20220209-CTF-MISC-BUUCTF-修改图片宽高--ARCHPR工具的使用



 qq_51550750
 □
 已于 2022-02-09 15:08:04 修改
 ○
 566 % 收藏 1

 分类专栏:
 CTF刷题 文章标签:
 ctf buuctf misc

 于 2022-02-09 15:06:43 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/qq_51550750/article/details/122832648
 版权



CTF刷题 专栏收录该内容

50 篇文章 1 订阅 订阅专栏

CTF-MISC-BUUCTF-大白



看不到图? 是不是屏幕太小了注意:得到的 flag 请包上 flag{} 提交

... 379140b0-c...

Flag



CSDN @qq_51550750

下载附件:

379140b0-c2aa-4aa6-b372-031beb2007f0.zip

解压,得到一张图片:





已经损坏。

[kali⊛kal] [\$ binwalk ∠	i)-[∼] home/kali/Deskto	p/379140b0-c2aa-4aa6-b372-031beb2007f0.zip	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 size: 150560	0×0 , name: dabai.pn	Zip archive data, at least v2.0 to extract, compressed size: 149931, uncom g	pressed
150061	0×24A2D	End of Zip archive, footer length: 22	CSDN @gg 51550750

(kali⊛kal : ∮ binwalk <u>/</u>	i)-[∼] home/kali/Deskto	p/dabai.png	
DECIMAL	HEXADECIMAL	DESCRIPTION	
0 91	0×0 0×5B	PNG image, 679 x 256, 8-bit/color RGBA, m Zlib compressed data, compressed	non-interlaced CSDN @qq_51550750



明显是图片高度被修改了,导致图片只显示了一半 菜单栏选择Analyze-》File Format--> 查看图片数据



File format report

File: dabai.png Read 24c20 bytes	
Chunk: Critical – necessary for display of image MUST BE recognized to proceed Public Unsafe to copy unless known to software Hex:	
49484452 Ascii:	
IHDR	
Data length = 13 bytes	
CRC = 6d7c7135	
Calculated CRC = 8e14dfcf	
Width: 2a7 (679)	
Height: 100 (256)	
Bit Depth: 8	
OK CSDN @qq_51550750	5

为了修改图片的高度,结合上面得到的,用010editor打开dabai.png,然后找到值,将高度修改为两倍100—》1000:

File Form	nat Analysis	aesum		ukankan.com	Ċ		(↓
File form	nat report						Ŭ
File: dabai.png Read 24c20 bytes			👒 /Users/apple/Down		常用十六进制照表代码查询 石	E线颜色选择色查询对照表 拶	探索 300,000 7章-C
Chunk:		i 🎒 🖿 🚰 i 🏷 📭 🛙	🗄 ର ଜା 🍗 🏷 🤌	🗅 🔶 🛴 🧾 Hex 📰	M 🔢 📐 I 🔜 🔯 🚧	📠 🕺 🔏 ->>> 💷 -	
Critical - necessary for disp	lay of Startup daba	i.png x			$\langle \rangle \bigtriangledown \mathbf{x} \bullet$	Workspace	
recognized to proceed				1567894BCDEE		The Deth	
Public	0000h: 89 50 4E 47		0D 49 48 44 52 SPNG	IHDR	「「「「「「」」		
Unsafe to copy unless know	/n to s 0010be 00 00 02 A	00 00 01 00 08 06 00	00 00 6D 7C 71§	m q	Op 🦻 🔁	en Files	
Hex:	0020h: 35 00 00 00	01 73 52 47 42 00 AE	CE 1C E9 00 00 5	.sRGB.®Î.é		abal.png /Users/nioads/	
49484452	0030h: 00 04 67 41	4D 41 00 00 B1 8F 0B	FC 61 05 00 00gA	MA±üa			
Ascii:	0040n: 00 09 70 48	59 73 00 00 0E C4 00	00 0E C4 01 95pH	YSAA.•	7	17png /Users/nloads/	
IHDR	0060h: A0 45 57 59	A FE FE FE RE 4E 9B DE	93 4C 7A OF 84 ¥WY	.y≢IDATX^I/2. îÿî¾Ω₃Þ"Iz	燥 Bo	okiles	
Data length = 13 bytes	0070h; 24 24 60 00	04 A5 2B 20 45 10 10	BB 88 8A A8 57 \$\$`.	.¥+ E»^Š"W	· · · · · · · · · · · · · · · · · · ·		
CRC = 60/C/135	0020h: BD FC EF BD	7A F5 5A AE 7A BD 5E	CB BD 2A 62 05 ½üï½	zõZ®z½^˽*b.			
W_{idth} $2_{2}7 (670)$	0090h: 04 69 52 04	E9 01 42 48 48 42 7A	EF 7D 52 A6 CF .iR.	é.BHHBzï}R¦Ï			
Hoight: 100 (256)	00A0h: 9C 7E 76 FE	D 3F BF F7 DB EF 39 6B	76 F6 4C 26 C9 œ~vý	?¿÷Uï9kvöL&E			
Bit Denth: X	00C0h: 15 2C 47 8	CE 59 78 F5 DE 9E 6F	70 68 AD AF DU L23{ 25 14 04 30 00 6Ž	$P_{0} = \frac{1}{2}$			
	00D0h: DF 63 6F F	A5 53 C0 93 8D A7 D3	E9 F4 54 66 C5 Pcov	¥SÀ".§ÓéôTfÅ			
	OK 00E0h: 62 D1 E5 34	4 BC 34 0D AD 56 CB 1A	8D 86 35 9B 4D bÑå4	44Vˆ5>M			
	00F0h: 17 B3 B3 B3	3 36 37 37 E7 72 98 21	70 87 DC 6E B7 .333	577çr~!p‡Ün∙			
	0100h: 3D FC 90 01	E1 11 0F 61 22 CA E5	B2 8B 4A A5 62 =ü	áa"Êå² ‹J¥b	- <u>3</u> 33		
	0110h: A5 52 C9 D5	5 B5 5A CD AA D5 AA CB	88 7A BD EE 22 ¥REO	JZI*0*E`Z½I"		Workspace 🔀 🔿	
	0130h 30 88 E4 A1	DE 9D DB 7E E4 BB D9	1R 3F 39 72 10 02.0	.eφ/ε.* +4/. Σ Û~ô»Ù 29r		Inspector	
	0140h: 0E D8 3E D9	9 B4 9C 9C E6 C8 91 23	C7 41 8C 18 C2 .Ø>Ù	´œœæÈ´#CAŒ.Â		Type Value	
	0150h: FB 89 4D 64	A 9E 12 1F D4 88 7E 32	99 CA B8 1D 14 û‰Mj	žÔ^~2™Ê,	DOCT		
	0160h: 5E 6A D6 6F	OF A1 1C 1F 1F B7 6D	DB B6 D9 8E 1D ^jÖo	.¡∙mÛ¶ÙŽ.	DOSTI	ME 10:04:18	
	0170h: 3B 6C E7 CE	9D 2E 63 36 3D 3D 6D	93 93 93 2E 26 ;1çI	c6==m""".&	FILETIN	ИЕ 08/24/390	
	01001. 26 26 9C 9C	J 4E 4D 4D CD 93 53 08	21 EI 47 IC 91 &&@. D6 C9 12 64 09 Ô.1	NMMI S.!aG. E@PC r ÖÈ i	OLETIN	ИЕ	
	01A0h: F9 C8 C8 88	R 13 D4 F1 F1 61 5B BC	78 B1 9B 2D 5A éÈÈ^	. Ôááa [¼x+>-7	time_t	11/29/200	
	01B0h: B4 C8 C6 C6	5 C6 5C 3F 3A 3A EA F2	F2 E5 CB 6D D9 ÉÆÆ	E\?::êòòåËmÙ	time64	t	
	01C0h: B2 65 EE 1E	12 3B 08 FD F1 01 D2	16 E9 45 44 1A ²eî.	.;.ýñ.Ò.éED.	GUID	{474E508	
	01D0h: 30 47 0E 3F	20 DC F5 BB 0F 3B 10	E1 85 3E 47 8E 0G.?	Uõ».;.á>GŽ	Opcod	e (X86-32) mov dwor	
	01E0h: E4 21 P4 45	9 CD 91 23 47 8E 83 10	29 B1 49 D5 20 A.99	1'#GZj.)±10 \$P#7Ü :Pt b	Opeed	o (X96_64) mov dwor	
	flag 0200bi 04 05 46 4	24 02 05 CF 00 00 10	42 80 00 82 8F 01 8		Opcod	e (X80-64) mov dwor	gg_51550750

	<u> </u>											
	0	1	2	3	4	5	6	7	8	9	А	B
1:	89	50	4E	47	0D	0A	1A	0A	00	00	00	0D
1:	00	00	02	Α7	00	00	10	00	08	06	00	00
1:	35	00	00	00	01	73	52	47	42	00	AE	CE
1:	00	04	67	41	4D	41	00	00	B1	8F	0B	FC
:	00	09	70	48	59	73	00	00	0E	C4	00	00



这道题不建议大家放到Mac或者kali的环境下去做,明显图片打开不了,不能查看

CTF-MISC-BUUCTF-基础破解



基础破解

1

给你一个压缩包,你并不能获得什么,因为他是四位数字加密 的哈哈哈哈哈哈哈。。。不对==我说了什么了不得的东 西。。注意:得到的 flag 请包上 flag{} 提交



下载,解压:



Iz \\vmware-host\S	hared Folc	lers\apple\ l	Downloads\	基础破解.ra	r\						X
文件(F) 编辑(E) 查看	昏(V) 书签	(A) 工具(T)	帮助 (H)								
 	➡ ¥ 移动 删除	<mark>1</mark> 信息									
🦻 🔛 \\vmware-ho	st\Shared	Folders\app	ole\Downlo	ads\基础破	⊈.rar∖						•
名称	大小	压缩后大	修改时间	创建时间	访问时间	属性	加密	固实	注释	之前分割	之后分
tlag.txt	52	64	2015-07			A	+	-	-	-	
 洗定 1 / 1 个项目	52	52	201	5-07-14 09	:14:13				CSDI	V@qq_515	50750



20220208--CTF MISC-- BUUCTF--二维码 1--binwalk-john-(工具的 使用:分析文件/暴力破解压缩包密码)

于是我把这道题的基础破解.rar这个压缩包拖到kali的环境下:

	5 3 (~) d o d	+ Er <	🖻 Kali-Linux-2021.3-vmware-amd64		đ
😤 📰 🖻 🛛	👌	🗲 Burp Suite Community E 돈 kali@kali: ~		01:37 AM 🗖 📣 🌲	8 🔒 G
Trach			kali@kali:~	_ = ×	
TIdSIT		File Actions Edit View Help			
0					
File System					
Home	010 Editor				
	基础破解.rar				
					CSDN @aa 51550750



CSDN @qq_51550750

没办法只能尝试第二种方法: 用ARCHPR破解



得到密码是2563

打开flag.txt

flag.txt - 记事本			ζ
文件(F) 编辑(F) 格式(O) 查看(V) 帮助(H) ZmxhZ3s3MDM1NDMwMGE1MTAwYmE30DA20DgwNTY2MWI5M2E1Y30=			*
CSDN	@qq_5	155075	50 . -
ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWl5M2E1Y30= 用base64进行解码:			
Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyz			
Burp Project Intruder Repeater Window Help			
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options Oser optio	ns		
ZmxhZ3s3MDM1NDMwMGE1MTAwYmE3ODA2ODgwNTY2MWI5M2E1Y30=			

flag{70354300a5100ba78068805661b93a5c}

最终得到flag:flag{70354300a5100ba78068805661b93a5c}