

第 8 章 Visual Basic 程序

 电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY



声明：本电子文档是《加密与解密(第三版)》的配套辅助电子教程！电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：(010) 88254396；(010) 88258888

传 真：(010) 88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

说明：本篇文档是对《加密与解密》第三版“第 8 章 Visual Basic 程序”补充，为了降低书的价格，直接以电子文档提供给图书购买者。

看雪软件安全网站

http://www.pediy.com
kanxue

2008-6-1

8.4 SmartCheck调试工具

SmartCheck 是 NuMega 公司推出的一款针对 Visual Basic 的错误检测和调试工具。它能够自动检测和诊断 VB 运行时的错误，并将一些表达不清楚的错误信息转换为确切的错误描述。实际上，SmartCheck 不仅能分析 VB 程序，也能用来辅助分析其他语言类程序，如 VC 等。SmartCheck 能运行在 Windows 9x/2000/XP 系统上，但与 Windows ME 系统不兼容，不能返回调试信息。

1. 配置

首先运行 SmartCheck，打开上一节的 String.exe 程序。单击菜单“Program/Settings”打开配置对话框。在“Error Detection（错误侦察）”选项上（图 8.2）选取除“Report errors immediately”外的所有选项。

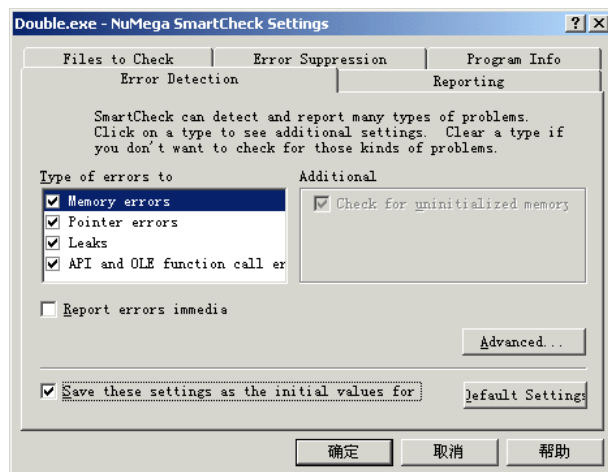


图 8.2 错误侦察

- Report errors immediately: 立即报告错误信息；
- Save these settings as the initial values for new programs: 将当前设置作为默认配置以

适用于新程序。

单击图 8.2 中所示的“Advanced”按钮后，出现图 8.3 所示的选项。

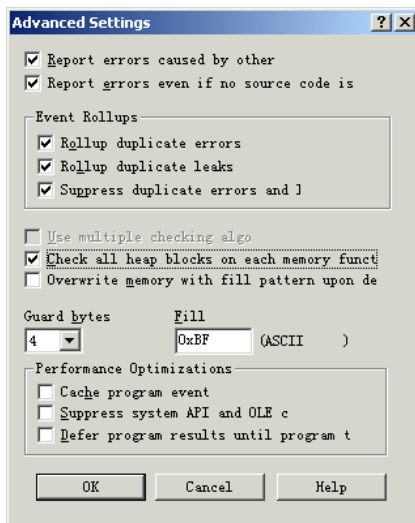


图 8.3 错误侦察高级设置

在“Advanced Settings（高级设置）”对话框上选中前面几项，确保“Suppress system API and OLE calls”未被选上。

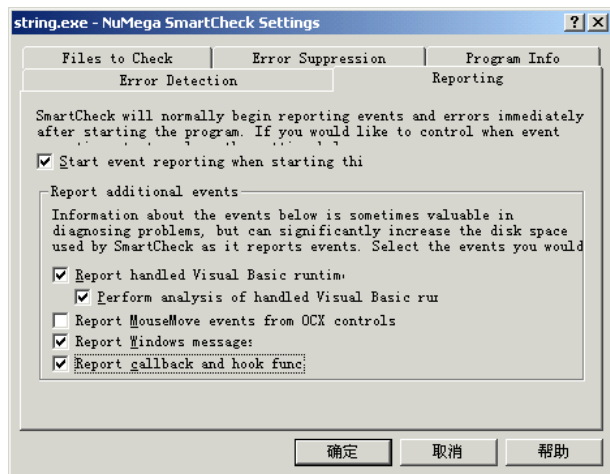



图 8.4 报告清单设置

在“Reporting(报告)”选项卡上，选中除了“Report MouseMove events from OCX controls”外的其余选项，如图 8.4 所示。只有这样配置，SmartCheck 调试 Visual Basic 程序时，才能反馈大量有用的信息。

2. SmartCheck操作

用 SmartCheck 打开光盘实例 String.exe 后，单击菜单“Program/Start”、按 F5 键或单击工具栏上的  按钮装载程序。被调试的程序将在 SmartCheck 环境里运行起来，最后在 SmartCheck

里出现 3 个窗口（见图 8.5）。

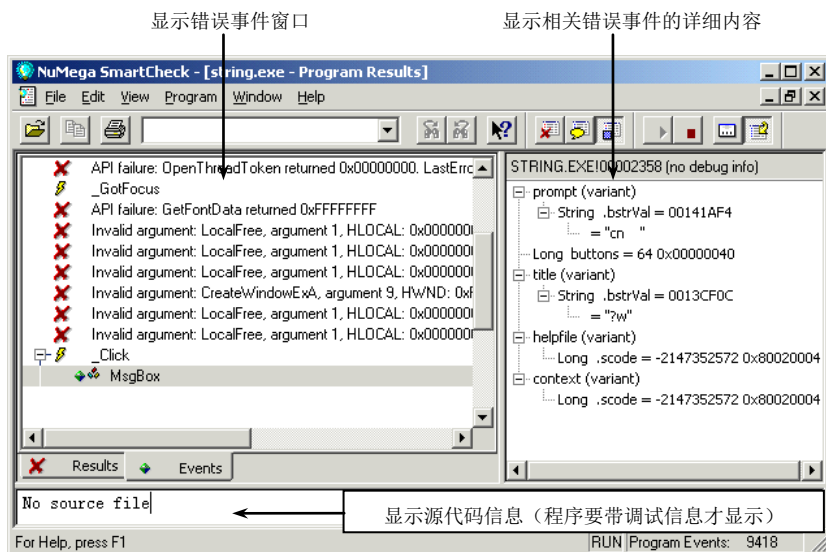




图 8.5 SmartCheck主界面

注意：有时，SmartCheck 只会出现一个主窗口，其他两个消失了，怎么回事呢？原来其

他两个（右边和下边）缩到边上（右边和下边）去了，可用鼠标把它们拖出来。

此时在运行的 String 程序中输入序列号“1212”，该程序将告知序列号错误，然后单击菜单“Program/End”或按  按钮关闭应用程序。

SmartCheck 主窗口中将出现一个单击事件“_Click”，该事件里记录了程序执行的信息。在保证光标在这一行上的情况下，执行 SmartCheck 菜单中的“View/Show All Events”命令或按  按钮，显示所有的调试信息。如果没出现更多的信息，说明 SmartCheck 配置有问题，重新按上文要求配置。

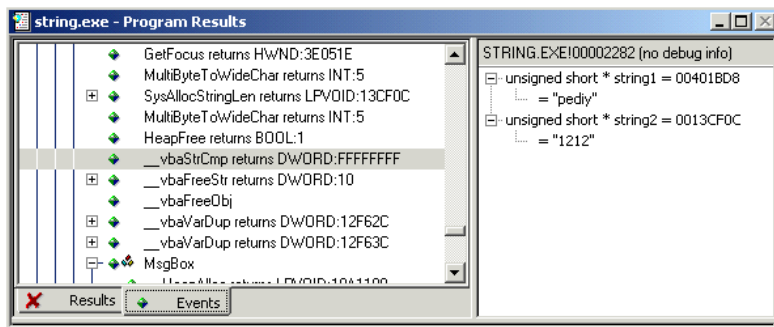


图 8.6 显示详细事件信息

将光标移到“_VbaStrCmp”一行上，将在右窗口中看到详细的调试信息，如图 8.6 所示。String 程序调用了__VbaStrCmp 函数直接比较数据，SmartCheck 将该函数的参数详细信

息显示出来：一个是正确的序列号“pediy”，另一个是输入的序列号“1212”。

3. SmartCheck 常见事件信息

这里将常见的一些 SmartCheck 事件信息含义汇总一下，用粗体表示在 SmartCheck 中显示的内容。

(1) SysAllocStringLen

****.Text 如. Text1.Text

如果单击前面的“+”符号，将看到其他的几行，寻找 SysAllocStringLen

如：SysAllocStringLen(PTR:00000000, DWORD:00000029) returns LPVOID:410584

从文本框中取出键入的字符并放置在内存 00410584 处。

(2) __Vbasrtcmp

Vbasrtcmp(String:"zzzz",String:"yyyy")returns DWORD:0

__Vbasrtcmp 用来比较字符串，例如“zzzz”和“yyyy”的比较。这里可能看到正确序列号和输入字符串比较。returns DWORD:0：是返回值，为 0

(3) __vbafreestr

__vbafreestr(LPBSTR:0063F3F0)

单击上面“+”寻找 SysFreeString

如：SysFreeString(BSTR:00410584)

内存地址 00410584 处的字符串被清除。

(4) __vbaVarCopy

__vbaVarCopy(VARIANT:String:"12345", VARIANT:Empty) returns DWORD:63FA30

单击前面的“+”号寻找 SysAllocStringByteLen

如：

SysAllocStringByteLen(LPSTR:004023F0, DWORD:0000000C) returns LPVOID:4103CC

“12345”被复制到内存 004103CC 中。类似于__vbaVarMove。

(5) Mid

Mid(VARIANT:String:"abcdefg", long:1, VARIANT:Integer:1)

从位置 1 得到字符串“abcdefg”的第一个字符。

(6) SysAllocStringByteLen

单击上面 Mid 下的“+”号寻找 SysAllocStringByteLen

如：

SysAllocStringByteLen(LPSTR:004103F0, DWORD:00000002) returns LPVOID:410434

“a”将被复制到内存 00410434 处。

(7) Asc

```
Asc(String:"T") returns Integer:84
```

得到 “T” 的 ASCII 码的十进制 84。

(8) SysFreeString

```
SysFreeString(BSTR:004103F0)
```

释放 004103F0 处的内存。当单击它们时，在右边窗口将会看到被释放的字符串。此时，正确的序列号和密码有可能在此。

(9) __vbaVarCat

```
vbaVarCat(VARIANT:String:"aa", VARIANT:String:"bb") returns DWORD:63F974
```

连接 “bb” 和 “aa” 以形成 “aabb”。

(10) __vbaFreeVar

```
__vbaFreeVar(VARIANT:String:"abcdefg")
```

单击 “+” 寻找 SysFreeString

例: SysFreeString(BSTR:0041035C)

从内存 0041035C 中释放 “abcdefg”。单击这行，在右边可能会发现所要的东西。

(11) __vbaVarTstEq

```
vbaVarTstEq(VARIANT:****, VARIANT:****) returns DWORD:0
```

__VbaVarTstEq 通常用来比较变量。如果它们不一样，DWORD=0 (EAX=0)；如果它们一样，DWORD 将为 FFFFFFFF (EAX=FFFFFFFF)。类似于 __vbaVarCmpEq。

(12) Len

```
Len(String:"PEDIY") returns LONG:5
```

得到字符串 “PEDIY” 的长度为 7。

(13) ****.Text

```
****.Text <-- "Wrong! Try Again!!" (String)
```

在文本框中显示 “Wrong! Try Again!!”。

(14) __vbaVarAdd

```
vbaVarAdd(VARIANT:Integer:2, VARIANT:Integer:97) returns .....
```

2+97=99，返回 99。

(15) __vbaVarDiv

```
vbaVarDiv(VARIANT:Integer:97, VARIANT:Long:1) returns.....
```

97 除以 1。

(16) __vbaVarMul

```
vbaVarMul(VARIANT:String:"1", VARIANT:String:"2") returns ...
```

1 乘 2。

(17) __vbaVarSub

```
vbaVarSub(VARIANT:String:"2", VARIANT:String:"34") returns ...
```

“34” - “2”，返回 32。

(18) MsgBox

```
MsgBox(VARIANT:String:"Welcome www.pediy.com", Integer:0,  
VARIANT:String:"Hello!", VARIANT:.....)
```

创建一个消息框，标题是“Hello”，内容为“Weclome www.pediy.com”。