# 1.huaji

用010打开在识别内人里面找到唯一一串数字字母,将其锁定为突破口,随后用赛博厨子破解

<b>&gt; </b> 01	0 Edi	tor -	C:\U	sers\	\ad\(	DneD	)rive\	桌面	\huaj	ji?																_				$\times$	
File	Edit	Sel	ect	Fin	ıd Y	View	Fo	orma	t S	crip	ots	Tem	npla	tes	Deb	oug	Proj	ect	Тос	ols	Wind	ow	He	elp		_				_	
	· 📂	~				¢.	∖ %		1	5	3	- >	À	s 🍫	<b>&gt;</b>				× 💱	¶		L, I		<b>?</b>	*	<u>ah.</u>	*_	*			••
Startı	ıp ×	hua	aji?	×													Å	2.4		0.1-2-				- \	Nor	ksp	ace	9			• ×
0840	00	00	200	 00	4	5 00	6 00	00	8 00	9	A 00	<u>в</u>	00	00	⊢ 00	⊢ 00					_DEF						Fil	es			Ê
0850	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									ا <b>0 4</b> ا	pen Juai	File	s			
0860	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	••••	•••							Pr	oje	ct				
0870	36	33	37	34	36	36	35	66 22	34 22	65 22	34	39	35	33	34	31 20	637	466	55†4 1222	e495 ว (	5341				🏓 Fa 🗅 Da	vor	ite I	Files			
0890	37	33	36	31	35	66	33	32	33	30	33	32	33	32	00	00	736	15f	323	20 0323	32			Ľ	- Ke		10 FI C-70	nes n	_		~
08A0	00	02	92	80	00	04	00	00	00	01	00	00	00	00	EA	1C					ê.				🖻 V	Vorl	kspa	ice	•	PI <	>
08B0	00	07	00	00	80	0C	00	00	80	A0	00	00	00	00	1C	EA					ê			<u> </u>	nsp	ect	or				- ×
0380	00	00	00	08 00	00	00	00	00	00	00	00	00	00	00	00	00									٦	Гуре	9		Valu	le	<u>^</u>
08E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									linar	у		11	111	111	
08F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00								5	igne	ed B	lyte	-1			
0900	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00									ian	gneo od s	a B bor	25 + 0	005		
0910	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00										eu s		9	905		~
0020		00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			• • • •					<u> </u>	🔶 li	nspe	ecto	or	1 V	ar <	
Outp	ut																														• × .
≅ Ou Opene	tput ed file	e 'C:	Fin (Use	d Re rs\a	sults d\Or	s 🕵	Fin	nd in 桌面\	Files huaj	s 👔	? Co	omp	are	<u>l</u> da	Hist Pos	ogra :: 0 [(	ım ₌ )h] V	₽ C ′al: 2	heck 255 Fl	sum Fh S	🐖 ize: 4	Proc 3,72	:ess :3	e po H€	" Dis ex A	sass NS	emł I LII	oler T	<u>د</u> (	⊃VR च	
	] 		<b>生</b> 1条									判♪へ 63746	65f4	e4953	415f32	230323	<mark>32</mark>					leng	th: 26	; 1i	nes:	1	Т			-	
D	ーフへ)世市! elimiter	J 좌冊 Q 년 박	受快																												
N	one																														
												输出	1									start end length	: 0 : 13 : 13	tir lengt line	ne: 1m :h: 1 :s:	ns 13 1	8	ē	ſ.	5	:3
												ctf_N	IISA_2	2022																	

成功破解出压缩包的密码,将压缩包成功压缩打开得到flag



注;一般用010识别文件头是啥,然后将文件后缀改为识别的文件包,随后点开属性查看可以发现更多信息,偶尔也可以用到exiftool打开文件查看更加详细的信息。

## \*\*2.what 1s BASE

下载打开是一串字符, 厨子直接破解

	新建文本文	文档.txt	1.txt	base星期四.txt	×	+
文件	编辑	查看				
TGIO	Q1RGe0t(	GQ19DcjR6eV9UaHVyM2	2RheV9WX21IXzUwfQ==			

配方	2 🖿 🗊	输入	length: 48 lines: 1	+		€	Î	Т
Base64 转文本	⊘ 11	TG10Q1RGe0tGQ19DcjR6eV9UaHVyM2RheV9WX211XzUwfQ==						
Alphabet A-Za-z0-9+/=	Ŧ							
Remove non-alphabet chars	Strict mode							
		输出	length: 34 lines: 1	8	D	(†)		0
		LitCTF{KFC_Cr4zy_Thur3day_V_me_50}						

#### 更改正确格式正确提交

# 3.签个道叭

#### 打开下载的文档

### 文件 编辑 查看 63 $\begin{bmatrix} (0) + (0) + (1) + ($ $+(1+i)))(i_{1}+i$ + [+(+)]) + (0 + [)((((++))) + (1) + ((1)) + (0)) + (1 + 1 + (1)) + ((1) + (1)) + (1) + (1) + (1)) + (1) +[i+0] + (i) + (i+0+(+0))+(!!0+0)(!+1+0)+(!0+0)(!+1+0)+(!0+0)(!+1+0+1+0))+(!0+0)(!+1+0+1+0)(!+0)(!+0)+(!0+0)(!+1+0+1+0))+(!0+0)(!+1+0+1+0))+(!0+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0)(!+0+1+0)(!+0+1+0))+(!+0+1+0)(!+0+1+0+1+0)(!+0+1+0+1+0)(!+0+1+0+1+0+1+0+1+0)(!+0+1+0+1+0+1+0)(!+0+1+0+1+0+1+0)(!+0+1+0+1+0+0)(!+0+1+0+1+0+0+0+0+0= 0 + (0)(0) + (0) + (1)+(0) + ((1) + (0) + (1+ (1+(1)) + (1+(1)+(1+(1)) + (1+(+ (1) + (1行1,列1 9.343 个字符 Windows (CRLE) LITE-9

#### 去密码网站识别其属于JSFUCK密码·

DCODE		密码标识符 密码学,密码标识符	
搜索工具		加密消息标识符	(
<ul> <li>▲ 通过关键字在 bCobE 上搜索工 例如,输入"数独"</li> <li>▲ 浏览完整的 bCobE 工具列目</li> <li>结果</li> </ul>	.具: 。 是	(i)日子(1)((i)(i)(i)(i)(i)(i)(i)(i)(i)(i)(i)(i)(i	•
dCode's analyzer suggests to inv	estigate:		
11	ţ†	▶分析	
<u>JSFuck Language [][(![]+</u> [])		Смотритетакже: 频率分析 — 重合指数	
Substitution Cipher	-	付亏怀识付	
Shift Cipher	٥	▶ 转到: 符号密码列表	

#### 然后在随波逐流打开选择次密码解密成功破译



## 4.基尼太镁

得到一张高度过高的图片



拉到ppt里面去改高度大小



开头Zmxh得知其为base64密码,随波逐流破解





将两个flag拼接即为所寻

### 5.随便拉的杂项

压缩打开

CTFshow 交流群:372619038 本群倡导友好、和谐、欢乐、进取的学习精神。 严格遵守等级制度,进来的一律以大佬自称,并逐步升级为菜狗、菜鸡、菜鸟、菜虫、菜笔、菜刀。不准 自称菜狗这么荣耀的称号,必须自称本大佬。 近期每天一道红包题,作者也秉承恶搞又不失内涵的作风,为大家学习路上增添欢乐! CTF, show 全体管理敬上 By: 多次拒绝赵丽颖



根据重复两次出现的docProps/PK判断其中有多张图,剪切掉第一个

# 6.喜欢我的压缩包么

提示密码为6位



打开爆破软件长度设置为6位,先是只勾选了数字直接破解压缩包密码、

	🔏 ARCH	IPR 4.54 ·	- 100	%						$\times$		
	文件(F)	恢复(R)	帮	助(H)								
	2	. 18		R	٢	-					相	似推
	打开	开始	<u>†</u> !	停止	基准测试	升级	帮	助	关于	退出		
	加密的	ZIP/RAR/	ACE/A	ARJ 文件		攻击类	型					
	D:\学习	]资料啊.z	zip			暴力				$\sim$		
	范围	长度(	う ゆうしゅう しゅうしゅう しゅうしゅう しゅうしゅう しゅうしゅう こうしゅう しゅうしゅう しゅう	朋文	自动保存	诜顶	宫纲					
	暴力范	113选项	177	-11/		100-100	181-7%				nation	
	所有	秋写拉丁	- Yo	今已成功	恢复!	-					100000000000000000000000000000000000000	×
	□ 所有	孙与拉」 ] 数字(0 -	9)							法计位自己		
	□所有	特殊符号	3( L	<u> </u>	Adva	nced Arc	nive Pas	swora H	(ecovery 3	说计信息:		-
	空格	ई बनाधारणने	-2 5	品计口令				114,51	1			
		16111664		急计时间				53ms				
	状态窗			P均速度	(口令/秒)			2,160,	584			
١	2024/8	6 20:26:5	5 j	这个文件	的口令			114514	ŧ			- Ca
	2024/8	6 20:26:5	55	十六进制	口令			31 31 3	34 35 31 3	4		6
	2024/8	6 20:26:5	55		口仍左					V 72-		
	当前口令		1		1末1子。					♥ 明正		
1	已用时间 验证口令	): 				剩余时间	8):				得オ	不喝
					100	%					10-0	
	ARCHPR v	ersion 4.5	4 (c)	1997-201	2 ElcomSoft C	o. Ltd.						







打开文件图片





<u>a</u> (	010 Ed	litor	- C:\	User	s\ad	\One	Driv	e\杲	围\ei	noji.j	png														-	_		×	5
File	Edit	Se	elect	t Fi	ind	Vie	w	Forn	nat	Scr	ipts	Те	mpl	ates	De	ebug	Pr	rojec	t T	ools	Wind	wob	He	elp					
	~ 📂	~		1	1 🖿	i 🍙	i   1	խ ∥	` [	<u> </u> 5	<b>で</b>	1	• 🗚	B 🍃	• →	• • •	2	31	Hex	🛱 ¶		<b>\</b>		7	🦇 📠	<u>, *</u>	🌿 mov		
Star	tup	en	noji.	.png	×																				Works	space			<del>-</del> ×
		0	1	2	3	4		6		8	9	А	В	, C	D	Е	Ě	012	2345	6789	PABCD	)EĚ				Fil	es		
8:A6	520	10	42	5C	8A	A1	30	55	80	21	F0	DD	D1	37	2F	7E	B6	. B)	\Šį0	00.10	ðÝŇ7/	′~¶			🍃 Ope	n File	25		
8:A6	530	F4	4E	DD	69	33	67	AE	C2	51	21	84	10	42	08	21	84	ÖN	13g	geaq	!".B.				em	noji.p	ng		
8:A0	540 550	10	B/	80	C2	51	21	84	10	42	88	2B 2B	10 A 2	BA	6F	5E 70	D5	. · ŧ	EAU!	".В	0°£+ ∕ريد،	0^0			📴 PN	G.bt			
8 · 40	560	F6	69	F7	9D	99	55	56	75 77	18	15	8F		21	84	10	42	J" öi-	.a74µ. ⊹™l	ivc	ž r Ž l	۲۱ R			🎐 Proj	ect orite	Files		
8:A6	570	5C	31	5D	D7	E5	A2	2B	E5	BA	C3	5D	21	84	B8	6E	E0	\1	l×å¢	:+å°	.2" Ã1!	nà		ų	Doc	ont E	loc		×
8:A6	580	C7	FE	3F	20	17	06	AB					00	00	00	00	49	Çþ	?		fg	. I			🖻 Wo	orkspa	ace 🛛	<mark>⊧</mark> Pi≦	
8:A6	590	45	4E	44	AE	42	60	82	53	45	52	44					64	EN	D®B`	, SEI	RDVEZ	27 <b>d</b>			Inspe	ctor			<del>-</del> ×
8:A6	5A0	30	55	78	59	7A	42	33	4D	31	38	78	4D	46	39	49	52	0U>	xYzE	3M18	BxMF9	)IR			Tv	pe	Va	alue	
8 : A6	5B0	47	4E	30	5A	6C	39	4E	4D	54	56	6A	66	51	3D	3D		GN(	DZ19	PNMT	VjfQ=	-			Rinary		010	10011	
																									Signed	l Byte	83		
																									Unsian	ed B.	83		
																									Sianed	l Shoi	rt 1774	47	
																							晟	1	4				
																								<u> </u>		pecto	or 📙	Var	
Out	out																												₹ ×
Exec	uting	tem	plat	te '	c:\u	lsers	s\ad	\0ne	Driv	/e\文	档\S	weet	Sca	pe\0	10 T	empl	ates	:\Rep	osit	ory\P	PNG.bt	' on	'C	:\U	sers\a	d\0ne	Drive	桌面\。	emo
Exec	uting	ne 3 tem	i <u>32:</u> mpla	te '	C:\U	lsers	asse s\ad	d en \0ne	d of Driv	re\文	e an 档\S	veet	Scap	pie/0	data 10 T	a. empl	ates	:\Rep	osit	ory\(	010.bt	' on	'C	:\U	sers\a	d\0ne	Drive	文档\9	Swe
Temp	late (	exec	ute	d su	cces	sful	lly.																						
<u> </u>																													
× = c	utout		) c:	nd D	ocul	to 1	<u>م</u>	indi	n Eil	22	2 0	`om	narc	. IA		tog	ram	7	Cha	okoun	n 🗖	Dro		me		com	alor		-
Cont					esui	cs i		niu i		cs	10 C		pare			ACO.	76111						75	¥.		senii.	T P		
င်ဝဉ်	ea: 40	7 [28	snj t	ytes	0							stai	n: 50	0093	5 [8,	A69.	/nj :	ser: 4	<del>1</del> 0 [2	onj S	size: 50	00,9	75	Н	ex AN	ISI LI	լ և	-0VF	× .:

### 用随波逐流一键破解

<b>以</b> [随波逐	流]CTF编码工	具 V6.0 2024	0708							_		$\times$
Base/Rot	字符解密1	字符解密2	字符解密3	编码转换	带key解密	多key解密	在线解密	进制转换	其他工具	文件图片	题库&	更新
≥ 密文↓	(字数:40)	🙋 密	钥key/dict	/url:						3 0 Ø	一键解	码 =>
ERDVEZ7d	OUxYzB3M18	kMF9IRGN0Z	19NMTVjfQ=	-								

解密结果 🖡 💼	■ [随波逐流]CTF编码工具 V6.0 修复离线错误,已重新发布	搜索	↑解密结果↑
- 键 解 码:	解码结果(注:在线解密密码不参与一键解码)		
ase64解码:	HD <mark>CTF{</mark> wE1c0w3_10_HD <mark>ctf</mark> _M15c}		
ase32解码:			1
aseio用和句: ase85(a)解码:			
ase85(b)解码:			
ase58解码:			
ase36解码:			
ase91解吗: ase92解码·	tI¥22ÛÊÛ∫αzâ ⊵ÛH%Ê(Υ <mark>K</mark> ܰ ð		
ase62解码:			
ase62(ASCII)解	码:		
age16-32-64-91			
isBase6	4 True SERDVEZ7dOUxYzB3M18xMF9IRGNOZ19NMTVjfQ==		
解码结界	HDCTF {wE1c0w3_10_HDctf_M15c}		
口果最后一个的[角	QP[码结果]是乱码,倒数第二个就是正确是正确答案。		

## 8.MISC签到

打开为一张图片,010打开发现文件头为jpg,看到结尾发现疑似flag还要类似压缩包的文件头



🥦 010 I	Editor - (	C:\Us	ers\ad	d\Or	neDri	ve\§	和)(面,	ilag.j	pg															_	(		$\times$
文件(F)	编辑(E)	搜	索(S)	视	图(V	) 柞	各式((	D)	脚本	(I)	模板(	L)	调试	(D)	项	∃(P)	ΤÌ	₹(T)	窗	□(W)	帮助	力(H)					
📄 🗸 🔁	🗲 ~ 🔚		<b>.</b> I	•	<b>1</b>	‰		<b>1</b>	ຈເ	וע	ړ 🔍	<b>B</b>	<b>p</b> -	<b>≻</b> 1		<b>5</b>			¶		. 1 💷	6	i 🥋	<u>a.</u> *	1	mov »	1 11
起始页	flag.j	pg ×																					工作	X			<b>.</b> ,
	0 Í	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	012	2345	678	9AB	CDEF	. 883	^		文件		路往	ž
ECD0h ECE0h ECF0h ED00h ED10h ED20h ED30h ED40h ED50h ED60h	03 F4 DE 28 DD 8D 00 00 00 00 00 00 A7 E4 50 4B 55 00	EF 92 FD 76 08 00 00 98 05 00	98 35 C0 75 00 00 EF 06 00	8F 5E 94 24 66 01 85 00 00	16 BF 78 53 00 6C 00 C5 00 00	22 75 50 40 00 61 18 D7 00	69 D0 4B 15 00 67 00 01 00	08 3C 01 37 00 2E CC A7 01	48 05 02 41 00 74 4B E4 00	B1 0B 3F 2F 00 78 C3 9B 01	44 34 00 00 74 D2 EF 00	97 B5 0A 00 20 0A 7D 85 5A	33 2E 00 00 00 C5 C5 00	C9 DC 01 23 00 20 D7 D7 00	C9 4C 08 00 00 01 01 01 00	.ôi Þ(' Ý.ý  §ä, PK. U	ï~ ′5^¿ vuTS \$. fl Å	"i. uĐ< PK. @.7  ag. Ì 	H±D 4 .?. A/. txt KÃÒ ä>ï	_3ÉΕ μ.ÜL # }Å× Å× Ζ		<	▶打行项收最行最书	开的文 lag.jpg 同 近的文 lag.pn 近 签 的文	(件 g ( (件 (件 () () () () () () () () () () () () ()	::\U\ś ::\U\ś 项目	
模板结果	₹ - JPG	.bt ≈																					检查	器			<b>~</b> >
	名称					偐	Ī		Ŧ	F始		大小	lv –		颜色				汨	释				类型		值	-
> stru	ct DHT	dht[C	)]						1F7E	h	21	h		Fg:	E	3g:							二进制	刮	C	010100	00
> stru	ct DHT	dht[1	]						1F9F	h	B7	'n		Fg:	E	3g:							有符	弓字节	8	30	
> stru	ct DHT	dht[2	2]						2056	ōh 	21	h		Fg:	E	3g:							无符	弓字节	8	30	
> stru	ct DHT	dht[3	3]						2077	′h 	B7	h		Fg:	E	3g:							有符	弓短型	1	9280	
> stru	ct SOS e	scans	start						212E	ih 	Eh			Fg:	E	3g:							无符	弓短型	1	9280	
> char	scanDa	ata[52	2067	]					2130	Ch 	CB	63h		Fg:	E	3g:							有符	弓整型	6	573247	52
enu	m M_ID	EOIN	/larke	er I	M_E	DI (F	FD9	h)	EC9F	<sup>-</sup> h	2h			Fg:	E	3g:							无符	弓整型	6	573247	52
$\rightarrow$ char	unkno	wnPa	ddin	1	סאי	]			ECA	lh	C5	h		Fg:	E	3g:							4 +	△本型		ಮೇ 🖽	
S )#		A							T1/-			~ ~ ~			107							il distant	1		J 📲	又王	
选定:191	/ [C5h] ⁄	个子主	) ()el	劃: 6	057	/ [E(	LA1h	I] ∄ 7	十始:	605	77 [E	CA1	hji	远定:	197	[C5ł	1] 大	小: 6	0,77	4	十六进	±制(	H) A	N2L \]	「「雨	면 2	i 置

改了后缀之后查看图片属性有隐藏信息

📝 flag.jpg 属性		×
常规 安全	属性修改 详细信息 以前的版本	
屋性	店	
治田	18	1.1
たち		
主顎		
公级	the the the the	
标记		
备注	this is password	
	pass	
作者		
拍摄日期		
程序名称		
获取日期		
版权		
图像 ———		_
图像ID		
分辨率	640 x 422	
宽度	640 像素	
高度	422 像素	
水平分辨率	72 dpi	
垂直分辨率	72 dpi	
位深度	24	
FT #2		
删除属性和个人		
	确完 取消 成	田(A)
	1941AE 14X/F3 ///	(A)

在虚拟机手动分离得到压缩包



影将输入定向到该虚拟机,请将鼠标指针移入其中或按 Ctrl+G。

密码为属性哪里查到的隐藏信息打开为flag文件

	新建文本	文档.txt	1.txt	base星期四.txt	HEU4000_Debug.txt	audit.txt	flag.txt	×	+	-	×
文件	编辑	查看									£33
flag{,	ab32056r	fanla1238	0asf13gpnsan}								
行1,	列 1	35 个字符					100% Wi	ndows (CRLF	-)	UTF-8	