A&DCTF

转载

weixin_30730053 于 2017-11-13 22:16:00 发布 84 收藏
文章标签： php python 密码学
原文链接：http://www.cnblogs.com/linwx/p/7828526.html

ADCTF WRITEUP

方向：Reverse 解题数：2

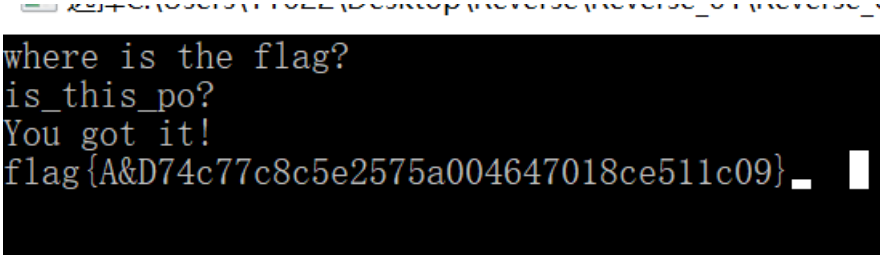
题目：Reverse_01

解题过程：

用ida打开反汇编查看代码，看main函数发现

```
if ( 1 > 3 )
{
  if ( !strcmp((const char *)v4, "is_this_po?") )
  {
    get_flag(a);
    printf("You got it!\n%s", a);
    getchar();
    getchar();
    free(v4);
    return 0;
  }
  printf("Try again...");
  getchar();
  getchar();
}
```

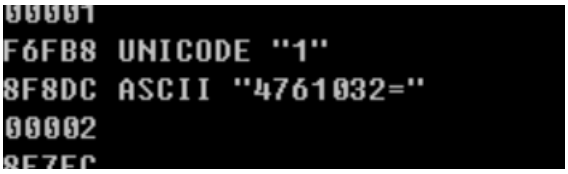
关键部分，字符串比较，竟然是直接比较”is_this_po?”相等，然后连续输入这字符串（因为之前的逻辑）最后得到flag



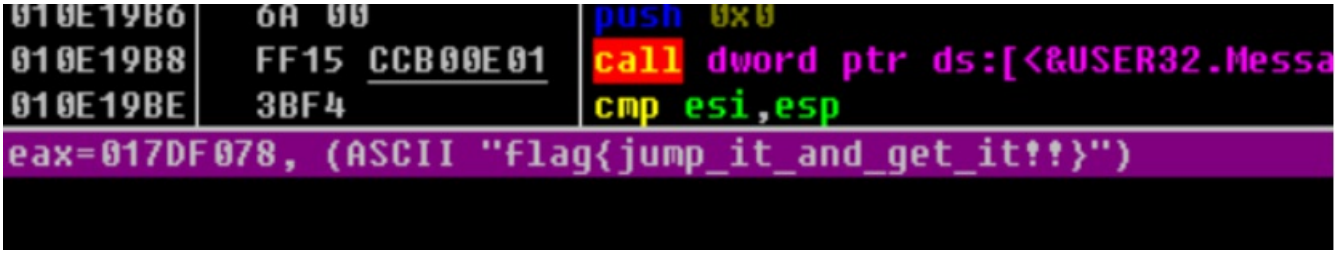
题目：baby_crack

解题过程：

看到题目下载exe文件，用OD反汇编，在关键字断点，看到



觉得有些奇怪，应该是哪个验证码，输入后可得还真的是



方向：MISC　解题数：5

题目：文件名

解题过程：

先分析图片文件发现图片结尾有pk压缩包，然后用binwalk工具查看隐藏的压缩包，发现有zip文件，用foremost分离，压缩后发现zip文件有名flag压缩包，可需要密码，还有一张gif图片，细思极恐，用stegsolve工具分帧一波发现图片上有一行字75DB7807E1，猜测是密码，果然是密码，可得
flag{97771C2B239C9A6C28BFDBA6E6AF0494}

题目：encryptORbroken

解题过程：

看这题目，搞得我心生恐怖，下载文件后看到

```
**************************************
**************************************
******0QTEzMzY5N0Y4NTc5Mn0=**********
**************************************
**************************************
```

不简单，不简单，后面有=，试试base64,不对，试了好久，突然脑袋灵光一闪，加密解密，套上flag{}，正确。

flag{0QTEzMzY5N0Y4NTc5Mn0=}

题目：broken

解题过程：

一看题目？？爆破？下载好压缩包，打开，发现里面的flag文件要解压密码？？作为老司机看看另外一个tip文件，发现密码为6位数？？猜测到可能是zip文件伪密码，用工具打开查看50 4B 01 02 后面 的字段，发现好像有个地方修改01 00，修改回00 00，惊喜万分可是不对，尝试另一种方法，得到密码为123456，最后flag文件里有kqfl{ymnsprtwjitrtwj}，一眼看出是凯撒加密，解之。

flag{thinkmoredomore}

题目：小明飙车

解题过程：

用notepad++打开，发现文件开头为 JFIF，脑袋灵光一闪，可能是个jpg图片（伪装的好，可是逃不过我的法眼），修改文件头打开就可以看到flag

flag{You_Find_it!}

题目：小明飙车2

解题过程：

下载到一张jpg图片，在nopad++打开文件，发现有好多数据，pk啥的，果断放在Linux下binwalk一下，发现里面藏着文件，

```
root@kali:~# binwalk 能干.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.02
30            0x1E            TIFF image data, little-endian offset of first image directory: 8
416           0x1A0           JPEG image data, JFIF standard 1.02
10225         0x27F1          JPEG image data, JFIF standard 1.02
19256         0x4B38          Unix path: /www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf
mlns:xmp="http://ns.adobe.com/xap/1.0/" xmlns:tiff="http:
78100         0x13114         Microsoft executable, portable (PE)
90979         0x16363         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/crtexe.c
100388        0x18824         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/tlssup.c
102049        0x18EA1         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/charmax.c
103275        0x1936B         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/mingw_helpe
104501        0x19835         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/xtxtmode.c
106359        0x19F77         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/_newmode.c
106708        0x1A0D4         Unix path: /crossdev/src/mingw-w64-v3-git/mingw-w64-crt/crt/natstart.c
```

用foremost分离出来发现一个exe文件，然后果断放在OD里面，发现啥都没有仔细看看发现一串字符串，

```
sub esp,0x10
call 00000152.00401E80
mov dword ptr ss:[esp],00000152.0040400 huovuz tulgesioa lvwa luouwa lhvxzaou rfkpsrsi gtitglh gtotsio ouawz rfkpsrsi ouhuz
call <jmp.&msvcrt.printf>
```

题目说丢下一个键盘，肯定与键盘有关，猜测为键盘上的字母形状，但是发现不对劲，然后再看看题目，发现飘移13个（有问题。。），rot13解码，可得

```
uhbijm ghytrfvbn yijn yhbhjn yuikmnbh esxcfefv tgvgtyu tgbgfvb bhnjm esxcfefv bhujm
```

根据键盘上（坑啊）可得flag

flag{keyboardman}

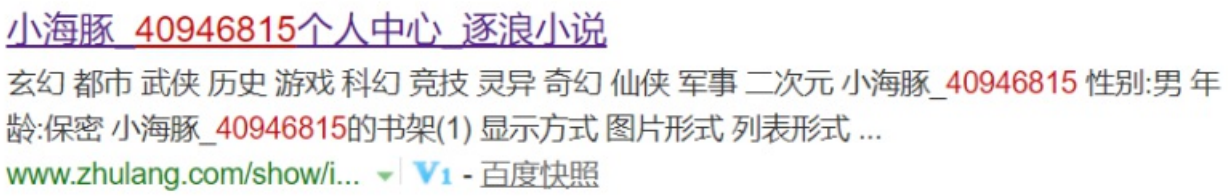
方向：社会工程学　解题数：1

题目：社会工程学

解题过程：

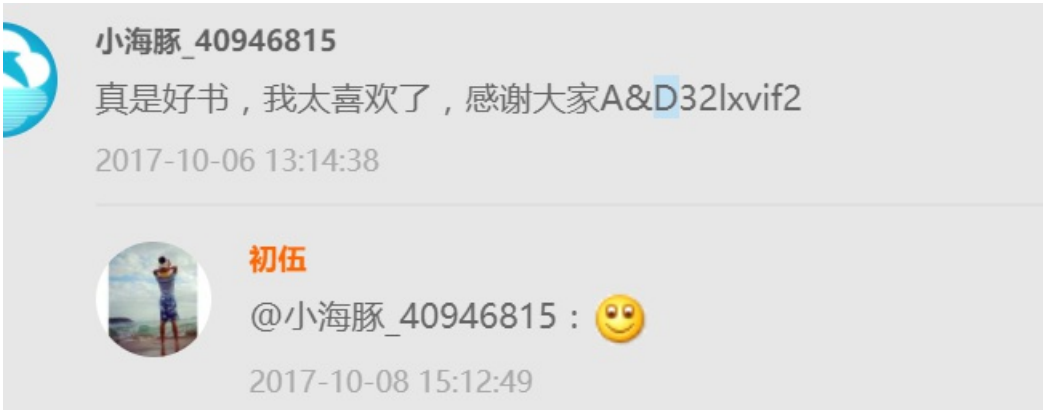
打开页面看到一段话

小明是一位小说迷，常年活跃于各大小说网。作为一名id为40946815的小海豚，2017-10-06那天，一不小心在看他最喜爱的书时泄露了很重要的信息。直觉告诉我，id为40946815，小海豚，2017-10-06不是白给你的，百度一波，发现



点了进来，想起日期，肯定是与它有关。

自觉地翻到更新日期，最后在书评中找到，隐藏的深。。出题人怎么找到这里来的？？



方向：Web　解题数：8

题目:签到题1

解题过程：

我在你眼前？？ 看到地址栏，发现有一串编码字符ZmxhZ3t4Y3YyM3NkbEswOTN9，猜测base64,发现正确

flag{xcv23sdlK093}

题目：签到题2

解题过程：

查看源代码，注释flag{welcometoctf>_<}

题目：input

解题过程：

查看源代码，将maxlength长度修改为11,填入。

flag{xcvpweiigdlclbmawwpp}

题目：Function property

解题过程：

查看源代码发现php代码，大致意思是字符串替换nihao，然后在与nihao比较；构造ninihaohao，有点意思有点意思。

flag{nvKK03L2sk34}

题目：coding

解题过程：

JSFuck编码，在控制台上运行得到

题目：代码审计

解题过程：

属于PHP代码审计，看PHP代码得知

username=admin&&pass=password相等才能通过，仔细看一下代码，发现md5加密，想到md5碰撞，0exxxxxxx==0xggggg 在php弱类型语言中是相等的，然后密码构造为240610708，填入可得flag

flag{bbfpgekakdkixklwklcxc}

题目：暴力破解

解题过程：

打开页面查看源代码，发现一段注释，以一枚菜鸡也知道他想暗示什么

```
<form method="post" action="check.
<!--
admin
password.txt-->
```

用户名为admin,密码的话，有个password.txt文件，说明在根目录下有password.txt，进入根目录后发现好多串一样的字符串

(缩小了，知道就可以啦。)

再看看题目，往往题目都是比较关键的，暴力破解？？,那就暴力破解，那么用什么密码字典好呢？？Password.txt????，哈哈哈,这就是密码字典了。打开burpsuite(大法好)，破解得

题目：Ultra vires

解题过程：

查看源代码，发现如下

```
</div>
<!--
username=guest
password=123456
-->
```

登录后发现getflag要管理员权限，细想极恐。旁边还有个修改密码按钮？心想：可不可伪造管理员修改其密码，利用burpsuite抓包，发现修改密码为如下语句

```
a/changepassword.php?username=guest&new_password=123 HTTP/1.1
.36.58
```

猜测管理员的用户名为admin，修改其密码，果然成功，然后登录，得到flag。

方向：密码学　解题数：2

题目：playfair

解题过程：

了解波费雷密码的用法用密钥画出矩阵，

```
h a c k i
n g s t e
w x y b d
f l m o p
q r u v z
```

再用密文还原明文为welcome to adseclabz

题目：简单的RSA

解题过程：

根据n 算出p,q,然后算出密文d,python脚本如下：

打开(O)　rsa.py

```
n=0x52532714731F3349551751F75155157F3951713
c=0x1B64EACD005FEBAE0884B94D816998EF0C3047C
d=0x3C71EFEC6EBCC0FE6F3F1200ED7474B75FDED31
print  (c^d)%n
```

算出明文m.

题目：easyencrypt

解题过程：

看到程序

```
int main(){
    char ch[]= "###########";              //flag
    int i,j,x,c;
    x=(rand()%(34-17+1))+17;    //22
    for (i=0;ch[i]!='\0';i++){
        c=(int)ch[i];
        j=2;
        while (c>1){
            if(c%j==0){
```

发现x是个常数，而且等于22，然后根据程序逻辑推出输出的数除于22后相乘得到其assic码值，然后逐一查找可得

flag{thisisnorealflag}

转载于:https://www.cnblogs.com/linwx/p/7828526.html