[XCTF-Reverse] 93 phrackCTF_findKey

原创

石氏是时试 于 2022-03-31 11:36:18 发布 64 收藏
分类专栏： CTF reverse 文章标签： reverse

这个题给的附件并不是ISC2016训练赛 phrackCTF--findkey那个pyc的题，但上传flag要传那道题的。

本wp只针对下载的附件

先用ida打开，发现主要函数无法反编译。根据网上的说法，先把函数部分选中拉灰，再按P生成函数就能反了（网上说右链，其实这时右键里是没那项菜单的，不过快捷键P还能正常用）

```
if ( Msg > 0x111 )
{
  if ( v12 == 517 )
  {
    if ( strlen((const char *)&String1) > 6 )
      ExitProcess(0);
    if ( strlen((const char *)&String1) )
    {
      memset(&v22, 0, 0x100u);
      v6 = strlen((const char *)&String1);
      memcpy(&v22, &String1, v6);
      v7 = strlen((const char *)&String1);
      hash_hex(&String1, v7, (LPSTR)&String1);
      if ( &v10 && !&v10 )
        JUMPOUT((char *)&loc_40191D + 2);
      strcpy(&v18, "0kk`d1a`55k222k2a776jbfgd`06cjjb");
      memset(&v19, 0, 0xDCu);
      v20 = 0;
      v21 = 0;
      strcpy(v14, "SS");
      v15 = 0;
      v16 = 0;
      v17 = 0;
      v8 = strlen(&v18);
      xor_ss(v14, (int)&v18, v8);             // "0kk`d1a`55k222k2a776jbfgd`06cjjb" ^X
      if ( _strcmpi((const char *)&String1, &v18) )
      {
        SetWindowTextA(hWndParent, "flag{}");
        MessageBoxA(hWndParent, "Are you kidding me?", "^_^", 0);
        ExitProcess(0);
      }
      memcpy(&v13, &unk_423030, 0x32u);
      v9 = strlen(&v13);
      xor_ss(&v22, (int)&v13, v9);
      MessageBoxA(hWndParent, &v13, 0, 0x32u);// flag{n0_Zu0_n0_die}
    }
    ++dword_428D54;
  }
```

主要功能就这么一点，先是输入的6字节进行md5和hex后得到一个串，与v18那个串与S异或后的串比较。先把v18异或后得到md5值，然后网上搜到原值为123321

再往下走，他用同样方法把unk_423030用123321作了个异或然后输出

```
v18 = b'0kk`d1a`55k222k2a776jbfgd`06cjjb'
v18 = bytes([i^ord('S') for i in v18])
print(v18)
#c8837b23ff8aaa8a2dde915473ce0991
#123321
v22 = b'123321'
a = bytes.fromhex('575E5254495F016D6946026E5F026C575B544C')
for i,v in enumerate(a):
    t = v^v22[i%6]
    print(chr(t), end='')

#flag{n0_Zu0_n0_die}
#PCTF{PyC_Cr4ck3r} 网站上上传的flag是另外一个题的，名字相同
```

运行得到的这个flag并不是网站要求上传的，网上搜到另外一题，名字与这个相同，上传那个题的flag成功。