

Web

没..没做出来…光第一题的 LFI(大概…)就拦了我三天…

以后本菜鸡签完到就研究上周的 WP 了…

RE

Pro 的 python 教室 (二)

pyc 文件找工具反编译掉，得到 py 文件看源码

```
enc = input()
len = len(enc)
enc1 = []
enc2 = ""
aaa = 'ioOavquaDb}x2ha4[~ifqZaujQ#'
for i in range(len):
    if i % 2 == 0:
        enc1.append(chr(ord(enc[i]) + 1)) # 奇数位 ascii 码+1 加入 enc1
        continue
    enc1.append(chr(ord(enc[i]) + 2)) # 偶数位 ascii 码+1 加入 enc1
    ↑ 得到 enc1 长度与输入的 flag，即 enc 相同

s1 = []
for x in range(3): # 外循环三次
    for i in range(len): # 内循环长度次
        if (i + x) % 3 == 0:
            s1.append(enc1[i]) # 得到 s1
            continue

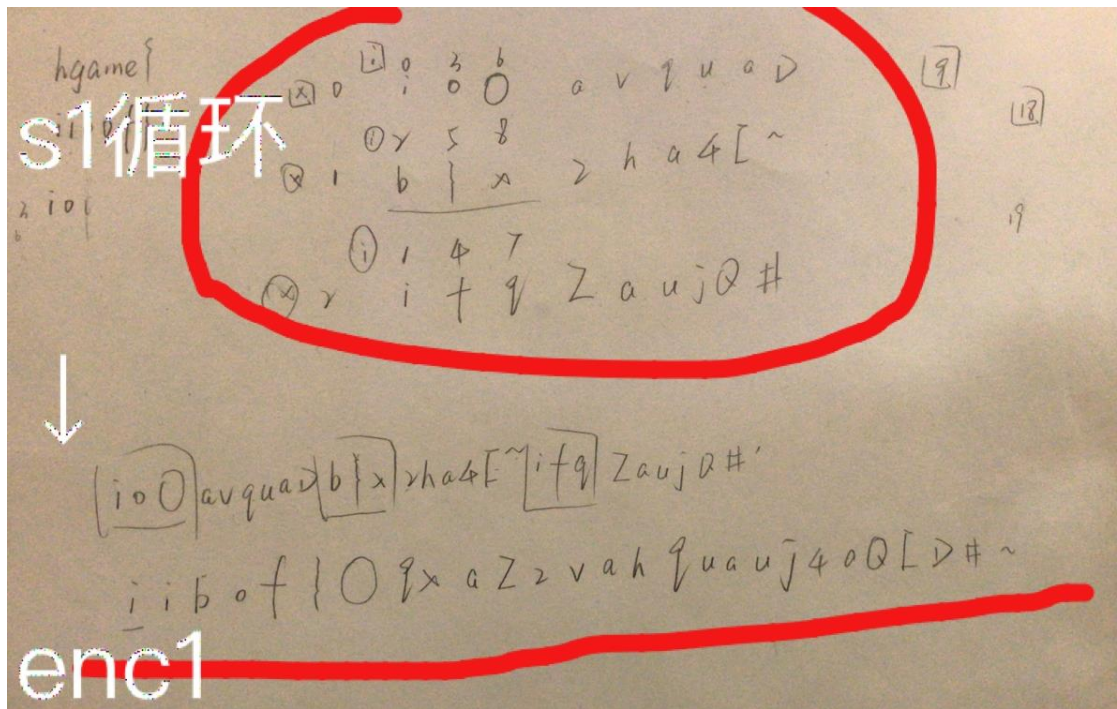
enc2 = enc2.join(s1) # 似乎就是 enc2 = s1
if enc2 in aaa: # 得到的 s1 字符串含于 aaa 中
    print ("You 're Right!")
else:
    print ("You're Wrong!")
    exit(0)
```

代码之外，输入的 enc 知道前五位 hgame{

从第一个循环入手，得出 enc1 的前五位 iibof}

代入 s1 的循环，

不大好说…上个草稿截图吧…



然后根据第一个循环用 ascii 码推出 flag

PWN

我..念旧，今年和去年一样...没..没做出来。

MISC

1. Are you familiar with DNS Recoders?

DNS 记录，cmd 中 nslookup 查看，从 A 查到 TXT，在 TXT 记录中找到 flag。

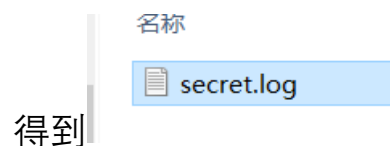
2. 找得到我嘛？小火汁

pcapng 文件 winhex 打开

搜索范围	时间
329	2019/01/30 2...
108781504B0304	2019/02/09 1...

ffset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	ANSI ASCII
82816	6A	41	AA	04	93	81	D2	1D	F3	EE	3B	EB	40	06	21	29	jA* " ò ói;èø !)
82832	70	14	70	A1	09	A2	B6	FD	26	10	EE	78	80	31	81	B8	p p; çÿ& ixel ,
82848	DF	E3	CD	4D	D5	89	2C	81	DF	63	8F	73	8B	14	03	74	ðáîMöñ, ðc sc t
82864	60	1E	FE	1B	50	4B	01	02	3F	00	14	00	00	00	08	00	' b PK ?
82880	CC	69	3C	4E	87	28	96	C5	46	07	00	00	02	0E	00	00	ïi<N+(-ÄF
82896	0A	00	24	00	00	00	00	00	00	00	20	00	00	00	00	00	\$
82912	00	00	73	65	63	72	65	74	2E	6C	6F	67	0A	00	20	00	secret.log
82928	00	00	00	00	01	00	18	00	4B	A8	32	54	C8	B6	D4	01	K'2TÈQÔ
82944	CD	D5	FA	E7	C8	B6	D4	01	17	EF	C6	4A	C8	B6	D4	01	íóúçÈQÔ iÈJÈQÔ
82960	50	4B	05	06	00	00	00	00	01	00	01	00	5C	00	00	00	PK \
82976	6E	07	00	00	00	00	00	00	84	02	00	00	06	00	00	00	n "
82992	58	00	00	00	00	00	00	00	7D	80	05	00	0E	F3	9A	FA	X }e óšü

藏了个 zip，扒出来

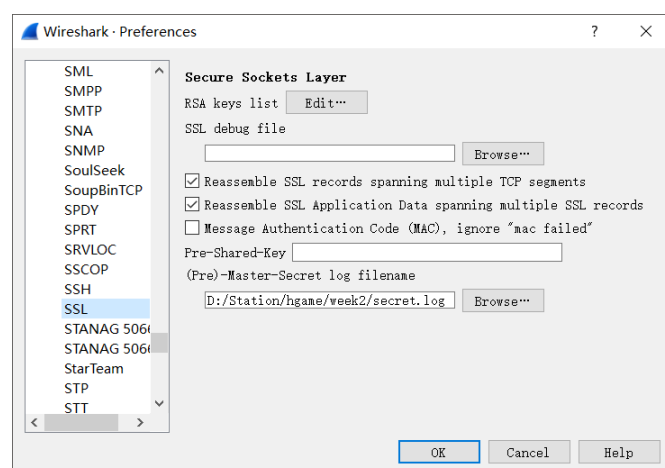


secret.log - 记事本

文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

SSL/TLS secrets log file, generated by NSS
CLIENT_RANDOM

Wireshark 配置



导入文件再找

http 对象

1.tar 解压得

flag.jpg

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
16	192.168.61.135	text/html	41 bytes	\
19	192.168.61.135	text/html	1282 bytes	favicon.ico
20	192.168.61.135		1460 bytes	favicon.ico
22	192.168.61.135		908 bytes	favicon.ico
25	192.168.61.135	text/html	41 bytes	index.html
58	192.168.61.135	text/html	41 bytes	\
64	192.168.61.135	text/html	3650 bytes	favicon.ico
194	192.168.61.135	application/octet-stream	116 kB	1.tar

```
5 72 2E 20 | ClipImgGet ver.  
1 8F 68 67 | 1.0.2   +   ± hg  
2 61 74 69 | ame{Congratulati  
5 5F 47 6F | ons_ ȳb You_Go  
3 00 43 00 | t_The_Flag}ȳ C  
2 02 02 04
```

Winhex 打开得 flag

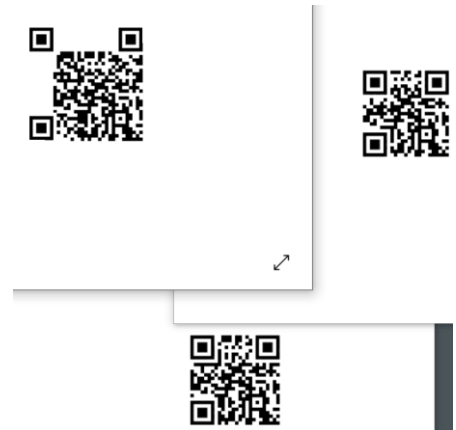
3. 初识二维码

首先呢，强调两点…一是三个“回”字的识别区，二是二维码尺寸。

题干说二维码缺损，那就尺寸往大了整…我呢…整了好久才意识到尺寸问题，25x25 的根本啥也扫不出来嘛…

最后 ps 一共做了三张二维码，

25 的 29 的 33 的…嗯，33 的才是答案



CRYPTO

1. 浪漫的足球圣地

百度一下，嗯，曼彻斯特。

也就是曼彻斯特编码了，一共两种编码规则

1. 0x5(0101)表 00

0x9(1001)表 10

0x6(0110)表 01

0xA(1010)表 11

2. 0x5(0101)表 11

0x9(1001)表 01

0x6(0110)表 10

0xA(1010)表 00

本题为第一种加密方法，将文本转化后二进制转文本即可。

2. Vigenere~

维吉尼亚密码，找工具复制粘贴。

由工具得出密匙 guess，flag 在明文。

维吉尼亚密码在线解密

请输入要加密的明文

The Vigenere ciphe is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It is a form of polyalphabetic substitution. The cipher is easy to understand and implement, but it resisted all attempts to break it for three centuries, which earned it the description le chiffre indechiffirable. Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In eighteen sixty three, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers. The Vigenere cipher was originally described by Giovan Battista Bellaso in his one thousand five hundred and fifty-one book La cifra del. Sig. Giovan Battista Bellaso, but the scheme was later misattributed to Blaise de Vigenere in the nineth century and so acquired its present name. flag is gfyuytuxxariyydfijplwsxdbzwwqt

加密

无密钥解密

密钥: guess

密钥长度(选填)

有密钥解密

请输入要解密的密文

Zbi Namyrwik wnhzk cw s eknlgv uz ifuxstlata edhnufwlow xwpz vc mkohk s kklmwk uz mflklagnkh Gswyuv uavbijk, huwww uh xzw ryxlwxm sx s qycogxx. Ml ay u igis ij hgrsedhnufwlow wmtynmlmzcsf. Lny gahnvy ak kuwq lu orvwxmsfj urv asjpwekhx, tmz cx jwycwlwj upd szniehzm xg txyec az zsj liliw ukhxmjoyw, ozowl wsxhiv az nlw vkmgiavnmgt ry gzalzv atxiuzozijshfi. Ests twqvfi zsby xjakh xg asjpwekhx wfilchloir kunyqwk zbel sxy ikkhhxasrfc Namyrwik wnhzklw. Af kokzikyr kadnc lzxyi. Xjoyhjaib Oskomoa ogm xzw lcvtl zi tmtrowz s myrwjgf qwlaih gx jvgahnvyafm Pmywtyvw uoijwiy. Nlw Noaifwxy gahnvy osy ivayohedde xikuxcfwv hs Kagbur Tsznmklq Viddgms af ncw gfk nlgmyurv xopi zmtxvww ghg xalnc-gfk vsgc Ru gaxxu hwd. Yck. Yaupef Tgnxakzu Fwdruwg, tan xzw ywlwek gek dgnij eomelxcfmikx xg Trumkw iy Zaykhjiw oh xzw tcrwln wifalc sfj ms suwomjiwj cxx hxywwfz heew. Ifey ay ajqmenycpglmqjzndhrqwpvhtaniz