

PL/SQL













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...

 Code Smell	
Track uses of "TODO" tags	
 Code Smell	
Neither DES (Data Encryption Standard) nor DESede (3DES) should be used	
 Vulnerability	
"SYNCHRONIZE" should not be used	
 Bug	
Global public variables should not be defined	
 Code Smell	
A primary key should be specified during table creation	
 Code Smell	
Track lack of copyright and license headers	
 Code Smell	
SHA-1 and Message-Digest hash algorithms should not be used in secure contexts	
 Vulnerability	
Sensitive "SYS" owned functions should not be used	
 Vulnerability	
"FORMS_DDL('COMMIT')" and "FORMS_DDL('ROLLBACK')" should not be used	
 Bug	
"DBMS_OUTPUT.PUT_LINE" should not be used	
 Code Smell	
"WHEN OTHERS" should not be the only exception handler	
 Code Smell	

Track uses of "TODO" tags

Analyze your code

 Code Smell
  Info
 
 cwe

TODO tags are commonly used to mark places where some more code is required, but which the developer wants to implement 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.

See

- MITRE, CWE-546 - Suspicious Comment

Available In:

sonarlint  | **sonarcloud**  | **sonarqube**  Developer Edition