实验吧-逆向-该题不简单

原创

Flemington、 于 2017-11-30 23:09:56 发布 1001 收藏

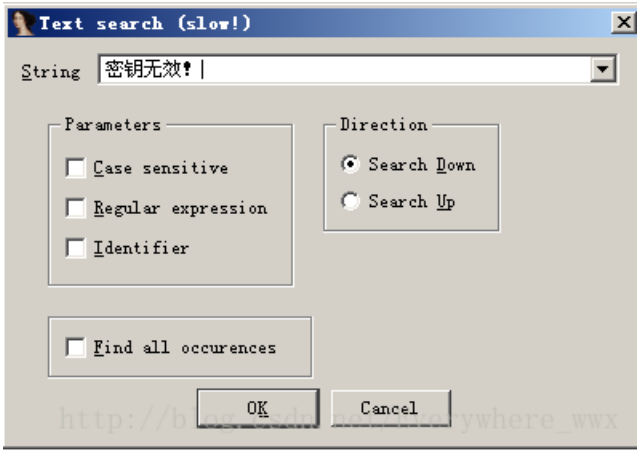
分类专栏： RE 文章标签： 实验吧 逆向工程 writeup

本文链接：https://blog.csdn.net/Everywhere_wwx/article/details/78682172

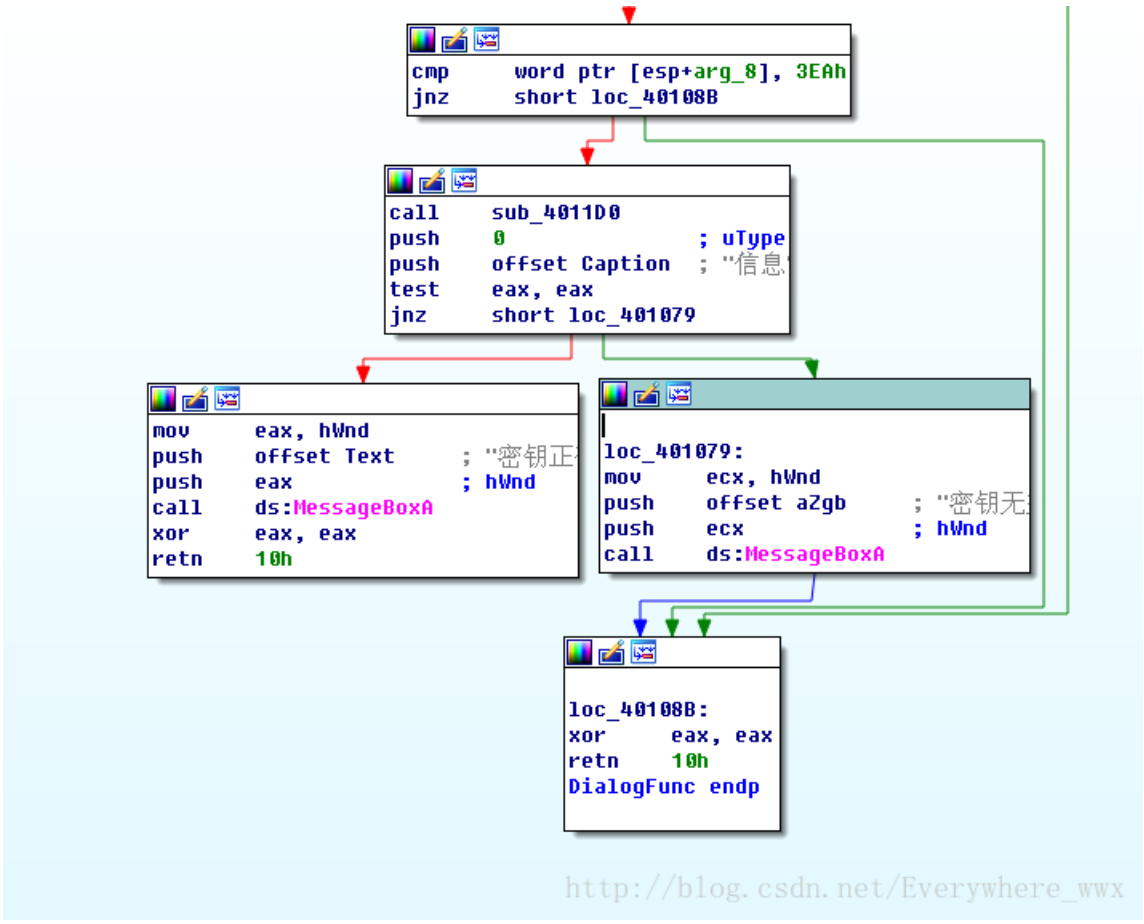
解题链接

http://www.shiyanbar.com/ctf/14

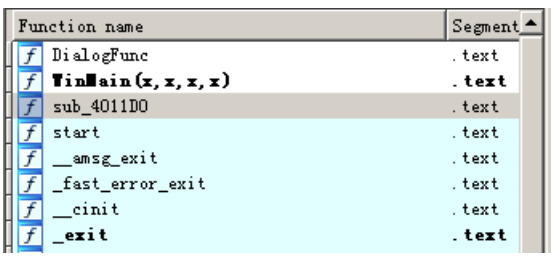
直接下载，我是拖到虚拟机中（xp，吾爱破解版，文章最后附上链接），先随便输入用户名注册码，得到密钥无效!然后就可以根据密码无效用IDA pro x86搜索

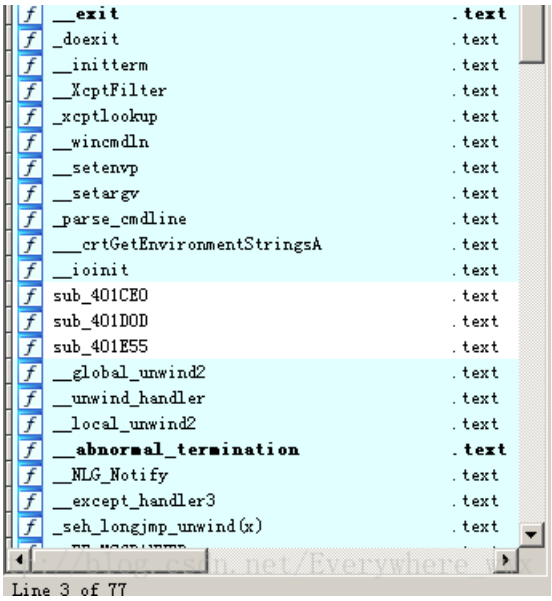


看到如下图所示的，密钥无效



在左侧看出这个调用了 : sub_4011D0
分析可知道，当返回值不为 0 的时候 , 就跳转到 密钥无效 的分支
转到 sub_4011D0
直接 f5 反编译为 C代码
（f5得看版本，64和32如果和程序不对应得情况，f5失效）






```
String[0] = 0;
memset(&String[1], 0, 0x1Cu);
v3 = 0;
v4 = 0;
String1 = 0;
memset(&v10, 0, 0x1Cu);
v11 = 0;
v12 = 0;
String2 = 0;
memset(&v6, 0, 0x1Cu);
v7 = 0;
v8 = 0;
if ( GetDlgItemTextA(hDlg, 1000, String, 16) >= 5 )
{
  GetDlgItemTextA(hDlg, 1001, &String1, 16);
  v1 = 0;
  if ( strlen(String) != 0 )
  {
    do
    {
      *(&String2 + v1) = (v1 + v1 * String[v1] * String[v1]) % 0x42 + 33;
      ++v1;
    }
    while ( v1 < strlen(String) );
  }
  strcpy(String, "Happy@");
  lstrcatA(String, &String2);
  result = lstrcmpA(&String1, String) != 0;
}
else
{
  result = 1;
}
return result;
```


c语言代码可以读得懂，这段代码会将

1.用户输入的用户名的每个字符遍历一遍
2.把每个字符的序号(从 0 开始算)与这个字符的ASCII码的平方相乘
3.然后整体再加上序号
4.得到的和继续对 0x42 求余
5.最后将结果加上 33
6.然后再转为ASCII码
7.最后再将上述结果连接在字符串 'Happy@' 之后构成注册码

可用python写脚本运行
代码如下
username ——>u
counter ——>c
password——>p

```
u= "Hello"
c= 0;
p= "Happy@"
for i in u:
    p = p + chr((c + c * ord(i) * ord(i)) % 0x42 + 33)
    c = c + 1
print(p)
```

Python2.7运行

Happy@!GA0U

得到flag

吾爱破解虚拟机链接:
https://www.52pojie.cn/thread-661779-1-1.html
有安装问题可以私聊我~