1.404notfound

打开文件图片



010打开检查开头和结尾均无特别之处,直接搜寻ctf直出flag

<u>></u> 0	10 Edi	itor -	C:\U	sers\	ad\(DneD)rive\	桌面	ì\1.p	ng														-			2	\times
File	Edit	Sel	lect	Fin	d١	View	/ Fo	orma	at S	Scrip	ots	Tem	nplat	tes	Deb	bug	Proje	ct .	Tools	s W	'indow	He	elp					
	~ 📂	~		1		ð.	8	- P	R	ອ	3	, ,	ÂB	\$	⇒				R •	¶			1	🧼 🗽	*	🔨 ma		
Start	up	1.p	ng ×																					Work	space			+ ×
0080 0090 00A0 00B0 00C0 00D0	3D 70 63 61 3A 3A	1 27 43 39 20 6E 52	2 EF 65 64 78 73 44 74	3 BB 68 27 6D 3A 46	4 BF 69 3F 6C 6D 20	5 27 48 3E 6E 65 78	6 20 7A 0A 73 74 6D	69 72 3C 3A 61 6C	8 64 65 78 78 2F 6E 74	3D 53 3A 3D 27 73 73	A 27 7A 78 27 3E 3A	B 57 4E 6D 61 0A 72	35 54 70 64 3C 64	4D 63 6D 6F 72 66	30 7A 65 62 64 3D	 4D 6B 74 65 66 27 62 	0123 ='ï» pCeh c9d' a xm :ns: :RDF	456 ¿' iHz ?>. lns met xm	/89/ id= <x:> :x= a/'></x:>	ABCL W5M zNTc xmpn adc >. <r :rd1</r 	DEF 10M czk net obe df		Â	De Ope 1.p Proj Fave P Rec /11	Fil en File ong ject orite l ent Fi -7- orkspa	es Is Files Ies	Pi	
00E0 00F0 0110 0120 0120 0130 0140 0150 0160	4C 75 65 3C 20 78 74 69 27	69 74 7D 72 72 6D 70 6F 3E	74 5F 79 64 64 62 3A 6E 0A	 43 31 6E 66 6E 2F 2E 20 20 	54 74 3A 3A 73 2F 63 20	46 73 61 44 61 3A 6E 6F 3C	7B 5F 78 65 62 41 73 6D 41 72	49 6E 2D 73 6F 74 2E 2F 74	 74 30 6E 63 75 74 61 61 74 61 61 74 61 61 74 61 61 74 61 <	73 74 73 72 74 72 74 64 72	5F 5F 23 69 3D 69 74 73 69	 34 61 27 70 27 62 72 2F 62 C 	30 5F 3E 74 27 3D 69 31 3A 71	34 70 0A 69 0A 27 62 2E 41 35	61 0A 6F 20 68 75 30 64	62 67 20 6E 20 74 74 2F 73 20	ut_1 e}yn <rdf rdf xmln tp:/ ion. '>.</rdf 	ts_ tax :De :ab s:A /ns com <a< td=""><td>n0t -ns scr out ttr .at /ads</td><td>_402 _a_p #'>. ipti =''. ib=' trik s/1. ib:/</td><td>+_D pag .on ht out 0/</td><td></td><td>~</td><td>Inspect Ty Binary Signec Unsign Signec \neq Ins</td><td>ctor pe I Byte Ied B. I Shor pecto</td><td>V 010 67 67 t 215 or</td><td>alue 0001 71 Var</td><td>• × 1 <></td></a<>	n0t -ns scr out ttr .at /ads	_402 _a_p #'>. ipti =''. ib=' trik s/1. ib:/	+_D pag .on ht out 0/		~	Inspect Ty Binary Signec Unsign Signec \neq Ins	ctor pe I Byte Ied B. I Shor pecto	V 010 67 67 t 215 or	alue 0001 71 Var	• × 1 <>
Find	Resu Adc ound 3h 16h	lts dress	s ccur (Va renc CTF CTF	alue es o	f'ctf																						▼ ×
≅ Oi (1/2)	utput Found	▲ 2 o 2 b	Fin	d Re reno	sults ces o	of 'ct	t Fir f'. (p	id in iress	File Esc	s 🚦 to h	? Co nide	ompa resu	are Its)	<mark>اللا</mark> St	Hist tart:	ogra 227	m ₌Σ [E3h] ≲	Che Sel: 3	ecksu 3 [3h]	ım] Siz	<i>न</i> Pro e: 43,4	cess 42	₽° H	• Disas lex AN	ssemt ISI LI	oler F C	e ov	'R "

2.欢迎参加强网杯

打开题目直接显示flag, 改形式提交

题目	讨论区 (6)	WriteUp	详细数据	版本		
[广3	东强网杯	2021	个人组]欢迎参加	强网杯	
1分	沙盒逃逸 编码分析	f RCE 🕇	* * * *	\\$1 +		
题目描述						
flag{We 该题目缘 使用NS	c10m3_to_QwbCt 夏现环境尚未取得 SCTF{}格式提交。	·F} 主办方及出题 <i>)</i>	人相关授权,如	1果侵权,请联系管	管理员删除。得 到	的flag请
	NSSCTF{Wec	10m3_to_Qw	bCtF}			
			提交			
上一是	返回题库				随机一题	下一题

3.这羽毛球怎么只有一半啊

打开得到提示要改图片宽高

题目	讨论区 (2)	WriteUp	详细数据	版本			
[LitC 级)	TF 202	23]这羽	毛球怎么	公只有	-半啊	(恼 (初
1分 宽震 题目描述 所以下半身	修改)图片隐写 是什么呢(ww	8 图片修复 🔺	* * * *	• 0 +			
出题人: 探 Flag格式 N	独 SSCTF{}						
			开启90 ~				
上一题	返回题库				随机一题	题 下一;	题
用puzzlesovle	er爆破						
DuzzleSo	lver v1.0.4 Au	thor: Byxs20			-	- 🗆	×
BaseTools	Frequenc	yCount	FrequencyColo	FileTo	ools	mageTools	1
总选项:	[1] FIX-PNG						\sim
img1路径:	C:/Users/H	HelloCTF_OS	/Desktop/羽╕	毛球.png			
	打开img1		开始执行		清空输出	4	
[*] Fix-PNG	执行完毕,图片	已经保存在文件所	所在的目录中或者	同名目录中!			^
[-] Byxs20プ [-] 宽度: 15:	b您温馨提示: 正 87, hex: 0x633	在并行爆破图片:	正确的宽度和高度	臣中			
[-] 高度: 224	45, nex: 0x8C5 [为: 0小时 0分	钟 0秒 17毫秒					~

成功得到隐藏的flag



4.签到

打开得到提示重点;一串表情和GAME



在老师博客发现此为表情密码-AES, 钥匙为GAME便成功破译

解密

要解密,请选择约定的旋转(如果自定义),输入表情符号字符串,然后输入预共享的加密密钥。



5.签个到

打开为两个损坏的压缩包,用010打开发现其中一个的文件头,另外一个平平无奇,随后改了出现文件 头的那个后缀

<u></u> 0 🧭	10 Edi	tor -	C:\U	sers\	ad\(DneD)rive\	桌面	\hel	lo.zip)											_			\times	
File	Edit	Sel	ect	Fin	d١	View	/ Fo	orma	at S	Scrip	ots	Tem	plat	es	Deb	oug	Project	Tools	Window	He	elp					
	~ 📂	~ 📙		.		ð.	- %		R	5	3	. 🔎	ÂB	\$	≯		🗾 📕		í 💵 📐 i		1	🦛 📠	* 🔞	🙋 mov 🗄		
Start	up	hell	lo.zi	р×																		Works	pace		-	
0000 0010 0020 0030 0040 0050 0060 0070	89 00 70 36 1E 7F 70 0E	50 00 00 10 9B 01 80 90	4E 01 00 40 9E 04 8C 11	47 1C 05 C1 AA FE E0 1C	0D 00 A7 38 03 3E 00 20	0A 00 49 C8 8C 7D 19 23	1A 01 44 FD 64 03 C1 38	0A 0E 41 AF 8D C0 01 40	00 08 54 EC FC EB 32 46	00 06 78 C4 C0 10 82 70	00 00 9C AB 45 1C 03 80	0D 00 ED EF A3 20 64 8C	49 00 DD 8D E7 23 04 E0	48 5B 41 01 ED 38 07 00	44 EA 6E DA FD 40 C8 19	52 A8 EC A1 3F 46 08 C1	<pre>b PNG. p§] 6.@Á8i .>žª.(0 b>] p€Œà</pre>	 IDATxœ Èý¯ìÄ« Ed.üÀE }.Àë .Á.2,. #8@Fp€	.IHDR [ê ["] íÝAnì ïÚ _j £çíý? #8@F dÈ. ŒàÁ		Î	 ➢ Oper hell ➢ Proje ➢ Favo ➢ Rece अज = ○ Wor Inspect 	Files o.zip ect rite Fi nt File kspac	s iles es	Pi <	× ×
0080 0090 00A0 00B0 00C0 00D0 00E0 Find	01 AC 79 23 04 3A 77 Resu	32 AE 62 38 07 75 C2 Its	82 1D 4D 40 C8 E7 09	03 DA 93 46 08 74 07	64 F9 F7 70 0E F0 C8	FE CC F5 80 90 D4 08	79 56 8F 8C 79 C9 0E	F2 AE A7 E0 74 D9 90	C3 B9 9E 00 D2 9B 11	DF 7A BF 19 78 BF 1C	DE BD 13 C1 D5 EF 20	DE 9D 0E 01 CD 0F 23	9E 6B 90 32 3F 37 38	FC 3 93 0 11 2 82 7 FE 7 DF 3 40	F8 56 1C 03 B9 FF 46	AB AE 20 64 7B E9 70	.2,.d ¬®.ÚùÌ ybM"÷ć #8@Fp€ È :uçtðĆ wÂÈ.	þyòÃßÞ⊧ ÌV®¹z½. €ŒàÁ. .ytÒxÕÍ ÔÉÙゝ¿ï. #	Þžüø« k"V® .2,.d Í?þ¹{ .7ßÿé #8@Fp			Typ Binary Signed Unsigned Signed	e Byte d B Short ector	Valu 10001 -119 137 20617	ue 001 ar	^ ~ ~ ~
	Ado	lress	;	Va	alue																					
≣ 0	utput		Find	d Re	sults		t Fin	ıd in	File	s 🚦	? Co	ompa	are	<u>lan</u>	Hist	ogra	m ₌Σ C	hecksu	m <i>គ</i> 7 Pro	cess	P	• Disass	embl	er		
Open	ed file	e 'C:\	Use	rs\ad	d\Or	neDr	ive∖	和)	hell	o.zip	o'.				Pc	os: 0	[0h] Val:	137 89	h Size: 1,5	04	Н	lex ANS	SI LIT	G (OVR	

出现了一张二维码的图片



扫码得到了flag

• • •

xaflagii_am_a_tupian}

6.破损的图片

点图片直接打不开,010打开发现文件头很奇怪就去篡改前面试着改为其他文件头第一个想到常见的png



在文件添上后缀之后成功打开图片得到flag



7.猜谜

28

80 八卦图

30 三十而立

07 北斗七星

04 四大才子

20 歼20号

02 两只黄鹂鸣翠柳

17 一起去看流星雨

23 乔丹

01

12 十二个

总结·280830070420021723011219

根据题目提示

题目	讨论区 (10)	WriteUp	详细数据	版本							
[羊	成杯 202	1]签到	题		Ø						
1分	猜谜 🚖 🚖 🔺 🕇	• • • 3	+								
题目描述											
简简单单 该题目象 使用NSS	单猜数字01-30 San 夏现环境尚未取得当 SCTF{}格式提交。	gFor{md5(E办方及出题人)} (32位md5) 相关授权,如身	果侵权,请联系管理员删除。得到的flag请							
			开启号0	~							
上一題	返回题库			随机一题下一题							

在线搜找md5网站先是解密没有结果,再是加密直接得到32位

	AFTNIMO: 日硬盘超过	5、sna1、sna256等全球通用公 <u>t</u> 3PB,查询成功率95%以上,很	公开的加密算法进行反问登词, 很多复杂密文只有本站 <u>才可查</u> 说	一 <u>通过另举了</u> 得组合的方式 可。本站专注于各种 <u>公开算</u>	,可建了 法,已稳	明又密又对应查问数据严 定运行18年。	〒, 回建町10家約90
							首页
	Pass:	28-08-30-07-04-20-02-17	-23-01-12-19	UTF8		<u>\$[HEX</u>	
	Salt:			- HE	x		
	Hash:						
		toss					
		UNES:					
Result:							
base64: MigtMDgtM	zAtMDctl	MDOtMiAtMDItMTctMiMtMDE	tMTItMTk=				
md5: d93b7da <u>38d8</u> 9	9c19f4 <u>8</u> 1	le710ef1b3558b					
md5_middle: 8d89c	19f481e	710e					
	abd165c	5aa7fef8673601271d73b83d	d7				
md5(md5(md5(\$pas	ss))): a6	b7c2ce64cd358365b83b2ael	bf9eb91				
md5(unicode): 125f	9456b8d	17ebc735caaaf760980786					
md5(base64): 2Tt9c	042JwZ9	IHnEO8bNViw==					
mysql: 7d68139c773	300b49						
mysql5: ddc400e8e9	9550739	e1b1151359c923b5f580623	1				
ntlm: 051d6493eba	543109c	5e872b70b6911f					
sha1: 61c5b7b49f40)6eb9522	27266638e42035af97640f					
sha1(sha1(\$psss)):	d732286	5a32e825c25f231bb26796fc:	1f6f62bdf4				
sha1(md5(\$psss)):	dd33244	2b0a6d2a15422cc8330bf39	ee4217b45c				
md5(sha1(\$psss)):	baec3ed	bf12e421b17fb154219f76f99	9				
sha256: 662136620	2cb1bc4	cd646f2fda433900bf2d1587	71a76478fab8b4d9f3cect	b2			
sha256(md5(\$pass)): 493b7	7a561c6733053f7a74d11bdb	od6e7fcc58a224f8ca9751a	e912b5f4361baa			
sha384: bf50b1fbea	7abbc2b	6843392341b217e7656bd8d	dd6fb4bb7b61a23121a23	91ea9a794fe9f6c251a4	11e4c19	9cad64d2be	
sha512:							
a05008933280ff5ef3	35024f4f	b687ff34ac51c716a755e7c7	75f82fca20399219f81f516	8e116ca4fe87fb49d57	94db8c	d4629de0c5cf2c7963	39ea7c079fd584
md5(md5(\$pass).\$s	alt):VB:I	DZ: abd165c5aa7fef867360	1271d73b83d7				
md5(\$pass.\$salt); d	193b7da3	38d89c19f481e710ef1b3558					
md5(\$salt.\$pass): d	193b7da3	38d89c19f481e710ef1b3558	- b				
	alt). 403	b7da38d89c19f481e710ef1b	35586				

改变格式成功提交

8.welcome

直接改变正确形式提交

题目	讨论区 (6)	WriteUp	详细数据	版本		
[MN	1ACTF 2	2015]w	elcom	е		\oslash
1分	其他 MISC 签	到 ★ ★ ★	* * 🖤 0	+		
题目描述						
The flag 得到的fl	is MMA{Welcom ag使用NSSCTF{}	ie_To_MMACTF 格式提交	: !!}.			
			开启号0	~		
上一題	返回题库				随机一题	下一题
野口坛公						`



根据提示打开老师博客了解到使用stegsolve

题目	讨论区 (1)	WriteUp	详细数据	版本		
ſHU	IBUCTF	2022	新牛寨1	最简单	的misc	
[110	boon				HJIIIIOC	
1分 [LSB 图片隐写	二维码 📩 📩	* * * (♥ 2 +		
题目描述	≘ 					
你具的有	国个儿吗?					
			开启⊜0	\sim		
上一题	返回题库				随机一题	下一题
题目标签						>
用虚拟机打	丁开并跟着学习教	程弄出另外一张	长图为二维码			
٨					- 0	× ×
			Extract Preview			
a4b43f3b6 86114d86a	42a81cf ec6d32a0 99df708 f822364	1069f3900? 233d7a323M	;d*m29. "6B3#			Ê
f3f6ffe13 213779341	6e7e4be c8daacf 5lecbca e3ld2a8	36e04b6fc 931178938 !7y	.6n 4*.18			
64a3a9488 d78bb0dbe	da92492 854aae5 07b8b6c 119d2ef	89c9771b0 d 57702aabc	H\$J.Xq. {.lw			- Ka
6394bf7f6 984c07ccb	7da29ef 0f154ff	57a8c43ae c 140a8833b .L.	□g.)O.z.C. eemm@;			199
c95923a84	3324a09 27d3 .	Y≇.C2J. '.				
Bit Planes				Order settings		
Alpha	all 7 6	5 4 3	2 1 0	Extract By () R	ow 🔾 Column	

Bit Order 💿 MSB First 🔾 LSB First

Bit Plane Order

Þ

Red all 7 6 5 4 3 2 1 0

Green all 7 6 5 4 3 2 1 1



二维码用QR打开便成功得到flag

		一日本
	请输入数据	94諸等级 H(30%) ▼ 版本 Auto ▼ Auto ▼ Auto ▼
		• • •
已解码数据 1:		^
位置(22,3,28)+(990,3,32,8)+(32.7,990.5)+(990,3,990.5) 颜色正常,正像 斯蒂·3 2,1 1像 外错等级1,掩码-3 行容] NSSCTF[aacc4238460996/0178c18d7637c9dd5]		
		~
解码完成		
		^ ▶ 圓 記 ↔)中 20:34

注;前面有题好像二维码同样可以使用QR,当时没想起来下意识便直接手机扫码了

10.漂流记的马里奥

打开得到一个文件打不开,在010中也未发现特别之处,随后根据题目提示NTFS隐写,在网上学到了个工具学会使用后成功找到flag

KisStreamsEditor2	_		\times
NSE NtfsStreamsEditor http://blog.sina.com Ntfs数据流处理工具	m.cn/ad etsoft@s	vnetsoft ina.com by XGC	t J
按索 受 C\Windows\System32\1.bxtflag.bxt - □ 选择搜索类型 (文本](自动识别编码类型:TMBCSEncoding) swupctf{ddg_is_cute} ● 全部NTFSi磁盘 (文件)	×		
 ★ 文件 C:\\$Recycle. C:\\$Recycle. C:\\$Recycle. C:\\$Recycle. C:\\$Recycle. C:\\$Recycle. [16进制] C:\\$Recycle. 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF C:\\$Recycle. 000000000 73 77 75 70 63 74 66 7B 64 64 67 5F 69 73 5F 63 swupctf(ddg is c 	• •		
C:\\$Recycle. C:	·		
武 明宗 - ○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○	导出列表		