Parasoft Support for CWE 3.1 in dotTEST 10.4.1

The following table shows how Common Weakness Enumeration list (CWE 3.1) maps to Parasoft's static analysis rules for C#/VB.

CWE 3.1 ID	CWE 3.1 header/description	Parasoft rule ID(s)
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE.22.TDFNAMES
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	CWE.77.TDCMD
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CWE.78.VPPD, CWE.78.TDCMD, CWE.78.AUPS
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CWE.79.VPPD, CWE.79.TDRESP, CWE.79.TDXSS
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)	CWE.80.VPPD, CWE.80.TDRESP
CWE-88	Argument Injection or Modification	CWE.88.TDCMD, CWE.88.VPPD
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE.89.VPPD, CWE.89.TDSQL, CWE.89.TDSQLC
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')	CWE.90.VPPD, CWE.90.TDLDAP
CWE-99	Improper Control of Resource Identifiers ('Resource Injection')	CWE.99.TDFNAMES, CWE.99.TDNET
CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	CWE.120.AUK
CWE-131	Incorrect Calculation of Buffer Size	CWE.131.AUK
CWE-190	Integer Overflow or Wraparound	CWE.190.AIWIL
CWE-191	Integer Underflow (Wrap or Wraparound)	CWE.191.AIWIL
CWE-201	Information Exposure Through Sent Data	CWE.201.SELSPLAT
CWE-209	Information Exposure Through an Error Message	CWE.209.SENS, CWE.209.PEO, CWE.209.ACPST
CWE-250	Execution with Unnecessary Privileges	CWE.250.AUEP
CWE-259	Use of Hard-coded Password	CWE.259.HPW
CWE-285	Improper Authorization	CWE.285.TDSQL
CWE-306	Missing Authentication for Critical Function	CWE.306.ADSVSP
CWE-316	Cleartext Storage of Sensitive Information in Memory	CWE.316.RSFSS, CWE.316.SSFP
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	CWE.327.ICA, CWE.327.DNCCKS, CWE.327.ACCA
CWE-328	Reversible One-Way Hash	CWE.328.ICA
CWE-329	Not Using a Random IV with CBC Mode	CWE.329.ACCA

Generated from dottest/cwe/cwe.csv a42c2a4 (https://trove.parasoft.com/scm/xtest/rulemaps.git) on 2019-02-15, 15:46

CWE-330	Use of Insufficiently Random Values	CWE.330.USSCR
CWE-352	Cross-Site Request Forgery (CSRF)	CWE.352.VPPD, CWE.352.TDRESP
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	CWE.362.LOCKSETGET, CWE.362.DIFCS
CWE-369	Divide By Zero	CWE.369.ZERO
CWE-391	Unchecked Error Condition	CWE.391.LGE
CWE-395	Use of NullPointerException Catch to Detect NULL Pointer Dereference	CWE.395.NCNRE
CWE-396	Declaration of Catch for Generic Exception	CWE.396.NCSAE
CWE-397	Declaration of Throws for Generic Exception	CWE.397.NTSAE
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak')	CWE.401.DBDTFF, CWE.401.DCDSF, CWE.401.DCID, CWE.401.DDFODB, CWE.401.SRIF, CWE.401.TICUFDS, CWE.401.TIID, CWE.401.CBDM, CWE.401.IDWF, CWE.401.MDPP, CWE.401.ASC
CWE-402	Transmission of Private Resources into a New Sphere ('Resource Leak')	CWE.402.CSG
CWE-412	Unrestricted Externally Accessible Lock	CWE.412.NLT
CWE-416	Use After Free	CWE.416.DISP, CWE.416.FIN
CWE-434	Unrestricted Upload of File with Dangerous Type	CWE.434.TDFNAMES
CWE-476	NULL Pointer Dereference	CWE.476.NR, CWE.476.DEREF, CWE.476.CNFA
CWE-480	Use of Incorrect Operator	CWE.480.PUO
CWE-481	Assigning instead of Comparing	CWE.481.AWC
CWE-499	Serializable Class Containing Sensitive Data	CWE.499.CSG
CWE-502	Deserialization of Untrusted Data	CWE.502.IIDC, CWE.502.UIS, CWE.502.IDC, CWE.502.MGODWSPA
CWE-546	Suspicious Comment	CWE.546.TODO
CWE-554	ASP.NET Misconfiguration: Not Using Input Validation Framework	CWE.554.CUSTOM
CWE-563	Assignment to Variable without Use	CWE.563.POVR, CWE.563.VOVR
CWE-570	Expression is Always False	CWE.570.CC
CWE-571	Expression is Always True	CWE.571.CC
CWE-595	Comparison of Object References Instead of Object Contents	CWE.595.REVT
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	CWE.601.VPPD, CWE.601.TDNET
CWE-611	Improper Restriction of XML External Entity Reference ('XXE')	CWE.611.PDTDP
CWE-662	Improper Synchronization	CWE.662.DIFCS
CWE-676	Use of Potentially Dangerous Function	CWE.676.APDM
CWE-732	Incorrect Permission Assignment for Critical Resource	CWE.732.ADSVSP

Generated from dottest/cwe/cwe.csv a42c2a4 (https://trove.parasoft.com/scm/xtest/rulemaps.git) on 2019-02-15, 15:46

CWE-770	Allocation of Resources Without Limits or Throttling	CWE.770.LEAKS
CWE-776	Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	CWE.776.PDTDP
CWE-778	Insufficient Logging	CWE.778.ENFL
CWE-780	Use of RSA Algorithm without OAEP	CWE.780.UOWR
CWE-798	Use of Hard-coded Credentials	CWE.798.HARDCONN
CWE-829	Inclusion of Functionality from Untrusted Control Sphere	CWE.829.DMSC, CWE.829.ADLL
CWE-833	Deadlock	CWE.833.ORDER
CWE-862	Missing Authorization	CWE.862.UAA

Generated from dottest/cwe/cwe.csv a42c2a4 (https://trove.parasoft.com/scm/xtest/rulemaps.git) on 2019-02-15, 15:46