平时做题总结

原创

<u>m0re</u> 于 2020-05-09 22:25:05 发布 ○ 469 ☆ 收藏 2 分类专栏: <u>CTF</u> 文章标签: <u>CTF writeup</u>

m0re

本文链接: <u>https://blog.csdn.net/qq_45836474/article/details/105628152</u> 版权



CTF 专栏收录该内容

31 篇文章 3 订阅 订阅专栏

本文目录

Misc

[BJDCTF 2nd]EasyBaBa

安恒月赛——6G还会远吗

黄金六年

[安洵杯 2019]吹着贝斯扫二维码

Crypto

传统知识+古典密码

[NPUCTF2020]这是什么觅□

robomunication

Unencode

Web

变量1

web5

头等舱

管理员系统

Misc

[BJDCTF 2nd]EasyBaBa

222 Solves

[BJDCTF 2nd]EasyBaBa

1

https://buu-

1251267611.file.myqcloud.com/ew3jr3udh39dhendiew/ezbb.jpg

得到的flag建议用flag{}包上提交。

Flag Submit

https://blog.csdn.net/qq_45836474

下载图片后,很大的一张图片,里面必定有东西,foremost分离得到压缩包。

解压后是一张jpg格式的图片,但是打不开,猜想应该可能会是文件头缺少,打开010Editor,看一下,发现有点不对劲,



好像是个avi文件,改后缀。打开是一个小视频,好像看过,钉钉来着,全程在叫baba哈。看到中间有几张带二维码的图片闪过 去了。太快看不清,用放在PR里逐帧分离,用截图工具Snipaste截取二维码QQ截图也行,(注意截图时,不要截到其他部分, 否则修复二维码时会出现解码失败的现象)。 放在扫描工具里修复二维码并扫码



位置:(0.9,-0.3)-(62.6,-0.5)-(1.3,62.5)-(63.0,62.2) 颜色反色,正像 版本:1 纠错等级:L,掩码:2	
內谷: 316E677D	

全部扫出来,得到字符串,观察发现符合base16编码的特征。于是进行base16解码

6167696E5F6C6F76655F59424A447B696D316E677D	
	编码解码清空
agin_love_YBJD{im1ng}	

有圳

https://blog.csdn.net/qq_45836474-

这个答案好奇怪,栅栏也不是啊。难道是什么新的加密?看看比赛时给的wp,

7、 (其实这道题是有描述的不知道为什么 buu 通道没了) 可以社工出这是个伪栅栏, 调整一下顺序好啦

呃呃呃,是这样吗?????? flag: BJD{imagin_love_Y1ng}

安恒月赛——6G还会远吗

题目链接: http://server.zhaoj.in:8888/1GTest.file

1GTest.file http://server.zhaoj.in:8888/1GTest.file 819 B/s - 312 KB,共 977 MB,还剩 14 天	
暂停取消	https://blog.csdn.net/qq_45836474

14天啊,是挺无语的,当时想抓包改什么参数来着,全都失败。结果看了wp就是直接将没下载完的文件,放在winhex或 010Editor里看。

- 12																	
翊贞	hi	<u>gh. p</u>	ng	─────	・确り	70	096	8. ci	rdov	nlo	ad@	×					
编辑	方式:	ーナブ	、进制	∫(<u>H</u>)	\sim	运行	脚本	. Y	运行	ī模板	źΥ						_
	Ò						Ģ			9		B		Ď	Ę		<u> </u>
000h:	44	41	53	43	54	46	7B	77	65	6C	63	бF	6D	65	5F	74	DASCTF{welcome_t
010h:	6F	5F	44	41	53	5F	41	70	31	72	31	7D	CF	55	A3	88	o_DAS_Ap1r1}ÏU£^
020h:	D0	AB	01	F8	38	\mathbf{DF}	A 8	94	48	31	8A	28	C8	8D	B 8	1C	Ы.ø8ߨ"H1Š(È.
030h:	74	9B	AB	E1	56	63	AB	D5	A 5	85	42	80	46	AF	A1	05	t>«áVc«Õ¥…B.F⁻;.
040h:	Bб	24	64	4B	15	4B	9B	EE	C7	C6	D5	98	95	63	6B	AB	¶\$dK.K>îÇ <i>E</i> Õ~•ck«
)50h:	4D	85	77	C2	77	AC	80	E4	43	5A	35	D7	7B	D5	2B	6E	M…wÂw¬€äCZ5×{Õ+n
060h:	7D	6E	F7	C9	63	EF	84	ЗA	9B	D4	27	4F	8E	$\mathbf{A0}$	63	80	}n÷Écï":>Ô'OŽ c.
)70h:	29	DB	2D	51	AA	46	4 B	Α5	BC	51	54	66	FE	В3	EC	С9)Û-QªFK¥¼QTfþ³ìÉ
080h:	65	09	08	24	66	18	Eб	E7	BB	9E	32	43	E3	DB	C7	92	e .\$f.æc»ž2CãÛÇ
090h:	33	29	98	E 0	92	E3	61	9F	DB	48	F1	A4	72	5B	A 0	D7 ^m	upsymiggreatennevide 45836474

大写的服!

DASCTF{welcome_to_DAS_Ap1r1}

黄金六年

Challenge	115 Solves										
[RoarCTF2019]黄金6年											
	1										
得到的 flag 请任	回上 flag{}提交。										
🛓 attachment											
Flag	Submit	t									

https://blog.csdn.net/qq_45836474

之前学长给我们看过这个,所以直接进PR里一帧一帧看了,在四本书上看到了二维码,手机扫不出来,当然不是全部,反正我 的是扫不出来。

我用QR Research直接扫出来四个信息。

] 2. txt🛛

- 1 key1:i
- 2 key2:want
- 3 key3:play
- 4 key4:ctf

交flag发现不对,有点奇怪,然后才发现学长给我们看这个题,没让我们看完,还有接下来的步骤。 将视频拖进010Editor中滑到最后,发现了base64编码

:BBD0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:BBE0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:BBF0h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:BC00h:	00	00	00	00	00	00	00	00	00	00	00	00	00	DE	18	00	Þ
:BC10h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:BC20h:	00	00	00	00	00	00	00	00	01	F5	55	6D	46	79	49	52	ÕUmFyIR
:BC30h:	бF	48	41	51	41	7A	6B	72	58	6C	43	67	45	46	42	67	oHAQAzkrXlCgEFBg
:BC40h:	41	46	41	51	47	41	67	41	44	68	37	65	6B	35	56	51	AFAQGAgADh7ek5VQ
:BC50h:	49	44	50	4C	41	41	42	4 B	45	41	49	45	76	73	55	70	IDPLAABKEAIEvsUp
:BC60h:	47	41	41	77	41	49	5A	6D	78	68	5A	79	35	30	65	48	GAAwAIZmxhZy50eH
:BC70h:	51	77	41	51	41	44	A0	44	78	34	33	48	79	4F	64	4C	QwAQAD.Dx43HyOdL
:BC80h:	4D	47	57	66	43	45	39	57	45	73	42	5A	70	72	41	4A	MGWfCE9WEsBZprAJ
:BC90h:	51	6F	42	53	56	6C	57	6B	4A	4E	53	39	54	50	35	64	QoBSV1WkJNS9TP5d
:BCA0h:	75	32	6B	79	4A	32	37	35	4A	7A	73	4E	6F	32	39	42	u2kyJ275JzsNo29B
:BCB0h:	6E	53	5A	43	67	4 D	43	33	68	2B	55	46	56	39	70	31	nSZCgMC3h+UFV9p1
:BCC0h:	51	45	66	A0	4A	6B	42	50	50	52	36	4D	72	59	77	58	QEf.JkBPPR6MrYwX
:BCD0h:	6D	73	4D	43	4 D	7A	36	37	44	4E	2F	6B	35	75	31	4E	msMCMz67DN/k5u1N
:BCE0h:	59	77	39	67	61	35	33	61	38	33	2F	42	2F	74	32	47	Yw9ga53a83/B/t2G
:BCF0h:	39	46	6B	47	2F	49	49	54	75	52	2B	39	67	49	76	72	9FkG/IITuR+9gIvr
:BD00h:	2F	4C	45	64	64	31	5A	52	41	77	55	45	41	41	ЗD	3D	/LEdd1ZRAwUEAA==
:BD10h:	A0																•
																	https://blog.csdn.net/gg_458364
																	1 1 2

进行解码,看到是rar压缩包,

UmFyIRoHAQAzkrX1CgEFBgAFAQGAgADh7ek5VQIDPLAABKEAIEvsUpGAAwAIZmxhZy50eHQwAQAD Dx43HyOdLMGWfCE9WEsBZprAJQoBSV1WkJNS9TP5du2kyJ275JzsNo29BnSZCgMC3h+UFV9p1QEf JkBPPR6MrYwXmsMCMz67DN/k5u1NYw9ga53a83/B/t2G9FkG/IITuR+9gIvr/LEdd1ZRAwUEAA==

清空 加密 解密 网络结果以16进制显示

Rar!□□□□3劁□□□□□□□□0000<□□□ K쒑□ □flag.txt0□□□□07□#,V|!=XK□f% □IYVR3v�油6□t □屮□□_iQ□&@0=□□Â3>り歍c□`k 卖~Y□□□뼱□wVQ□□□□

Base编码系列: Base64 Base32 Base16

然后大佬们的办法是写脚本,我不会写,只能另外找办法。我就想到将base64编码转换成16进制,然后再保存为rar文件,好像可行。试一下。

田田秋洪• Base64	在线	解码、	编码				
Base64 Tool	CSS Base	64 ASN.1 To	ool DES Tool	3DES Tool	AES Tool RS	A Tool	□34533458 点击关闭
UmFyIRoHAQAz Dx43HyOdLMGV JkBPPR6MrYwX	krXICgEFBgAF VfCE9WEsBZpi msMCMz67DN	AQGAgADh7ek5 rAJQoBSVIWkJN /k5u1NYw9ga53	5VQIDPLAABKEAIEvs NS9TP5du2kyJ275Jzsł sa83/B/t2G9FkG/IITuR-	UpGAAwAIZmx No29BnSZCgM0 +9gIvr/LEdd1ZR	hZy50eHQwAQAD C3h+UFV9p1QEf AwUEAA=╡		
							li
		Soure Type : ®	Text OHex Decoded R	Result : Hex o	characters • En	coding : UTF	-8 • Encode Decode
00 01 02 03 0	04 05 06 07	Soure Type : •	Text Hex Decoded R	Result : Hex o	haracters • En	coding : UTF-	-8 • Encode Decode

网站地址: base64转换成16进制

然后,复制十六进制的编码粘贴到HxD中进行保存。

₩ HxD - [C:\Users\18101\Desktop\1.rar]

📓 文件(F) 编	辑(E)	搜	素(S)	视	图(V) 分	祈(A) I	具(1) 🗃	8□(\	N)	帮助	(H)			
1		-	9	ġ	-	÷ →	16	`	- \	Wind	ows	(Aľ	~	+六	进制	· ~		
🔛 1.rar																		
Offset	; (h)	00	01	02	03	04	05	06	07	08	09	٥A	0B	0C	OD	0E	OF	
00000	000	52	61	72	21	1A	07	01	00	33	92	B5	E5	0A	01	05	06	Rar!3′µå
00000	010	00	05	01	01	80	80	00	El	ED	E9	39	55	02	03	3C	BO	€€.áíé9U<°
00000	020	00	04	A1	00	20	4B	EC	52	91	80	03	00	08	66	6C	61	¡. KìR`€fla
00000	030	67	2E	74	78	74	30	01	00	03	OF	1E	37	1F	23	9D	2C	g.txt07.#.,
00000	040	C1	96	7C	21	ЗD	58	4B	01	66	9A	C0	25	0A	01	49	59	Á− !=XK.fšÀ%IY
00000	050	56	90	93	52	F5	33	F9	76	ED	A4	C8	9D	BB	E4	9C	EC	V."RÕ3ùví¤È.»äœì
00000	060	36	8D	BD	06	74	99	0A	03	02	DE	1F	94	15	5F	69	D5	6.½.t™Þ.″iÕ
00000	070	01	lF	26	40	4F	ЗD	1E	8C	AD	8C	17	9A	C3	02	33	3E	&@O=.Œ.Œ.šÃ.3>
00000	080	BB	0C	DF	E4	E6	ED	4D	63	OF	60	6B	9D	DA	F3	7F	C1	».ßäæíMc.`k.Úó.Á
00000	090	FE	DD	86	F4	59	06	FC	82	13	B9	1F	BD	80	8B	EB	FC	þ݆ôY.ü,.¹.¾€<ëü
00000	0A0	B1	1D	77	56	51	03	05	04	00								±.wVQ



提交正确。

[安洵杯 2019]吹着贝斯扫二维码



https://blog.csdn.net/qq_45836474

解压发现一堆文件

יניר		~=
🗋 6lk34u72te5s79kzj0dr	2019/11/6 1:16	文件
🗋 6q13s096tu512c8f7z8x	2019/11/6 1:16	文件
🗋 7vh669w0zagz936z28h5	2019/11/6 1:16	文件
🗋 09w91x992i4ijx6iqt27	2019/11/6 1:16	文件
🗋 9g896pxvd013rx16r0xf	2019/11/6 1:16	文件
🗋 14c6p1j84uis3453298a	2019/11/6 1:16	文件
🗋 64g80t29b7kjhi8nxoiu	2019/11/6 1:16	文件
🗋 67pt042zw26y3e350i4s	2019/11/6 1:16	文件
🗋 88u9ofh6oud8lx62r1h3	2019/11/6 1:16	文件
🗋 227j301wb8cq7l29qf9y	2019/11/6 1:16	文件
🗋 284rgt186c76v758xpc7	2019/11/6 1:16	文件
C 576lit819036i9i31s45	2019/11/6 1:16	文件

		~ 0
📄 1453k669k20puqnxjwrb	2019/11/6 1:16	文件
8151ltvll69t7n8dqd18	2019/11/6 1:16	文件
🗋 66068yso21h7m48kmjyr	2019/11/6 1:16	文件
448931j6ihj30h4v7llv	2019/11/6 1:16	文件
649882lp5734tuu48of2	2019/11/6 1:16	文件
] ag32l406e0h957h 类型: 文件	9/11/6 1:16	文件
□ bj245p444s05lfwx	9/11/6 1:16 9/11/6 1:16	文件
📕 flag.zip	2019/11/6 1:14	Winf
gu4c2ce0t7558a2lepos	2019/11/6 1:16	文件
📄 l5e87tbyb7n1q5l91yp0	2019/11/6 1:16	文件
	2010/11/6 1.16	+1/+

而且压缩包还是加密的,看看那些文件,发现都有JPEG,可能是jpg图片,先改一个看看。

♥ 🛍 ♡ 🤉 본 🤅



https://blog.csdn.net/gg_45836474

有点东西,总不能一个一个改吧?这么多,然后在百度的小角落里发现了一个工具——格式工厂(最喜欢工具了)



\rightarrow BMP] (\rightarrow GIF] (\rightarrow TIF] (\rightarrow TGA]		2K	完成	🛉 2K (109%)
		09w91x992i4ijx6iqt27	-> JPG	
		2К	完成	🔶 🛉 2K (113%)
		9g896pxvd013rx16r0xf	-> JPG	
Picosmos Picture Tools		2К	完成	🛉 2K (113%)
		14c6p1j84uis3453298a	-> JPG	
		ЗК	完成	🛉 4K (116%)
文档		64g80t29b7kjhi8nxoiu	-> JPG	
米班沿客/DV/D/CD/ISO	- 9 0	2К	https://bic 完成	g.csdn.net/gg_458364/4 3K (114%)

真快,看一下。





7pt042zw26y3 e350i4s.jpg







6k9e6sej74v7f6

yhpu7r.jpg





ag32l406e0h95



6lk34u72te5s79

kzj0dr.jpg

284rgt186c76v



gu4c2ce0t7558 a2lepos.jpg

6q13s096tu512

c8f7z8x.jpg

758xpc7.jpg





7vh669w0zagz9

36z28h5.jpg

l5e87tbyb7n1q

5l91yp0.jpg



09w91x992i4ijx

6iqt27.jpg

1453k669k20pu

m2b25yf40kr28 l98p4g6.jpg



9g896pxvd013r x16r0xf.jpg

8151ltvll69t7n8

dqd18.jpg





4v

64g8(

66068yso21h7 m48kmjyr.jpg



p0zx7csh96pr0 e1k497b.jpg

q6x39 ssx7



. uu48of2.jpg









74

好家伙,拼图。得到36张图,可以拼一张6x6的大图。 将文件夹拖进kali。然后使用工具拼图。 在文件夹内打开终端

montage *jpg -tile 6x6 -geometry 134x130+0+0 out.jpg

然后得到一张混乱无序的图。

注意这里的像素: 要和分裂的二维码残片的像素一致才能得出这样的二维码乱序图。如果像素不一样了, 就得不到这样 的图,当然后面的步骤也就无法进行下去。

而这张图的像素:打开一张二维码片段,然后看它的属性里面——详细信息

1J 7IX AAAAA 标记 备注 来源 作者 拍摄日期 程序名称 获取日期 版权 图像 图像 ID 公城玄 124 v 120



<i>レ」 サリ</i> +ᢡ	134 X 130				
宽度	134 像素				
高度	130 像素				
水平分辨率	۹6 dpi د				
垂直分辨率	s 96 dpi				
位深度	24				15026/7/
FT-45		nups.m	nog.csun.n	evqq_*	40000474



再使用gaps还原

gaps --image=out.jpg --generations=40 --population=36 --size=100

没还原出来,尴尬哈,,,,,不知道怎么回事,我试了n次了,就是还原不出来。奇怪了。最后我实在是没办法了,只上手了。 在PPT里拼的。md 累死,我拼了俩小时(泪流满面.gif)





扫描吧,终于可以扫了。

已解码数据1:

位置:(14.2,9.7)-(635.5,11.1)-(14.0,618.8)-(635.9,621.7) 颜色正常,正像 版本:6 纠错等级:H,掩码:3 内容: BASE Family Bucket??? 85->64->85->13->16->32

https://blog.csdn.net/qq_45836474

emmm,啥玩意儿。好像还有个flag.zip没看。

					_			_								
a	ttacł	men	t.zi	p	f1	ag. :	zip	×								
〕式:	ーナデ	∖进制	(H)	\sim	运行	脚本	. Y	运行	ī模板	ź: Z	IP.Ł	nt 🗸	⊳			
Ó						6			9		Ř		Ď			0123456789ABCDEF
50	4B												$4 \mathrm{F}$	7в	2C	PKfO{,
в1	в4														6C	±′"fl
61		2E			74	29	F8	82	0C	18	4C	30	3E	A 8	DF	ag.txt)ø,L0>¨ß
AE	AE	9A	C6	81	17	58	C9	91	5B	E 0	A 5	3C	90	56	26	®®šÆXÉ`[à¥<.V&
3B	AB	C2	CA	28	BE	3D	01	50	4B			3F			00	;«ÂÊ(¾=.PK?
01	00	00	00	12	08	66	4F	7в		в1	в4				00	fo{,±´"
16															08	
0.0										2E					00	flag.txt
20												A 8	8A	FA	93	Ñ™¨Šú``
D5			в1	в3							В1	в3			93	Õ.G±³õu 🐔 G±³ôù"
D5	01	50	4B											5A	00	Õ.PKZ.
00	00	48							4E			$4 \mathrm{F}$	$4\mathrm{D}$	4A	56	Hs.GNATOMO
49		5A		4B	4E	4A							4E		54	IQZUKNJXGRCTGNRT
47				4D	4E				4E			4B		4A	51	GI3EMNZTGNBTKRJW
47					4D				4E		44			(5A)	57	GI2UIMRRGNBDEQZW
47	49	33	44	4B	4D	53	46	47	4E	43	44	4D	52	4A	: 4	GI3DKMSFGNCDMRJT



嗷嗷,还有编码。复制出来解密。

上面扫出来的好像是加密顺序,因为题目中的二维码已经扫过了,还有贝斯。那应该是base编码。 这个编码好像是base32 编码,那就是解密过程,上面的是加密顺序,将它逆转一下。开始解码。 这题真的给我解吐了。转过来转过去。 得到压缩包密码,ThislsSecret!233 解压flag.zip得到

flag{Qr_Is_MeAn1nGfuL}

这一道题真是耗费我好长时间。

Crypto

传统知识+古典密码

Challenge	350 Solves	×
传	统知识+古典密	祏马
	1	
注意: 得到的1	flag请包上flag{}提交	
📩 d6f96e23-1f		
Flag		Submit

看着是年份,还是六十甲子年份。应该是要换成数字。于是百度对照表。把数字对照出来。而且背面还写了 +甲子 再加上60。一 甲子是六十

ıb.	key 🗙 🚺	🔒 题目.	txt⊠										
	小明某	一天收	て到一書	村密信,	信中国	う了 几イ	ト不同的	勺年份					
		辛	⊊卯,奚	≹巳,ቮ	5戌, 4	岸未,厚	€辰,多	資酉,	己卯,	癸巳	•		
		信	的背面	ī还写有	育"+甲∃	子",请	解出这	段密文	ζ.				
	key值:	CTF{	XXX }										
	辛卯	楽日	丙戌	文本	庫匾	华西	≓ún	彩巳					
	28	30	23	8	17	10	16	30					
	-												
	88	90	83	68	77	70	76	90					

第一想法应该是ASCII码表。对照出来。

本软件将字符与ASCII码相互转换! 欢迎使用!

请输入字符或相应的A	SCII码
88, 90, 83, 68, 77, 70	, 76, 90
俞入的若为ASCII码,请 1输入的内容尽量不要 转换后	12]西文逗号隔开!末尾无须加逗号,并 太多,否则出错!
XZSDMFLZ	
○ 字符->ASCII	● ASCII->字符
转换	https:/ 清空 j.csdn.net/qcj_45 退以 174

然后看着这一串字符,没了头绪。再看看题,没有提示了啊。然后发现一个重要的事,题目说传统密码加古典密码。我好像没用 到古典密码啊。脑中快速过了一遍古典密码。这么短的字符串,应该会是凯撒密码,还有栅栏密码,其他的一下子没想太多。 八个字符,栅栏可以分两栏和四栏,试过之后是两栏的。

🍓 栅栏密码加度	解密				• • •
操作					
密文:	XZSDMFL	Z			
明文:	XMZFSLD	Z			
栏数:	2 -		加密	https://blog.cs 的	密 [0_45836474
然后凯撒解密。 得到					

XMZFSLDZ

位移 5 加密	解密	
SHUANGYU		

至于是偏移5位,自己一个一个试出来的,就这个最靠谱。

[NPUCTF2020]这是什么觅□

这个比赛我也看了,当时就看这一道题能看出来点门道,当然我一道题都没做出来,没什么可丢人的。就把这道题复现一下。也 是成长过程。

下载得到一个文件,刚开始没有思路啊,没有想太多,不知道用什么方法打开,就直接payload++打开看了一眼,然后发现了

PKETXEOTDC4NULNULNULBSNULACKZ蝌狲。 x8AENONULXAB%ACKNULBSNULNULNULflag.jpgxECESCy 斶xF6ESCc纾
辽纪踵US" 瓶ETBM
DDLEOOdSUBX82 蕢
2 EF X91 ETX X98 DC1 xbqZ BS RS 憷? EOT (@ ES< ETBp XE3) 鄆 XB8) ETX m 淅噮 H 疖 峦 Ž? k 袳 斃 鄇 NUL XEB 皣 娙 鼢 U 탉 氎 V.
SOHIXBORSIXF6SUB粉 犯s DACK再鮩M蜕欐3XCDGS汰ES菌XE5-,ES,1ES,XCCD/1XDDSYNEMWC0EODC0EODC0EOCX
鰵魁1壥KEPSOKCBXFP緣拵前嫉
x82\$% /鄜xC6?ETBxE4ACKxE3SYN怪VT鳤\ 县F%STX旪ADC4b頯i颼axFE笉x86''x93!CANx82!CANx82!CANx82!P/
臺蟌4哚 xC6xEExC0 +~=k S0B g8 XE2ETXXE5 5r?b DC3 疹侎婷髁 XEE ?:麢SIK考 朱xECDC4抛xD5DC3带&BEE 椊!SOB踕=猪
裼8"燫SOH' X83 SOH栺X809yENOE%eNAK誥XE8? X97 EM~皉EOT 倱轻遼XB5DC4X94DC4X95NAK餵枲RDC3/?Q薆羍墴訾
xxxx,岻瘪鈓厘xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
茖GSvC(bBS縦汗v钡鳇☞)蜴 旊OOD]CANM溴顁褯X900/EF稂x1009通餘瘞帮Kr鄊u)b匜 s攫QX摆微ENOEDE厂性Nうr
SO4:顧USYN%幸yYM玖 踷`N 3GICAN XBD; SO XFFV碚 X83NAKFo X8F9 XE8 塹蓋注 XCD DC3 X89<
X8F;XF7ESCXD4ESOXDE:睪[XF6CAN X8EXFF焙二0+XCA X9C=v粤/*q譓LX89.珵 G妱XCI;/V哥X欌r.XDC*T
:k鲉 XFD+ v厥 DC1 XE9 DC3 挜葨0 蒇頽mY XF4 RSq纙诋 DC2?0Y 泾觉 BE1+ XEF) 奲" 眃4 ^{hin} (un7gU SKN; XD9 ACK3 ⁰³ X踪路

然后,foremost分离文件,得到了压缩包。



这个我没想到有什么古典密码是这个的,然后看着右下角的纸条,这种有空隙的,是不是键盘密码之类的,再仔细想想不对,放弃,后来看着上面的日历,在这里面找,没啥头绪。再回头看那串字符串。发现第一个字母都是大些且 F、W、S、S、T、S、W、S有个规律就是他们英文单词星期的首字母。这个一想就靠谱,就抓住这一点来想。后面跟数字,再看日历,第一排画圈了。没错的,就是这样,字母后面跟两个数字的都是在一周中又重复出现的。所以第一个字母是他们的顺序。第二个字母才是出题人想给的信息。这样看出来就是

3 1 12 5 14 4 1 18, 我不知道为什么把1算上了, 不是已经划了吗??

不过不纠结这个,我到这里卡住了。所以后面的看的师傅们的博客知道的。然后发现是字母表的,我之前一直在猜ascii码,就 这个没想到。所以一道题没做出来。最后 flag{calendar}

robomunication

Challenge	208 Solves	×					
robomunication							
1							
注意:得到的flag请包上flag{}提交							
➡ a320bccb-dd							
Flag Submit							

https://blog.csdn.net/qq_45836474

听得出来是摩斯密码,别说了,都是辛酸,这个哔哔哔波,纯手工。

空格	加密	短			ĸ	 解密	
			结	果			
		HEL	LOWHATISTHEI	KEYITISBOOPBEEP			

再把这个字符串看一下,最后是flag是BOOPBEEP

Unencode

Challenge	114 Solves							
	Unencode	e						
	1							
注意:得到的flag请包上flag{}提交								
📩 e414b69a-5.								
Flag		Submit						

什么提示都没有,,就一串编码,而且看着怎么也不想不起来什么密码是这样的,见识短浅了。 是UUencode编码 直接在线网站解就行了。 UUencode在线解码 flag{dsdasdsa99877LLLKK}

Web

web题先从简单的来,不然太容易被搞乱心态。

变量1

Challenge	10418 Solves	×
	变量1	
	60	
http://123.206.87	7.240:8004/index1.php	
Flag		Submit

代码审计:

```
flag In the variable ! <?php
error_reporting(0);
include "flag1.php";
highlight_file(__file__);
if(isset($_GET['args'])){
    $args = $_GET['args'];
    if(!preg_match("/^\w+$/",$args)){
        die("args error!");
    }
    eval("var_dump($$args);");
}</pre>
```

首先注意到的是正则表达式,关于正则表达式的学习,在学习PHP时了解过了,这个是要匹配正确的字符串。

\w 匹配任意一个数字或字母或下划线

如果不匹配则直接die,匹配的话就输出一个可变变量,重点就在可变变量这里。我刚开始进行尝试,构造 ?args=_lala_ 结果输出了NULL,好像与eval函数有关,发现对eval函数了解的不够,就又查了一遍。

定义和用法

eval()函数把字符串按照 PHP 代码来计算。

该字符串必须是合法的 PHP 代码, 且必须以分号结尾。

如果没有在代码字符串中调用 return 语句,则返回 NULL。如果代码中存在解析错误,则 eval() 函数返回 false。

nttps://blog.csdn.net/qq_45836474

\$\$args 代表一个变量,所以这里传一个全局变量给它,全局变量有九种,可以挨个试,九大全局变量在百度直接搜索就可以搜到。

1 \$_POST	[用于接收post提交的数据]
2 \$_GET	[用于获取ur1地址栏的参数数据]
3 \$_FILES	[用于文件就收的处理img 最常见]
4 \$_COOKIE	[用于获取与setCookie()中的name 值]
5 \$_SESSION	[用于存储session的值或获取session中的值]
6 \$_REQUEST	[具有get,post的功能,但比较慢]
7 SERVER	[是预定义服务器变量的一种,所有SERVER[是预定义服务器变量的一种,所有_SERVER [是预定义服务器变量的一种,所有_
SERVER开头的都	
8 \$GLOBALS	[一个包含了全部变量的全局组合数组]
9 \$_ENV	[是一个包含服务器端环境变量的数组。它是PHP中一个超级全局变量,我们可以在PHP 程序的任何地方直接访问它]

然后,用到了GLOBALS就得到了flag

web5

f12发现了非常多的编码,查百度,发现是jother编码,而且控制台可解。直接复制所有编码粘贴到控制台,回车即可。flag大 写。

头等舱

打开网页什么也没有,没有其他提示,回头看题目,"头"等舱。header。进行抓包尝试。成功找到flag

lequest	Response
Raw Headers Hex	Raw Headers Hex HTML Render
T /hd.php HTTP/1.1 st: 123.206.87.240:9009 er-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 efox/46.0 cept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 cept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 cept-Encoding: gzip, deflate IT: 1 nnection: close che-Control: max-age=0	HTTP/1.1 200 OK Server: nginx Date: Sat, 09 May 2020 13:40:02 GMT Content-Type: text/html Connection: close flag(Bugku_k8_23s_istra): Content-Length: 139 <html> <thml> <thtml> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <pre> <br< th=""></br<></pre></thtml></thml></html>
	https://blog.csdn.net/qq_45836475

管理员系统

f12查看有无有用信息,找到一个base64编码(==),解码得到test123,应该是密码了吧。 所以尝试登陆:发现登录失败,而且IP禁止访问,联系本地管理员。 所以可能是XFF。可以改一下,本地管理员那就改成本地的127.0.0.1 可以抓包添加,我直接使用chrome扩展插件添加了,然后刷新网页,得到flag。

管理员系统	
-------	--

Username:

Password:

Submit Reset

The flag is: 85ff2ee4171396724bae20c0bd851f6b

https://blog.csdn.net/qq_45836474