SAP NetWeaver Application Server, add-on for code vulnerability analysis

Features

The SAP NetWeaver AS, add-on for code vulnerability analysis (code vulnerability analyzer) is an ABAP program which allows to search for potential security vulnerabilities in ABAP source code. Using its built-in dataflow detection logic, the code vulnerability analyzer will be able to reduce the number of found false positives by eliminating findings where the data used in potentially dangerous expressions is coming from safe sources. Although the code vulnerability analyzer can be used standalone or via the SAP CodeInspector, it is recommended to be used solely via the ABAP Test Cockpit (ATC), as for instance exemptions can be used only with ATC.

The tool comes with extensive documentation, assisting a developer to fix the findings reported by the tool. The navigation support in ATC was improved to not only allow navigation to the potentially vulnerable statement but also to code identified by the dataflow logic as manipulating the input to the potentially vulnerable statement.

The code vulnerability analyzer is a separate licensed feature which is disabled by default.

The product is available with:
- SAP NetWeaver AS ABAP 7.0 EhP2 Support Package 14
- SAP NetWeaver AS ABAP 7.0 EhP3 Support Package 09
- SAP NetWeaver AS ABAP 7.3 EhP1 Support Package 09
- SAP NetWeaver AS ABAP 7.4 Support Package 05

Usage scenarios

By utilizing the code vulnerability analyzer, you can check development objects for security vulnerabilities like

- SQL Injections
- ABAP Code Injections
- OS Command Injections
- Insufficient protection against directory traversal attacks
- Backdoors
- Missing or incorrect authorization checks

Related Tools

ABAP Test Cockpit: The ABAP Test Cockpit (ATC) is an ABAP check toolset which allows running static checks and unit tests for your ABAP development objects.

Code Inspector: The Code Inspector is a tool for checking static ABAP coding and DDIC objects, also allowing customers to execute own checks (transaction SCI)

Extended syntax check: The extended syntax check performs complex source code analyses for one single program (transaction SLIN)

Related Documents

SAP Note 1697494 - Customer Code Scans

SAP Note 1921820 - SAP NetWeaver AS, add-on for code vulnerability analysis - support package planning

Blog: ABAP Security at TechEd 2013 - Scan, Analyze, and Fix Your Programs!

SAP Insider: Start your applications on solid ground

Security Guidelines for Best-Built Applications