Secrets
ABAP
Apex
C
C++
CloudFormation
COBOL
C#
CSS
Flex
Go
HTML
Java
JavaScript
Kotlin
Kubernetes
Objective C
PHP
PL/I
PL/SQL
Python
RPG
Ruby
Scala
Swift
Terraform
Text
TypeScript
T-SQL
VB.NET
VB6
XML

T-SQL static code analysis

Unique rules to find Bugs, Vulnerabilities, Security Hotspots, and Code Smells in your T-SQL code

All rules 80 | Vulnerability 1 | Bug 16 | Security Hotspot 4 | Code Smell 59

Tags

Search by name...

Track uses of "FIXME" tags
Code Smell

Redundant pairs of parentheses should be removed
Code Smell

Functions and procedures should not have too many parameters
Code Smell

Collapsible "if" statements should be merged
Code Smell

Unused labels should be removed
Code Smell

Using hardcoded IP addresses is security-sensitive
Security Hotspot

Column references should not have more than two-parts
Code Smell

Triggers should not "PRINT", "SELECT", or "FETCH"
Code Smell

"LIKE" clauses should not be used without wildcards
Code Smell

Jump statements should not be redundant
Code Smell

"CATCH" clauses should do more than rethrow
Code Smell

Track uses of "FIXME" tags

Analyze your code

Code Smell | Major | cwe

`FIXME` tags are commonly used to mark places where a bug is suspected, but which the developer wants to deal with later.

Sometimes the developer will not have the time or will simply forget to get back to that tag.

This rule is meant to track those tags and to ensure that they do not go unnoticed.

Noncompliant Code Example

```
CREATE TABLE notnull(col1 INTEGER NOT NULL)
INSERT notnull VALUES (@value) -- FIXME ensure @value is not null
```

See

- MITRE, CWE-546 - Suspicious Comment

Available In:

sonarlint | sonarcloud | sonarqube Developer Edition

© 2008-2022 SonarSource S.A., Switzerland. All content is copyright protected. SONAR, SONARSOURCE, SONARLINT, SONARQUBE and SONARCLOUD are trademarks of SonarSource S.A. All other trademarks and copyrights are the property of their respective owners. All rights are expressly reserved.
Privacy Policy