Parasoft Support for CWE Top 25 + On the Cusp 2020 in dotTEST 2021.1.0

The following table shows how 2020 CWE Top 25 + On the Cusp: Other Weaknesses to Consider (CWE Top 25 + On the Cusp 2020) maps to Parasoft's static analysis rules for C#/VB.

CWE ID	CWE name/description	Parasoft rule ID(s)
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CWE.79.VPPD, CWE.79.TDRESP, CWE.79.TDXSS, CWE.79.AXSSE, CWE.79.CSP
CWE-787	Out-of-bounds Write	CWE.787.ARRAY
CWE-20	Improper Input Validation	CWE.20.ARRAY, CWE.20.VPPD, CWE.20.TDNET, CWE.20.TDFNAMES, CWE.20.TDCMD, CWE.20.TDRESP, CWE.20.TDXSS, CWE.20.TDSQL, CWE.20.TDSQLC
CWE-125	Out-of-bounds Read	CWE.125.ARRAY
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE.119.ARRAY
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE.89.TDSQL, CWE.89.TDSQLC
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	CWE.200.SDE, CWE.200.SENS, CWE.200.PEO, CWE.200.ACPST, CWE.200.CSG, CWE.200.SENSLOG
CWE-416	Use After Free	CWE.416.DISP, CWE.416.FIN
CWE-352	Cross-Site Request Forgery (CSRF)	CWE.352.VPPD, CWE.352.TDRESP, CWE.352.VAFT
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CWE.78.TDCMD
CWE-190	Integer Overflow or Wraparound	CWE.190.AIWIL, CWE.190.AIOAC, CWE.190.INTOVERF
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE.22.TDFNAMES
CWE-476	NULL Pointer Dereference	CWE.476.NR, CWE.476.DEREF, CWE.476.CNFA
CWE-287	Improper Authentication	CWE.287.TDPASSWD, CWE.287.AAM, CWE.287.UAAMC, CWE.287.LUAFLA, CWE.287.IIPHEU
CWE-434	Unrestricted Upload of File with Dangerous Type	CWE.434.TDFNAMES
CWE-732	Incorrect Permission Assignment for Critical Resource	CWE.732.ADSVSP
CWE-94	Improper Control of Generation of Code ('Code Injection')	CWE.94.TDCODE
CWE-522	Insufficiently Protected Credentials	CWE.522.TDPASSWD

CWE-611	Improper Restriction of XML External Entity Reference	CWE.611.PDTDP, CWE.611.USXRS
CWE-798	Use of Hard-coded Credentials	CWE.798.HARDCONN, CWE.798.HPW
CWE-502	Deserialization of Untrusted Data	CWE.502.IIDC, CWE.502.UIS, CWE.502.IDC, CWE.502.MGODWSPA
CWE-269	Improper Privilege Management	CWE.269.IDENTITY
CWE-400	Uncontrolled Resource Consumption	CWE.400.LEAKS, CWE.400.TDLOG
CWE-306	Missing Authentication for Critical Function	CWE.306.ADSVSP
CWE-862	Missing Authorization	CWE.862.UAA
CWE-426	Untrusted Search Path	CWE.426.PBRTE
CWE-918	Server-Side Request Forgery (SSRF)	CWE.918.TDNET
CWE-295	Improper Certificate Validation	CWE.295.DNICV
CWE-863	Incorrect Authorization	CWE.863.AAM, CWE.863.UAAMC, CWE.863.AUTH
CWE-284	Improper Access Control	CWE.284.AUEP, CWE.284.TDPASSWD, CWE.284.HPW, CWE.284.IDENTITY, CWE.284.TDSQL, CWE.284.DNICV, CWE.284.ADSVSP, CWE.284.LUAFLA, CWE.284.IIPHEU, CWE.284.HARDCONN, CWE.284.UAA, CWE.284.AAM, CWE.284.UAAMC, CWE.284.AUTH
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	CWE.77.TDCMD
CWE-401	Missing Release of Memory after Effective Lifetime	N/A
CWE-532	Insertion of Sensitive Information into Log File	CWE.532.ALSI, CWE.532.SENSLOG
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	CWE.362.LOCKSETGET, CWE.362.DIFCS
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	CWE.601.TDNET, CWE.601.TDRESP
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	CWE.835.IVFLC, CWE.835.IVFLI, CWE.835.NSIVFLN
CWE-704	Incorrect Type Conversion or Cast	CWE.704.ECLTS
CWE-415	Double Free	N/A
CWE-770	Allocation of Resources Without Limits or Throttling	CWE.770.TDALLOC, CWE.770.UHCF
CWE-59	Improper Link Resolution Before File Access ('Link Following')	CWE.59.VLT