PARASOFT

Parasoft Support for CWE in .NET - dotTEST 9.x

The following table shows how Mitre's Common Weakness Enumeration (CWE) maps to Parasoft's static analysis rules for .NET.

CWE ID	CWE Name/Description	Parasoft Rule ID(s)
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection').	BD.SECURITY.TDCMD
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	SEC.VPPD, BD.SECURITY.TDCMD, SEC.AUPS
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').	SEC.VPPD, BD.SECURITY.TDRESP, BD.SECURITY.TDXSS
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS).	SEC.VPPD, BD.SECURITY.TDXSS
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').	SEC.VPPD, BD.SECURITY.TDSQL
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection').	SEC.VPPD, BD.SECURITY.TDLDAP
CWE-99	Improper Control of Resource Identifiers ('Resource Injection').	BD.SECURITY.TDFNAMES
CWE-209	Information Exposure Through an Error Message	BD.SECURITY.SENS, SEC.LGE, SPR.PEO, SEC.ACPST
CWE-244	Improper Clearing of Heap Memory Before Release ('Heap Inspection').	CS.SEC.SSFP, CS.SEC.RSFSS
CWE-259	Use of Hard-coded Password.	SEC.HPW
CWE-306	Missing Authentication for Critical Function.	SEC.ADSVSP
CWE-311	Missing Encryption of Sensitive Data.	CS.SEC.SSFP, CS.SEC.RSFSS
CWE-312	Cleartext Storage of Sensitive Information.	CS.SEC.SSFP, CS.SEC.RSFSS

CWE-327	Use of a Broken or Risky Cryptographic Algorithm.	SEC.ICA, SEC.DNCCKS
CWE-330	Use of Insufficiently Random Values.	SEC.USSCR
CWE-352	Cross-Site Request Forgery (CSRF).	SEC.VPPD, BD.SECURITY.TDRESP, BD.SECURITY.TDXSS
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	CS.TRS.LOCKSETGET
CWE-391	Unchecked Error Condition.	EXCEPT.NCSAE, EXCEPT.NCNRE, SEC.LGE
CWE-401	Improper Release of Memory Before Removing Last Reference ('Memory Leak').	BD.RES.LEAKS, GC.UFID, PB.CFSRLV, SEC.CDBC, SEC.CRIF, SEC.CDBCLV, SEC.CDRLV, IFD.DBDTFF, IFD.DCDSF, IFD.DCID, IFD.DDFODB, IFD.SRIF, IFD.TICUFDS, IFD.TIID, IFD.CBDM, IFD.DBV, IFD.IDWF, IFD.IDWBF, IFD.MDPP, IFD.SRII, GC.ASC
CWE-412	Unrestricted Externally Accessible Lock.	SEC.NLT
CWE-415	Double Free.	BD.PB.DISP
CWE-416	Use After Free.	BD.PB.FIN
CWE-457	Use of Uninitialized Variable.	CS.BRM.IEB
CWE-476	NULL Pointer Dereference.	BD.EXCEPT.NR, BD.PB.DEREF, CS.CNFA
CWE-546	Suspicious Comment.	PB.II.TODO
CWE-601	URL Redirection to Untrusted Site ('Open Redirect').	SEC.VPPD
CWE-732	Incorrect Permission Assignment for Critical Resource.	SEC.ADSVSP
CWE-770	Allocation of Resources Without Limits or Throttling.	SEC.CDRLV, SEC.CDBC
CWE-798	Use of Hard-coded Credentials.	SEC.HPW, SPR.HARDCONN
CWE-829	Inclusion of Functionality from Untrusted Control Sphere.	BD.SECURITY.TDXSS, SEC.DMSC, SEC.ADLL