攻防世界 Misc Ditf

原创

==Microsoft== ● 于 2022-03-05 12:41:50 发布 ● 2344 ☆ 收藏 分类专栏: Misc 文章标签: 安全 密码学 ctf misc 和你一起终身学习,这里是程序员Android 本文链接: https://blog.csdn.net/MrTreebook/article/details/123292179 版权



Misc 专栏收录该内容

50 篇文章 0 订阅 订阅专栏

攻防世界 Misc Ditf

1.winhex分析

2.binwalk分析

3.foremost分离

4.修改图片Ditf.png的高度

5.wireshark打开

6.exp

1.winhex分析

🚟 WinHex - [Ditf.pn	g]																							-	o ×
🎬 文件(F) 编辑(E)	搜索(S)	争航(N)	查看(V)	工具(T)	专业工具	(I) 选项	į(O) 窗	5□(W)	帮助(H)															20.3 9	GR-5 x64 _ ♂ ×
🗈 🎽 🗔 😂 💩	🗊 📑 🗌	n 🖻 I	B 🖪 🖻	010	M 👭	HEX 😘	HEX	→ - (8	 ← →	ن ې د ا	, 🎟 🌾	🗅 🦈 ۹	🦀 🛛 🎇 🖡	II .4 🕨											
Ditf.png Ditf.pcapn	Ditf.png																								
Offset	0 1	2	3 4	5 🤅	57	8	9 P	A B	С	DE	F	AN	SI ASCI	I		UTF-8	^							D	itf.png
00000000	89 50	4E 4	7 OD	DA 14	A 0 A	00 0	00 00	0 O D	49 4	8 44 5	2 <mark>2</mark> 91	IG	IHD	R 🗖		I IHDR								с	:\Users\17849\Des
00000010	00 00	03 9	E 00	00 05	5 4C	08 0)2 00	00 0	00 3	8 16 5	A	žL	8	Z CO										×	(件大小: 5.4 MB
00000020	34 00	00 0	0 09 '	70 48	3 59	73 0	10 00) OB	13 (0 00 0	в 4	рнү	s	40	🗆 pHYsl										5,610,069 字节
00000030	13 01	00 9	A 9C 3	18 00	00 (06 I	04 69	9 54	58 7	4 58 4	D	Š09	ÖiTXtX	M CO] tXM								5	省编辑模式
00000040	4C 3A	63 6	F 6D 3	2E 61	64	6F 6	52 65	5 2E	78 6	5D 70 0	0 L:0	com.ad	obe.xmp	L:	com.adol	ce.xmp□								H	(态: 原始的
00000050	00 00	00 0	0 3C	3F 78	3 70	61 6	53 6E	3 65	74 2	0 62 6	5	xp</td <td>acket b</td> <td>e DD</td> <td>DD<?xpa</td><td>cket be</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>10</td><td>6肖级数: 0</td></td>	acket b	e DD	DD xpa</td <td>cket be</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>10</td> <td>6肖级数: 0</td>	cket be								10	6肖级数: 0
00000060	67 69	6E 3	D 22 I	EF BE	3 BF	22 2	20 69	9 64	3D 2	2 57 3	5 gin	ı="	" id="W	5 gi	n=" "	id="W5								E.	兩撤消: 智无信息
00000070	4D 30	4D 7	0 43	65 68	3 69	48 7	/A 72	2 65	53 7	A 4E 5	4 MON	MpCehi	HzreSzN	T MOI	MpCehiH:	zreSzNT								ŧ	建时间022/03/05
08000000	63 7A	6B 6	3 39	64 22	2 3F	3E 2	20 3C	C 78	3A 7	'8 6D 7	0 czł	cc9d"?	> <x:xm< td=""><td>p cz</td><td>kc9d"?></td><td><x:xmp< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>10:42:36</td></x:xmp<></td></x:xm<>	p cz	kc9d"?>	<x:xmp< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>10:42:36</td></x:xmp<>									10:42:36
00000090	6D 65	74 6	1 20	78 6I	0 6C	6E 7	/3 3A	A 78	3D 2	2 61 6	4 met	ta xml	ns:x="a	d me	ta xmln:	s:x="ad								揮	后写入观题/03/05
0 A 000000	6F 62	65 3	A 6E '	73 37	A 6D	65 7	/4 61	L 2F	22 2	20 78 3	A obe	e:ns:m	eta/" x	: ob	e:ns:me	ta/" x:									11:27:40
000000B0	78 6D	70 7	4 6B :	3D 22	2 41	64 6	SF 62	2 65	20 5	8 4D 5	0 xmp	otk="A	dobe XM	P XM	ptk="Ad	obe XMP									性: A
000000000	20 43	6F 7	2 65 :	20 35	5 2E	36 2	2D 63	3 31	34 3	2 20 3	7 C	ore 5.	6-c142	7 C	ore 5.6	-c142 7								12	1000
000000D0	39 2E	31 3	6 30 3	39 32	2 34	2C 2	10 32	2 30	31 3	17 2F 3	0 9.1	L60924	, 2017/	0 9.	160924,	2017/0								核	試: 文本
000000E0	37 2F	31 3	3 2D 3	30 31	L 3A	30 3	36 3A	¥ 33	39 2	20 20 2	0 7/1	L3-01:	06:39	7/	13-01:0	5:39								19	移地址:十六进制 (而字节数:16-656
000000F0	20 20	20 2	0 20 3	22 3E	C 20	3C 7	/2 64	1 66	3A 5	2 4 4 4	6	">	<rdf:rd< td=""><td>F</td><td>"> <</td><td>rdf:RDF</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>(前帝曰: 2</td></rdf:rd<>	F	"> <	rdf:RDF									(前帝曰: 2
00000100	20 78	6D 6	C 6E	73 37	A 72	64 6	36 3E	22	68 7	4 74 7	0 xr	nlns:r	df="htt	p xi	mlns:rd	E="http								10	日总数: 3
00000110	3A 2F	2F 7	7 77 '	77 2E	5 77	33 2	2E 6F	72	67 2	F 31 3	9 :/,	/www.w	3.org/1	9 :/	/www.w3	.org/19								*	
00000120	39 39	2F 3	0 32 3	2F 32	2 32	2D 7	/2 64	4 66	2D 7	3 79 6	E 99,	/02/22	-rdf-sy	n 99	/02/22-:	rdf-syn								9	
00000130	74 61	78 2	D 6E .	73 23	3 22	3E 2	20 3C	2 72	64 6	6 3A 4	4 tax	<-ns#"	> <rdf:< td=""><td>D ta:</td><td>x-ns#"></td><td><rdf:d< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>500</td><td>I仔又性のEGB 空宗 Data\Local\Temp</td></rdf:d<></td></rdf:<>	D ta:	x-ns#">	<rdf:d< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>500</td><td>I仔又性のEGB 空宗 Data\Local\Temp</td></rdf:d<>								500	I仔又性のEGB 空宗 Data\Local\Temp
00000140	65 73	63 7	2 69 7	70 74	1 69	6F 6	5E 20) 72	64 6	6 3A 6	1 eso	cripti	on rdf:	a es	criptio	n rdf:a									buta (cocar(remp
00000150	62 6F	75 7	4 3D :	22 22	2 20	78 6	5D 6C	C 6E	73 3	A 78 6	D boı	it=""	xmlns:x	m po	ut="" xı	nlns:xm									
00000160	70 3D	22 6	8 74	74 70) 3A	2F 2	2F 6E	s 73	2E 6	64 6	F p='	http:	//ns.ad	o p=	"http:/	/ns.ado									
00000170	62 65	2E 6	3 6F	6D 21	78	61 7	/0 2F	7 31	2E 3	10 2F 2	2 be	.com/x	ap/1.0/	" be	.com/xaj	p/1.0/"									
00000180	20 78	6D 6	C 6E	73 32	A 78	6D 7	/0 41	5 4D	3D 2	2 68 7	4 xr	nlns:x	mpMM="h	t x	mlns:xmj	pMM="ht									
00000190	74 70	3A 2	F 2F	6E 73	3 2E	61 6	54 6F	F 62	65 2	E 63 6	F tp:	://ns.	adobe.c	o tp	://ns.a	dobe.co									
000001 A 0	6D 2F	78 6	1 70 :	2F 31	2E	30 2	2F 6E	D 6D	2F 2	2 20 7	8 m/z	kap/1.	0/mm/"	x m/:	xap/1.0	/mm/" x									
000001B0	6D 6C	6E 7	3 3A '	73 74	45	76 7	/4 3E	22	68 7	4 74 7	0 mlı	ns:stE	vt="htt	p ml:	ns:stEv	t="http									
000001C0	3A 2F	2F 6	E 73 :	2E 61	L 64	6F 6	52 65	5 2E	63 6	F 6D 2	F ://	/ns.ad	obe.com	/ :/.	/ns.adol	pe.com/									
000001D0	78 61	70 2	F 31 :	2E 30) 2F	73 5	54 79	9 70	65 2	F 52 6	5 xap	0/1.0/	sType/R	e xaj	p/1.0/s	ľype/Re									
000001E0	73 6F	75 7	2 63	65 45	5 76	65 6	бЕ 74	1 23	22 2	20 78 6	D sou	irceEv	ent#" x	m so	urceEve	nt#" xm									
000001F0	6C 6E	73 3	A 70	68 6I	74	6F 7	/3 68	8 6F	70 3	D 22 6	8 1n:	s:phot	oshop="	h ln	s:photo	shop="h									
00000200	74 74	70 3	A 2F 3	2F 6E	5 73	2E 6	64 15	4 6F	62 6	5 2E 6	3 tt	p://ns	.adobe.	c tt	p://ns.	adobe.c									
00000210	6F 6D	2F 7	0 68	6F 74	1 6F	73 6	58 6F	70	2F 3	1 2E 3	0 om,	/photo	shop/1.	0 om	/photosl	nop/1.0									
00000220	2F 22	20 7	8 6D	6C 6E	573	3A 6	54 63	3 3D	22 6	8 74 7	4 /"	xmlns	:dc="ht	t /"	xmlns:	dc="htt									
00000230	70 3A	2F 2	F 70	75 72	2 6C	2E 6	5F 72	2 67	2F 6	63 2	F p:,	//purl	.org/dc	/ p:	//purl.	org/dc/									
00000240	65 6C	65 6	D 65	6E 74	173	2F 3	31 2E	E 31	2F 2	2 20 7	8 ele	ements	/1.1/"	x el	ements/	l.1/" x									
00000250	6D 70	3A 4	3 72	65 61	74	6F 7	/2 54	4 6F	6F 6	GC 3D 2	2 mp	Creat	orTool=	" mp	:Creato	rTool="									
00000260	41 64	6F 6	2 65 3	20 50	68 (6F 7	/4 6F	73	68 6	F 70 2	0 Ado	obe Ph	otoshop	Ad	obe Pho	toshop									
00000270	43 43	20 2	8 57	69 6E	C 64	6F 7	/7 73	3 29	22 2	20 78 6	D CC	(Wind	ows)" x	m CC	(Windo	vs)" xm									
00000280	70 3A	43 7	2 65	61 74	1 65	44 6	51 74	4 65	3D 2	2 32 3	0 p:0	Create	Date="2	0 p:	CreateD	ate="20	~								
页 1 / 8,552						偏移)地址:						0				= 1	137 选块:	 	 	无 ナ	tds			无
・ ア 在这里	且输入你要打	腰的内	容			C	٠		V	6	-												^ 🛛 😣 🍽 🗊	的要人	11:38 022/5950f

• 看到了html代码,怀疑是一个网页

2.binwalk分析

(mss@kali)-[~/Desktop/git/ctf-misc] \$ binwalk Ditf.png 148 × 2 \$												
DECIMAL	HEXADECIMAL	DESCRIPTION										
0 aced	0x0	PNG image, 926 x 1100, 8-bit/color RGB, non-interl										
1822 989714	0x71E 0xF1A12	Zlib compressed data, default compression RAR archive data, version 4.x, first volume type:										
MAIN_HEAD		CSDN @==Microsoft==										

• 发现有一个rar文件

3.foremost分离

```
(rootEkali)-[/home/.../git/ctf-misc/output/png]
└─# foremost -i Ditf.png
```

- 打开rar文件发现需要密码
- .

4.修改图片Ditf.png的高度

🚟 WinHex - [Ditf.]	ong]																					
🏭 文件(F) 编辑(E) 搜索	E(S)	导航(N) 査	看(V)	工具	(T) 🕇	₩工具	l(I) 进	项(O)	窗口](W)	帮助(H)								
🗋 🦰 🔚 🤩 🕯	8 👔 🛛	1	5	a 🛱	C I	101 010	1 1	M 🕅	💏 🖏	в нех	-	• 📆	+-		3	i 🖓) 🥅 🔎 🦚	<u>_</u> 🥵	85 EE .	. ▶	Ø	
Ditf.png Ditf.pcapng Ditf.png																						
Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	Þ	Е	F		ANSI	I ASCII		UTF-8	^
00000000	89	50	4E	47	0D	0A	<u>17</u>	A 0	00	00	00	0D	49	48	44	52	%PNG		IHDR		🗆 🗆 IHDR	
00000010	00	00	03	9E	00	00	05	4C	80	02	00	00	00	38	16	5A	ž	L	8 Z		LOODD080Z	
00000020	34	00	00	00	09	70	48	59	73	00	00	0B	13	00	00	0B	4 g	HYs		4000	pHYsOOOOOO	
00000030	13	01	00	9A	9C	18	00	00	06	D4	69	54	58	74	58	4D	šœ	Ć	ÒiTXtXM		DDD tXM	
00000040	4C	3A	63	6F	6D	2E	61	64	6F	62	65	2E	78	6D	70	00	L:com.	adok	be.xmp	L:com	.adobe.xmp□	
00000050	00	00	00	00	3C	3F	78	70	61	63	6B	65	74	20	62	65	<3	2xpa	ket be	0000<	?xpacket be	
00000060	67	69	6E	3D	22	EF	BB	BF	22	20	69	64	3D	22	57	35	gin="b	Ľ»;"	id="₩5	gin="	" id="₩5	
00000070	4D	30	4D	70	43	65	68	69	48	7A	72	65	53	7A	4E	54	M0MpCe	ehiHz	zreSzNT	M0MpC	ehiHzreSzNT	
00000080	63	7A	6B	63	39	64	22	3F	3E	20	3C	78	3A	78	6D	70	czkc9c	: </th <th><x:xmp< th=""><th>czkc9</th><th>d"?> <x:xmp< th=""><th></th></x:xmp<></th></x:xmp<></th>	<x:xmp< th=""><th>czkc9</th><th>d"?> <x:xmp< th=""><th></th></x:xmp<></th></x:xmp<>	czkc9	d"?> <x:xmp< th=""><th></th></x:xmp<>	
00000090	6D	65	74	61	20	78	6D	6C	6E	73	3A	78	3D	22	61	64	meta 🗴	mlns	s:x="ad	meta	xmlns:x="ad	
000000 A 0	6F	62	65	ЗA	6E	73	ЗA	6D	65	74	61	2F	22	20	78	3A	obe:ns	s:met	:a/" x:	obe:n	GSAUt@7=-Mipro	osoft==

- 修改成05即可
- 再次打开图片可以看到密码



StRe1izia

CSDN @==Microsoft==

• 输入密码得到一个流量包文件

5.wireshark打开

• 搜索有关png的内容

	分约	且详情 ~	宽窄 ~	□ 区分大小写	字符串	~ png			
No.		Time	Source	Dest	ination		Protocol	Length	Info
	6971	20.304633	192.168.31.59	123.	206.131.120		TCP	54	33307 → 80
	6972	20.304869	123.206.131.120	192.	168.31.59		TCP	66	80 → 33306
	6973	20.304916	192.168.31.59	123.	206.131.120		TCP	54	33306 → 80
-++	6974	20.305051	192.168.31.59	123.	206.131.120		HTTP	432	GET / HTTP/
	6975	20.305749	112.10.47.131	192.	168.31.59		UDP	75	41733 → 248
	6976	20.313675	192.168.31.59	111.	147.144.142		UDP	1107	24889 → 406
	6977	20.313790	192.168.31.59	112.	10.47.131		UDP	1107	24889 → 417
	6978	20.317912	123.206.131.120	192.	168.31.59		TCP	54	80 -> 33307
	6979	20.318474	123.206.131.120	192.	168.31.59		HTTP	567	HTTP/1.1 20
		20. 21.0210	*** *** *** ***	100	100 01 00		1100		10001 010

	\n	
	<body>\n</body>	
	<pre>\tkimg src="/kiss.png" />\n</pre>	
	ZmxhZ3tPe180bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9	
	\n	
	\n	
0000	3r 68 74 6d 6r 3e 0a 20 20 3r 68 65 61 64 3e 0a	(html), (head).
0010	20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65	<pre>(met a http-e</pre>
0020	71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79	quiv="Co ntent-Ty
0030	70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78	ne" cont ent="tex
0010	74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d	t/html: charset=
0050	55 54 46 2d 38 22 20 2f 3e 0a 20 20 3c 2f 68 65	UTE-8" / >·
0060	61 64 3e 0a 20 20 3c 62 6f 64 79 3e 0a 20 20 09	ad> < ch odv>
0070	3c 69 6d 67 20 73 72 63 3d 22 2f 6b 69 73 73 2e	<pre>cimg spc ="/kiss.</pre>
0080	70 6e 67 22 20 2f 3e 0a 20 20 5a 6d 78 68 5a 33	$nng'' \rightarrow 7mxh73$
0000	74 50 65 6c 38 30 62 6d 52 66 53 47 6c 79 4d 46	tPel80bm RfSGlvMF
00a0	39 73 62 33 59 7a 58 30 5a 76 63 6a 4e 32 5a 58	9sb3YzX0 ZvciN2ZX
00b0	4a 39 0a 20 20 3c 2f 62 6f 64 79 3e 0a 3c 2f 68	19· ·
0000	74 6d 6c 3e 0a 0a	tml>··
		SSRN @Captain the H
		CSDN @노크Miehoso#42

- 发现base64加密的内容
- 使用工具解密



6.exp

```
import base64
basecode = "ZmxhZ3tPel80bmRfSGlyMF9sb3YzX0ZvcjN2ZXJ9"
result = base64.b64decode(basecode)
print(result)
```

• 得到flag

PS C:\Users\17849\Desktop> python exp.py b'flag{0z_4nd_Hir0_lov3_For3ver}' PS C:\Users\17849\Desktop>