

BUUCTF:Beautiful_Side

原创

wangjin7356 已于 2022-02-11 13:36:52 修改 298 收藏

分类专栏: [CTF](#) 文章标签: [安全](#)

于 2022-02-11 13:31:39 首次发布

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/wangjin7356/article/details/122878248>

版权



[CTF 专栏收录该内容](#)

49 篇文章 0 订阅

订阅专栏

题目链接

https://buuoj.cn/challenges#Beautiful_Side

解题过程

题目 [解题快手榜](#) ×

Beautiful_Side

1

听说最近二维码很火啊, 呐, 美丽的一半。注意: 得到的 flag 请包上 flag{} 提交

[ba678f49-8c...](#)

Flag

CSDN @wangjin7356

根据题目提示, 应该有一半的二维码。先打开压缩包看看, 是张漂亮的girl图片



老方法，先用010Editor打开分析，发现有张png图片

BeautifulSide.jpg x		无标题1.png															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
AD40h:	B5	D3	8F	E9	9B	51	48	07	40	40	E5	32	95	F2	FB	99	µ0.è»QH.@ã2•òd™
AD50h:	4E	B2	63	69	7A	9A	37	64	76	C2	D4	8C	5A	82	94	02	N²cizš7dvÄÖEZ,™.
AD60h:	77	7E	15	05	EC	25	A4	98	DC	8B	75	A9	31	4E	61	DF	w~.i%ª"Ù«u@1NaB
AD70h:	FA	AF	EC	8B	5A	E3	3A	51	67	91	F6	46	9C	1F	CA	8E	Û'i«Zã:Qg'òFø.ÊZ
AD80h:	79	EC	B5	8C	EA	E9	D2	DD	97	63	C2	78	CD	67	9D	C1	yipæééÖY-cÄxIg.A
AD90h:	EC	10	31	3D	E1	3D	60	EF	7D	08	65	E2	56	4A	CB	3B	i.1=á='i).eãVJE;
ADA0h:	40	4D	AA	40	EC	BE	7F	08	23	63	49	E4	7D	95	28	BC	@Mª@i%..#cIã)•(¼
ADB0h:	5B	B4	9A	60	F2	24	F9	C2	93	D2	74	7E	95	A7	A8	C2	['š'ò\$ÙÄ"Òt~•š"Ä
ADC0h:	FA	AC	6B	EF	C8	5D	24	8D	C8	1E	AB	D2	74	6C	BD	3A	Ù-kiÈ]\$.E.«òt1%:
ADD0h:	21	A4	9C	82	53	24	A7	23	CE	75	1D	3B	74	9A	B6	7C	!œ,ššš#Íu.;tš¶]
ADE0h:	AC	39	B2	41	47	29	97	A6	39	4C	63	AE	C8	71	82	B3	-9°AG)- 9Lc@Eq,ª
ADF0h:	CA	B3	23	B9	D3	DE	EA	BA	56	FC	C3	24	5B	DE	17	59	Êª#¹ÓpéªVuÃ\$[p.Y
AE00h:	76	3A	71	BA	D1	B6	4C	4A	5A	18	64	08	B4	F7	85	8A	v:q°Ñ¶LJZ.d.'÷...š
AE10h:	60	59	7F	74	21	BD	A6	45	4D	54	FC	03	C9	52	65	AC	'Y.t!% EÓTü.ÉRe-
AE20h:	48	E5	08	B6	82	4C	C8	FB	2C	D3	16	01	3C	AC	92	5C	Hã.¶.LEÜ.Ó..<~\
AE30h:	DB	AD	4A	02	59	1C	FE	13	AB	02	5B	71	75	6A	4D	BE	Û-J.Y.p.«.[qujM%
AE40h:	55	AB	00	41	EE	AD	58	A2	D3	7B	A1	26	D3	DF	F0	AD	U«.Aí-xc0{;&0Bã-
AE50h:	41	2D	20	1B	FE	14	54	1B	E5	09	65	A6	D7	E4	70	A4	A- .p.T.ã.e} ªãp
AE60h:	FF	D9	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D	49	48	yü&PNG.....IH
AE70h:	44	52	00	00	01	28	00	00	02	34	08	06	00	00	00	AE	DR...(...4.....@
AE80h:	FB	B4	64	00	00	0C	25	69	43	43	50	49	43	43	20	50	ù'd...%iCCPICC P
AE90h:	72	6F	66	69	6C	65	00	00	48	89	95	97	07	54	53	49	rofile..H«~.TSI
AEA0h:	17	C7	E7	95	54	12	5A	20	02	52	42	6F	A2	14	E9	52	.Çç•T.Z .RBoc.ér
AEB0h:	43	8B	54	A9	82	8D	90	04	12	4A	0C	09	41	C5	8E	2C	C«T@,....J..AAž,
AEC0h:	2A	B0	16	54	54	B0	A2	AB	22	B6	B5	00	B2	D8	B0	97	*°.TT°c«"¶µ.ª0°-
AED0h:	45	B1	F7	45	11	14	65	5D	2C	D8	50	F9	26	09	A0	EB	E±±E..e],ØPÙ&. è
AEE0h:	7E	E5	7C	F7	9C	79	EF	77	EE	DC	B9	F3	BF	EF	CD	9B	~ã ±œyiwíÜ'ó¿iÍ»
AEF0h:	F3	06	00	8D	18	AE	44	92	8D	6A	02	90	23	CE	93	C6	ó....@D'.j..#i"Æ
AF00h:	86	06	B2	C6	27	A7	B0	48	8F	01	02	E8	80	09	74	80	t.ªÆ'šªH...è€t€
AF10h:	03	97	27	93	04	C4	C4	44	00	68	83	F7	BF	DB	BB	9B	.-" .AAD.hf±¿Ü»
AF20h:	30	1A	DA	35	07	45	AE	7F	F6	FF	57	D3	E2	0B	64	3C	0.ÚS.E@.oyW0ã.d<
AF30h:	00	90	18	C8	69	7C	19	2F	07	F2	41	00	70	37	9E	44	...Èi ./..òA.p7žD
AF40h:	9A	07	00	A1	1B	FA	CD	A7	E5	49	20	13	A1	4A	A0	23	š..;úÍšãI .;j #
AF50h:	85	02	21	5B	28	38	43	C5	1E	0A	4E	53	71	84	32	26![(8CÁ..NSq,2&
AF60h:	3E	96	0D	39	15	00	32	8D	CB	95	66	00	A0	AE	D0	C5	>- .9..2.É•f. @ĐÄ
AF70h:	CA	E7	65	C0	3C	EA	65	90	1D	C5	7C	91	18	72	13	64	ÊçèÀ«èe..A 'r.d
AF80h:	5F	9E	90	CB	87	FC	19	F2	88	9C	9C	A9	90	35	6C	20	ž.É±ü.óªœ@.51
AF90h:	DB	A4	7D	97	27	E3	6F	39	D8	86	72	72	B9	19	43	AC	Ü» .ã90Írrr _C
AFA0h:	AA	45	69	E4	20	91	4C	92	CD	9D	F1	7F	3E	8E	FE	6D	«Tã T«CÍEš2VÍr

复制出来另存位png图片

```

0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
|OE0h: 00 A1 1B FA CD A7 E5 49 20 13 A1 4A A0 23 85 02 .j.úÍ$ãI .jJ #...
|OF0h: 21 5B 28 38 43 C5 1E 0A 4E 53 71 84 32 26 3E 96 ![(8CÁ..NSq.,2&>-
|100h: 0D 39 15 00 32 8D CB 95 66 00 A0 AE D0 C5 CA E7 .9..2.É+f. @ÐÁĒç
|110h: 65 C0 3C EA 65 90 1D C5 7C 91 18 72 13 64 5F 9E eA<ée.Á|'.r.d_ž
|120h: 90 CB 87 FC 19 F2 88 9C 9C A9 90 35 6C 20 DB A4 .E±ú.ò`œ@.5l Ūñ
|130h: 7D 97 27 E3 6F 39 D3 86 72 72 B9 19 43 AC AA 45 }-`áo90ttrr'.C-ªE
|140h: 69 E4 20 91 4C 92 CD 9D F1 7F 3E 8E FF 6D 39 D9 iä 'L'Í.ñ.>žym9U
|150h: F2 C1 39 CC 61 A3 09 A5 61 B1 8A 9A 15 CF 2D 6B óA9Iaē.ŷa±5S.I-k
|160h: 6A B8 82 69 90 CF 89 D3 A2 A2 21 6B 43 BE 2E E2 j. .i.İ%Ócc!kC%ã
|170h: 2B E3 15 DC 29 94 87 25 0C C4 7F E0 C9 D8 F0 99 +ã.Ū)`%±.Ä.àÉ0ð™
|180h: C1 F7 0C 50 1A 9F 1B 14 0E D9 10 B2 99 3C 2B 21 Á÷.P.Ÿ...Ū.²™<+!
|190h: 60 80 7D B9 52 E5 58 18 8F A6 14 08 E3 93 54 F9 `€)'RãX...|..ã"Tu
|1A0h: 51 B1 74 6A EC 40 7E B4 40 9C 1D 15 31 90 A7 4C Q±tji@~'œ...1.šL
|1B0h: 28 E0 0C 72 B5 40 16 1C 37 18 93 2E 0A E1 40 86 (à.rµ@..7."..â@f
|1C0h: EF 10 6D 10 E5 71 E2 07 72 9E CB 17 25 46 41 56 i.m.âqâ.ržĒ.%FAV
|1D0h: 87 7C 5F 96 15 17 3E 30 F6 79 81 90 1D 35 34 97 †|_...>0oy...54-
|1E0h: 3C 56 A1 19 BE 73 0C E4 C8 06 6B C1 2C D2 A5 21 <Vj.‰s.ãĒ.kĀ.Ōŷ!
|1F0h: B1 AA 78 CC 4D 28 E2 44 0D F8 23 F2 84 F1 61 AA ±ªXİM(ãD.ø#ò.ñªª
|200h: B1 D8 64 1E 57 A9 41 0F 72 A6 40 36 3E 62 50 0F ±0d.W@A.r!@6>bP.
|210h: 5F 10 14 AC D2 83 15 0A C4 09 03 3A B1 72 49 5E _..-Ōf..A...±rI^
|220h: 60 EC 40 FC 56 49 76 CC 40 3C D6 24 C8 0E 55 F8 `i@üVivİ@<Ō$Ē.Uø
|230h: CD 20 B7 C8 F2 E3 06 C7 F6 E4 C1 C5 A6 AA 05 07 Í .Éoã.ÇoaĀĀ!ª..
|240h: 99 DC B1 31 AA 79 71 1D 49 5E 4C BC 4A 1B CE 02 ™Ū±1ªyq.I^L%J.İ.
|250h: 11 80 0D 82 00 0B C8 61 4B 03 53 41 26 10 B5 74 .€. . .EaK.SA&.pt
|260h: D7 77 83 C1 9E 10 C0 05 52 90 01 04 C0 61 C0 33 *wfĀž.Ā.R...ĀaA3
|270h: 38 22 49 D9 23 86 D7 38 50 00 FE 84 24 00 B2 A1 8"İU#t×8P.p.,$.²;
|280h: 71 81 CA 5E 01 C8 87 FE 2F 43 5E D5 D5 01 A4 2B q.Ē.Ē.Ē±b/C^ŌŌ.ª+
|290h: 7B F3 95 23 B2 40 27 E4 1C DC 00 F7 C5 BD F1 08 {ó+ª²@'ã.Ū.÷Ā%ñ.
|2A0h: 78 F5 87 CD 19 F7 C0 3D 07 C7 B1 34 06 67 25 06 x0±İ.÷Ā=.Ç±4.g%.
|2B0h: 13 83 88 61 C4 10 A2 ED 14 51 A1 F4 87 BC 2C C0 .f`aĀ.Cí.Q;ó±¼.Ā
|2C0h: 83 15 64 C3 26 05 E1 F0 2E 80 55 29 34 88 07 B5 f.dĀ&.áð.€U)4".µ
|2D0h: 7F CB 43 E8 24 B4 12 1E 13 6E 10 DA 08 77 40 22 .ĒCés'. . .n.Ū.we"
|2E0h: 78 02 E3 44 FF A8 F0 5B 36 D1 90 2F 12 B4 C1 AC x.ãDy`ð[6Ñ./.'Ā-
|2F0h: 21 03 D5 A5 7D 5F 1D 6E 05 55 BB E2 81 B8 0F D4 !.Ōŷ}_.n.U»ã..Ō
|300h: 0F B5 E3 4C DC 00 38 E0 A3 61 25 01 B8 1F AC CD .µãLŪ.8àEa%...-İ
|310h: 15 7A BF 3D B5 7F A7 5D 3E A8 9A E2 48 41 29 C3 .zç=µ.š] >`šĀHA)Ā
|320h: 28 FE 14 9B 1F E3 D4 ED D4 5D 87 C6 28 6A FB 5E (p.>.ãŌiŌ]±Ē(jú^
|330h: A7 4A 57 DA 50 25 EC A1 9E 1F 67 63 7F 57 1B 1F $JWŪP%i;ž.gc.W..
|340h: DE C3 7F 8C C4 16 61 07 B0 B3 D8 09 EC 3C D6 84 bĀ.ĒĀ.a.º³0.i<Ō..

```

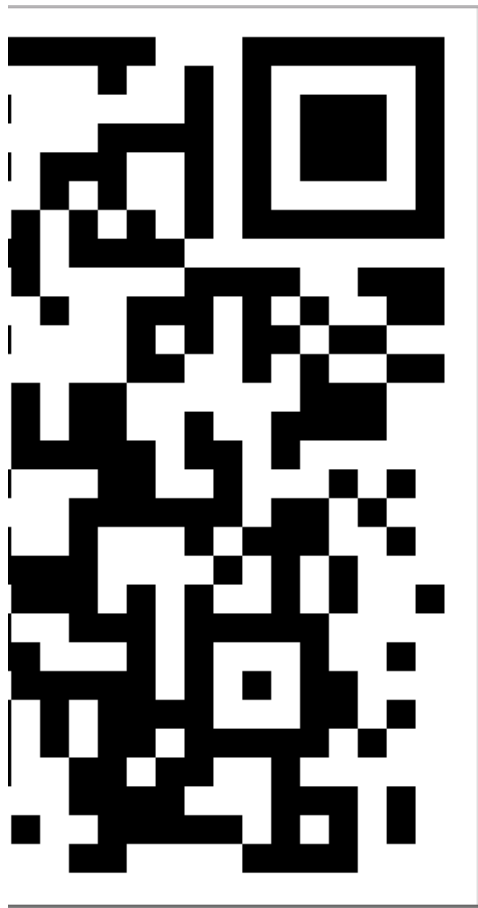
展板结果 - PNG.bt

名称	值	开始	大小	颜色	注释
> struct PNG_SIGNATURE sig		0h	8h	Fg: Bg:	
> struct PNG_CHUNK chunk[0]	IHDR (Critical, Pu...	8h	19h	Fg: Bg:	
> struct PNG_CHUNK chunk[1]	iCCP (Ancillary, P...	21h	C31h	Fg: Bg:	
> struct PNG_CHUNK chunk[2]	pHYs (Ancillary, P...	C52h	15h	Fg: Bg:	
> struct PNG_CHUNK chunk[3]	iTXt (Ancillary, Pu...	C67h	1A9h	Fg: Bg:	

CSDN @wangjin7356

版权声明

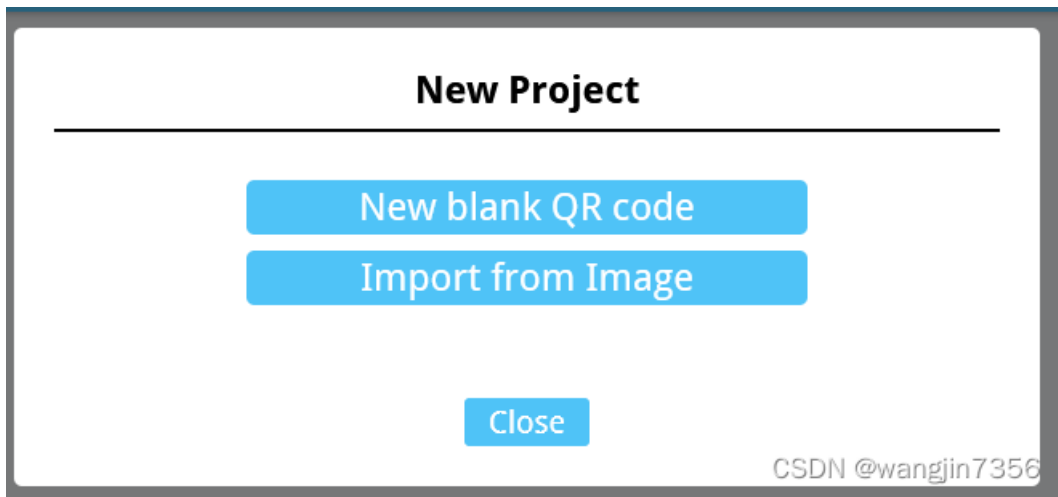
确实是半张二维码



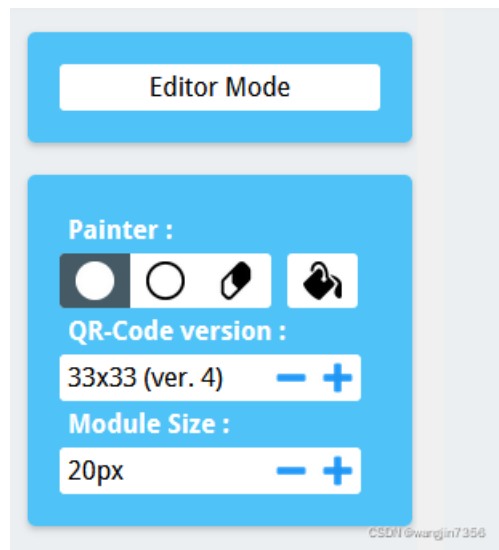
半张如何处理？参考joker-yan的博客，可以在线补全，打开网站试试



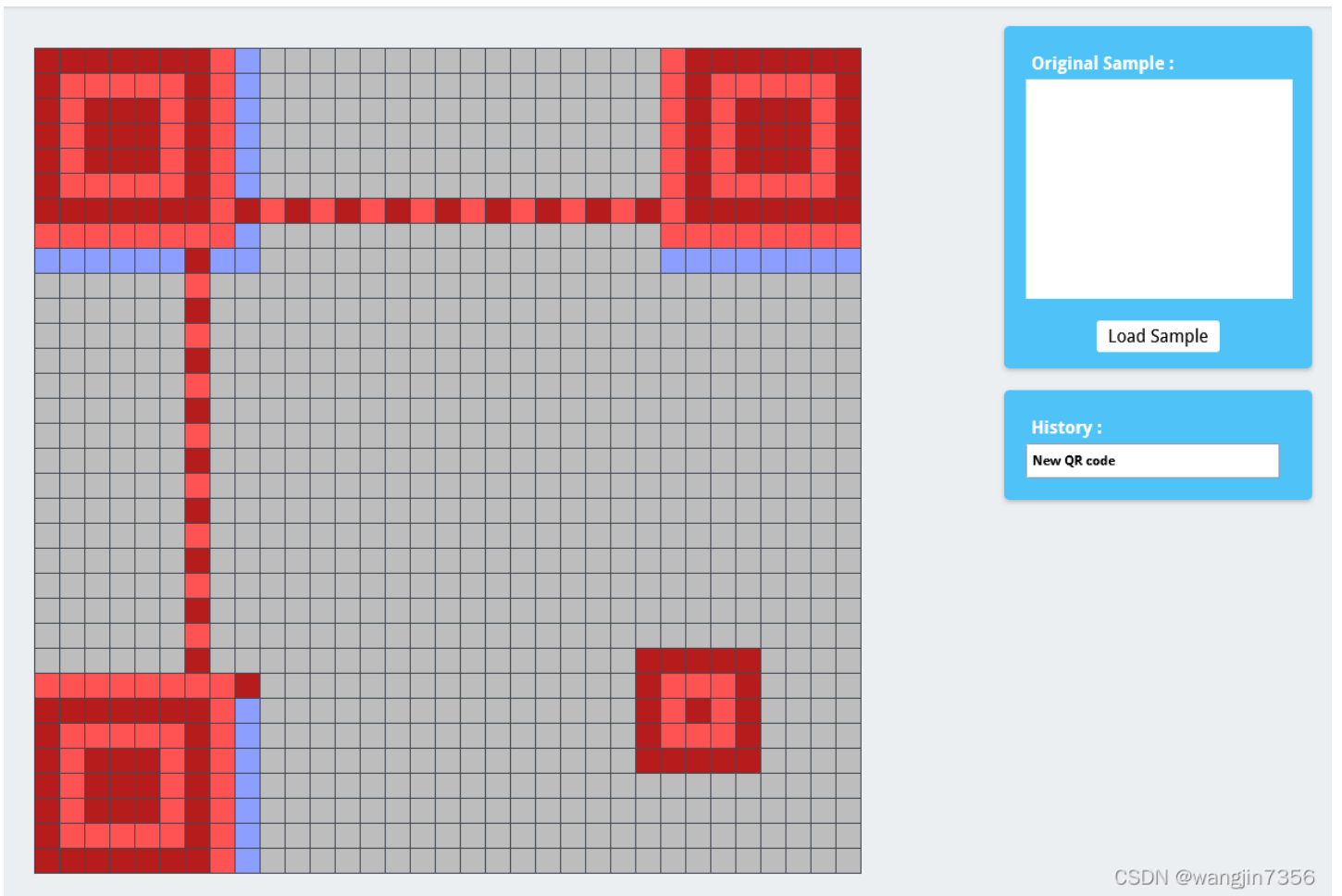
选择“New Project”



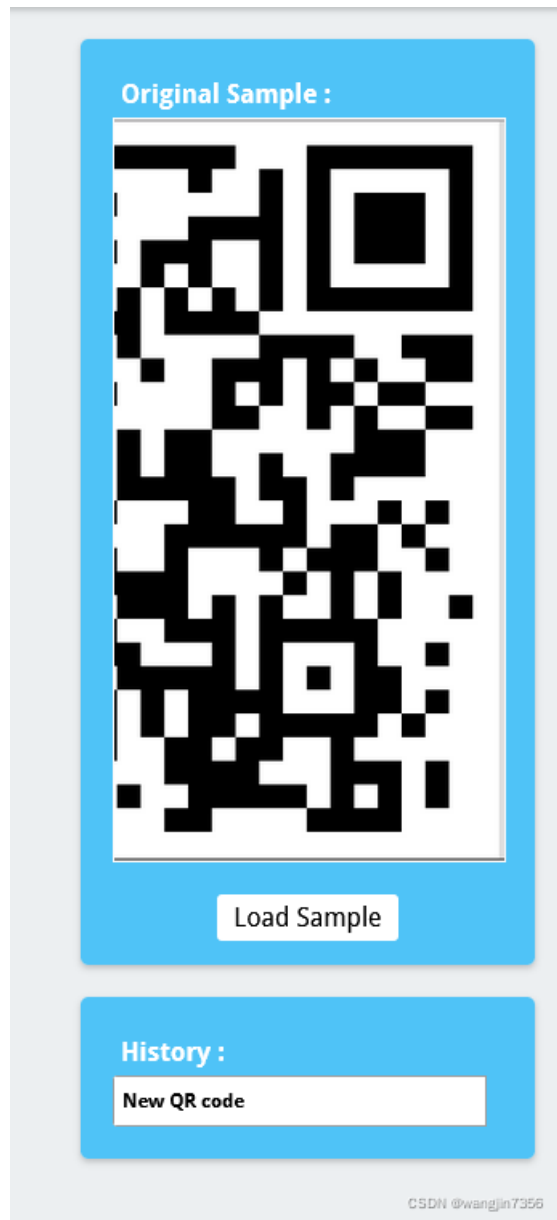
选择“New blank QR code”，选择合适的比例即可



效果如下



点击右侧“Load Sample”，加载二维码图片



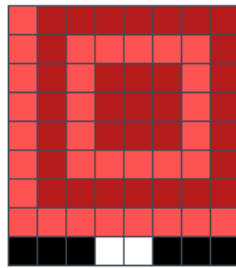
然后再左边方块位置用黑白填补，这步要有耐心。先用白色填满左半边区域，再用黑色慢慢的填。注意深红色方块也代表黑色，回字文周围的浅红色代表白色。补完后：



点击右上角回字文下边的浅蓝色的方块，淡蓝色方块中间的两块应该是白色，如图选择，然后保存

Format Info Pattern

Top Right ▾



Error Correction Level:

L M Q **H**

Mask Pattern :

0 1 **2** 3 4 5 6 7

Save

Cancel

CSDN @wangjin7356

点击菜单上的“Tools“

Tools List

Extract QR Information

Force decode and get information about the current QR code as much as possible

Reed-Solomon Decoder

Errors and Erasures correction by decoding Reed-Solomon blocks

Brute-force Format Info Pattern

Try all possibilities of Format Info Pattern when decoding

Data Masking

Simulate data masking (XOR) with Mask pattern

Padding Bits Recovery

Recover missing bits by placing terminator and padding bits

Data Sequence Analysis (*Experimental*)

Analyze data sequence of QR code

Close

CSDN @wangjin7356

选"Extract QR Information"

The screenshot displays the QRazyBox web application interface. The top navigation bar includes the QRazyBox logo and menu items: New, Load, Save, Tools, Help, and About. On the left sidebar, there are sections for 'Error Correction log' and 'Decoding Error', both with 'Show' buttons, and a 'Back to editor' button. The main content area shows the results of the 'Extract QR Information' tool. The results include: QR version: 3 (29x29), Error correction level: H, Mask pattern: 2, and Number of missing bytes (erasures): 32 bytes (45.71%). It also displays 'Data blocks' as a list of binary strings, 'Final data bits' as a long binary string, and 'Decoded data: Flag{OQWIC_4DS1A_S034S}'. The 'Final Decoded string' is highlighted in blue and matches the decoded data.

CSDN @wangjin7356

解码得到flag

Flag{OQWIC_4DS1A_S034S}

总结

1.知识点: png图片提取; 二维码补全



创作打卡挑战赛

[赢取流量/现金/CSDN周边激励大奖](#)