DevInspect for .NET QuickStart Guide

HP DevInspect is an easy and accurate tool for finding and fixing application security defects. It enables developers to build secure Web applications and services quickly and easily, without impacting schedules or requiring security expertise. DevInspect is the only developer security product that:

- Finds security vulnerabilities through hybrid analysis techniques that combine source code analysis and black box testing for unmatched accuracy.
- Automatically fixes security vulnerabilities in application code and configuration with SecureObjects vulnerability remediation technology.
- Protects applications in production by preventing malicious input, detecting attacks in real time and informing operations teams of attack attempts.
- Provides regular updates of vulnerability checks and information from expert security researchers.
- Integrates with Microsoft Visual Studio and Visual Studio Team System.
- Allows you to scan remote Web sites as well as those under development.

System Requirements

Before installing DevInspect, make sure that your system meets the following minimum requirements:

- English-language version of Windows XP SP2 or Windows Server 2003 SP1
- 1 GB of RAM
- 150 MB of free disk space (2 GB preferred)
- 1 GHz processor or better
- Microsoft Visual Studio 2005 Standard (or better) or Microsoft Visual Studio 2008 Standard (or better)
- Microsoft .NET Framework 2.0
- Microsoft SQL Server Express
- Screen resolution: 800 x 600 minimum (1024 x 768 preferred)

Getting Started

This Quick Start guide shows you how to begin using DevInspect for .NET as soon as you install the product.

Step 1: Install DevInspect

Install DevInspect on the Windows XP or Windows Server 2003 PC where you currently use Visual Studio. Close Visual Studio before installing.

Step 2: Open DevInspect Explorer

Start Visual Studio. Select **DevInspect Explorer** from the **View** menu.

Before proceeding, ensure that you have obtained a license key from HP. If necessary, call 866-774-2700.

Step 3: Enter an Activation Key

If you are requesting a trial version:

1. Click the Visual Studio **Tools** menu and select **Options**.
2. Expand the HP DevInspect node and select **Licensing**.
3. Complete all fields in the **Personal Information** section.
4. Click **Request Trial**.

   Upon receiving your request, HP will send you an e-mail containing an activation key. Return to this Licensing Options page and follow the instructions below.

If you have received an activation key:

1. In the **Activation Key** box, enter the activation (license) key provided to your organization by HP.
2. In the **License Service** box, enter the fully qualified URL of the licensing service. The default is https://licenseservice.spidynamics.com.
3. Click **Update License**.

Step 4: Analyze Web Application

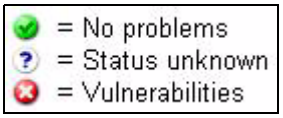
Once you have activated your installation, you are ready to find and fix your Web application's security vulnerabilities.

1. Open a Web site or Web application project.
2. On the DevInspect Explorer toolbar, click the Analyze Selected Web Site/Project icon  . You may optionally analyze individual pages by right-clicking an item in DevInspect Explorer and selecting **Analyze**.

DevInspect performs a security analysis of your entire application or site.

Step 5: Review Vulnerabilities

Once the security analysis is complete, DevInspect Explorer displays the security status of each resource in your site or project. The icons indicate each component's status, as shown by the key illustrated below.



All errors and warnings are displayed in the Error List. Right-click a vulnerability and select **Vulnerability Summary** to view detailed description, risk and remediation information in the Vulnerability Viewer.

Step 6: Fix Vulnerabilities

DevInspect's SecureObjects vulnerability remediation technology enables you to automatically fix many of the vulnerabilities that DevInspect finds.

1. Click the **Error List** tab.
2. Right-click an item in the Error List and select **Fix Vulnerability** to display the proposed changes.
3. Click either **Apply** (to accept the changes) or **Cancel** (to reject the modifications).
4. After applying changes, reanalyze the page or application to verify that the vulnerability no longer exists.