

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...

<div>  Code Smell </div> <div> SHA-1 and Message-Digest hash algorithms should not be used in secure contexts </div> <div>  Vulnerability </div>	<div>  Vulnerability  Critical  </div> <div> <p>The MD5 algorithm and its successor, SHA-1, are no longer considered secure, because it is too easy to create hash collisions with them. That is, it takes too little computational effort to come up with a different input that produces the same MD5 or SHA-1 hash, and using the new, same-hash value gives an attacker the same access as if he had the originally-hashed value. This applies as well to the other Message-Digest algorithms: MD2, MD4, MD6, HAVAL-128, HMAC-MD5, DSA (which uses SHA-1), RIPEMD, RIPEMD-128, RIPEMD-160, HMACRIPEMD160.</p> <p>Consider using safer alternatives, such as SHA-256, SHA-512 or SHA-3.</p> </div> <div> Noncompliant Code Example </div> <div> <pre>DBMS_CRYPTO.Hash(str, HASH_MD4); DBMS_CRYPTO.Hash(str, HASH_MD5); DBMS_CRYPTO.Hash(str, HASH_SH1);</pre> </div> <div> See </div> <div> <ul style="list-style-type: none"> OWASP Top 10 2017 Category A6 - Security Misconfiguration MITRE, CWE-328 - Reversible One-Way Hash MITRE, CWE-327 - Use of a Broken or Risky Cryptographic Algorithm SANS Top 25 - Porous Defenses SHAttered - The first concrete collision attack against SHA-1. </div> <div> Deprecated </div> <div> <p>This rule is deprecated; use {rule:plsql:S4790} instead.</p> </div> <div> <div>Available In:</div> <div>    <div>Developer Edition</div> </div> </div>
<div>  Code Smell </div> <div> Sensitive "SYS" owned functions should not be used </div> <div>  Vulnerability </div>	
<div>  Bug </div> <div> "FORMS_DDL('COMMIT')" and "FORMS_DDL('ROLLBACK')" should not be used </div>	
<div>  Code Smell </div> <div> "DBMS_OUTPUT.PUT_LINE" should not be used </div>	
<div>  Code Smell </div> <div> "WHEN OTHERS" should not be the only exception handler </div>	
<div>  Code Smell </div> <div> "INSERT" statements should explicitly list the columns to be set </div>	
<div>  Code Smell </div> <div> "%TYPE" and "%ROWTYPE" should not be used in package specification </div>	
<div>  Code Smell </div> <div> Functions and procedures should not be too complex </div>	