

实验吧逆向工程之100w--WP

原创

Neil-Yale 于 2017-05-02 17:36:48 发布 3461 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/yalecaltech/article/details/71086055>

版权

虽然不怎么玩逆向，不过这题也不同逆向去做

用按键精灵就可以了

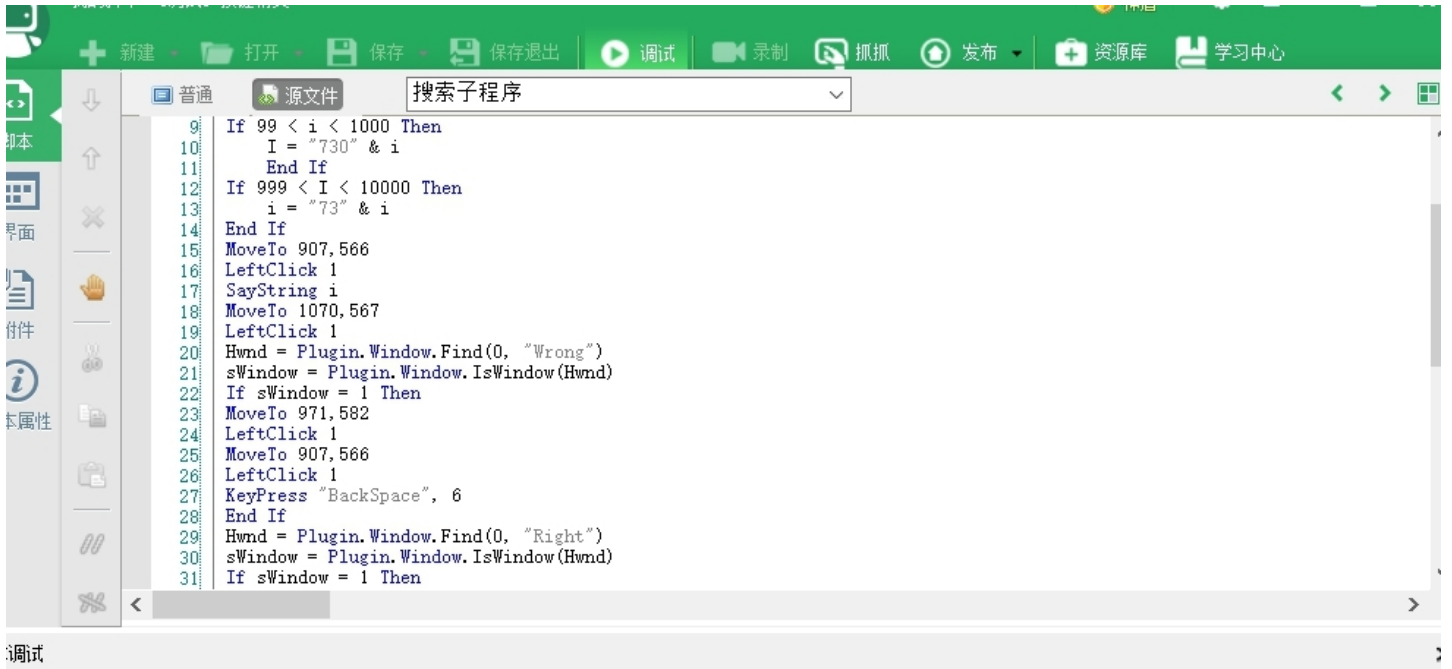
按键精灵是用脚本来运行的，对于给的这个小程序，我们在写脚本时要注意按键的坐标、尝试的次数、范围、判断正确与否等等

如何查看坐标可以详细参考这篇：

<http://jingyan.baidu.com/article/22a299b527eecf9e18376a41.html>

按键精灵的脚本如下：

```
For 10000
i = i + 1
If i < 10 Then
    i = "70000" & i
End If
If 9 < i < 100 Then
    i = "7000" & i
End If
If 99 < i < 1000 Then
    I = "700" & i
End If
If 999 < I < 10000 Then
    i = "70" & i
End If
MoveTo 907,566
LeftClick 1
SayString i
MoveTo 1070,567
LeftClick 1
Hwnd = Plugin.Window.Find(0, "Wrong")
sWindow = Plugin.Window.IsWindow(Hwnd)
If sWindow = 1 Then
MoveTo 971,582
LeftClick 1
MoveTo 907,566
LeftClick 1
KeyPress "BackSpace", 6
End If
Hwnd = Plugin.Window.Find(0, "Right")
sWindow = Plugin.Window.IsWindow(Hwnd)
If sWindow = 1 Then
    Exit For
End If
Next
```



调试

自定义界面

启动[F10]

中止[F12]

暂停[Pause/Break]

单步[Scroll Lock]

步过[Alt+Scroll Lock]

变量查看

变量名	值
点击这里...	

调试信息 同时记录脚本的执行次序 (会降低执行速度, 暂不支持多线程脚本)

脚本已经停止执行

<http://blog.csdn.net/yalecaltech>

这里尝试的范围是700000-800000

这是我从答案得出来的, 真正要爆破的话会很久, 随便写个范围感受一下就行

Right ×

CTF{4ef7836c744a0aaa0ac00dbc885849d3}



可以用星号密码查看器看下



星号密码查看器

