Microsoft

Visual Studio 2005 安全性增强

蔺华
ISV开发合作经理
平台及开发合作部
微软（中国）有限公司

msdn

Microsoft

您最担心的安全问题是什么?

#1 回答

“提高代码安全性的软件工具”

msdn

关于开发人员安全性的一些数据

Microsoft

- “75%的攻击都发生在应用程序中。” - *Gartner “Security at the Application Level”*
- “2003年CERT 组织发出的13个安全建议中的11个安全问题是发生在应用程序中，而不是操作系统里面。” - *Carnegie Mellon University*
- “如果50%的软件漏洞能够在发生之前解决的话，成本将减少75%。” - *Gartner “Security at the Application Level”*
- “在黑客和安全专家之间的战场已经有网络层转向到Web应用。" - *Network World*
- “64%的开发人员都对自己开发安全应用的能力不够自信。” - *Microsoft Developer Research*

msdn

Microsoft

```
// Example #1
#define MAX (50)
char szDest[MAX];
strncpy(szDest,pszSrc,strlen(pszSrc));
```

Wrong buffer size!

```
// Example #2
#define MAX (50)
char szDest[MAX];
strncpy(szDest,pszSrc,MAX);
pszDest[MAX] = '\0';
```

Wrote NULL to element 51, not 50!

```
// Example #3
string strQry = "SELECT
Count(*) FROM Users
WHERE UserName='" +
txtUser.Text + "' AND
Password='" +
txtPassword.Text + "'";
```

SQL Injection!

Or 1=1 --

➔SELECT Count(*) FROM Users WHERE UserName='' Or 1=1 --' AND Password=''
➔SELECT Count(*) FROM Users WHERE UserName='' Or 1=1
➔True

msdn

Microsoft

```
string Status = "No";
string sqlstring ="";
try {
    SqlConnection sql= new SqlConnection(
        @"data source=localhost;" +
        "user id=sa;password=password;");
    sql.Open();
    sqlstring="SELECT HasShipped" +
        " FROM Shipment WHERE ID='" + Id + "'";
    SqlCommand cmd = new SqlCommand(sqlstring,sql);
    if ((int)cmd.ExecuteScalar() != 0)
        Status = "Yes";
} catch (SqlException se) {
    Status = sqlstring + " failed\n\r";
    foreach (SqlError e in se.Errors) {
        Status += e.Message + "\n\r";
    }
} catch (Exception e) {
    Status = e.ToString();
}
```

Connecting as sysadmin

Hard to guess password!

String concat for dynamic SQL

Telling the bad guy too much on failure

msdn

Visual Studio Team System

Microsoft

Process and Architecture Guidance

Visual Studio Industry Partners

VSTE for Software Architects

- Application Designer
- Logical Datacenter Designer
- Deployment Designer

VSTE for Software Developers

- Dynamic Code Analyzer
- Static Code Analyzer
- Code Profiler
- Unit Testing
- Code Coverage

VSTE for Software Testers

- Load/Web Testing
- Manual Testing
- Test Case Management

- Class Modeling
- Visio and UML Modeling
- Team Explorer + CAL
- Visual Studio Professional

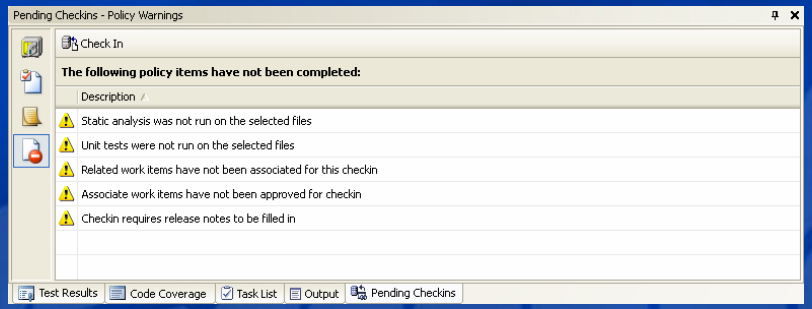
Visual Studio Team Foundation

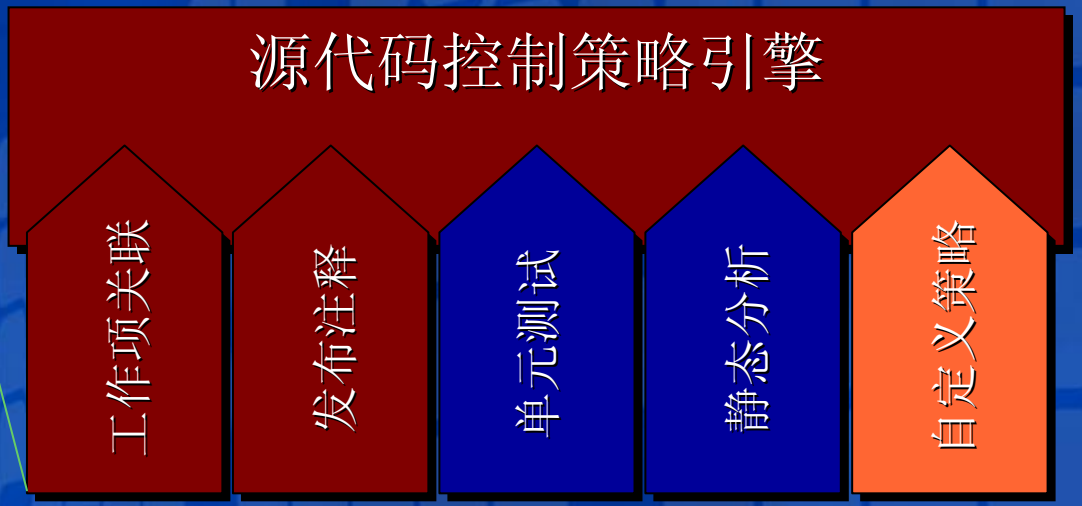
- Change Mgmt – SCC
- Reporting
- Integration Services
- Build Server
- Work Item Tracking
- Project Site
- Project Management

msdn

创建项目策略

- 用VSTS围绕测试来创建项目策略



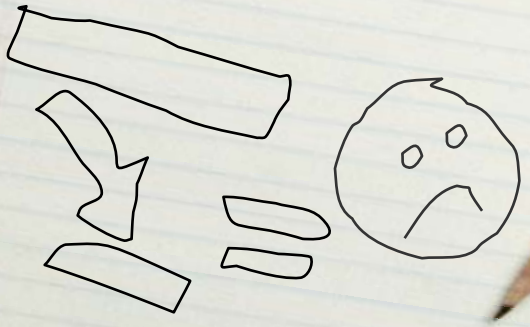


策略定义
- .NET 程序集
- 返回的通过、失败及其消息
- 客户的可扩展性
- 用户的可重载性

Microsoft

听听我们客户怎么说的

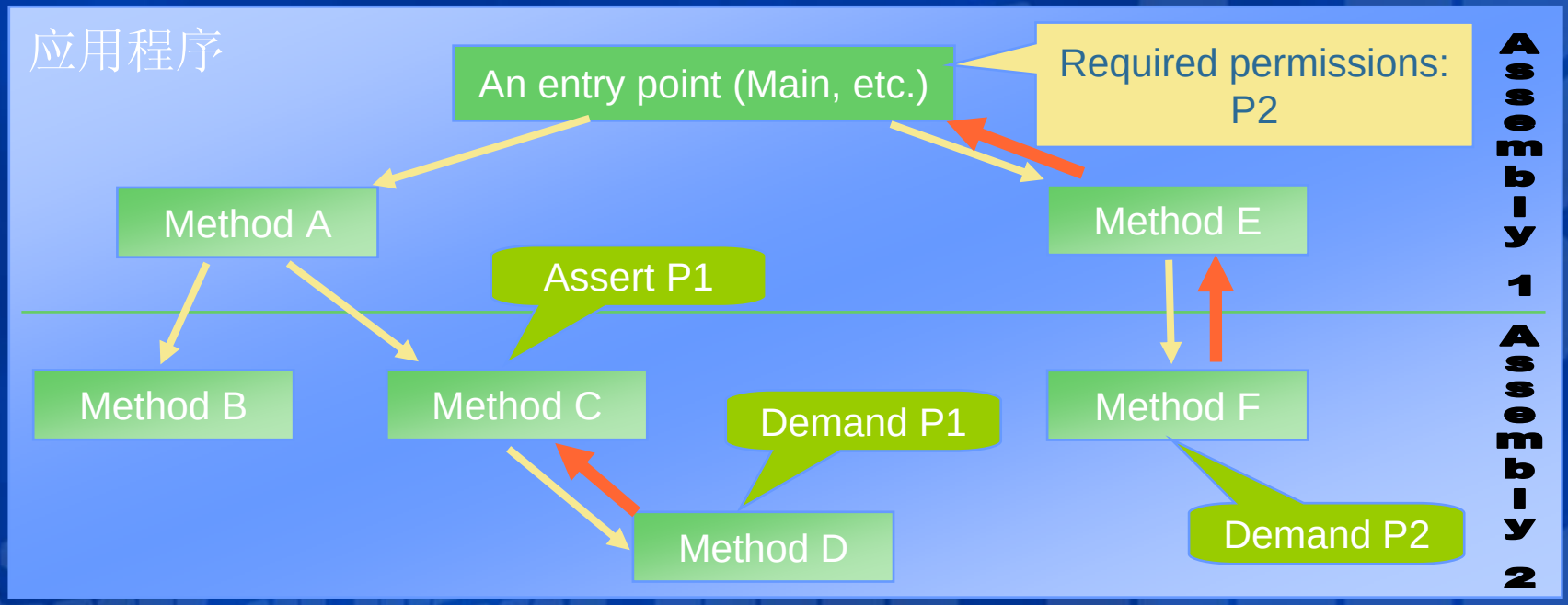
- “我有一个复杂应用。为什么就没有一个工具帮我找出我应用的最小安全需求呢？”
- “我经常需要写一个不需要全部信任的应用，但是就没有一个比较简单的方式来测试和调试这样的应用。”



msdn

权限许可计算器

- 检查应用的安全性需求
- 针对调用的**API**做静态分析和检查
  - 返回每个函数库**API**的权限集
- 输出运行该应用所需要的最小权限许可集

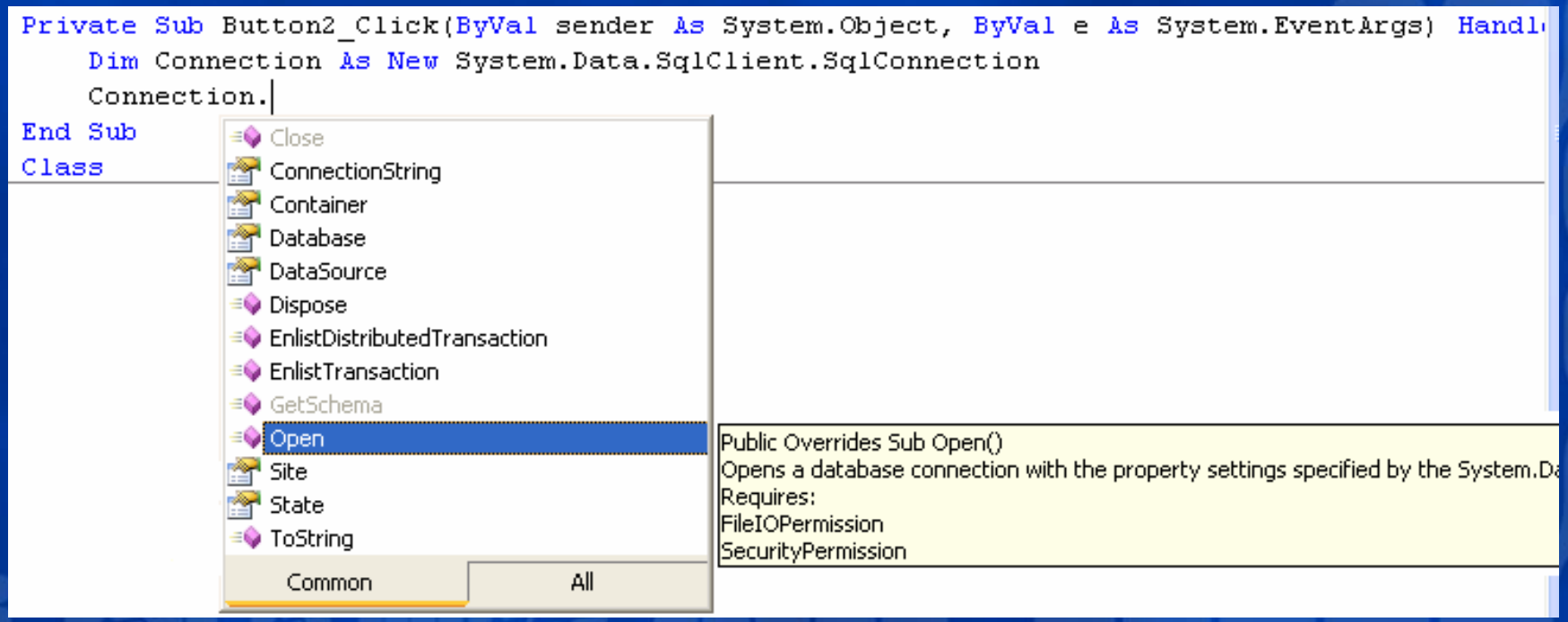


编写部分信任应用

- 用最小权限来开发和调试
  - 如果要开发一个权限很小的应用，那就需要用最小权限的帐户来登录进行开发。
- 代码访问安全性
  - 让开发者编写托管代码来运行有自定义权限的沙盒中的代码

智能感知——防范于未然

- 设定一个区域
- 把智能感知列表中可能违反安全设置的项目灰掉
- 让开发者在写代码之前就了解安全隐患



VB.NET My Classes

Microsoft

- 用最简单的方式来提供函数
  - My.User.IsAuthenticated
  - My.User.CurrentPrincipal.Identity
  - My.User.IsInRole
  - My.User.Name

msdn

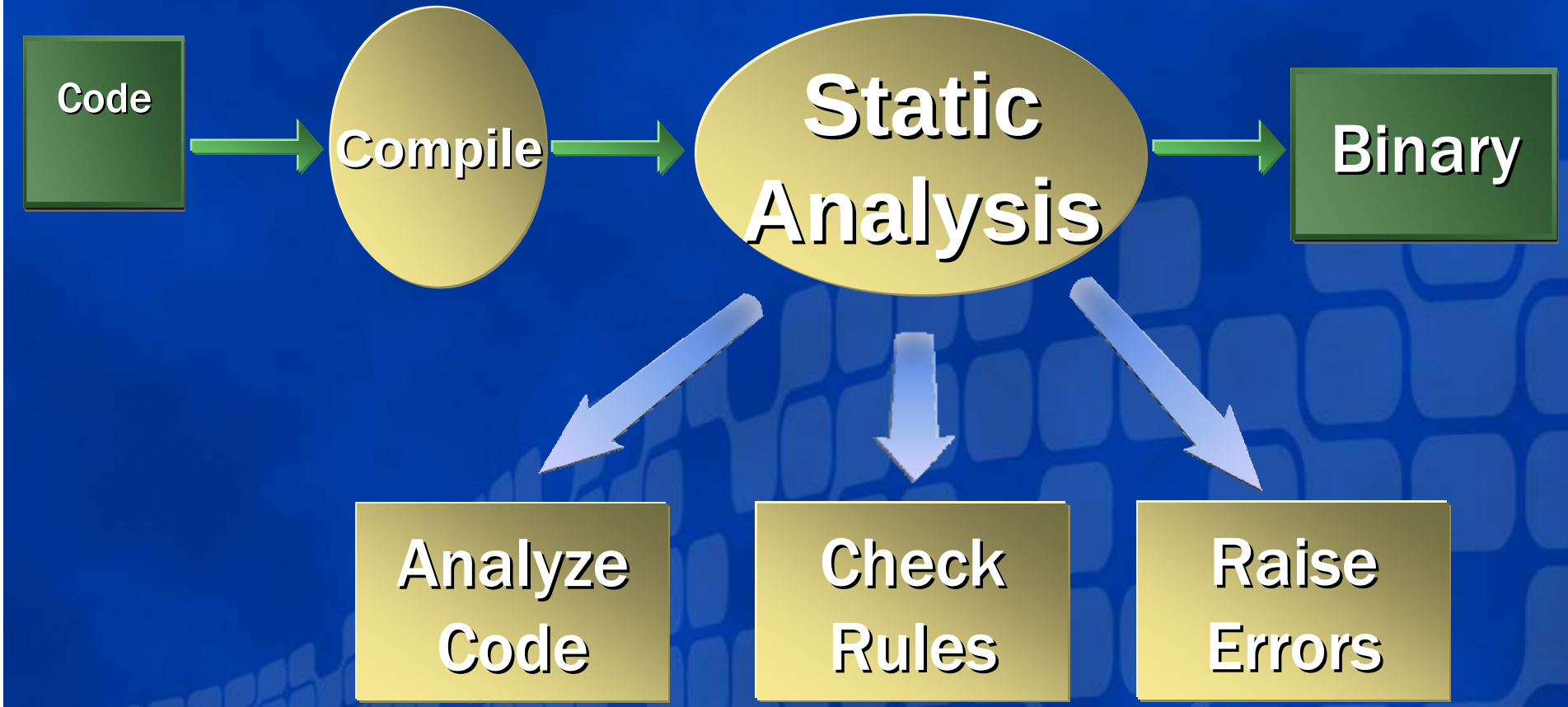
数据保护 API

Microsoft

- 内建到 .NET Framework 2.0中
- 更加容易来保护数据
- 充分利用Win 2K及以上版本的潜在特性
  - 添加 System.Security.dll 引用
  - 使用System.Security.Cryptography
  - ProtectedData 类
  - ProtectedMemory 类
  - Protect 方法
  - Unprotect 方法

msdn

静态分析


Code
Compile
Static Analysis
Binary
Analyze Code
Check Rules
Raise Errors

静态分析工具

Microsoft

- PREfast
  - 扫描那些用C/C++来构建的应用的安全性缺陷
    - 如:
      - Buffer overruns （缓冲区溢出）
      - 未初始化的内存
      - 内存泄露

msdn

静态分析工具

Microsoft

- FxCop
  - 能扫描托管代码的200多种缺陷
    - 如:
      - SQL injection
      - 权限许可
      - 指针
  - 可以自定义规则

msdn

更加安全的C/C++运行库

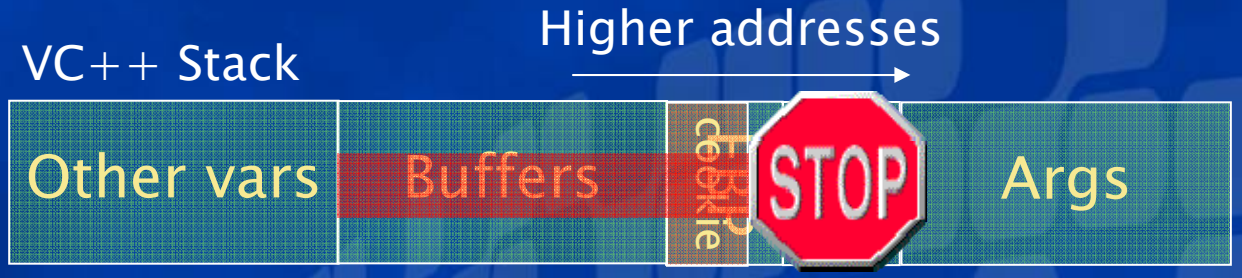
Microsoft

- 为了更安全的使用C/C++运行库
- 复查了2000 多个C/C++ 库函数
- 默认对不安全的函数提出警告
  - #define _CRT_SECURE_NO_DEPRECATE
- 创建了大约 400 更安全的变体函数
  - strcpy -> strcpy_s
- 增加了参数验证机制
  - _invalid_parameter_handler
  - Release:自动调用 Windows Error Reporting; Debug: Assert.
- 所有 VS和C++ 库都在使用SaferCRT

msdn

/GS 开关

- /GS 开关
  - 用来降低缓冲区溢出的发生率
  - 曾经用来编译 **Windows XPSP2** 和 **Windows Server 2003**
  - 默认打开



Application Verifier

Microsoft

- 主要检测应用安全性和质量相关的问题：
  - heap corruption
  - handle
  - locks
- 使得：
  - 更好的软件质量
  - 增强的安全性
  - 减少调试时间
- 主要适用于非托管代码

msdn

集成的Bug跟踪

- 轻松的整合到开发过程中
- 设计你自己的流程 – Fields, Forms, States, Rules
- 可扩展的链接 – bugs, reports, artifacts
- 提醒

代码覆盖和压力测试

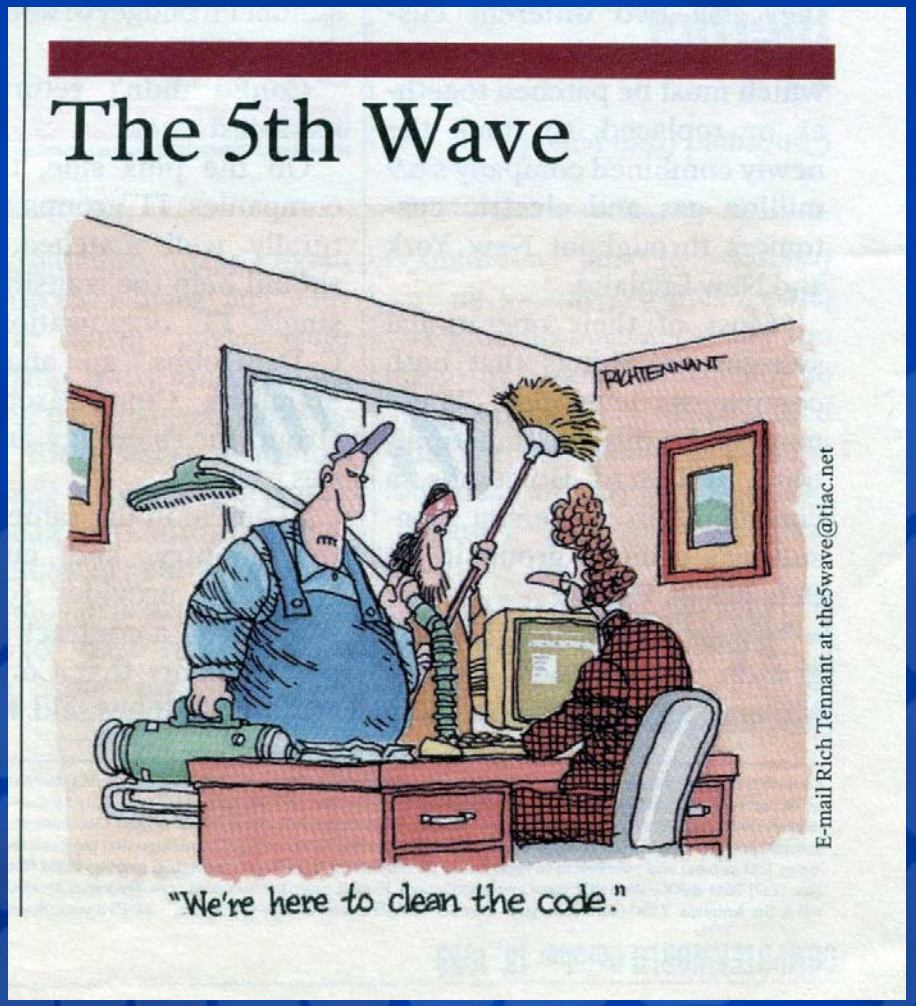
Microsoft

- 代码覆盖
  - 代码覆盖分析
  - 让开发团队清楚地了解已经测试了多少代码和那些代码，使得集中精力在最薄弱的环节成为可能。
- 负载/压力测试
  - 经常只在服务器在承受压力/负载的时候才暴露缺陷
  - Web应用一般都需要进行负载/压力测试

msdn

总而言之

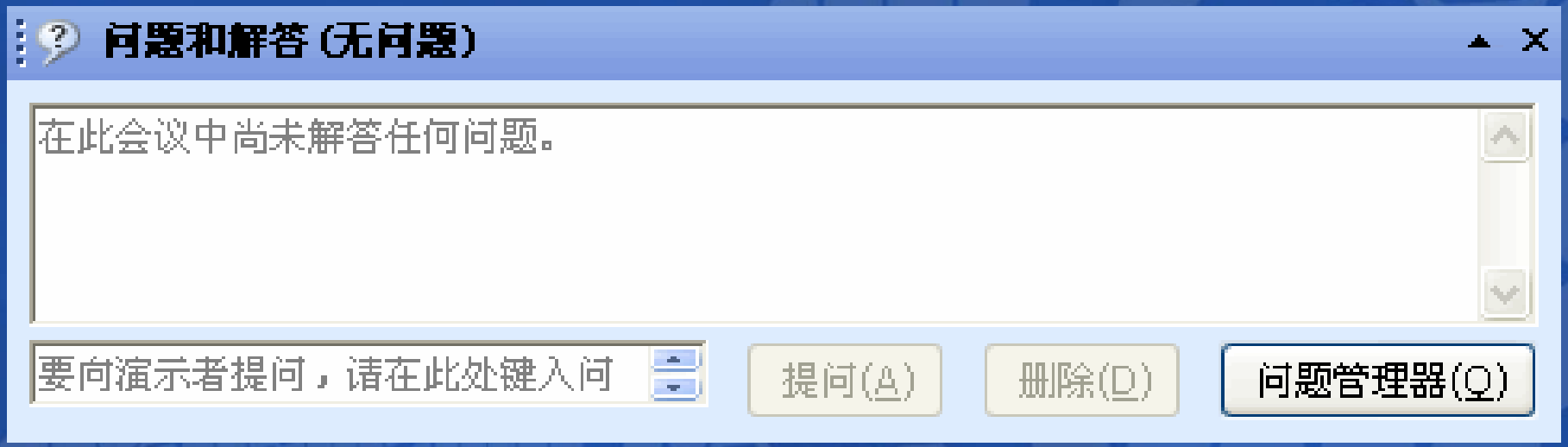
- 安全性依旧是个问题
- 人，流程，和工具
- Visual Studio 2005 将用创新的工具和功能帮助你编写更加安全的代码



http://msdn.microsoft.com/security

Question & Answer

如需提出问题，请单击“提问”按钮并在随后显示的浮动面板中输入问题内容。一旦完成问题输入后，请单击“提问”按钮。




Microsoft
Microsoft
Your potential. Our passion.™
msdn