

bugku ctf 杂项 隐写2

原创

就是217 于 2019-05-18 11:50:00 发布 924 收藏 1

分类专栏: [bugku ctf](#) 文章标签: [图片隐写](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_42777804/article/details/90313230

版权



[bugku ctf](#) 专栏收录该内容

61 篇文章 2 订阅

订阅专栏

下载打开后 是一个图片



想拿到flag? 心の中ないいくつかB数かの?

(心里没点b数我是不会来做题的)

图片隐写无疑了

直接改后缀名为 .zip 解压后打开



flag.rar



提示.jpg

https://blog.csdn.net/qq_42777804

查看图片提示

告诉你们一个秘密，密码是3个数哦。

查理曼：

查理曼，法兰克王国国王，征服了西欧与中欧大部分土地，具有了至高无上的权威，下令全国人民信仰基督教，查理重振了西罗马帝国。

雅典娜：

女神帕拉斯·雅典娜，是希腊神话中的女战神也是智慧女神，雅典是以她命名的。

兰斯洛特，

英格兰传说中的人物，是亚瑟王圆桌骑士团中的一员。看上去就是一个清秀年轻的帅小伙儿，由于传说中他是一名出色的箭手，因此梅花J手持箭支。兰斯洛特与王后的恋爱导致了他与亚瑟王之间的战争。

Hint:

其实斗地主挺好玩的。

https://blog.csdn.net/qq_42777804

有用的信息就一个 密码是3个数

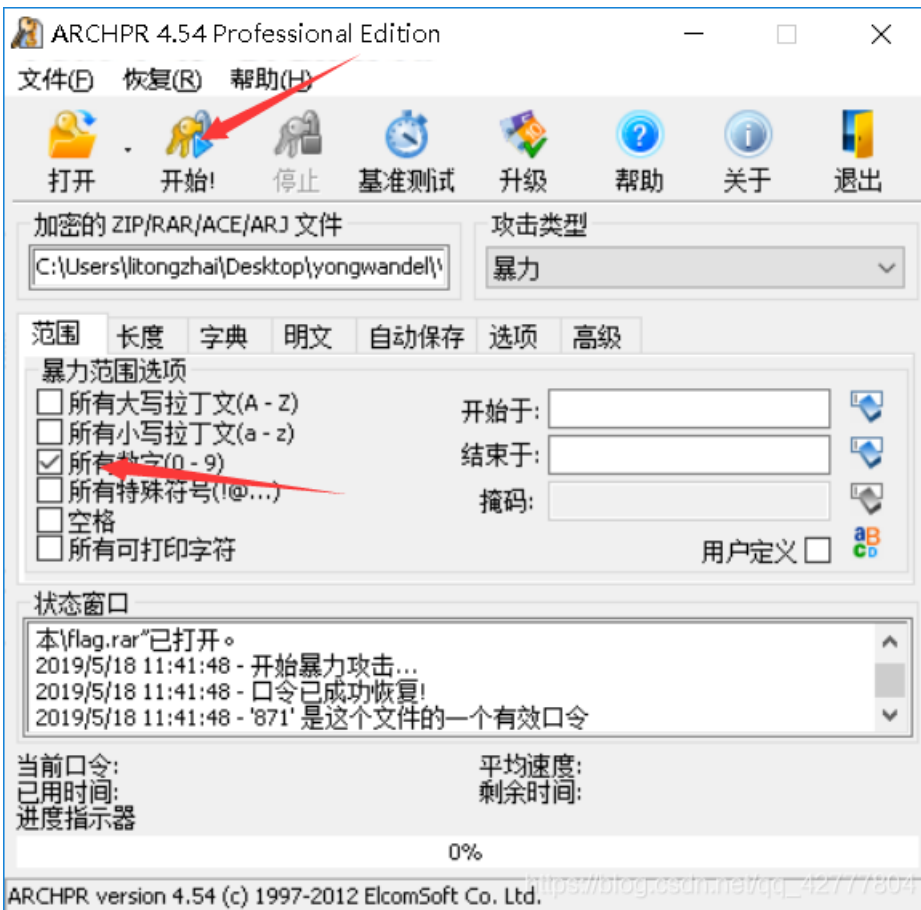
那就简单了 直接暴力破解

附上工具 archpr，是一种密码恢复工具，用于解密RAR压缩包的密码。

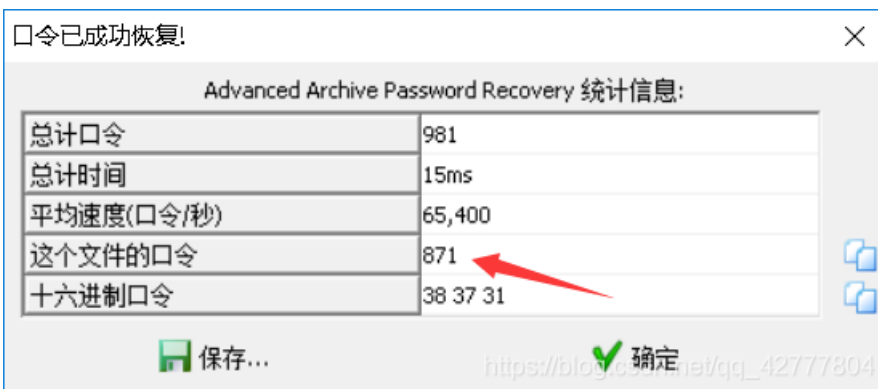
链接：<https://pan.baidu.com/s/1J9osF84zZqfWyOHoM9tLCQ>

提取码：wxym

用工具打开 另一个flag.rar文件 进行破解



轻轻松松得到密码 为 871



那么对文件进行解压 打开



还是用winhex打开把

拉到最下面

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
000017A0	84	6D	54	F0	88	AE	B9	48	1B	DC	C5	9A	2C	9D	15	00	„mTô^@+H UĂš,
000017B0	0B	D6	24	B1	1B	04	5B	4B	C3	4D	4A	A2	83	11	9C	DD	ÖS± [KÄMJçf œý
000017C0	43	79	1B	4D	3F	E1	84	1E	AC	78	7E	E1	37	FF	00	72	Cy M?á„ -x-á7ý r
000017D0	CC	06	81	1B	9D	4D	12	85	B8	C2	2A	22	D2	80	E2	B9	ì M „,Ă*“òeá†
000017E0	F0	79	C4	C0	00	D2	62	0C	4D	90	B9	80	A6	98	89	3F	šyÄÄ òb M †e! ?%?
000017F0	94	61	DE	B3	89	91	8C	20	02	F8	8F	91	72	36	E6	A5	“aF°%‘GE ø ‘r6æš
00001800	BB	D5	7C	93	DB	1E	08	5B	D8	AF	7B	0F	18	59	93	A6	»Ø ‘ú [ø{(Y‘
00001810	F6	BB	EE	DD	DB	6E	F9	DE	22	6D	21	28	88	53	40	D0	ò»îYŮnùE“m!(^SØB
00001820	89	37	E7	04	8F	84	63	6A	08	95	05	1A	0C	31	52	15	%7ç „Cj • 1R
00001830	56	39	45	0B	31	E1	82	B4	41	15	01	39	96	A9	4E	EE	V9E 1á,‘A 9-@Ni
00001840	B7	95	A2	D1	20	F3	5E	28	EB	BF	0F	AF	68	A1	53	8D	••ñ ó^(èç Th;s
00001850	3D	83	5B	B7	59	77	71	EC	96	D0	6D	6D	34	53	DC	D1	=f[·Ywqi-Èmm4SŮŮ
00001860	06	91	4B	98	A3	43	22	0D	29	54	4D	62	19	22	A2	04	‘K‘èC“)Tmb “ç
00001870	10	D6	0E	46	0D	C1	4A	0E	11	A1	54	D8	0D	EE	5D	FB	Ö F ÁJ ;Tø îjù
00001880	4C	A6	69	B4	E4	B4	1D	DE	04	DB	CF	7A	5E	6A	2D	84	L i‘á‘ E ŮÍz^j-„
00001890	DE	38	C7	6C	F1	F7	A6	B5	2A	C8	A1	64	5A	6E	C3	20	E8Çlñ+!µ*È;dznÄ
000018A0	F6	14	19	60	5E	0B	66	B1	92	80	C9	77	41	5F	23	0E	ò ^`ft‘eÈwa #
000018B0	20	F6	8E	B9	7F	AC	34	1B	BF	4D	EC	0A	02	7A	2A	F9	òž+ -4 çMi z*ù
000018C0	F2	61	2A	4A	63	68	1F	0E	70	03	06	DE	18	2A	76	0C	òa*Jch p E *v
000018D0	44	0A	53	AC	45	FD	B7	F5	81	8C	12	7D	9E	B2	6A	0B	D s-Eý·ò E }ž*í
000018E0	CD	E4	C0	64	84	B3	C3	ED	F8	FA	29	BE	5F	E7	66	ED	íàÄd,°Áiêu)¼_çfí
000018F0	17	83	C9	F3	AE	30	93	B4	EE	DA	19	9B	11	81	E9	F8	fÉó@0“‘iú > éø
00001900	BF	EF	78	41	81	5B	14	A4	E7	E3	9F	39	5C	2A	02	9B	çixA [*çãY9* >
00001910	DE	9C	B0	18	6B	EC	9C	73	5C	FE	90	B8	C5	44	74	D9	Eø° kioes\p ,ÄDtŮ
00001920	E0	FF	00	3E	99	04	AD	43	CF	59	05	7A	19	C2	71	3B	ày >™ -CIY z Äq;
00001930	E7	34	32	50	02	78	C2	17	D3	5F	8F	FC	C4	96	0D	BB	ç42P xÄ Ó úÄ- »
00001940	43	83	8F	77	1F	D7	69	76	21	B9	5F	7C	88	C0	E0	08	Cf w xivl¹_ ^àà
00001950	07	83	29	DE	FF	00	01	F3	9B	2E	5A	88	01	83	F3	C7	f)Éý ó >.Z^ fócç
00001960	EB	E9	B6	D1	1F	A5	C2	A3	2C	A0	02	AF	9C	23	A5	56	ééŹŮ ŹÄé, “œ#šV
00001970	1C	F7	B1	FC	E1	CE	D8	4A	32	BB	C4	84	00	96	9F	BC	+±uáîøJ2»Ä„ -Y¼
00001980	DD	B7	61	98	79	66	D8	DA	1A	9B	3B	39	C5	2C	51	19	Ý·aYfðŮ >;9Ä, Q
00001990	FE	36	06	F5	EF	70	05	C5	A7	93	81	BA	E7	57	D4	E7	þ6 ðip ÄS“ °çWÖç
000019A0	26	90	9C	25	9D	71	1A	FB	E1	02	C0	6F	44	95	0D	57	& œš q úá ÄoD• W
000019B0	9E	C2	AF	59	1B	9E	6F	1A	DD	6B	B5	E7	58	F8	34	1E	žÄ`Y žo ÝkuçXø4
000019C0	EB	C8	58	81	3B	7B	0D	60	23	2C	14	E0	14	13	4D	9C	eÈX ;{ `#, à Moe
000019D0	F1	F2	89	C2	0B	C0	9C	0A	C7	BE	BF	78	68	50	25	31	ñò%Ä Äœ Ç¼çxhPš1
000019E0	0A	83	C7	43	BF	38	35	0B	11	D3	98	2D	4D	EF	EF	83	fçç¿85 Ó“-Miiif
000019F0	95	4D	9A	5C	01	54	DA	3A	F1	8E	2D	1E	6A	56	F1	B1	•Mš\ TÚ:ñž- jVát
00001A00	76	83	BE	19	02	12	19	85	DD	F5	2F	71	D9	F8	ED	F8	vf¼ „Ýò/qùeieø
00001A10	D6	32	7B	25	E4	F1	53	17	8C	80	50	37	D7	1D	BF	9C	Ó2{šáñš œEP7× çœ
00001A20	A0	2E	B0	29	AC	A6	B1	AD	38	00	A3	62	CF	8C	69	6D	“)-!±-8 ðbÍEim
00001A30	CB	15	9F	6F	6C	A0	86	25	6E	12	70	EB	BC	69	6B	41	È Yø†šn pèšika
00001A40	23	E4	67	D4	FF	D9	20	20	20	20	66	31	40	67	7B	65	#ägÖyŮ f1@gte
00001A50	54	42	31	49	45	46	79	5A	53	42	68	49	47	68	41	59	TB1IEFyZSBhIGhAY
00001A60	32	74	6C	63	69	45	3D	7D	20	20	20	20	20	0D	0A	20	2t.lciE=} .net/qq_42777804
00001A70	1A																

发现 f1@g{eTB1IEFyZSBhIGhAY2tlciE=} 显然是base64加密的

对括号里内容在线解密得到

y0u Are a h@cker!

按格式输入即可（发现格式不对）

f1@g{y0u Are a h@cker!}

这样才正确

隐写2

60

Welcome_.jpg

Flag

Submit

Correct

https://blog.csdn.net/qq_42777804