# 2021"西湖论剑"网络安全大赛Writeup

# 原创

Le1a ● 于 2021-11-21 13:46:30 发布 ● 7242 ☆ 收藏 6 分类专栏: CTF 文章标签: 安全 网络安全 版权声明:本文为博主原创文章,遵循 CC 4.0 BY-SA 版权协议,转载请附上原文出处链接和本声明。 本文链接: https://blog.csdn.net/weixin\_52091458/article/details/121452876 版权



CTF 专栏收录该内容

12 篇文章 3 订阅 订阅专栏

## 2021"西湖论剑"网络安全大赛Writeup

我只写了自己做的部分,完整WP请访问: https://www.yuque.com/docs/share/4c901b3e-a9c4-4e67-9d1c-3030108ca4a0?# 密码: slhq

## Web

详见fmyyy师傅: https://blog.csdn.net/fmyyy1/article/details/121451279?spm=1001.2014.3001.5501

#### Misc

真·签到

	表题详情。 第1991年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日
题目名称:	真·签到
题目内容:	扫码进入西湖论剑网络安全大赛微信公众号,发送语音说出"西湖论剑2021,我来了。"即可获得 本题 flag: )
题目分数:	100
当前答出前3名:	第一名 DebuGGer 第二名 ReT0 第三名 财贸夺Flag队
相关附件:	下载附件下载

扫码关注公众号,发送语音即可



flag:

DASCTF{welc0m3\_t0\_9C51s\_2021}

## YUSA的小秘密

表题详情。 1993年———————————————————————————————————							
题目名称:	YUSA的小秘密						
题目内容:	LSB,但又不是LSB,众所周知不止RGB。yusa,我的yusa,嘿嘿						
题目分数:	100						
当前答出前3名:	第一名 H4F 第二名 南门辣子鸡 第三名 0x401						
相关附件:	"YUSA的小秘密"的题目附件 下载						

这题跟去年的ByteCTF的 Hardcore Watermark 01 几乎一模一样,官方wp链接: https://bytectf.feishu.cn/docs/doccnqzpGCWH1hkDf5ljGdjOJYg#

这题采用的不是RGB通道的LSB隐写,而是采用的YCrCb通道。通过 cv2.cvtColor(img, cv2.COLOR\_BGR2YCrCb) 对 img 图片数 据进行色彩空间转换,即可得到三个通道的数据,然后对三个通道的数据分别根据奇偶做二值化处理并保存为图片

```
cv.imwrite('a.png', (a % 2) * 255) #对三个通道中的数据分别根据奇偶做二值化处理,并分别保存为图片
cv.imwrite('b.png', (b % 2) * 255)
cv.imwrite('c.png', (c % 2) * 255)
```

所以完整脚本如下:

from cv2 import *	
import cv2 as cv	
<pre>img=cv2.imread('C:\\Users\\XXX\\Desktop\\yusa\\yusa.png')</pre>	
<pre>src_value=cv2.cvtColor(img, cv2.COLOR_BGR2YCrCb)</pre>	
a, b, c = cv.split(src_value)	
cv.imwrite('a.png', (a % 2) * 255)	并分别保存为图片
cv.imwrite('b.png', (b % 2) * 255)	
cv.imwrite('c.png', (c % 2) * 255)	

运行后会得到三个通道的图片,在其中 a.png 即可清晰看到flag



flag:

DASCTF{2947b683036d49e5681f83f7bc3fbb34}

### Yusa的秘密

	表题详情。 第1991年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日									
题目名称:	Yusa的秘密									
题目内容:	Sakura组织即将进攻地球,此时你意外得到了该组织内某个成员的电脑文件,你能从中发现本次 阴谋所用的关键道具吗。(注:题目中包含了五个彩蛋,目彩蛋对解题本身没有任何影响,快去 发现吧!) https://gcsis-2021-misc-atta-1251267611.file.myqcloud.com/3iuryh387ryh34eiud/Yus a%E7%9A%84%E7%A7%98%E5%AF%86.zip									
题目分数:	200									
当前答出前3名:	第一名 香香嘴炒饭	第二名 n03tAck	第三名 EDI							

下载附件,发现这是一个内存取证的题目,先用命令获取一下内存镜像的进程

now profile-WinZCD1x64 n

DC

VOI.EXE -1 HUSA-P	C.I awprofite=will/3	F 1X04	+ havat	ew								
											_	
C:\Windows\System	32\cmd.exe											$\times$
Microsoft Windows	[版本 10.0.22000.318]											
(c) Microsoft Corp	oration。保留所有权利。											
						1 04						
C:\Users\YiJiale\D	esktop\4X业之vol.exe -i ! ion Valatility Enomenant	usa-l	PC.raw -	profi	Le=Win7SP.	1x64 psz	view					
Offect (P)	Namo	2.0 PTN	neliet	neccan	thrdproc	nencid	oeree	enseion	dockthrd Fr	itTimo		
0x00000003f242b30	conhost.exe	1356	True	True	True	True	True	True	False			
0x00000003e464b30	svchost.exe	1272	True	True	True	True	True	True	True			
0x00000003e91d920	conhost.exe	1344	True	True	True	True	True	True	False			
0x00000003e2af890	svchost.exe	1836	True	True	True	True	True	True	True			
0x00000003f949060	audiodg. exe	2744	True	True	True	True	True	True	True			
0x00000003e449470	taskhost.exe	1244	True	True	True	True	True	True	False			
0x00000003fa2e590	dllhost.exe	1168	True	True	True	True	True	True	False			
0x00000003e646b30	svchost.exe	712	True	True	True	True	True	True	True			
0x00000003e6a4b30	svchost.exe	856	True	True	True	True	True	True	True			
0x00000003e7703a0	svchost.exe	348	True	True	True	True	True	True	True			
0x00000003e516630	svchost.exe	1408	True	True	True	True	True	True	True			
0x00000003e9008f0	winlogon.exe	432	True	True	True	True	True	True	True			
0x00000003e455810	dwm. exe	2260	True	True	True	True	True	True	False			
0x00000003e122890	SearchIndexer.	2552	True	True	True	True	True	True	True			
0x00000003e434910	spoolsv.exe	1212	True	True	True	True	True	True	True			
0x00000003e6b5830	svchost.exe	884	True	True	True	True	True	True	True			
0x00000003e6763e0	svchost.exe	772	True	True	True	True	True	True	False			
0x00000003fab2b30	DumpIt.exe	820	True	True	True	True	True	True	False			
0x00000003e58f060	vmtoolsd.exe	1520	True	True	True	True	True	True	True			
0x00000003e6ca750	cmd. exe	2536	True	True	True	True	True	True	False			
0x00000003e0804b0	vmtoolsd.exe	2380	True	True	True	True	True	True	False			
0x000000003fb54b30	svchost.exe	1232	True	True	True	True	True	True	False			
0x00000003e96e1d0	services.exe	488	True	True	True	True	True	True	False			

这些进程都分析了一下,发现有StikyNot.exe进程,这是windows的便签程序,可以尝试寻找snt文件来查看便签的内容。这里就 直接来用filescan查找文件,用windows的findstr命令筛选一下,先查看下压缩包

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r 'zip'

C:\Users\YiJiale\Desktop\取证>vol.exe -f Yusa-PC.raw Volatility Foundation Volatility Framework 2.6 0x00000003e444a60 15 0 Rr-d \Device\Harddis 0x00000003e522e0 16 0 Rr-d \Device\Harddis 0x00000003f2f49e0 15 0 Rr \Device\Harddis 0x00000003f3356f0 1 0 Rrw- \Device\Harddis C:\Users\YiJiale\Desktop\取证>	profile=Win7SF kVolume2\Windc kVolume2\Progr kVolume2\Progr kVolume2\PROGF	Plx64 filescan ows\System32\z am Files\VMwa am Files\VMwa A~1\MSBuild\M	a   findstr /r sipfldr.dll re\VMware Too re\VMware Too HCROS~1\WINDO	"zip" ls\zip.exe ls\zip.exe W~1\key.zip	р	
有一个 <mark>key.zip</mark> 。直接使用命令dump下来,重命名为1.zip						
vol.exe -f Yusa-PC.rawprofile=Win7SP1x64 dumpfil	es -Q 0x00000	0003f3356f0	-D C:\Users\>	(XX\Deskto	p\取	证
里面是一个exp文件,但是压缩包加密了,需要寻找密码						
<b>IIZ</b> C:\Users\YiJiale\Desktop\取证\1.zip\				_		×
文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H)						
中 ▼      ・・・・・・						
₱ I C:\Users\YiJiale\Desktop\取证\1.zip\						~
名称	大小	压缩后大小	修改时间	创建时间		访问时间
exp	453	273	2021-10-2	2021-10-2	2	2021-10-

#### 刚刚查找进程提到过便签的进程,这里来尝试查找一下snt文件

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "snt"

C:\Users\YiJiale\Deskt	top\取i	E>vol	.exe -f	Yusa-PC.rawprofile=Win7SP1x64 filescan   findstr /r "snt"				
Volatility Foundation	Volati	lity	Framewo	rk 2.6				
0x000000003e2d29d0	16	Ō	Rr-d	\Device\HarddiskVolume2\Windows\System32\zh-CN\sntsearch.dll.mui				
0x00000003e9033d0	2	0	Rr-d	\Device\HarddiskVolume2\Windows\System32\sysntfy.dll				
0x00000003fb306e0	16	1	RW-r	\Device\HarddiskVolume2\Users\Yusa\AppData\Roaming\Microsoft\Sticky Notes\Sticky				
Notes. snt								
C:\Users\YiJiale\Desktop\取证>								

发现了便签文件,我们将他dump下来查看

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003fb306e0 -D C:\Users\XXX\Desktop\取证

将其重命名为 StickyNotes.snt,用记事本打开是看不到上面东西的,既然数win7的便签,我们就将其传入win7虚拟机尝试打开 (这里因为VMware tools始终无法装上,便采用QQ传输文件),后来发现家庭普通版的Win7居然没有便签这个程序,我是 Win11,没有便签程序,于是我尝试下Win10虚拟机

将snt文件放入C:\Users\XXX\AppData\Roaming\Microsoft\Sticky Notes\路径下,然后打开便签程序,便可以得到



得到了一个密码:世界没了心跳

0% 正在复制			_	
已用时间: 剩余时间:	00:00:02	总大小: 速度: 司孙珊·		453
又曰: 压缩率:	输入密码	<u>二</u> 处理:		0
exp	输入密码: 世界没了心跳			
	✓ 显示密码(S)			
	确定	取消		
	后台(B)	暂停(P)		取消

用这个密码成功打开刚刚的exp的压缩包,得到exp文件

```
from PIL import Image
import struct
pic = Image.open('key.bmp')
fp = open('flag', 'rb')
fs = open('Who am I', 'wb')
a, b = pic.size
list1 = []
for y in range(b):
    for x in range(a):
        pixel = pic.getpixel((x, y))
        list1.extend([pixel[1], pixel[0], pixel[2], pixel[2], pixel[1], pixel[0]])
data = fp.read()
for i in range(0, len(data)):
    fs.write(struct.pack('B', data[i] ^ list1[i % a*b*6]))
fp.close()
fs.close()
```

通过分析exp可以发现,目前还缺少两个文件便可以得到flag文件,分别是Who\_am\_l和key.bmp文件

这里Who am I,既然是Yusa的秘密,那用户应该就是Yusa了,使用命令来获取一下用户名的hash密码

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 hashdump

C:\Users\YiJiale\Desktop\取证>vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 hashdump Volatility Foundation Volatility Framework 2.6 Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::: HomeGroupUser\$:1002:aad3b435b51404eeaad3b435b51404ee:84f851a4a47f1a1c9408b7e1ab7b469e::: Yusa:1003:aad3b435b51404eeaad3b435b51404ee:74869621853fe4de089dc07679c2475b:::

C:\Users\YiJiale\Desktop\取证>\_

使用 Passware Kit 13 来破解Yusa用户的密码

打开软件,点击 Memory Analysis 功能,再选择 Windows User 功能

🛃 Passware Password Recovery K	Kit Forensic	_	×
File View Tools Help			
🚱 Back 🛞 Forward 🥎 Star	art Page 🛛 🔚 Save Results 📚 Print 🚽 Check for Updates 🤱 Support 🕜 Help		
Attack Summary 🛠 Passwords found:	C:\Users\YiJiale\Desktop\职证\Yusa-PC.raw Protection: Memory Image Complexity: Instant Unprotection		
1 password Total time elapsed: 21 sec. Estimated completion time:	Memory image file:       Yusa-PC.raw         Folder:       C:\Users\YiJiale\Desktop\取正\         Protection:       Memory Image - 1 Password(s)         Complexity:       Instant Unprotection		~
[completed]	YUSA-PC\Yusa password: [YusaYusa520] (no brackets) <copy></copy>		
			~
	Passwords found ( Attacks ) Log /		
Please select a file to recover its pa	password, or drag and drop a file to this window to start the recovery		

#### 发现得到了密码为: YusaYusa520

成功打开了Who\_am\_I的压缩包得到了Who\_am\_I文件,题目描述中出现了Sakura组织,所以这里也查找一下相关文件

题目名称:	Yusa的秘密			
题目内容:	Sakura组织即将进攻地球, 阴谋所用的关键道具吗。 发现吧! ) https://gcsis-20 a%E7%9A%84%E7%A7%	此时你意外得到了该组 (注:题目中包含了五个; 21-misc-atta-12512676 。98%E5%AF%86.zip	织内某个成员的电 彩蛋,且彩蛋对解。 11.file.myqcloud.cc	脑文件,你能从中发现本次 题本身没有任何影响,快去 om/3iuryh387ryh34eiud/Yus
题目分数:	200			
当前答出前3名:	第一名 香香嘴炒饭	第二名 n03tAck	第三名 EDI	

#### vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r "Sakura"

C:\Users\YiJiale\Deskt	op\取证	>vol.exe −f	Yusa-PC.rawprofile=Win7SP1x64 filescan   findstr /r "Sakura"
Volatility Foundation	Volatil:	ity Framewo	rk 2.6
0x000000003e58ada0	1	0 Rr	\Device\HarddiskVolume2\Program Files\MSBuild\Microsoft\Windows Workflow Foundat
,ion∖Sakura-didi			
0x00000003e78c6a0	1	0 Rr	\Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura鏂困欢\Sakura-鍏 憡
0x00000003f2ae290	1	0 Rr	\Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura鏂困欢\Sakura-egg5
0x00000003f959980	1	0 Rr	\Device\HarddiskVolume2\Users\Yusa\Desktop\Sakura鏂困欢\Sakura-澶囧繕褰?

~ 配 C:\Users\YiJiale\Desktop\取证\2.zip\				- 0	×				
文件(F) 编辑(E) 查看(V) 书签(A) 工具(T) 帮助(H)									
中 ▽ 中 → × 1       添加 提取 测试 复制 移动 删除 信息									
₱ Interview of the second secon					~				
名称	大小	压缩后大小	修改时间	创建时间	访问时间				
🛋 key.bmp	1 254	1 266	2021-10-2	2021-10-2	2021-10-				

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003e58ada0 -D C:\Users\XXX\Desktop\取证

打开压缩包,里面确实是key.bmp文件,但是还是需要密码,接下来就只需要去找密码了

联想到一开始分析进程的时候,除了便签程序,还有一个平时很少遇到过的wab.exe,这是通讯录的程序,我们试着找一下其中的联系人,联系人contact文件,用filescan搜索一下

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 filescan | findstr /r <u>"contact"</u>

一共得到了两个联系人的文件,分别是Yusa.contact和Mystery Man.contact

C:\Users\YiJiale\Deskt	op\取证	>vol. @	exe -f	Yusa-PC.raw -	-profile=W	/in7SP1x64 fi	lescan	findstr /1	c "contact"
Volatility Foundation	Volatil	ity Fi	ramewo	ork 2.6					
0x000000003e748f20	1	0 R-	r-d	\Device\Harddi	skVolume2\	Users\Yusa\C	ontacts\	Yusa. contac	et
0x000000003fa09070	1	0 R-	r-d	\Device\Harddi	skVolume2\	Users\Yusa\C	ontacts\	Mystery Mar	n. contact

我们分别dump下来分析一下

vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x000000003e748f20 -D C:\Users\XXX\Desktop\取证 vol.exe -f Yusa-PC.raw --profile=Win7SP1x64 dumpfiles -Q 0x00000003fa09070 -D C:\Users\XXX\Desktop\取证



打开里面是base64编码,解码得到一张Yusa的bmp图片



但这并不是我们想要的东西,接着看另一个联系人文件

藚 file.None.0xfffffa8003b86010.dat - 记事本			_		$\times$
文件(F) 编辑(E) 格式(O) 视图(V) 帮助(H)					
xml version="1.0" encoding="UTF-8"</td <td>'?&gt;</td> <td></td> <td></td> <td></td> <td></td>	'?>				
<c:contact <="" c:version="1" td="" xmlns:c="http&lt;/td&gt;&lt;td&gt;://schei&lt;/td&gt;&lt;td&gt;mas.microsoft.c&lt;/td&gt;&lt;td&gt;om/C&lt;/td&gt;&lt;td&gt;Contac&lt;/td&gt;&lt;td&gt;:t"></c:contact>					
xmlns:xsi="http://www.w3.org/2001/XM	<b>ALSche</b>	ma-instance"			- 1
xmlns:MSP2P="http://schemas.microso	ft.com/	Contact/Extend	ed/Ⅳ	ISP2P	">
<c:notes c:mo<="" c:version="2" td=""><td>dificatio</td><td>onDate="2021-1</td><td>0-</td><td></td><td>- 1</td></c:notes>	dificatio	onDate="2021-1	0-		- 1
28T11:47:56Z">LF2XGYPPXSGOPO4E46	5YPZM	IITLSYRGXGWS7	OIO,	EL42C	2
LZFYQDSLRKXEXO56LCVB566IZ2FPW7	537K7H	IQK46LLUM42E.	JB354	4RTSL	31
HFR6VONHEJ4S4ITZNEVHTJPNXJS62OI	<b>HAECG</b> 2	ZGCWWRVOBU	XMN	KMGJ	TT 📗
KTDZME2TKU3PGVMWS5ZVGVYUKYJS	KY2TOI	N3ZJU2VSK3W0	GVGF	IK3BV	′G
VJW6NLBGZCDK33NKQ2WE6KBGU3XK	RJVG52	2UQNJXOVNDK	TBSN	/142TK	(4
KFGVRGK3BVLFLTGNBUINBTKYTFNQ2	/SVZTG	VNEOOJVLJBU4	4NKN	/IGZSI	DK
NCXNY2UY4KHGVGHSZZVG52WMNSL	MVCTK	WLJLI2DIQ2DM	EZFN	/NJXC	35
4WCT2EJF3VSV2NGVGW2SJVLJVFKNC	NKRIXS	WLNJJUVS6SJG	NMT	ERLZJ	5
KFM3KNK5HG2TSEM46Q=== <td>tes&gt;<c:< td=""><td>CreationDate&gt;2</td><td>021-</td><td>10-</td><td></td></c:<></td>	tes> <c:< td=""><td>CreationDate&gt;2</td><td>021-</td><td>10-</td><td></td></c:<>	CreationDate>2	021-	10-	
28T05:56:31Z <c:exte< td=""><td>nded xs</td><td>si:nil="true"/&gt;</td><td></td><td></td><td></td></c:exte<>	nded xs	si:nil="true"/>			
<c:contactidcollection><c:co< td=""><td>ontactIE</td><td>C:ElementID="</td><td>c814</td><td>82a1-</td><td></td></c:co<></c:contactidcollection>	ontactIE	C:ElementID="	c814	82a1-	
44bc-43bf-bfc0-159ab6a43962"> <c:va< td=""><td>alue&gt;17</td><td>'6e8955-bc8e-4</td><td>88a-</td><td>9cb2-</td><td></td></c:va<>	alue>17	'6e8955-bc8e-4	88a-	9cb2-	
b4fbffa547b3 <td>&gt; <td>ontactIDCollectio</td><td>&gt;n&gt;&lt;</td><td>c:Nan</td><td>ne</td></td>	> <td>ontactIDCollectio</td> <td>&gt;n&gt;&lt;</td> <td>c:Nan</td> <td>ne</td>	ontactIDCollectio	>n><	c:Nan	ne
Collection> < c:Name c:ElementID="86et	i8fab-e	13d-4b52-9cf5-			
ec0601898181"> <c:title>保持神秘<td>itle&gt;<c< td=""><td>::FormattedNam</td><td>ie&gt;M</td><td>ystery</td><td>/</td></c<></td></c:title>	itle> <c< td=""><td>::FormattedNam</td><td>ie&gt;M</td><td>ystery</td><td>/</td></c<>	::FormattedNam	ie>M	ystery	/
Man <c:givennan< td=""><td>ne&gt;Mys</td><td>stery</td><td></td><td></td><td></td></c:givennan<>	ne>Mys	stery			
Man <td>ameCol</td> <td>lection&gt;<c:pho< td=""><td>toCol</td><td>lectio</td><td>n&gt;</td></c:pho<></td>	ameCol	lection> <c:pho< td=""><td>toCol</td><td>lectio</td><td>n&gt;</td></c:pho<>	toCol	lectio	n>
<c:photo c:elementid="fdfaef8f-b334-4&lt;/td&gt;&lt;td&gt;&lt;b&gt;1c80-8&lt;/b&gt;1&lt;/td&gt;&lt;td&gt;3c-83d391488&lt;/td&gt;&lt;td&gt;∍b4"></c:photo>	> <c:u< td=""><td>rl</td></c:u<>	rl			
行1,列1	100%	Windows (CRLF)	UTF-	8	

🥌 [随波逐流]	CTF编码工具	V1.0 20201	022					—		<
Base加解密	字符加解密	字符编码转换	已知key解密	进制转换	其他工具	赞赏作者				
需要解密的	文本↓	密钥(ke	y):			字数统计	一键解码	粘贴剪切板	清空内容	547
LF2XGYPPXSG J4S4ITZNEVH 3NKQ2WE6KBG ZZVG52WMNSLJ ====	DPO4E465YP2 IJPNXJS62OF J3XKRJWG52U WVCTKWLJLI2	EMITLSYRGXGWS HAECGZGCWWRYO JQNJXOVNDKTBS EDIQ2DMEZFMNJ	70JOEL4202L BUXMNKMGJTT M42TK4KFGVR XG54WCT2EJF	ZFYQDSLRK: KIDZME2IKI SK3BVLFLIG SVSV2NGVG	XEXO56LCV U3PGVMWS5 SNBUINBIK W2SJVLJVF	B566IZ2FPW7 ZVGVYUKYJSK YTFNQ2VSVZI KNCNKRIXSWL	S37K7HQK46LLUJ Y2TON3ZJU2VSK3 GVNEOOJVLJBU4N NJJUVS6SJGNMTH	N42EJB354RTSL3] 3WG VGHK 3BVG VJW6 VKMG ZSDKNCXNY2U 3RLZJ5KFM3KNK5H	HFR6VONHE INLBGZCDK3 IY4KHGVGHS IG2TSEM46G	
解密结果↓						1	夏制内容	↑解密结果转	至文本框	t
— 键 解 码: base64解码: base32解码: Lul55So5a6D! YWM5MmI5ZjU4 base16解码:	结 Yusa, 5omT5byA57u 4MTQyYmJiYz	果 组织刚刚派下き iE57uH57uZ5L2 zI3Y2EyOTVmMW	来一个任务,请 g55qE5be15Y WmNDg=	f快点完成, #344CC5bei	你只有三 15Y₩35ZG9	 天时间。6L+Z 5ZCN5L6d54₩	5piv5L2g5Lya5 n5LqG5Lyg57uf6	5505Yiw55qEa2V5 8KeE5YiZ44CCa2V	577yM5Y+v5 7577ya0DIv	

发现是base32编码,后面还有一段base,接着解密

🛩 [随波逐流	。CTF编码工具	V1.0 20	201022					_		×
Base加解密	字符加解密	字符编码转	换 已知key解密	进制转换	其他工具	赞赏作者				
需要解密的	〕文本↓	密钥(	key):			字数统计	一键解码	粘贴剪切机	反 清空	内容
6L+Z5piv5L2 d54¥n5LaG5L	g5Lya55So51 yg57uf6KeE	Yiw55qEa2V 5Yi744CCa2	577yM5Y+v5Lul8 V577vaODIwYWM9	55505a6D50 MmT57.iII4N	mT5byA57u TGyYmTiYz	E57uH57uZ5L2; I3Y2Ev0TVmMW	g55qE5be15YW NmNDg=	344CC5be15Y	₩35ZG95ZC	N5L6 🔺
do s mondo on	Jeonaronon	511244000db	1011340528188			.101023014.000	1000 8			
初家社田士						5	御山家	▲ &2 con 4± F	ᄟᅔᅎᆇᅿ	-+≂ + I
群省纪未↓	· 14					夏	利内合	「解省纪月	長特王义4	>11± T
一 健	• 」结 这是你	· 奈用到的kej	y,可以用它打开	组织给你的	コート	【命名依照了传统	统规则。key:	820ac92b9f5	8142bbbc2	7ca2
95f1cf48 base32解码:										
base16解码:	<u>ה</u> ר									

得到了key: 820ac92b9f58142bbbc27ca295f1cf48, 这应该就是key.bmp的密码了



成功得到了,接着把文件都跟刚刚的exp放同一个目录下尝试运行



运行完成后,并没有看到flag,后来发现,flag跟Who\_am\_l文件需要在exp中互换一下位置

因为刚刚运行了一下导致Who\_am\_l为空了,所以这里重新导入Who\_am\_l文件,运行一下,得到了一张gif图,我们改一下后缀,发现是在放烟花



逐一分帧查看后得到了flag



flag:

DASCTF{c3837c61-77f1-413e-b2e6-3ccbc96df9f4}

**Cry**部分

密码人集合

		赛题详	情
题目名称:	密码人集合		
题目内容:	A gift for u. enjoy it.	XD	
题目分数:	100		
当前答出前3名:	第一名 V&N	第二名 Nu1L	第三名 坏女人万岁
相关附件:	靶机附件 下载		

直接nc上去,得到一副矩阵,上面有<mark>我要拿西湖论剑第一</mark>的字样,看起来很像数独游戏

	_	_		_		_		ι	e1a@u	Jbu	ntu: ~/桌面	ī	_	_	 _	
文	牛(F)	编辑	‡(E)	查看	(V)	搜索(	S)	终端(T)	帮助	(H)						
Be	hap	ру₀														
相	言我	不需	要再	解释	如何	可玩〕	这个	游戏了	。那	么	开始吧					
论 * *	* 湖 *		* * 拿	* *	*   *   *	我 一 *	* * *	* * *								
* *	*	*   论   *	第 * 一	* *	*   *   *	要 * *	* * *	* * 西								
* * *	* * 拿	我   *   剑	* * *	* , * ,	*   *   *	* * 第	拿 * *	* 我湖								
· 连adg输>	式 o c f i ab 输	cdef 入答	, 入, ghi[ 案字	例如 即可。 符串	〕完整 。 ::	整矩[	阵为	]								

把 我要拿西湖论剑第一 转化为 1-9 的数字, 找一个在线网站填上去

在线网址: https://shudu.gwalker.cn/

6	2	9	4	5	7	1	8	3
1	5	3	2	6	8	9	4	7
4	7	8	3	9	1	5	2	6
3	1	5	8	4	6	2	7	9
9	4	6	1	7	2	3	5	8
7	8	2	9	3	5	6	1	4
5	6	1	7	8	9	4	3	2
8	9	4	5	2	3	7	6	1
2	3	7	6	1	4	8	9	5
		清白	3		返回			

## 数独求解器

然后再把这些数字按照刚刚的转换顺序,再转回汉字,写个小脚本





运行得到:

论要一我湖拿西剑第西湖剑要论第拿一我我第拿一西剑湖要论拿我湖一西论剑第要第西论我剑要一拿湖要剑一拿湖第论我西湖论我第一西要拿剑剑 第一湖要拿论我西西拿要剑论我第一湖

把这个粘贴回虚拟机里,Enter一下,即可得到flag



flag: