BUUCTF-Misc-[BJDCTF2020]纳尼

Dexret 于 2022-02-17 17:23:42 发布 2764 收藏

下载该文件，发现里面只有一个gif文件以及一个txt文件

其他gif文件无法打开，显示文件损坏，打开另一个txt文件

咦！这个文件怎么打不开?

CSDN @Dexret

发现没什么可以利用的地方

通过winhex去分析该gif文件，发现该文件虽然问gif文件，但是并没有gif的文件头

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	ANSI ASCII
00000000	39	61	80	04	88	02	F7	00	00	02	02	02	0A	01	02	00	09	01	01	02	0B	0A	02	0B	02	0A	09	09	08	0A	9a€ ˆ ÷
0000001E	11	00	00	12	00	0B	11	08	03	02	02	12	0A	01	13	01	02	1B	02	09	17	2E	06	00	34	01	02	3A	01	01	4 .
0000003C	3C	00	0B	38	0F	13	01	02	2C	00	0D	23	01	02	33	08	00	33	00	09	33	01	01	3C	08	02	3C	45	00	0D	< 8 , # 3 3 3 < <E
0000005A	47	01	03	5D	02	02	59	05	05	4C	12	04	64	01	01	6C	00	01	62	02	0A	6E	00	0D	67	08	02	71	00	0D	G] Y L d l b n g q
00000078	75	00	0D	7E	43	1B	02	03	42	02	04	4A	06	04	46	03	01	59	01	02	63	02	00	6C	0B	01	66	05	04	75	u ~C B J F Y c l f u
00000096	04	34	7E	00	67	5D	64	65	46	8C	35	02	8C	3C	01	88	3A	09	93	35	00	94	3B	02	9A	39	00	9F	36	09	4~ g]deF<5 <<· ^: "5 "; š9 Ÿ6
000000B4	8A	41	08	B5	5F	00	9E	6C	00	AD	65	03	AB	6A	00	AE	67	0A	B4	65	01	BC	66	02	B4	69	01	BB	6A	02	ŠA µ_ žl -e «j ®g ´e ¼f ´i »j
000000D2	B7	67	0B	B2	68	15	B6	71	0C	B2	5F	2B	B8	67	3A	C4	64	02	C8	62	00	C0	60	14	DE	8E	2B	CF	8D	36	·g ²h ¶q ²_+,g:Äd Èb À` ÞŽ+Ï 6
000000F0	DB	8C	3A	D6	92	3D	DA	92	35	E4	8D	2A	E5	95	3A	DA	8F	45	DC	92	45	D7	93	4A	E1	93	41	FC	B4	5B	ÛŒ:Ö'=Ú'5ä *å•:Ú EÜ'E×"Já"Aü´[
0000010E	FA	B8	59	FF	AE	65	FF	AE	6C	EC	BE	69	ED	B6	66	FD	B4	63	FE	B8	63	FD	B4	6A	FF	B9	6A	FE	B6	73	ú¸Yÿ®eÿ®lì¾ïí¶fý´cþ¸cý´jÿ¹jþ¶s
0000012C	EA	B5	7F	EA	C2	7A	01	3B	8A	01	38	85	01	3D	92	02	3A	9C	05	37	96	00	41	8F	00	40	90	0C	5B	9B	êµ êÂz ;Š 8… =' :œ 7- A @ [>
0000014A	00	62	AD	05	68	AC	01	65	B3	01	6B	B4	01	64	BB	01	6A	BC	09	66	B8	13	67	AD	04	69	C6	41	90	8A	b- h¬ e³ k´ d» j¼ f, g- iÆA Š
00000168	3A	87	CC	33	93	CF	35	8E	DC	3C	8D	DD	3A	8B	D4	3B	92	DA	33	92	D5	2F	94	DC	3B	8C	E1	36	8B	E6	:‡Ì3"Ï5ŽÜ< Ý:<Ô;´Ó/"Ü;<á6<æ
00000186	3A	91	E5	47	8B	D6	42	92	D7	47	8C	E5	5D	B4	FF	5B	B7	FA	63	B4	FE	6A	B4	FF	64	BA	FD	67	BB	F5	:'åG<ÖB'×GÇå]´ÿ[·úc´þj´ÿdºÿg»õ
000001A4	74	B4	F7	72	BE	F8	6E	AE	F6	7F	DD	F7	9B	D9	B4	EF	DC	8D	FE	DB	B4	FE	D7	8B	F8	DB	88	FD	D4	95	t´÷r¾øn®ö Ý÷›Ù´ïÜ þÛ´þ×‹øÛˆýÔ•
000001C2	FD	DB	93	F7	DA	98	F8	E3	8B	FF	DC	A2	FD	E1	A2	FD	FD	AE	FD	FF	A3	FE	FE	B4	F6	FE	BC	FF	FE	BB	ýÛ"÷Ú˜øã‹ÿÜ¢ýá¢ýý®ýÿ£þþ´öþ¼ÿþ»
000001E0	F4	FF	B5	8E	DC	FF	8A	DA	F9	93	D6	FE	94	DB	FF	99	DA	F8	A9	DA	F6	88	E2	FB	95	E1	FF	96	E2	FB	ôÿµŽÜÿŠÚù"Öþ"Ûÿ™Úø©Úö^âû•áÿ–âû
000001FE	AF	FF	F7	AB	FE	FD	AB	F7	F7	B5	FF	F7	B6	FE	FD	BB	FE	FE	B8	FF	F7	FD	FE	C3	FB	FB	CC	FF	FE	D5	¯ÿ÷«þý«÷÷µÿ÷¶þý»þþ¸ÿ÷ýþÃûûÌÿþÕ
0000021C	FF	F5	DC	FE	FE	DB	F6	FF	D6	CB	F9	F9	D4	FE	FE	DA	FD	FD	D9	FA	FB	EF	FC	EA	FE	FD	E4	FF	F7	ED	ÿõÜþþÛö ÿÖËùùÔþþÚýýÙúûïüêþýäÿ÷í
0000023A	F5	FF	EC	FD	FD	ED	F8	F9	E5	FF	EF	FC	EF	FD	F5	E2	FD	FE	ED	FE	FE	E1	F9	F9	F4	F6	F5	FE	F6	F5	õÿìýýíøùåÿïüïýõâýþíþþáùùôöõþöõ
00000258	F5	FE	F5	FD	FD	F5	F5	F6	FC	FF	F6	FE	F5	FE	FD	FF	FF	FF	00	00	00	00	00	00	00	00	00	00	00	00	õþõýýõõöüÿöþõþýÿÿÿ
00000276	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000294	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000002B2	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000002D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000002EE	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	21	F9	04		!ù
0000030C	00	32	00	00	00	21	FF	0B	4E	45	54	53	43	41	50	45	32	2E	30	03	01	00	00	00	2C	00	00	00	80		2 !ÿ NETSCAPE2.0 , €
0000032A	04	88	02	00	08	FE	00	95	09	1C	48	B0	A0	C1	83	08	13	2A	5C	C8	B0	A1	C3	87	10	23	4A	9C	48	B1	ˆ þ • H° Áƒ *\È°¡Ã‡ #J>œH‡
00000348	A2	C5	8B	18	33	6A	DC	C8	B1	A3	C7	8F	20	43	8A	1C	49	B2	A4	C9	93	28	53	AA	5C	C9	B2	A5	CB	97	¢Å‹ 3jÜÈ±Ç CŠ I²¤É"(S³ª\É²¥Ë—
00000366	30	63	CA	9C	49	B3	A6	CD	9B	38	73	EA	DC	C9	B3	A7	CF	9F	40	83	0A	1D	4A	B4	A8	D1	A3	48	93	2A	0cÊœI³¦Í›8sêÜÉ³§ÏŸ@ƒ J´¨Ñ£H"*
00000384	5D	CA	B4	A9	D3	A7	50	A3	4A	9D	4A	B5	AA	D5	AB	58	B3	6A	DD	CA	B5	AB	D7	AF	60	C3	8A	1D	4B	B6	]Ê´©Ó§P£ JªÕ«X³jÝÊµ«×¯`Ã‹ K¶
000003A2	AC	D9	B3	68	D3	AA	5D	CB	B6	AD	DB	B7	70	E3	CA	9D	4B	B7	AE	DD	BB	78	F3	EA	DD	CB	B7	AF	DF	BF	¬Ù³hÓª]˶Û·pãÊ K·®Ý»xóêÝË·¯ß¿
000003C0	80	03	0B	1E	4C	B8	B0	E1	C3	88	13	2B	5E	CC	B8	B1	E3	C7	90	23	4B	9E	4C	B9	B2	E5	CB	98	33	6B	€ L¸°áÃˆ +^Ì¸±ãÇ #KžL¹²åË˜3k
000003DE	DE	CC	B9	B3	E7	CF	A0	43	8B	1E	4D	BA	B4	E9	D3	A8	53	AB	5E	CD	BA	B5	EB	D7	B0	63	CB	9E	4D	BB	ÞÌ¹³çÏ C‹ Mº´éÓ¨S«^Íºµë×°cË žM»
000003FC	B6	ED	DB	B8	73	EB	DE	CD	BB	B7	EF	DF	C0	83	0B	1F	4E	BC	B8	F1	E3	C8	93	2B	5F	CE	BC	B9	F3	E7	¶íÛ¸sëÞÍ»·ïßÀƒ N¼¸ñãÈ"+_Î¼¹óç
0000041A	D0	A3	4B	9F	4E	BD	BA	F5	EB	D8	B3	6B	DF	CE	BD	BB	F7	EF	E0	C3	FE	8B	1F	4F	BE	BC	F9	F3	E8	D3	Ð£KŸN½ºõëØ³kßÎ½»÷ïàÃþ‹ O¾¼ùóèÓ
00000438	AB	5F	CF	BE	BD	FB	F7	F0	E3	CB	9F	4F	BF	BE	FD	FB	F8	F3	EB	DF	CF	BF	BF	FF	00	06	28	E0	80		«_Ï¾½û÷ðãËŸO¿¾ýûøóëßÏ¿¿ÿ (à€
00000456	04	16	68	E0	81	08	26	A8	E0	82	0C	36	E8	E0	83	10	46	28	E1	84	14	56	68	E1	85	18	66	A8	E1	86	hà &¨à, 6èà ƒ F(á„ Vhá… f˜á†
00000474	1C	76	E8	E1	87	20	86	28	E2	88	24	96	68	E2	89	28	A6	A8	E2	8A	2C	B6	E8	E2	8B	30	C6	28	E3	8C	vèá‡ †(âˆ$–hâ‰(¦¨âŠ,¶èâ‹0Æ(ãŒ
00000492	34	D6	68	E3	8D	38	E6	A8	E3	8E	3C	F6	E8	E3	8F	40	06	29	E4	90	44	16	69	E4	91	48	26	A9	E4	92	4Öhã8æ¨ãŽ<öèã @)ä D iä'H&©ä'
000004B0	4C	36	E9	E4	93	50	46	29	E5	94	54	56	69	E5	95	58	66	A9	E5	96	5C	76	E9	E5	97	60	86	29	E6	98	L6éä"PF)å"TViå•Xf©å–\véå—`†)æ˜
000004CE	64	96	69	E6	99	68	A6	A9	E6	9A	6C	B6	E9	E6	9B	70	C6	29	E7	9C	74	D6	69	E7	9D	78	E6	A9	E7	9E	d–iæ™h¦©æšl¶éæ›pÆ)çœtÖiç x愩çž
000004EC	7C	F6	E9	E7	9F	80	06	2A	E8	A0	84	16	6A	E8	A1	88	26	AA	E8	A2	8C	36	EA	E8	A3	90	46	2A	E9	A4	|öéçŸ€ *è ¡, jè¡ˆ&ª裌6êè£ F*é¤
0000050A	94	56	6A	E9	A5	98	66	AA	E9	A6	9C	76	EA	E9	A7	A0	86	2A	EA	A8	A4	96	6A	EA	A9	A8	A6	AA	EA	AA	"Vjé¥˜fªé¦œvêé§ †*ê¨¤–jꩨ¦ªêª
00000528	AC	B6	EA	EA	AB	FE	B0	C6	2A	EB	AC	B4	D6	6A	EB	AD	B8	E6	AA	EB	AE	BC	F6	EA	EB	AF	C0	06	2B	EC	¬¶ê�þ°Æ*ë¬´Öjë¸æªë®¼öêë¯À +ì
00000546	B0	C4	16	6B	EC	B1	C8	26	AB	EC	B2	CC	36	EB	EC	B3	D0	46	2B	ED	B4	D4	56	6B	ED	B5	D8	66	AB	ED	°Ä kì±È&«ì²Ì6ëì³ÐF+í´ÔVkíµØf«í
00000564	B6	DC	76	EB	ED	B7	E0	86	2B	EE	B8	E4	96	6B	EE	B9	E8	A6	AB	EE	BB	F0	C6	2B	EF	¶Üvëí·à†+î¸ä–kî¹è¦«î»ðÆ+ï
00000582	BC	F4	D6	6B	EF	BD	F8	E6	AB	EF	BE	DF	26	63	0C	32	02	19	23	50	31	CA	10	93	8C	32	C6	10	7C	B0	¼ôÖkï½øæ«ï¾ß&c 2 #P1Ê "Œ2Æ |°
000005A0	32	C7	08	1C	B0	32	C8	1C	53	70	32	C5	20	93	F0	40	C6	08	0C	8C	31	C9	00	2C	D0	C2	CA	1C	9C	31	2Ç °2È Sp2Å "ð@Æ Œ1É,ÐÂÊ œ1

在该winhex里添加gif的文件头

```
47 49 46 38
```

添加成功后，再去打开该gif文件，发现为一段字母

Q1RGe3d

通过ps对其进行帧数分析

得到一串字母

Q1RGe3dhbmdfYmFvX3FpYW5nX2lzX3NhZ0=

从该字母格式判断为base64加密

利用小葵转换工具对其进行解密

得到该flag值

CTF{wang_bao_qiang_is_sad}

修改CTF为flag即为该题的flag

flag{wang_bao_qiang_is_sad}