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

PL/SQL static code analysis

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

| All rules 188 | 🔒 Vulnerability ④ | 🐛 Bug ㊺ | 🛡 Security Hotspot ② | ☢ Code Smell 137 |

Tags ⌄

Search by name...

"LIKE" clauses should not start with wildcard characters
☢ Code Smell

Column names should be used in a SQL "ORDER BY" clause
☢ Code Smell

Procedures and functions should be documented
☢ Code Smell

SQL statements should not join too many tables
☢ Code Smell

Function and procedure names should comply with a naming convention
☢ Code Smell

Columns to be read with a "SELECT" statement should be clearly defined
☢ Code Smell

"CASE" structures should not have too many "WHEN" clauses
☢ Code Smell

Deprecated LONG and LONG RAW datatypes should no longer be used
☢ Code Smell

Sections of code should not be commented out
☢ Code Smell

Unused procedure and function parameters should be removed
☢ Code Smell

SQL EXISTS subqueries should not be used
☢ Code Smell

"LIKE" clauses should not start with wildcard characters

Analyze your code

☢ Code Smell   🔺 Major ⑦   🏷 performance sql

When the value of a `LIKE` clause starts with '%' or '_', indexes on the searched column are ignored, and a full table scan is performed instead.

Noncompliant Code Example

```
SELECT FIRST_NAME, LAST_NAME FROM PERSONS
WHERE LAST_NAME LIKE '%PONT'
```

Available In:

sonarlint | sonarcloud | sonarqube Developer Edition