DevInspect for Java QuickStart Guide

DevInspect simplifies security for developers by finding application security defects and advising how to eliminate them. This enables you to build secure Web applications and Web services quickly and easily, without impacting schedules or requiring extensive knowledge of Web application security.

DevInspect is the only developer security product that finds security vulnerabilities through hybrid analysis techniques that combine dynamic, static and configuration analysis approaches for unmatched accuracy and precision.

You can scan all or part of your dynamic Web project, multiple Web projects, or remote Web sites.

System Requirements

- Windows XP SP2
- 1 GB of RAM
- 1.2 GB of free disk space required (2 GB preferred)
- 1 GHz processor or better
- Microsoft .NET Framework 2.0
- Microsoft SQL Server 2005 Express Edition SP1 (note that Express Edition must be installed even if other SQL Server 2005 versions are present)
- For plug-in versions: Eclipse 3.2 or above, Rational Software Development Platform 6 or 7.

Getting Started

The DevInspect 5.0 for Java installation package is a single executable that you can obtain from the path specified in the e-mail message you received from HP. DevInspect can be installed in the following configurations:

- Standalone - Installs Eclipse with the DevInspect features built in. You can choose this option no matter what Java IDE you are using, even if Eclipse is already installed. This includes a full Eclipse 3.3 with WTP 1.5.
- Eclipse plug-in - Installs DevInspect features into an existing installation of Eclipse 3.2 or higher. You must allocate at least one gigabyte of RAM for the maximum heap size used by Eclipse applications. To do so, simply add the following parameter to the eclipse.ini file: -Xmx1024m.
- IBM Rational Software Development Platform plug-in - Installs DevInspect features into an existing installation of IBM Rational Software Development Platform 6 and 7 products, including Rational Application Developer, Web Developer and Software Architect.

Install Using Installation Program

Double-click on the installation package and follow the instructions. The installer will place DevInspect in the following locations.

Program files:
C:\Program files\SPI Dynamics\DevInspect for Java

Scan files and logs:
C:\Documents and Settings\ <username> \Application Data\SPI Dynamics\DevInspect\Eclipse\5.0

Install Using HP Application Security Center Update Site

DevInspect can also be installed from within your existing Eclipse installation through the HP Update Site if you are choosing the Eclipse or IBM Rational Software Development Platform plug-in options.

1. Click **Help** > **Software Updates** > **Find and Install**.
2. On the Install/Update dialog, select **Search for new features to install** and click **Next**.
3. Click **New Remote Site**.
4. On the New Update Site dialog, in the **Name** box, enter HP Update Site.
5. In the **URL** box, enter one of the following, depending on your target Eclipse platform:

   Eclipse 3.2:
   http://updates.spidynamics.com/eclipse/eclipse-3.2/site.xml

   Eclipse 3.3:
   http://updates.spidynamics.com/eclipse/eclipse-3.3/site.xml

   RSDP6:
   http://updates.spidynamics.com/eclipse/RSDP6/site.xml

   RSDP7:
   http://updates.spidynamics.com/eclipse/RSDP7/site.xml

6. Click **OK** and make sure only **HP Application Security Center** is checked in the **Sites to include in search** list.
7. Click **Finish**.
8. On the Search Results panel, select DevInspect for Java (<target>) <version>, where <target> is your platform and <version> is the latest version number.
9. Click **Next** and follow the on-screen instructions to complete the installation.

Note: When you install from the update site, the Eclipse Update Manager automatically downloads and installs .NET Framework 2.0 and SQL Server 2005 Express Edition, if needed.

Running DevInspect

The first time you run DevInspect, you will need to activate the product with the license provided to you by HP, using the following procedure:

1. Activate DevInspect.
   a. Start DevInspect for Java.
   b. On the Welcome page, select **Go to Workbench**.
   c. Click **Window** > **Preferences**.
   d. Expand the **Web Application Security** group.
   e. Click **Licensing**.
   f. Enter the activation key provided to you and enter all personal information.

g. Confirm the license service URL as https://licenseservice.spidynamics.com/service.asmx

h. Click **Apply** to activate the product.

2. Connect to AMP (Optional)

   Follow the steps below if your license requires or permits you to access the HP Assessment Management Platform (AMP):

   a. In the list of Web Application Security preferences, click **AMP Connectivity**.

   b. Enter the URL or IP address of the AMP server.

   c. Enter a user name and password.

   d. Click **Test Connection**.

   e. In the list of Web Application Security preferences, click **Policy**.

   f. Select a policy from the list downloaded from AMP.

3. Configure the Server

   DevInspect's hybrid analysis requires a local development server to be controlled from within the Eclipse development environment. Any Java application server is supported and is simply configured as a server runtime in Eclipse. The following example demonstrates how to configure DevInspect to use a local Tomcat server:

   a. On the Preferences window, expand the **Server** group and select **Installed Runtimes**.

   b. Click **Add**.

   c. On the New Server Runtime window, choose **Apache Tomcat v5.5** and click **Next**.

   d. Select an installation directory (C:\Program Files\Apache Software Foundation\Tomcat 5.5) and click **Finish**.

   e. Click **OK** to close Preferences.

   f. Click **Window** > **Open Perspective**> **J2EE**.

4. Import your Project

   If you have your application source code in the Eclipse workspace, DevInspect can perform hybrid analysis, combining the depth of source code analysis with the accuracy of black box testing. To perform black box testing only, skip this step. If you are not currently using Eclipse, you can import the code manually from the file system, WAR or EAR files. To import an existing Eclipse project, follow these steps.

   a. Click **File** > **Import**

   b. Expand the **General** group and select **Existing Projects into Workspace**.

   c. Select the root directory or archive file of your existing Eclipse project. The project will then be available in the Project Explorer.

   d. In the Servers window at the bottom of the Workbench, right-click the Tomcat server entry and select **Add and Remove Projects**.

   e. Select your project and click **Add**.

   f. Click **Finish**.

   g. Right-click the Tomcat server entry again and select **Publish**.

   h. Right-click the Tomcat server entry again and select **Start** to start the server.

You are now ready for testing.

Test for Vulnerabilities

To test your local project with hybrid analysis:

1. Click the DevInspect icon on the toolbar or click the **DevInspect** menu and select **Test for Vulnerabilities**.

2. Select **Choose targets to test**, select your application from the list, and click **OK**.

3. As your security analysis runs, you will see vulnerabilities populated to the Problems window. Analysis progress is displayed in the Console window.

4. Right-click a vulnerability in the Problem window and select **Explain Vulnerability** for detailed vulnerability information.

To test a remote server or conduct a black box only test:

1. Add the target host as an Allowed Host in DevInspect preferences. All hosts not explicitly enabled in the Allowed Host configuration will be ignored so that DevInspect does not attack external sites. Your DevInspect license must also allow access to the IP address that you are targeting.

2. Click the DevInspect icon on the toolbar or click the **DevInspect** menu and select **Test for Vulnerabilities**.

3. Select **Test a specific target URL** and enter the URL.

4. Click **OK**.

Other Areas to Explore

After configuring the environment and running an initial security analysis, you can explore these other areas of DevInspect:

- Generate vulnerability reports from the security analysis results: Select **DevInspect** > **Generate Report**.
- Configure advanced security analysis settings: Select **Window** > **Preferences** > **Web Application Security**.

Update the Application

DevInspect allows you to check for updates on demand via a Web service that keeps DevInspect current with HP vulnerability research. To update vulnerability tests, click **DevInspect** > **Tools** > **SmartUpdate**.

DevInspect for Java uses the Eclipse Update Manager to distribute updates to the product features. To check for DevInspect feature updates, or if you receive notification from HP that a new release is available, follow these steps:

- Click **Help** > **Software Updates** > **Manage Configuration**.
- In the Product Configuration dialog, select DevInspect for Java.
- In the right-hand pane, select **Scan for Updates**.
- If updates are found, follow the on-screen instructions to upgrade to the latest version of DevInspect.