writeup 2019“新华三杯”中国医疗机构网络安全攻防演练大赛CTF（复赛）

原创

ggzhifeng 于 2019-11-05 21:20:55 发布 2582 收藏 8
分类专栏： ctf 文章标签： ctf writeup 新华三

2019年10月31日，由《中国数字医学》杂志社主办、紫光旗下新华三集团支持的2019“新华三杯”中国医疗机构网络安全攻防演练大赛（复赛），在武汉光谷科技会展中心火热开赛。来自全国30多个省市的150家医疗机构,518人参加了本次复赛，这也是迄今为止中国境内规模最大的医疗行业攻防大赛。

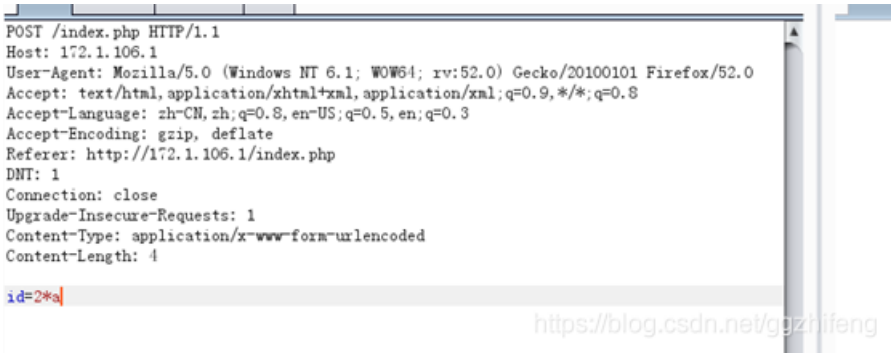
复赛共2小时，分为理论题和CTF题，同时进行，CTF共10到题，并且要在2小时内提交writeup…以下是部分题目的writeup，少了一题web综合题，当时没时间去看，现在也没环境了…

1.签到题

题目中已显示 flag，直接填入正确答案。

2.SQL注入

注入点在id



直接使用sqlmap跑，可以跑出flag

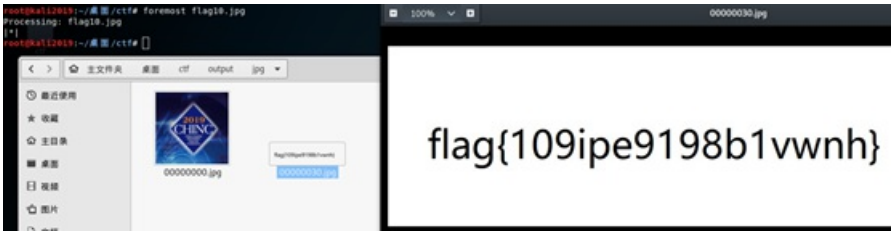
3.图片隐写

Binwalk发现图片里面藏着其他图片

无法binwalk直接解压，使用winhex，查找jpeg的文件头，从FFD8开头，截取后面的文件，导出图片，成功发现flag

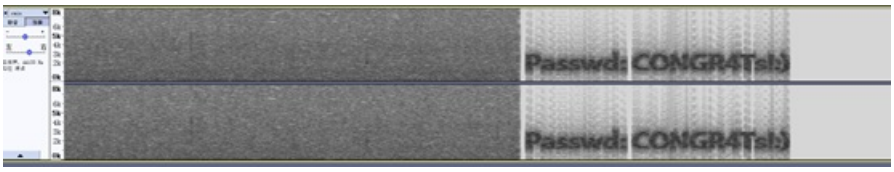
后来听说直接foremost就可以解出来了….果然，好香…

Foremost flag10.jpg



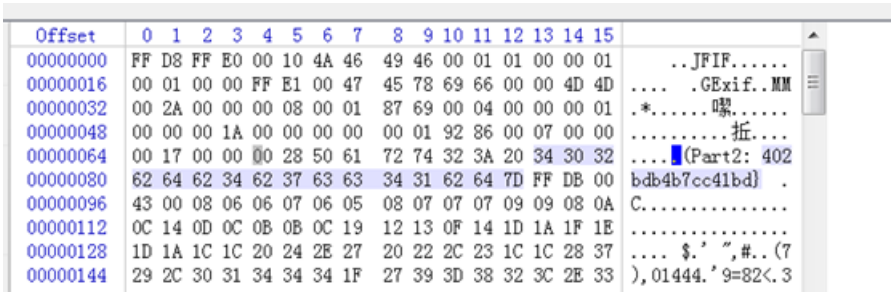
4. 音频隐写

使用音频软件打开，调出频谱图



发现压缩包密码，打开压缩包，获取到part1 flag

使用winhex打开图片，发现flag2



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	FF	D8	FF	E0	00	10	4A	46	49	46	00	01	01	00	00	01	..JFIF.....
00000016	00	01	00	00	FF	E1	00	47	45	78	69	66	00	00	4D	4D	.... .GExif..MM
00000032	00	2A	00	00	00	08	00	01	87	69	00	04	00	00	00	01	.*.....嗅.....
00000048	00	00	00	1A	00	00	00	00	00	01	92	86	00	07	00	00	.....抵....
00000064	00	17	00	00	00	28	50	61	72	74	32	3A	20	34	30	32	....(Part2: 402
00000080	62	64	62	34	62	37	63	63	34	31	62	64	7D	FF	DB	00	bdb4b7cc41bd} .
00000096	43	00	08	06	06	07	06	05	08	07	07	07	09	09	08	0A	C.....
00000112	0C	14	0D	0C	0B	0B	0C	19	12	13	0F	14	1D	1A	1F	1E	.....
00000128	1D	1A	1C	1C	20	24	2E	27	20	22	2C	23	1C	1C	28	37	.... $.' ",#..(7
00000144	29	2C	30	31	34	34	34	1F	27	39	3D	38	32	3C	2E	33	),01444.'9=82<.3

成功获取整个flag

flag{1a6b4d4e0c36581e8256a1a58402bdb4b7cc41bd}

5. 本地文件包含

通过目录扫描，发现phpinfo页面，发现

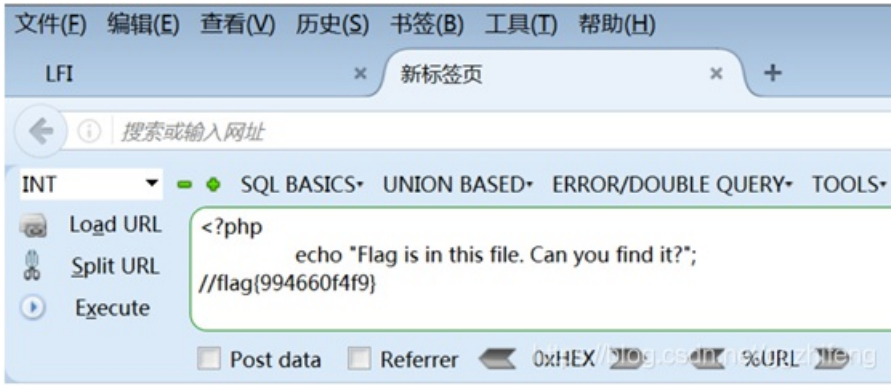
allow_url_fopen on

allow_url_include off

直接包含flag.php发现直接运行了脚本，没有flag，猜测flag藏在注释中，需要读取到php源码才可以，所以只能使用伪协议命令，输出 flag.php 的 base64 编码

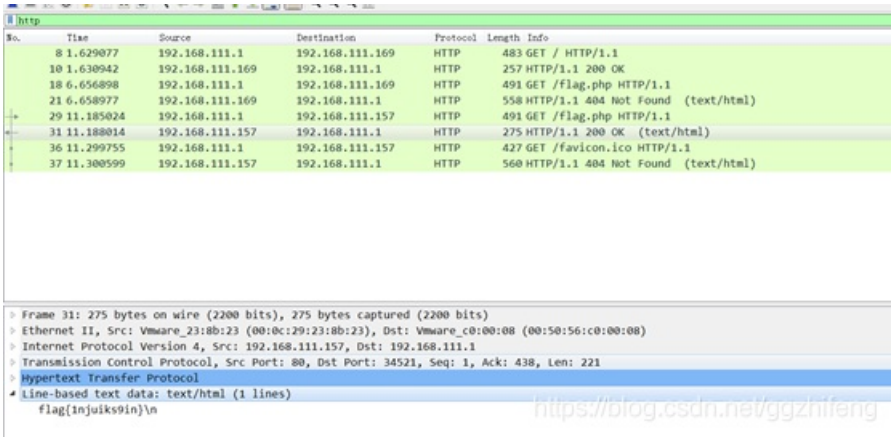
?page=php://filter/convert.base64-encode/resource=flag.php

Base64解码发现flag藏在注释中



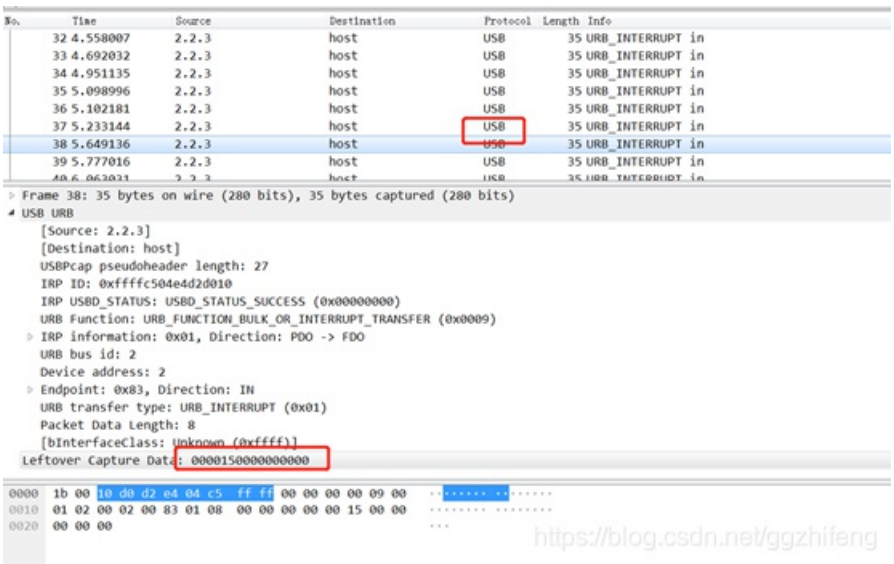
6. 数据包分析1

过滤http数据，直接发现flag



7. 数据包分析2

下载文件回来，发现一个压缩文档，需要密码，不是伪加密，另外有个pcap流量文件，打开发现是usb流量，USB协议数据部分在Leftover Capture Data域中，键盘数据包的数据长度为八个字节。其中键盘击键信息集中在第三个字节中。数据如下图所示：。



具体的键位映射关系可参考：《USB键盘协议中键码》中的HID Usage ID，链接：https://www.shsu.edu/csc_tjm/fall2000/cs272/scan_codes.html

所以压缩文档的密码在这个流量包的usb键盘流量中

1. 使用kali linux中的tshark 命令把cap data提取出来：

tshark -r usb.pcap -T fields -e usb.capdata > usbdata.txt

1. 根据《USB键盘协议中键码》中的HID Usage ID将数据还原成键位，github上有脚本，但不知道为什么，一直没跑出来....

https://github.com/WangYihang/UsbKeyboardDataHacker

https://ctf-wiki.github.io/ctf-wiki/misc/traffic/protocols/USB-zh/

跑出来也密码不正确

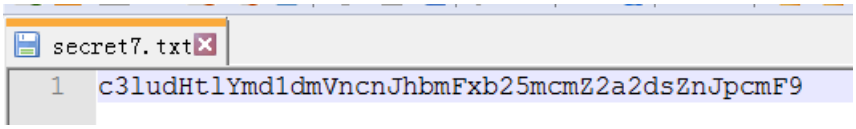
```
tthiisismmypasswword1

D:\3.Coding\python\test>python keyboardstest.py password.txt
```

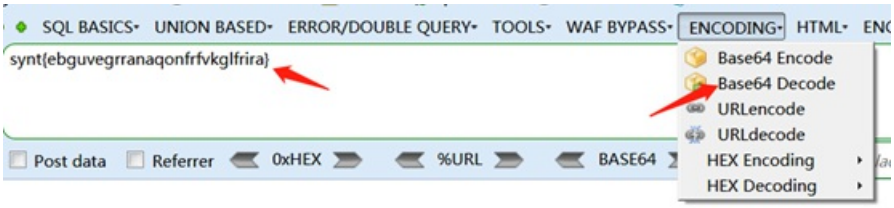
8.EasyCrypto

源码

c3ludHtlYmd1dmVncnJhbmFxb25mcmZ2a2dsZnJpcmF9



经过Base64解码后如下：



synt{ebguvegrranaqonfrfvkglfrira}

发现是flag格式，说明字母进行了转换，与flag{xxx}对比，发现是字母assic码往后减13，直接转了下，发现存在特殊字符，提交flag提示错误，猜想如果减完后的值小于a的assic码97，则要加上26，使其还原成字母范围，在上面字符串去掉{}后转为assic码，写了个python脚本，成功跑出flag（因为现场没有网络，忘记python中string和assic码如何转换了，所以手工使用工具进行转换然后再python脚本简单的加减和判断）。

```
temp1=[115,121,110,116,101,98,103,117,118,101,103,114,114,97,110,97,113,111,110,102,114,102,11
8,107,103,108,102,114,105,114,97]
for i in range(len(temp1)):
    temp2=temp1[i]-13
    if temp2<97:
        temp2=temp2+26
    print temp2
```

现在查了下，发现很简单，number = ord(char)，char = chr(number)，最后的脚本如下

```
temp1="syntebguvegrranaqonfrfvkglfrira"
flag=""
for i in range(len(temp1)):
    temp2=ord(temp1[i])-13
    if temp2<97:
        temp2=temp2+26
    flag=flag+chr(temp2)
print flag
```

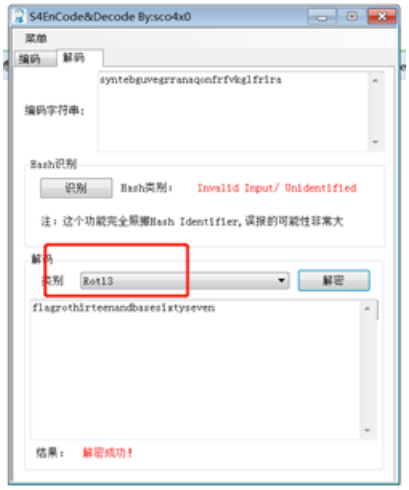
```
for i in range(len(temp1))
Run:  test
D:\program\Python27\python.exe D:/3.Coding/python/test/php/test.py
flagrothirteenandbasesixtyseven

Process finished with exit code 0
```


前后添加{}就是最终的flag

Flag{rothirteenandbasesixtyseven}

后来听说是rot13加密方式，直接使用工具就可以解开了……..



9. Easy RSA

当时不懂RSA并且没有网络无法安装相应的Crypto库，运行不了脚本，所以没有做

打开压缩包，发现存在3个文件，通过看py脚本，发现cipher.txt是flag加密后的密文，pubkey.txt是RSA参数中的e和N

所以情况很明了，分解N，算出p和q，然后计算d，就可以解析出明文了（当然也可以直接运行脚本，穷举p和q，然后判断是否得出的N等于原始给的N，这样也可以获取P和Q）

但是发现N特别的大，

如果n小于256bit，可以使用本地工具进行暴力分解，例如windwods平台的RSATool，可以在数分钟之内完成256bit的n的分解。

如果n大于768bit，可以尝试利用在线网站http://factordb.com， 这一类在线网站的原理是储存了部分n分解成功的的值。

这里的N有617位，又没有网络，所以最终比赛结束，都没有人算出来.....

E=65537

N=337741676001996910724704248988429281685705599403627707860606993209895468516951064669241

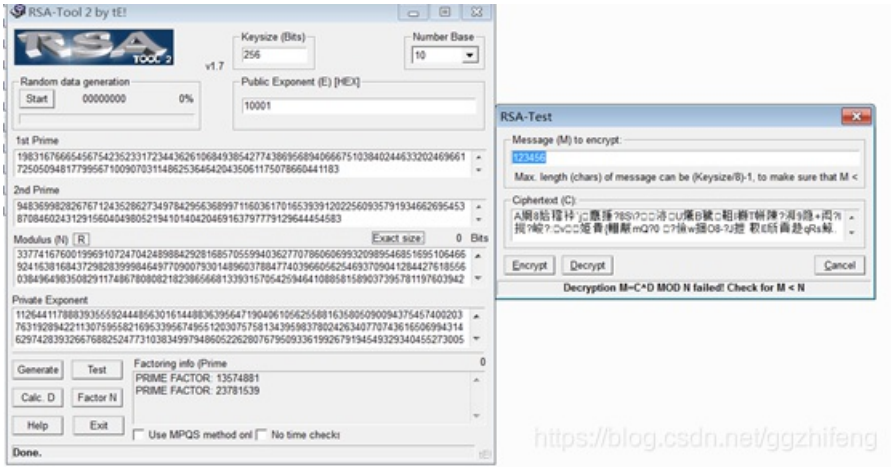
P=177993461816075408240866752227210319316825574291000376727523991315086097605063837563341

Q=189749484366449861630736482622030204229600074936733397229668738586605895979811823994021

使用RSATool，得到D

D=112644117888393555924448563016144883639564719040610562558816358050900943754574002037631

理论上应该是这样就能够接触来了，可是不知道为什么不对……



附件：

本次比赛能下载的题目，已上传百度云

链接：https://pan.baidu.com/s/14SR1m-vKEUaO_cMDjnQsUw

提取码：9fbv