本实验室提出了许多行之有效的代码混淆方法，比如基于3x+1难题的混淆方法，基于异常处理的混淆方法，基于神经网络的混淆方法等。同时也注意到，在代码混淆的实践过程中，混淆点的选择对最终代码保护的效果也有着重要影响。

代码混淆的目的是增大逆向工程的难度。在逆向工程中，无论是自动化分析，还是人工手动分析，关注点都是程序的输入数据。比如污点标记符号执行技术，关注的是被打上污点的输入数据及与之相关的代码；而软件破解，关注的是与注册码等相关的软件使用权验证部分代码。因此从攻击者的角度出发，我们需要对攻击者关注的部分进行混淆，从而提高攻击者的攻击难度。

通过污点标记技术，对攻击者关注的输入数据进行污点标记，可以追踪记录程序中与污点相关的可混淆点。在对程序进行混淆保护时，可以根据污点记录有针对行地对代码进行保护。同时注意到一般安全性高的混淆方法效率相对较低，效率较高的则安全性稍有下降。通过对污点数据进行人工级别划分，级别较高的用安全性较高的混淆方法，级别较低的用效率较高的混淆方法，可以在安全性与效率之间进行合理的平衡。

根据上述方法，完成一套针对C语言的混淆点选择参考软件。该软件输入是C代码与被标记为污点的数据源，输出为被标记为污点的可混淆点，从而帮助代码保护者有针对性地对代码进行混淆保护。