【MISCshow misc30-misc5总结】

原创

 Htt9999
 □ 日子 2022-03-25 09:34:27 修改
 ● 4640 ℃ 收藏

 分类专栏:
 CTF show 文章标签:
 网络安全

 于 2022-03-23 22:20:37 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/Htt9999/article/details/123686692
 版权



CTFshow 专栏收录该内容

2篇文章 0 订阅 订阅专栏

MISCshow总结

本文章均来自于CTFshowhttps://ctf.show/challenges#misc2-21

1· 红包第一弹

打开发现全是压缩包

📴 flag.z	zip (评估版	本)												_		×
文件(F)	命令(C)	<u> </u>	收藏夹(O)	选项(N)	帮助(H)										
添加	解示到	》 试	香看		●		(i) 信息	日描病毒	日							
↑ 🚦	flag.zip\	flag - ZIP E	玉缩文件,	解包大小为	1,648,3	41 字节		1								
名称	^		大小 F	玉缩后大小	举刑		修改	र्मान	CRC32							
				TNH/H > C 3	文件夹		12100		CITCOL							
		19	.136	19.136	WinRAI	R ZIP 压缩	2020)/2/11 15:	693FD5	B5						
2.zip		18	,909	18,909	WinRA	R ZIP 压缩	2020	/2/11 15:	531E4F	83						
3.zip		18	,932	18,932	WinRA	R ZIP 压缩	. 2020	/2/11 15:	E1E9FA	6A						
4.zip		19	,082	19,082	WinRA	R ZIP 压缩	2020	/2/11 15:	3057D7	89						
5.zip		19	,093	19,093	WinRA	R ZIP 压缩	2020	/2/11 15:	0AC7F9							
📴 6.zip		19	,131	19,131	WinRA	R ZIP 压缩	. 2020	/2/11 15:	2BFED9	0F						
🚰 7.zip		19	,126	19,126	WinRA	R ZIP 压缩	2020	/2/11 15:	6446B8	5A						
🧧 8.zip		19	,165	19,165	WinRA	R ZIP 压缩	. 2020)/2/11 15:	AD3267	·						
🤷 9.zip		19	,267	19,267	WinRA	R ZIP 压缩	. 2020)/2/11 15:	8B9D06							
🌆 10.zip)	19	,491	19,491	WinRA	R ZIP 压缩	. 2020)/2/11 15:	E3C18D	4B						
🌆 11.zip)	19	,506	19,506	WinRA	R ZIP 压缩	. 2020)/2/11 15:	67064B	97						
🌆 12.zip)	19	,492	19,492	WinRA	R ZIP 压缩	. 2020)/2/11 15:	A5DC9	5						
🏰 13.zip)	18	,873	18,873	WinRA	R ZIP 压缩	. 2020)/2/11 15:	5798A8	B7						
🏰 14.zip)	17	,479	17,479	WinRA	R ZIP 压缩	2020	/2/11 15:	0611F9	E3						
🌆 15.zip)	18	,739	18,739	WinRA	R ZIP 压缩	. 2020)/2/11 15:	DC1745	FF						
🌆 16.zip)	19	,302	19,302	WinRA	R ZIP 压缩	. 2020)/2/11 15:	9F70AF	FD						
🌆 17.zip)	19	,634	19,634	WinRA	R ZIP 压缩	. 2020)/2/11 15:	A2C256	7E						
🌆 18.zip)	19	,075	19,075	WinRA	R ZIP 压缩	. 2020)/2/11 15:	6D0855							
19.zip)	18	,243	18,243	WinRA	R ZIP 压缩	. 2020)/2/11 15:	FA1B76	D4						
										总计 8	6 文件, 1,648,	341 字节		CSE	N @Hti	t9999

1.zip	(评估版本)													-	_	×
文件(F)	命令(C)	工具(S)	收藏夹(C	D) 选项(N)	帮助(H)											
<mark>读</mark> 添加	解 国	了 测试	查看		重找	向导	信息 日描病毒	日本	自解压格式	;						
1	1.zip - Z	IP 压缩文	件, 解包大	小为 19,034	字节											\sim
个 2000	1.zip - Z	IP 压缩文	件, 解包大 大小	:小为 19,034 压缩后大小	字节 类型		修改时间	CRC32			 	 	 			 ~
个 名称 ■	1.zip - Z	IP 压缩文	件, 解包大 大小	:小为 19,034 压缩后大小	字节 类型 文件夹		修改时间	CRC32			 	 	 			 ~

总计 1 文件, 19,034 字节

打开每个压缩包发现全是一张图片,用010editor打开第一张图片发现二进制的最后有一串base64的编码

 IPEON:
 32
 IF
 D0
 24
 93
 04
 48
 D3
 56
 0A
 57
 F8
 C7
 40
 BE
 F0
 2.05**.HOV.WØÇ@%d

 I9F0h:
 72
 85
 10
 08
 00
 3B
 62
 20
 61
 20
 73
 20
 65
 20
 36
 20
 r.....;b a s e 6

 IA00h:
 34
 20
 3A
 20
 69
 56
 42
 4F
 52
 77
 30
 4B
 47
 67
 6F
 41
 4
 : iVBORw0KGgoA

 IA10h:
 41
 41
 41
 42
 55
 67
 41
 41
 51
 51
 41
 AAANSUhEUgAAAQQA

 IA20h:
 41
 41
 45
 43
 41
 59
 41
 41
 41
 44
 45
 43
 45
 6F
 4B
 AAAEECAYAAADOCEoK

 IA20h:
 41
 41
 45
 51
 56
 52
 34
 58
 75
 33
 64
 AAAY3ELEQVR4Xu3d

 IA40h:
 34

由于图片比较多,直接脚本上手



![在这里插入图片描述](https://img-blog.csdnimg.cn/1a51e214aab143d78caef0f14b6ffa1f.png?x-oss-

process=Image/watermark,type_d3F5LXpibmniaQ,snadow_50,text_Q1NETIBASHR001K50Q==,size_20,color_FFFFF,t_70,g_se,x_16

直接base64解码得到flag: flag{gif_is_so_easy}

**

2·stega10

**

又是一个压缩包打开是一个图片

🏰 hear	t.zip (评估)	反本)									_		×
文件(F)	命令(C)	工具(S)	收藏夹(0)) 选项(N)	帮助(H)								
添加	解反到		香素		●		信息	(2)	日				
10×34	heart.zi	o - ZIP 压	 宿文件, 解	包大小为 41		143KB	1DvGv	1-11-11-11-11-11-11-11-11-11-11-11-11-1	/_/+				~
名称	^		大小	压缩后大小	类型		修改的	间	CRC32				
—					文件夹								
🔳 heart.	.jpg	4	1,653	41,513	JPG 文件		2020/	2/13 11:	58608E	A			
🔳 🖘 E	经选择13	7件, 41,6	53 字节							总计 1 文件, 41,653 字节	CSD	N @Htts	9999

不用想直接010editor打开看看里面到底有啥

010 Editor - C:\Users\HTT\Downloads\heart.jpg

文件(<u>F</u>)	编辑	髯(<u>E</u>)	搜	索(<u>S</u>)	视	图(<u>V</u>) 格	各式(<u>(</u>	<u>O)</u>	脚本	(<u>l</u>)	模板	(<u>L</u>)	调证	t(<u>D</u>)	Τi	具(<u>T</u>) 窗口(<u>W</u>) 帮助(<u>H</u>)
📄 🗸 🕑	- ~		.	. I	b 🕯	7 I	≽	È.	7 -	ຈ (ן ע	۶	<mark>a</mark> ₿ I	> -	→ 1		🧕 Hex 🕄 ¶ 🔢 📐
起始页	1.j	pg	h	eart.	jpg	×											
	0	1	2	3	4	5	6	7	- Š	9	Α	В	С	D	Е	F	0123456789ABCDEF
000h:	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	ÿØÿàJFIF
010h:	00	01	00	00	FF	DB	00	43	00	80	06	06	07	06	05	80	ÿÛ.C
020h:	07	07	07	09	09	80	0A	0C	14	0D	0C	0B	0B	0C	19	12	
030h:	13	0F	14	1D	1A	1F	1E	1D	1A	1C	1C	20	24	2E	27	20	\$.'
040h:	22	2C	23	1C	1C	28	37	29	2C	30	31	34	34	34	1F	27	",#(7),01444.'
050h:	39	3D	38	32	3C	2E	33	34	32	FF	DB	00	43	01	09	09	9=82<.342ÿÛ.C
060h:	09	0C	0B	0C	18	0D	0D	18	32	21	1C	21	61	48	52	30	2aHR0
070h:	63	48	4D	36	4C	79	39	33	64	33	63	75	62	47	46	75	cHM6Ly93d3cubGFu
080h:	65	6D	39	31	63	79	35	6A	62	32	30	76	61	54	6C	69	em91cy5jb20vaTli
090h:	4D	47	74	7A	5A	41	00	00	32	32	32	32	32	32	32	32	MGtzZA22222222
0A0h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	2222222222222222222
0B0h:	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	222222222222222222222222222222222222222
0C0h:	32	32	32	32	32	32	32	32	32	FF	C0	00	11	80	01	F4	222 22 22 22 29 Htt 99 89

竟然发现了一串类似于base64的编码,解码之后是个网站

Input

annoonnocybbabcabar aciibteybJbzovarttinaezzn

Output

https://www.lanzous.com/i9b0ksd

CSDN @Htt9999

打开这个蓝奏云链接,我们下载到了一个加密的压缩包



直接爆破得到密码,成功解压出来n.png,但却无法打开 用010editor发现是个倒序的,Python脚本走起





得到一个二维码![在这里插入图片描述](https://img-blog.csdnimg.cn/d4870b31ccd445739b12defd287cd759.png?x-oss-

process=image/watermark,type_d3F5LXplbmhlaQ,shadow_50,text_Q1NETiBASHR0OTk5OQ==,size_18,color_FFFFF,t_70,g_ se,x_16

```
扫码得flag:flag{我好难啊}
**
```

3-stega11

**

打开压缩包是一个图片的格式

å fla	ag.zip (评估版	反本)													_		×
文件(F) 命令(C)	工具(S)	收藏夹(O)	选项(N)	帮助(H)												
d				Ŵ	Q			8	Ę								
添	加解压到	测试	查看	删除	查找	向导	信息	扫描病毒	注释	自解压格式							
1	🜆 flag.zip	- ZIP 压缩	文件, 解包:	大小为 81,()78字节								 				~
名称	~		大小	玉缩后大小	类型		修改日	间	CRC32								
<mark>—</mark> 📄 flа	a ina	8.	1 078	77 025	文件夹		2010	/11/27 1	802001	40							
= 11a	9.169	0	1,076	11,955	JFG X1+		2019	11/2/ 1	002001	40							
										总计 1	文件, 81,078	字节			CSDI	V @Htt	9999;

Input

ÿÙMZWGCZ33GZTDCNZZG5SDIMBYGBRDEOLCGY2GIYJVHA4TONZYGA2DMM3FGMYH2ÿØÿà

Output

flag{6f1797d4080b29b64da5897780463e30}

CSDN @Htt9999

1

得到flag: flag{6f1797d4080b29b64da5897780463e30} **

4·misc4

**

下载是一个没有后缀的东西,但是看到名称明白了,应该是的rar的压缩包,直接改后缀

iar.z	ip (评估版	本)									 	 	 _	×
文件(F)	命令(C)	<u>工具(S)</u>	收藏夹(0)) 选项(N)	帮助(H)									
天 fu	解压到		西寿		●			(2)		(四日)				
1000JH	rar.zip	RAR 压缩	上 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	」 大小为 112		10.2			//+			 	 	
名称	^		大小	压缩后大小	类型		修改日	时间	CRC32					
.					文件夹									
🖻 ታሪያ	て档.doc	1	12,049	108,263	Microso	ft Word	2019	/11/6 15:	8BC7EE16					

总计 1 文件, 112,049 字节

CSDN @Htt9999

结果解压后的文档打不开,结果010editor分析得到还是一个压缩包还是改后缀

起始页	fla	g.jp	g	办2	\$文桂	ắ.do	c×										
	Ŏ	1	2	3	4	5	6	7	8	9	А	В	С	D	Е	F	<u>0</u> 123456789ABCDEF
0000h:	50	4B	03	04	14	00	00	00	00	00	23	7E	66	4F	00	00	PK#~fO
0010h:	00	00	00	00	00	00	00	00	00	00	09	00	00	00	64	6F	do
0020h:	63	50	72	6F	70	73	2F	50	4B	03	04	14	00	00	00	08	cProps/PK
0030h:	00	00	00	21	00	4F	BB	FB	E9	18	01	00	00	2B	02	00	!.0»ûé+
0040h:	00	11	00	00	00	64	6F	63	50	72	6F	70	73	2F	63	6F	docProps/co
0050h:	72	65	2E	78	6D	6C	A5	91	3D	4F	C3	30	10	86	77	24	re.xml¥'=OÃO.†w\$
0060h:	FE	43	E4	3D	71	DC	20	54	59	49	ЗA	80	3A	51	09	89	þCä=qÜ TYI:€:Q.‰
0070h:	20	10	9B	65	5F	53	8B	F8	43	B6	21	ED	BF	C7	49	DA	>e_S<øC¶!í¿ÇIÚ
0080h:	B4	88	6E	8C	E7	F7	B9	47	E7	BB	72	B5	57	5D	F2	0D	[^nŒç÷¹Gç»rµW]ò.
0090h:	CE	4B	A3	2B	44	B2	1C	25	A 0	B9	11	52	B7	15	7A	6D	ÎK£+D².% ¹.R∙.zm
00A0h:	D6	E9	12	25	3E	30	2D	58	67	34	54	E8	00	1E	AD	ΕA	Öé.%>0-Xg4Tèê
00B0h:	DB	9B	92	5B	CA	8D	83	67	67	2C	B8	20	C1	27	D1	A4	Û›'[Ê.fgg, Á'Ѥ
00C0h:	3D	E5	B6	42	BB	10	2C	C5	D8	F3	1D	28	E6	B3	48	E8	=å¶B».,ÅØó.(æ³Hè
00D0h:	18	6E	8D	53	2C	C4	D2	B5	D8	32	FE	C9	5A	C 0	8B	3C	.n.S,ÄÒµØ2þÉZÀ‹<
00E0h:	BF	C7	0A	02	13	2C	30	3C	08	53	3B	1B	D1	51	29	F8	¿Ç,O<.S;.ÑQ)ø
00F0h:	AC	B4	5F	AE	1B	05	82	63	E8	40	81	0E	1E	93	8C	E0	<u>¬´_®,cè@"Œà</u>
0100h:	33	1B	C 0	29	7F	B5	61	4C	2E	48	25	C3	C1	C2	55	F4	3.À).µaL.H%ÃÁÂUô
0110h:	14	CE	F4	DE	CB	19	EC	FB	3E	EB	8B	01	1D	E6	27	F8	.ÎôÞË.ìû>ë‹æ'ø
0120h:	7D	F3	F4	32	7E	35	95	7A	D8	15	07	54	97	82	53	EE	}óô2~5∙zØT–,Sî
0130h:	80	05	E3	EΑ	4D	89	2F	AA	F2	38	E2	F4	00	22	89	6A	€.ãêM‱/ªò8âô."‰j
0140h:	ЗA	0D	72	4A	DE	8A	87	C7	66	8D	ΕA	45	4E	96	29	C9	:.rJÞŠ‡Çf.êEN-)É
0150h:	D3	82	34	A4	A 0	C5	1D	5D	2C	3F	A2	EB	77	FF	59	A 8	Ó,4¤ Å.],?¢ëwÿY¨
0160h:	E2	D9	B6	F2	1F	C6	49	30	28	F1	9F	F3	D6	3F	50	4B	âÙ¶ò.ÆI0(ñŸóÖ?PK
0170h:	03	04	14	00	00	00	80	00	00	00	21	00	AA	ЗA	AD	A6	!.a:-
0180h:	85	04	00	00	D4	07	00	00	17	00	00	00	64	6F	63	50	ÔdocP
0190h:	72	6F	70	73	2F	74	68	75	6D	62	6E	61	69	6C	2E	6A	<pre>rops/thumbnail.j</pre>
01A0h:	70	65	67	ED	91	6B	54	8B	71	1C	C7	FF	CF	AE	CF	6A	pegí'kT‹q.ÇÿÏ®Ïj
01B0h:	A3	75	D1	C5	D4	5A	63	4B	44	13	49	28	A3	24	27	14	£uÑÅÔZcKD.I(£\$'.
01C0h:	2B	16	62	85	98	A4	88	C2	54	CA	2D	89	DC	65	C9	52	'nġ⋻Ňŗ∂ĴIJÊġġĠŔ
01D0h ·	44	F9	10	F9	4A	57	F7	48	F7	40	61	63	15	FD	74	A3	Dé é W÷H÷Lac 1+f

NAC文档.zip (评	古版本)						_	-				_	\times
文件(F) 命令(C)	[][(S) 收藏夹	(O) 选项(N)	帮助(H)										
添加 解压到			 查找 向导 	① ② 信息 扫描病毒	日本	自解压格式	;						
🔨 🚺 办公文档.	zip - ZIP 压缩文(牛, 解包大小为	1 479,404 字节										`
名称	大小	压缩后大小	类型	修改时间	CRC32								
—			文件夹										
_rels	567	251	文件夹	2019/11/6 15:									
adocProps	2,559	1,437	文件夹	2019/11/6 15:									
Documents	29,409	2,408	文件夹	2019/11/6 15:									
E Resources	445,536	103,758	文件夹	2019/11/6 15:									
Content_Type	1,013	331	XML文档	1980/1/1 0:00	543C60	6							
FixedDocSeq.f	320	160	FDSEQ 文件	1980/1/1 0:00	995F1F4	4							

🚥 🖘 已经选择 1 文件夹, 2,559 字节

CSDN @Htt9999 .

解压之后发现这么多文件,一个一个打开看看能不能发现什么,一个个翻,在Documents\1\Pages\1.fpage中发现不同

```
\times
   1.fpage.text - 记事本
文件
      编辑
                                                                    ණ
             查看
 </Glyphs>
 <Glyphs Name="a3" BidiLevel="0" Fill="#FF000000"
 FontUri = "/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
 FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="214.13"
 OriginY="83.664" UnicodeString=" " Indices="" xml:lang="en-US">
 </Glyphs>
 <Glyphs Name="a4" BidiLevel="0" Fill="#FF000000"
 FontUri = "/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
 FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="90.024"
 OriginY="99.024" UnicodeString="f" Indices="" xml:lang="en-US">
 </Glyphs>
 <Glyphs Name="a5" BidiLevel="0" Fill="#FF000000"
 FontUri="/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
 FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="93.264"
 OriginY="99.024" UnicodeString=" " Indices="" xml:lang="en-US">
 </Glyphs>
 <Glyphs Name="a6" BidiLevel="0" Fill="#FF000000"
 FontUri = "/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
 FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="90.024'
 OriginY="114.62" UnicodeString="l" Indices="" xml:lang="en-US">
 </Glyphs>
 <Glyphs Name="a7" BidiLevel="0" Fill="#FF000000"
 FontUri = "/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
 FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="92.424'
 OriginY="114.62" UnicodeString=" " Indices="" xml:lang="en-US">
 </Glyphs>
 <Glyphs Name="a8" BidiLevel="0" Fill="#FF000000"
 FontUri = "/Resources/71DC1C0E-6285-77FF-2208-3511F4077B72.odttf"
 FontRenderingEmSize="10.56" StyleSimulations="None" OriginX="90.024'
 OriginY="130.22" UnicodeString="a" Indices="" xml:lang="en-US">
 行64,列19
                            100%
                                      Windows (CRLF)
                                                        CUDN@Htt9999
```

最后得到flag:flag{xps?Oh,Go0d!}	
**	

5·misc31

解压压缩包得到好多文件,一个一个试试会怎么样

isc31.zip (评估)	版本)						_		×
文件(F) 命令(C)]	[具(S) 收藏夹(O) 选项(N)	帮助(H)						
↑ State misc31.zi	o - ZIP 压缩文件。	. 解包大小为	15.012.270 字节						
2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-	+/\	压缩后于小	**刑	修改时间	CRC32				
	X		文件夹	IS ICCU SING	ChC52				
file	33,176	23,760	文件	2020/2/14 14:	004FE0EE				
hint.txt	37	36	文本文档	2020/2/14 14:	5D9E5E9F				
💿 xiaomotuo.wav *	11,538,510	9,056 <mark>,4</mark> 79	WAV 文件	2020/2/14 16:	3942C517				
峇 送你几朵小fafa	43,248	40,918	PDF Document	2020/2/14 14:	FA25DC				
● 听歌识曲.mp3	3,397,299	3,302,992	MP3 文件	2020/2/14 14:	3AD5A6				
						总计 5 文件, 15,012,270 字节	CSD	N @Htts	9999

两个不加密,三个加密肯定就要对不加密的进行分析

打开file结果发现一串base64的代码,用base64解密没结果,想一下可能是base64的图片类型

(https://tool.jisuapi.com/base642pic.html) 在线网址

ÿØÿà;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;	$ \begin{bmatrix} M & 00 & \times & 00 & 00 & 00 & 00 & 00 & 0$	Í
$\begin{array}{c} e_{iii} & & & e_{ii} 0 B \sim YA_{iii} i i i i i i i i i i i i i i i i i$		
	™™®™:TY®®®AGGaon drasmani®#D±yra	
[™] %&'()*456789:CDEFGHIJSTUVWXYZcdefg [₩] ¢£¤¥¦§¨© ^{a23} ´µ¶·,¹ºÂÃÄÅÆÇÈÉÊÒÓÔÕÖ [™] ®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®®	hijstuvwxyz團腳醫醫醫醫醫醫醫醫醫醫醫醫醫醫醫醫 >רÙÚáâãäåæçèéêñòóôõö÷øùúÿÄ寶智醫醫	~

打开图片是一个dlddddhm

道前位置:站长	753-756同HJ 工具 > base64图片					广告 电销机房 实力	推广 Q:16687430 老A实贷	ē信QQ: 93
在线调色板	网页常用色彩	中日传统色彩	传图识色	WEB安全色	网页颜色选择器	颜色代码查询、RGB颜色值	base64图片在线转换工具	
					/hzwd4T8lQ rV3Z+q2Ciii KKKACiiigAc //1/380000 A0000AKKK 00AKKKKAP	ISW3hXR7HSIpiGkWyt44A5HQ rMAooooAKKKKACiiigAooooA JoooaKKKKACiiigAooooAKKKK AKKKACiiigAooooAKKKKACiii (KACiiigAooooAKKKKACiiigAoo ,	sA3Y7ZrpKKh04uXO1r3N44c KKKACiiigAooooAKKKKACiii ACiiigAooooA JAooooAKKKKACiiigAooooA ooAKKKKACiiigAooooAKKKK	tGk6EZtQe gAooooAK KKKACiiig ACiiigAoo



CSDN @Htt9999

直接在线解密(https://www.qqxiuzi.cn/bianma/wenbenjiami.php?s=huaduo)在线网址

☆*✿֎֎֎*✿✿֎֎֎֎֎֎֎	
加密 解密 □使用密码	
qwertyuiop	
	CSDN @Htt9999

但是我们用010editor进行对PDF查看时发现PDF有隐写



打开方式:	法 迅读PDF大师主程序 更改(C)…
位置:	C:\Users\HTT\Downloads
大小:	42.2 KB (43,248 字节)
占用空间:	44.0 KB (45,056 字节)
创建时间:	2022年3月23日,22:04:51
修改时间:	2020年2月14日, 14:25:05
访问时间:	2022年3月23日, 22:04:51
属性:	□ 只读(R) □ 隐藏(H) 高级(D)
	确定 取消 CSDN @Htt9999

使用工具 wbStego4.3open 进行pdf 解密,秘钥设置为空。

wbStego4.3open				>	<
Los gehts!					
Schritt	Aktuelle Einstellungen: Ver鋘derte Datei: 送你几朵小fafa.pdf				_
		Informati	on		×
		i	Decodierv	organg abgesc	hlossen.
Hilfe	keine Verschijteselung Klicken Sie auf Weiter, um n			ОК	
Einstellungen			« Rack	CSDN @F	fit9999

得到一串数字ENTYNSTLWNRNTKYW13287484 目前pdf中解出了:

qwertyuiop

ENTYNSTLWNRNTKYW13287484

我们用关键字解密(http://www.hiencode.com/keyword.html)

— 关键字密码 Keyword Cipher

ENTYNSTLWNRNTKYW13287484			
			4
qwertyuiop			
	加密	解 密	
CVEFVWETBVDVESFB13287484			

CSDN @Htt9999

用CVEFVWETBVDVESFB13287484进行war的解密 解出的密码,成功解出了xiaomotuo.wav文件。 使用steghide 工具进行解密,密码是xiaomotuo,解出flag: flag{du_du_du_du}**

6·misc5

**

解压过后的文件用010editor打开

-	010	Editor -	C:\l	Jsers\HTT	\Down	loads\	flag.p	ong
---	-----	----------	------	-----------	-------	--------	--------	-----

文件(<u>F</u>)	编辑	髯(<u>E</u>)	搜	索(<u>S</u>)	视	图(<u>)</u>	<u>/</u>) †	各式(<u>O)</u>	脚本	-(<u>I</u>)	模板	(<u>L</u>)	调证	t(<u>D</u>)	ΤÌ	具(<u>T)</u> 窗口(<u>₩</u>) 帮助(<u>H</u>)
🗋 🗸	- ~			.	i i	P 1	ծ		1	ຈ (ר ב	۶	<mark>a</mark> ₿ I	> -	→ 1		🧕 Hex 詫 ¶ 🔢 📐 .
起始页	fla	ig.jp	g	file	1	fla g .	png	×									
	Ŏ	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	0123456789ABCDEF
020h:	3F	00	00	00	19	74	45	58	74	53	6F	66	74	77	61	72	<pre>?tEXtSoftwar</pre>
030h:	65	00	41	64	6F	62	65	20	49	6D	61	67	65	52	65	61	e.Adob <u>e ImageRea</u>
040h:	64	79					00	00	03	20	69	54	58	74	58	4D	dyqÉe≤ iTXtXM
050h:	4C	ЗA	63	6F	6D	2E	61	64	6F	62	65	2E	78	6D	70	00	L:com.adobe.xmp.
060h:	00	00	00	00	3C	3F	78	70	61	63	6B	65	74	20	62	65	xpacket be</td
070h:	67	69	6E	3D	22	EF	BB	BF	22	20	69	64	3D	22	57	35	gin="" id="W5
080h:	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	7A	4E	54	MOMpCehiHzreSzNT
090h:	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	78	6D	70	czkc9d"?> <x:xmp< td=""></x:xmp<>
0A0h:	6D	65	74	61	20	78	6D	6C	6E	73	ЗA	78	3D	22	61	64	meta xmlns:x="ad
0B0h:	6F	62	65	ЗA	6E	73	ЗA	6D	65	74	61	2F	22	20	78	ЗA	obe:ns:meta/" x:
0C0h:	78	6D	70	74	6B	3D	22	41	64	6F	62	65	20	58	4D	50	xmptk="Adobe XMP
0D0h:	20	43	6F	72	65	20	35	2E	30	2D	63	30	36	30	20	36	Core 5.0-c060 6
0E0h:	31	2E	31	33	34	37	37	37	2C	20	32	30	31	30	2F	30	1.134777, 2010/0
0F0h:	32	2F	31	32	2D	31	37	ЗA	33	32	ЗA	30	30	20	20	20	2/12-17:32:00
100h:	20	20	20	20	20	22	3E	20	3C	72	64	66	3A	52	44	46	"> <rdf:rdf< td=""></rdf:rdf<>
110h:	20	78	6D	6C	6E	73	ЗA	72	64	66	3D	22	68	74	74	70	xmlns:rdf="http
120h:	3A	2F	2F	77	77	77	2E	77	33	2E	6F	72	67	2F	31	39	://www.w3.org/19
130h:	39	39	2F	30	32	2F	32	32	2D	72	64	66	2D	73	79	6E	99/02/22-rdf-syn
140h:	74	61	78	2D	6E	73	23	22	3E	20	3C	72	64	66	ЗA	44	tax-ns#"> <rdf:d< td=""></rdf:d<>
150h:	65	73	63	72	69	70	74	69	6F	6E	20	72	64	66	ЗA	61	escription rdf:a
160h:	62	6F	75	74	3D	22	22	20	78	6D	6C	6E	73	ЗA	78	6D	bout="" xmlns:xm
170h:	70	3D	22	68	74	74	70	ЗA	2F	2F	6E	73	2E	61	64	6F	p="http://ns.ado
180h:	62	65	2E	63	6F	6D	2F	78	61	70	2F	31	2E	30	2F	22	be.com/xap/1.0/"
190h:	20	78	6D	6C	6E	73	ЗA	78	6D	70	4D	4D	3D	22	68	74	xmlns:xmpMM="ht
1A0h:	74	70	ЗA	2F	2F	6E	73	2E	61	64	6F	62	65	2E	63	6F	tp://ns.adobe.co
1B0h	6D	2	70	61	70	2⊏	21	2⊏	20	2⊏	60	60	2	22	20	70	$m/y_{2}n/1 = 0/mm/!! y$

10011.		~ 1	, 0			21	5	~ -	50	~ 1	00	00	21	~ ~ ~	20	, 0	
1C0h:	6D	6C	6E	73	3A	73	74	52	65	66	3D	22	68	74	74	70	mlns:stRef="http
1D0h:	ЗA	2F	2F	6E	73	2E	61	64	6F	62	65	2E	63	6F	6D	2F	://ns.adobe.com/
1E0h:	78	61	70	2F	31	2E	30	2F	73	54	79	70	65	2F	52	65	xap/1.0/sType/Re
1F0h:	73	6F	75	72	63	65	52	65	66	23	22	20	78	6D	70	3A	<pre>sourceRef#" xmp:</pre>
200h:	43	72	65	61	74	6F	72	54	6F	6F	6C	3D	22	41	64	6F	CreatorTool="Ado
210h:	62	65	20	50	68	6F	74	6F	73	68	6F	70	20	43	53	35	be Photoshop CS5
220h:	20	57	69	6E	64	6F	77	73	22	20	78	6D	70	4D	4D	3A	Windows" xmpMM:
230h:	49	6E	73	74	61	6E	63	65	49	44	3D	22	78	6D	70	2E	InstanceID="xmp.
240h:	69	69	64	ЗA	34	37	44	32	42	38	30	37	34	46	38	42	iid:47D2B8074F8B
250h:	31	31	45	41	38	43	33	44	44	41	31	45	38	42	33	34	11EA8C3DDA1E8B34
260h:	41	35	32	38	22	20	78	6D	70	4D	4D	3A	44	6F	63	75	A528" xmpMM:Docu
270h:	6D	65	6E	74	49	44	3D	22	78	6D	70	2E	64	69	64	3A	<pre>mentID="xmp.did:</pre>
280h:	34	37	44	32	42	38	30	38	34	46	38	42	31	31	45	41	47D2B8084F8B11EA
290h:	38	43	33	44	44	41	31	45	38	42	33	34	41	35	32	38	8C3DDA1E8B34A528
2A0h:	22	3E	20	3C	78	6D	70	4D	4D	3A	44	65	72	69	76	65	"> <xmpmm:derive< td=""></xmpmm:derive<>
2B0h:	64	46	72	6F	6D	20	73	74	52	65	66	3A	69	6E	73	74	dFrom stRef:inst
2C0h:	61	6E	63	65	49	44	3D	22	78	6D	70	2E	69	69	64	3A	anceID="xmp.iid:
2D0h:	34	37	44	32	42	38	30	35	34	46	38	42	31	31	45	41	47D2B8054F8B11EA
2E0h:	38	43	33	44	44	41	31	45	38	42	33	34	41	35	32	38	8C3DDA1E8B34A528
2F0h:	22	20	73	74	52	65	66	ЗA	64	6F	63	75	6D	65	6E	74	" stRef:document
300h:	49	44	3D	22	78	6D	70	2E	64	69	64	3A	34	37	44	32	ID="xmp.did:47D2
310h:	42	38	30	36	34	46	38	42	31	31	45	41	38	43	33	44	B8064F8B11EA8C3D
320h:	44	41	31	45	38	42	33	34	41	35	32	38	22	2F	3E	20	DA1E8B34A528"/>
330h:	3C	2F	72	64	66	ЗA	44	65	73	63	72	69	70	74	69	6F	
340h:	6E	3E	20	3C	2F	72	64	66	3A	52	44	46	3E	20	3C	2F	n> </td
350h:	78	ЗA	78	6D	70	6D	65	74	61	3E	20	3C	3F	78	70	61	x:xmeananaahffaaaa
1360h ·	63	6R	65	74	20	65	6F	64	3D	22	72	22	3F	3F	E6	59	cket end="r"?>#Y

发现图片中有东西,使用stegsolve,在blue plane 4 发现flag



flag: flag:{so_good_you_are}

