<https://www.52pojie.cn/thread-1358649-1-1.html>

想学[破解](https://www.52pojie.cn/)，花了很多时间还是没有多少进步？网上很多教程，看来看去，到头来还是一头雾水？其实，很正常，不是你的问题，是没有遇到能教会你的人！我也是刚刚入门，在学习中遇到过和你同样的问题。所以，“别抱怨自己”！始终用“玩破解”的心态来面对就可以了。毕竟，我们不靠破解来生存，只是兴趣而已。既然是兴趣，那就要开心快乐才行。我用大家最容易理解的思维和语言来和大家一起玩玩破解，相信对于刚刚步入破解门槛的小白会有“大”帮助。  
  
**第一、破解到底破什么？**  
我们既然学破解，首先就要清楚我们的目标在哪？敌人是谁？可以这么说，破解的对象是软件的使用验证。什么是软件的使用验证？比如你花了一个月写了一个软件，你想让其他人花钱才可以用，你怎么办？当然，你要给你写好的软件再增加一个使用验证，就像你租房，你当然要先上锁，谁花钱租房，你就给他钥匙。锁就是房子使用的验证。现在明白了吧，我们破解破的不是可用的软件，而是限制使用软件的那把锁。所以，找到锁的位置和锁的构造才是破解的关键！锁的位置我们可以称为关键验证位置，锁的构造称为验证机制。因此，我们学习破解就学两步，第一步是学习如何找到关键位置，第二步是能够分析出验证机制。  
  
**第二、怎么破解？**  
要破解当然需要工具。还拿开锁的例子，你是不是要准备好手电、开锁的各种工具才可以。破解软件最基本的工具就是别人写好的专门用于破解分析的软件，这样的软件很多，最基本的是三个。老大叫[PEID](https://www.52pojie.cn/thread-12865-1-1.html)，老二叫DIE64，老三叫OD。遇到要破解的软件，兄弟依次上阵。老大先上，作用是查一下这个软件有没有加壳，是什么壳？壳就是软件的防弹衣，这个防弹衣是用专门的程序编写的，这个防弹衣是在软件有了使用验证以后又增加的一层保护。其目的就是对付我们使用的破解工具，让我们不好下手。我们的老大查了以后，知道这个防弹衣的型号就可以用对应的脱防弹衣的工具来对付它了。接着，老二再上，作用是识别这个软件是什么语言编写的，通常来说有C、VC、VB、DELPHI、易语言等，因为不同的语言有特殊的破解方法。知道有没有壳？是什么语言编写的？然后老三就闪亮登场了。OD的作用就是分析软件。分析什么？就是要找出验证的关键位置，分析验证机制。清楚了吧，只要有这三兄弟，我们就可以玩破解了。  
[size=18.6667px]  
  
第三、如何找到验证的关键位置  
  
首先我们换位思考下，如果是我们要对自己的软件增加使用验证，我们最简单的做法就是在我们的软件窗口打开之前，增加一个窗口，这个窗口我们叫做验证登陆窗口，必须输入正确的密码后登陆窗口消失、软件使用窗口打开。这个验证登陆窗口怎么实现验证的呢？就是当我们输入密码以后，然后点击登陆按钮，会产生两种结果，成功的结果和失败的结果。假定：如果密码正确，就提示正确信息，比如“恭喜你！”，如果密码错误，就提示错误信息，比如“密码不正确！”。我们破解的目的当然是要获得成功的结果。我们先看一下这个验证流程。获取我们输入的假码——真假码比较——结果。换句话说验证流程可分为三步：验证前、验证中、验证后。这三步，关键位置当然是验证中，这个位置是真假码的比较。如果能直接到达第二步当然是最好，可惜很难直接找到，因为一个程序里面有很多不同的判断。我们要找关键位置是不是必须依靠线索。最直接的线索就是验证后的不同结果。所以我们搞破解，最常用的办法就是通过验证后的结果来反查到关键位置。一种结果是有提示的字符串，比如“成功”“失败”等，我们的破解思路就在程序代码中先定位到这些字符串，然后往前找关键比较代码。如何定位这些字符串呢？OD里面有一个“中文搜索引擎”工具，可以用于查找定位。一种结果是弹出正确或者错误的对话框。你可以搜索对话框里面的字符串，你还可以在程序中定位弹出对话框的代码，然后再反查到关键位置。如何定位弹出对话框呢？编程中弹出对话框要用到一个命令，叫做MessageBox，你在这个函数上下断点，让程序暂停，然后再反查即可。通过结果来反查是我们最主要的做法，对于不同的结果，要用不同的办法。比如有提示字符串，有错误对话框，有窗口，让程序退出等等。最怕的是没有错误结果，那我们就需要从验证前的线索入手了。如果新人觉得不错，就顶一个，我就继续写。