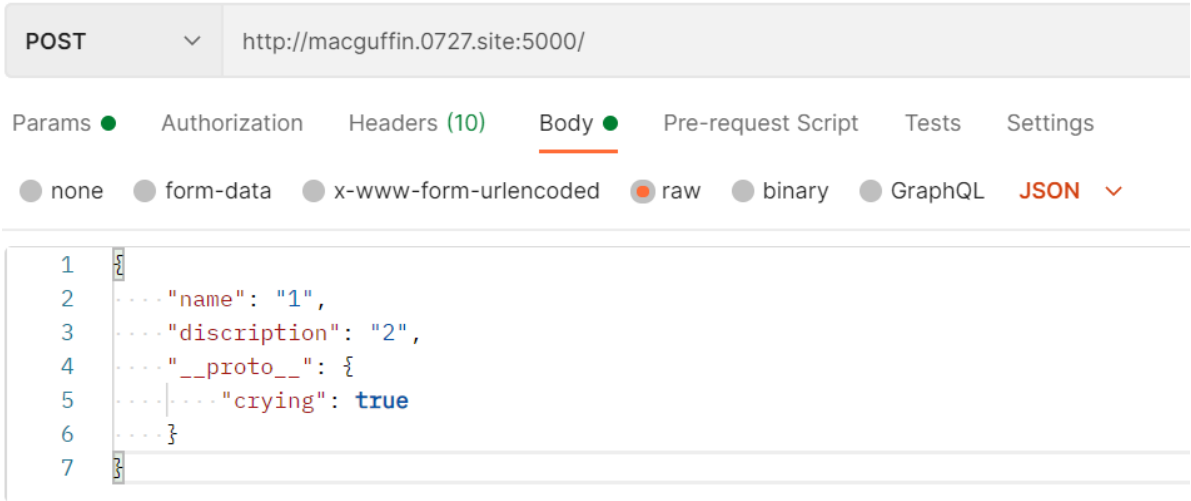
```
app.all('/', (req, res) => {
    let data = { name: "", discription: "" }
    if (req.ip === "::ffff:127.0.0.1") {
        data.crying = true
    }
    if (req.method == 'POST') {
        Object.keys(req.body).forEach((key) => {
            if (key !== "crying") {
                data[key] = req.body[key]
            }
        })
        req.session.crying = data.crying
        req.session.name = data.name
        req.session.discription = data.discription


        return res.redirect(302, '/show');
    }

    return res.render('loop')
})
```

可以看到限制了访问ip，以及过滤post数据的key不能是crying。

构造如下请求，以json格式发送

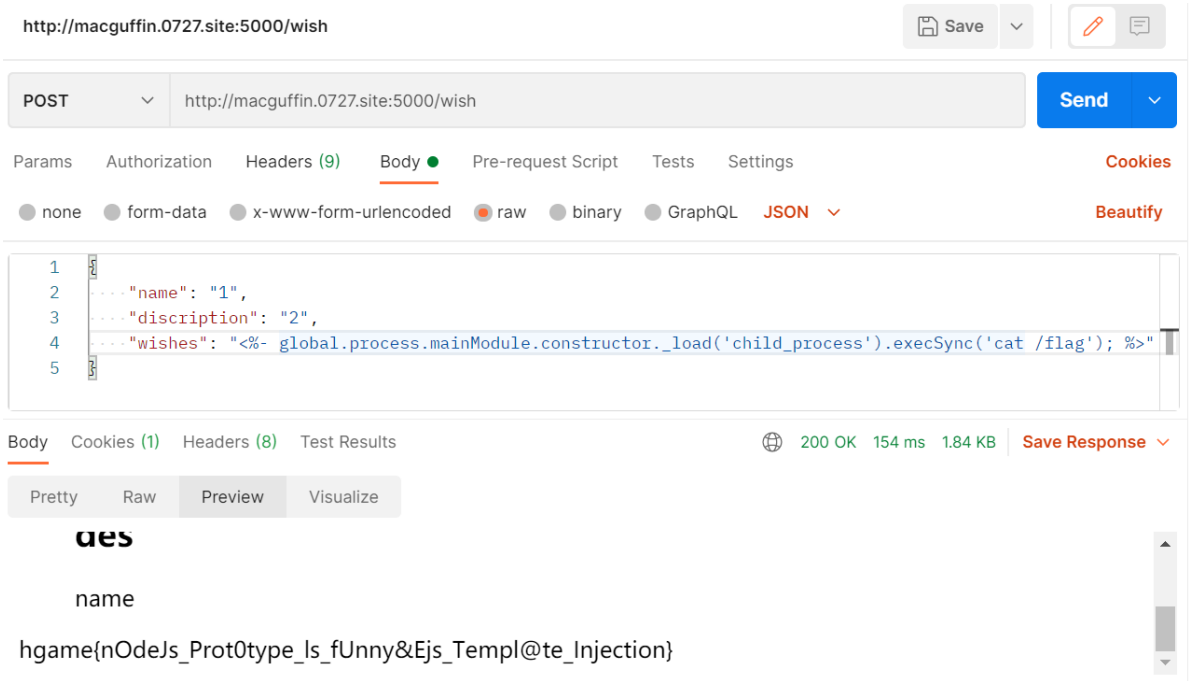


成功访问/wish，好像每过一段时间就得重新污染才能访问。

发现wishes可以模板注入，一开始一直使用`__proto__`，最后在 **耐心的4qE同志** 帮助下才成功使用模板注入

~~差点没来得及交flag~~

根据hgame2020 week4 sekiro 构造以下请求，命令成功执行。



flag为`hgame{nOdeJs_Prot0type_ls_fUnny&Ejs_Templ@te_Injection}`

Misc

Akira之瞳-1

根据raw文件以及"dump出来"题意，联想内存取证，使用volatility分析如下

```
PS D:\CTF\Tools\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\important_work.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\CTF\Tools\volatility_2.6_win64_standalone\important_work.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf8000403b0a0L
          Number of Processors : 16
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff8000403cd00L
                KPCR for CPU 1 : 0xfffff88004700000L
                KPCR for CPU 2 : 0xfffff88004776000L
                KPCR for CPU 3 : 0xfffff880047ec000L
                KPCR for CPU 4 : 0xfffff88004840000L
                KPCR for CPU 5 : 0xfffff880048b6000L
                KPCR for CPU 6 : 0xfffff8800492c000L
                KPCR for CPU 7 : 0xfffff880049a2000L
                KPCR for CPU 8 : 0xfffff880049d8000L
                KPCR for CPU 9 : 0xfffff88004a94000L
               KPCR for CPU 10 : 0xfffff88004b0a000L
               KPCR for CPU 11 : 0xfffff88004b80000L
               KPCR for CPU 12 : 0xfffff88004c00000L
               KPCR for CPU 13 : 0xfffff88004c76000L
               KPCR for CPU 14 : 0xfffff88004cec000L
               KPCR for CPU 15 : 0xfffff88004d62000L
            KUSER_SHARED_DATA : 0xfffff78000000000L
          Image date and time : 2021-02-18 09:47:25 UTC+0000
    Image local date and time : 2021-02-18 17:47:25 +0800
```

分析进程，发现important work压缩包

```
PS D:\CTF\Tools\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\important_work.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa800cd34040 System                    4      0    158      487 ------      0 2021-02-18 09:45:38 UTC+0000
0xfffffa800d975b30 smss.exe                364      4      2       44 ------      0 2021-02-18 09:45:38 UTC+0000
0xfffffa800d88f9d0 csrss.exe               456    420      9      539      0      0 2021-02-18 09:45:41 UTC+0000
0xfffffa800cd52060 wininit.exe             500    420      4       95      0      0 2021-02-18 09:45:41 UTC+0000
0xfffffa800e139b30 csrss.exe               520    508     11      235      1      0 2021-02-18 09:45:41 UTC+0000
0xfffffa800e182910 services.exe            568    500     14      283      0      0 2021-02-18 09:45:41 UTC+0000
0xfffffa800e193910 lsass.exe               576    500     10      618      0      0 2021-02-18 09:45:41 UTC+0000
0xfffffa800e198b30 lsm.exe                 584    500     11      167      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e3b0060 winlogon.exe            680    508      7      139      1      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e3c4b30 svchost.exe             720    568     13      411      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e3e8060 vm3dservice.ex          780    568      3       59      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e3fb3e0 svchost.exe             820    568      7      315      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e42bb30 svchost.exe             896    568     21      455      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e42a750 svchost.exe             940    568     23      487      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e445740 svchost.exe             968    568     44      900      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e479b30 audiodg.exe             180    896      6      149      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e49a890 svchost.exe             400    568     14      600      0      0 2021-02-18 09:45:42 UTC+0000
0xfffffa800e4bb3a0 svchost.exe             212    568     22      432      0      0 2021-02-18 09:45:43 UTC+0000
0xfffffa800e5f4410 spoolsv.exe            1184    568     17      360      0      0 2021-02-18 09:45:43 UTC+0000
0xfffffa800e614520 svchost.exe            1212    568     27      367      0      0 2021-02-18 09:45:43 UTC+0000
0xfffffa800e745b30 VGAuthService.         1532    568      5      121      0      0 2021-02-18 09:45:44 UTC+0000
0xfffffa800e7bd060 vmtoolsd.exe           1584    568     11      285      0      0 2021-02-18 09:45:44 UTC+0000
0xfffffa800e84ab30 WmiPrvSE.exe           1848    720     11      202      0      0 2021-02-18 09:45:44 UTC+0000
0xfffffa800e832b30 dllhost.exe            1292    568     36      297      0      0 2021-02-18 09:45:45 UTC+0000
0xfffffa800e8fab30 svchost.exe             444    568      7      111      0      0 2021-02-18 09:45:45 UTC+0000
0xfffffa800e708960 dllhost.exe            2148    568     17      240      0      0 2021-02-18 09:45:45 UTC+0000
0xfffffa800e9524e0 msdtc.exe              2240    568     16      173      0      0 2021-02-18 09:45:45 UTC+0000
0xfffffa800e994060 VSSVC.exe              2440    568      6      134      0      0 2021-02-18 09:45:46 UTC+0000
0xfffffa800eae1b30 WmiPrvSE.exe           2692    720     12      307      0      0 2021-02-18 09:46:04 UTC+0000
0xfffffa800eb54950 WmiApSrv.exe           2800    568      7      129      0      0 2021-02-18 09:46:05 UTC+0000
0xfffffa800eb8b630 taskhost.exe           2960    568     10      196      1      0 2021-02-18 09:46:50 UTC+0000
0xfffffa800ec09b30 dwm.exe                1540    940      7      131      1      0 2021-02-18 09:46:51 UTC+0000
0xfffffa800ec12b30 explorer.exe           2232   3064     32      713      1      0 2021-02-18 09:46:51 UTC+0000
0xfffffa800ecaf210 vm3dservice.ex         1364   2232      5       81      1      0 2021-02-18 09:46:54 UTC+0000
0xfffffa800ec313e0 vmtoolsd.exe           1268   2232      9      180      1      0 2021-02-18 09:46:54 UTC+0000
0xfffffa800e5ab460 taskmgr.exe            2780    680     12      144      1      0 2021-02-18 09:46:59 UTC+0000
0xfffffa800e5c6b30 SearchIndexer.         1252    568     13      647      0      0 2021-02-18 09:47:00 UTC+0000
0xfffffa800ed50b30 wmpnetwk.exe           2572    568     13      251      0      0 2021-02-18 09:47:00 UTC+0000
0xfffffa800ed2eb30 svchost.exe            2596    568     13      182      0      0 2021-02-18 09:47:00 UTC+0000
0xfffffa800f246670 SearchProtocol          736   1252      7      245      1      0 2021-02-18 09:47:11 UTC+0000
0xfffffa800f248060 SearchFilterHo         2552   1252      5      101      0      0 2021-02-18 09:47:11 UTC+0000
0xfffffa800f263b30 important_work         1092   2232      1       16      1      1 2021-02-18 09:47:15 UTC+0000
0xfffffa800f260060 conhost.exe            1372    520      2       63      1      0 2021-02-18 09:47:16 UTC+0000
0xfffffa800f29fb30 cmd.exe                1340   1092      1       29      1      1 2021-02-18 09:47:16 UTC+0000
0xfffffa800ec13590 dllhost.exe            3128    720      6      102      1      0 2021-02-18 09:47:21 UTC+0000
0xfffffa800f2ba750 dllhost.exe            3184    720      6       99      0      0 2021-02-18 09:47:22 UTC+0000
0xfffffa800f277b30 DumpIt.exe             3216   2232      2       75      1      1 2021-02-18 09:47:22 UTC+0000
0xfffffa800edc6240 conhost.exe            3224    520      2       61      1      0 2021-02-18 09:47:22 UTC+0000
```

扫描命令行，发现import work有参数

```
PS D:\CTF\Tools\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\important_work.raw --profile=Win7SP1x64 cmdscan
Volatility Foundation Volatility Framework 2.6
**************************************************
CommandProcess: conhost.exe Pid: 1372
CommandHistory: 0x2bb6240 Application: important_work.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x10
**************************************************
CommandProcess: conhost.exe Pid: 1372
CommandHistory: 0x2bb7420 Application: cmd.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x88
**************************************************
CommandProcess: conhost.exe Pid: 3224
CommandHistory: 0x2a95f60 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x64
```

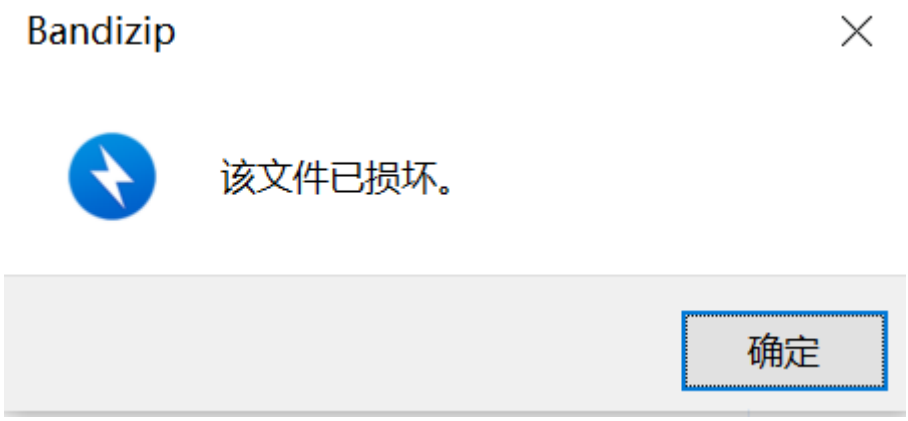
查看参数，发现有个work.zip

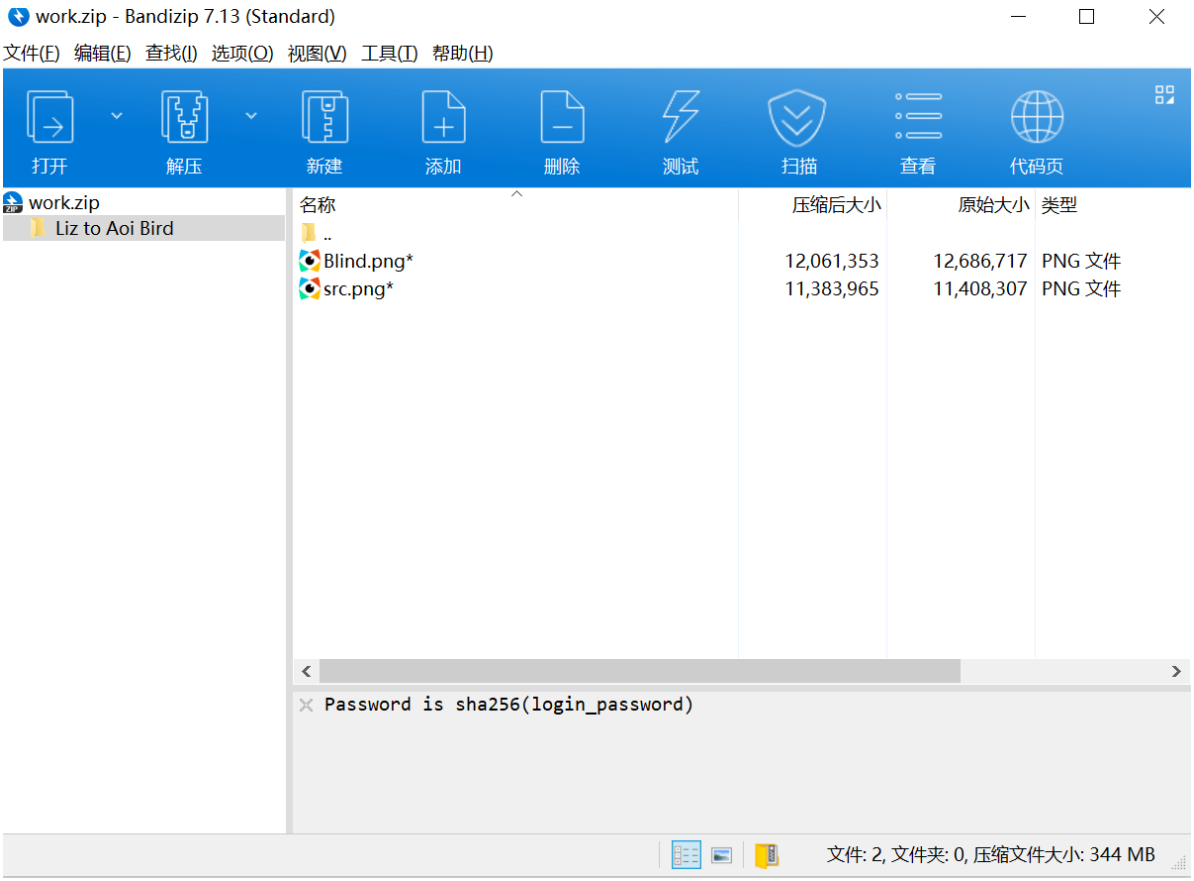
```
Data\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"  "1"
**********************************************************************
SearchFilterHo pid:   2552
Command line : "C:\Windows\system32\SearchFilterHost.exe" 0 584 588 596 65536 592
**********************************************************************
important_work pid:   1092
Command line : "C:\Users\Genga03\Desktop\important_work.exe" C:\Users\Genga03\Desktop\work.zip
**********************************************************************
conhost.exe pid:   1372
Command line : \??\C:\Windows\system32\conhost.exe
**********************************************************************
cmd.exe pid:   1340
Command line : C:\Windows\system32\cmd.exe /c pause
**********************************************************************
dllhost.exe pid:   3128
Command line : C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
**********************************************************************
dllhost.exe pid:   3184
Command line : C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
**********************************************************************
DumpIt.exe pid:   3216
Command line : "C:\Users\Genga03\Desktop\DumpIt.exe"
**********************************************************************
conhost.exe pid:   3224
Command line : \??\C:\Windows\system32\conhost.exe
```

提取文件

```
PS D:\CTF\Tools\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\important_work.raw --profile=Win7SP1x64 memdump -p 1092 -D .
Volatility Foundation Volatility Framework 2.6
************************************************************************
Writing important_work [  1092] to 1092.dmp
```

改名成work.zip，虽然提示错误但是可以打开





需要login_password。查询资料后猜测要用NTLM获取密码。

```
PS D:\CTF\Tools\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\important_work.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Genga03:1001:aad3b435b51404eeaad3b435b51404ee:84b0d9c9f830238933e7131d60ac6436:::
```

找到一个在线解密的网站，发现前面两个没有结果，第三个的结果为asdqwe123

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
31d6cfe0d16ae931b73c59d7e0c089c0
31d6cfe0d16ae931b73c59d7e0c089c0
84b0d9c9f830238933e7131d60ac6436
```

进行人机身份验证 reCAPTCHA 隐私权 - 使用条款

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
31d6cfe0d16ae931b73c59d7e0c089c0	NTLM	
84b0d9c9f830238933e7131d60ac6436	NTLM	asdqwe123

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

sha256后得到压缩包密码为

`20504cdfddaad0b590ca53c4861edd4f5f5cf9c348c38295bd2dbf0e91bca4c3`

解压后发现两张一样的图，根据文件名blind猜测是盲水印。

查资料发现工具：https://github.com/chishaxie/BlindWaterMark

```
PS D:\CTF\Tools\BlindWaterMark-master> python .\bwmforpy3.py decode .\src.png .\Blind.png wm.png
image<.\src.png> + image(encoded)<.\Blind.png> -> watermark<wm.png>
PS D:\CTF\Tools\BlindWaterMark-master>
```

在多次失败尝试后，询问`友好的Akira前辈`得知需要64位的python。

努力翻译后，盲~~画师~~做题人诞生

flag为`hgame{7he_f1ame_brin9s_me_end1ess_9rief}`

Akira之瞳-2

也是和上一题类似的raw文件，先查看系统版本，似乎和上一题差不多。

```
PS D:\CTF\Games\HGAME2021\MISC\WEEK4\Akira之瞳-2> .\volatility_2.6_win64_standalone.exe -f .\secret_work.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7S
1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\CTF\Games\HGAME2021\MISC\WEEK4\Akira之瞳-2\secret_work.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf80003ff7120L
          Number of Processors : 16
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80003ff9000L
                KPCR for CPU 1 : 0xfffff88004500000L
```

查看进程，感觉notepad比较可疑

```
0xfffffa801b475b00 notepad.exe            456   2372      1       63      1      0 2021-02-19 08:19:52 UTC+0000
0xfffffa801a154060 SearchProtocol        3732   1308      8      294      0      0 2021-02-19 08:22:20 UTC+0000
0xfffffa801a175b00 SearchFilterHo        2080   1308      5      118      0      0 2021-02-19 08:22:20 UTC+0000
0xfffffa801b172060 chrome.exe            3948   2372     43      815      1      0 2021-02-19 08:22:27 UTC+0000
0xfffffa801b15e060 chrome.exe            4052   3948      8       92      1      0 2021-02-19 08:22:27 UTC+0000
0xfffffa801bb6f8b0 chrome.exe            3572   3948      2       56      1      0 2021-02-19 08:22:28 UTC+0000
0xfffffa801bb82b00 chrome.exe            1300   3948     11      247      1      0 2021-02-19 08:22:28 UTC+0000
0xfffffa801b154970 chrome.exe            1004   3948     21      384      1      0 2021-02-19 08:22:28 UTC+0000
0xfffffa801b9025f0 chrome.exe            2916   3948     32      337      1      0 2021-02-19 08:22:28 UTC+0000
0xfffffa8018ed8b00 WmiPrvSE.exe          2204    700     13      315      0      0 2021-02-19 08:22:31 UTC+0000
0xfffffa801b57eb00 WmiApSrv.exe          4088    560      8      128      0      0 2021-02-19 08:22:33 UTC+0000
0xfffffa801b5563d0 chrome.exe            1160   3948     24      471      1      0 2021-02-19 08:22:46 UTC+0000
```

查看cmdline，发现有个dumpme.txt

```
**************************************************************************
notepad.exe pid:    456
Command line : "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Genga03\Desktop\dumpme.txt
**************************************************************************
```

~~memdump出来太大，打不开~~

根据hint，换成dumpfiles。

```
PS D:\CTF\Games\HGAME2021\MISC\WEEK4\Akira之瞳-2> .\volatility_2.6_win64_standalone.exe -f .\secret_work.raw --profile=W
in7SP1x64 filescan | findstr dumpme
Volatility Foundation Volatility Framework 2.6
0x000000007ef94820      2      0 RW-r-- \Device\HarddiskVolume1\Users\Genga03\Desktop\dumpme.txt
0x000000007f2b5f20      2      0 RW-rw- \Device\HarddiskVolume1\Users\Genga03\AppData\Roaming\Microsoft\Windows\Recent\d
umpme.txt.lnk
```

```
PS D:\CTF\Games\HGAME2021\MISC\WEEK4\Akira之瞳-2> .\volatility_2.6_win64_standalone.exe -f .\secret_work.raw --profile=W
in7SP1x64 dumpfiles -Q 0x000000007ef94820  --dump-dir=.
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x7ef94820   None   \Device\HarddiskVolume1\Users\Genga03\Desktop\dumpme.txt
```

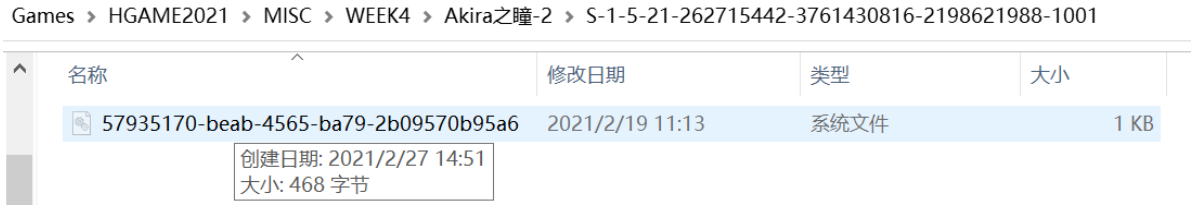
得到提示

```
zip password is: 5trqES&P43#y&1TO
And you may need LastPass
```

解压后得到空文件夹

显示系统文件后能看到

~~emmm这.....~~



根据lastpass和Akira的提示，找到volatility插件

https://github.com/kevthehermit/volatility_plugins/tree/master/lastpass

从lastpass中得到windows密码

```
Found LastPass Entry for
live.com,bing.com,hotmail.com,live.com,microsoft.com,msn.com,windows.com,windows
azure.com,office.com,skype.com,azure.com
UserName: windows login & miscrosoft
Pasword: vIg*q3x6GFa5aFBA
```

使用mimikatz获取masterkey，由于mimikatz没有help，询问了Akira前辈才知道需要什么参数

```
dpapi::masterkey /in:S-1-5-21-262715442-3761430816-2198621988-1001\57935170-beab-4565-ba79-2b09570b95a6 /password:vIg*q3x6GFa5aFBA /sid:S-1-5-21-262715442-3761430816-2198621988-1001
```

得到masterkey

```
key :
3cafd3d8e6a67edf67e6fa0ca0464a031949182b3e68d72ce9c08e22d7a720b5d2a768417291a28fb79c6def7d068f84955e774e87e37c6b0b669e05fb7eb6f8
sha1: 8fc9b889a47a7216d5b39c87f8192d84a9eb8c57
```

然后解Cookies

```
dpapi::chrome /in:Cookies /masterkey:3cafd3d8e6a67edf67e6fa0ca0464a031949182b3e68d72ce9c08e22d7a720b5d2a768417291a28fb79c6def7d068f84955e774e87e37c6b0b669e05fb7eb6f8

Host  : localhost ( / )
Name  : VeraCrypt
Dates : 2021/2/19 14:08:59 -> 2022/2/19 14:00:00
 * masterkey     :
3cafd3d8e6a67edf67e6fa0ca0464a031949182b3e68d72ce9c08e22d7a720b5d2a768417291a28fb79c6def7d068f84955e774e87e37c6b0b669e05fb7eb6f8
Cookie: !bWjAqM2z!iSoJsV*&IRV@*AVI1VrtAb
```

根据提示使用VeraCrypt，加载加密磁盘Container得到ADS.jpg

根据文件名ADS提示，找到工具ntfsstreamseditor，查看ADS.jpg获得flag

flag为`hgame{Which_0nly_cryin9_3yes_c4n_de5cribe}`