Parasoft Support for CWE Top 25 + On the Cusp 2020 in Jtest 2020.2.0

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 Java.

CWE ID	CWE name/description	Parasoft rule ID(s)
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	CWE.79.TDXSS, CWE.79.EACM, CWE.79.VPPD, CWE.79.TDRESP, CWE.79.ARXML, CWE.79.TDXML, CWE.79.TDDIG
CWE-787	Out-of-bounds Write	CWE.787.ARRAY, CWE.787.ARRAYINP
CWE-20	Improper Input Validation	CWE.20.TDLIB, CWE.20.APIBS, CWE.20.TDLOG, CWE.20.PLUGIN, CWE.20.EV, CWE.20.DFV, CWE.20.ARRAY, CWE.20.ARRAYINP, CWE.20.FREE, CWE.20.BSA, CWE.20.BUSSB, CWE.20.TDRFL, CWE.20.NATV, CWE.20.NATIW, CWE.20.TDINPUT, CWE.20.TDRESP, CWE.20.IOF, CWE.20.ICO, CWE.20.CACO, CWE.20.INTOVERF, CWE.20.CLP, CWE.20.SYSP, CWE.20.UCO, CWE.20.CSVFV, CWE.20.AEAF, CWE.20.CAI, CWE.20.TDALLOC
CWE-125	Out-of-bounds Read	CWE.125.ARRAY, CWE.125.ARRAYINP
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE.119.ARRAY, CWE.119.ARRAYINP, CWE.119.FREE, CWE.119.BSA, CWE.119.BUSSB
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE.89.UPS, CWE.89.TDSQL
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	CWE.200.CONSEN, CWE.200.SENSLOG, CWE.200.EWSSEC, CWE.200.PEO, CWE.200.ACPST, CWE.200.SENS, CWE.200.SIO
CWE-416	Use After Free	CWE.416.FREE
CWE-352	Cross-Site Request Forgery (CSRF)	CWE.352.TDXSS, CWE.352.VPPD, CWE.352.EACM, CWE.352.UOSC, CWE.352.TDRESP, CWE.352.DCSRFJAVA, CWE.352.DCSRFXML, CWE.352.REQMAP
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.IOF, CWE.190.BSA, CWE.190.ICO, CWE.190.CACO, CWE.190.INTOVERF, CWE.190.CLP
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE.22.TDFNAMES
CWE-476	NULL Pointer Dereference	CWE.476.NP, CWE.476.DEREF

CWE-287	Improper Authentication	CWE.287.HCCS, CWE.287.HCCK, CWE.287.PLAIN, CWE.287.HV, CWE.287.VSI, CWE.287.HTTPRHA, CWE.287.DNSL, CWE.287.MLVP, CWE.287.PWDPROP, CWE.287.USC, CWE.287.UTAX, CWE.287.PWDXML, CWE.287.TDPASSWD, CWE.287.UPWD, CWE.287.PCCF, CWE.287.PTPT, CWE.287.WCPWD, CWE.287.WPWD, CWE.287.SSM, CWE.287.PBFA, CWE.287.CKTS
CWE-434	Unrestricted Upload of File with Dangerous Type	CWE.434.TDFNAMES
CWE-732	Incorrect Permission Assignment for Critical Resource	CWE.732.SCHTTP
CWE-94	Improper Control of Generation of Code ('Code Injection')	CWE.94.DCEMSL, CWE.94.ASAPI, CWE.94.TDCODE
CWE-522	Insufficiently Protected Credentials	CWE.522.PWDPROP, CWE.522.USC, CWE.522.UTAX, CWE.522.PWDXML, CWE.522.PLAIN, CWE.522.TDPASSWD, CWE.522.UPWD, CWE.522.PCCF, CWE.522.PTPT, CWE.522.WCPWD, CWE.522.WPWD
CWE-611	Improper Restriction of XML External Entity Reference	CWE.611.DXXE, CWE.611.XMLVAL
CWE-798	Use of Hard-coded Credentials	CWE.798.HCCS, CWE.798.HCCK
CWE-502	Deserialization of Untrusted Data	CWE.502.SC, CWE.502.RWAF, CWE.502.SSSD, CWE.502.MASP, CWE.502.AUXD, CWE.502.VOBD
CWE-269	Improper Privilege Management	CWE.269.LDP, CWE.269.PCL, CWE.269.DPANY
CWE-400	Uncontrolled Resource Consumption	CWE.400.DMDS, CWE.400.ISTART, CWE.400.TDALLOC, CWE.400.LEAKS
CWE-306	Missing Authentication for Critical Function	CWE.306.SSM
CWE-862	Missing Authorization	CWE.862.PERMIT, CWE.862.LCA
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.HV, CWE.295.VSI
CWE-863	Incorrect Authorization	CWE.863.DSR, CWE.863.SRCD

CWE-284	Improper Access Control	CWE.284.LDP, CWE.284.PCL, CWE.284.DPANY, CWE.284.JXCORS, CWE.284.DNSL, CWE.284.VSI, CWE.284.PERMIT, CWE.284.LCA, CWE.284.DSR, CWE.284.SRCD, CWE.284.SCHTTP, CWE.284.HCCS, CWE.284.HCCK, CWE.284.PLAIN, CWE.284.HV, CWE.284.HTTPRHA, CWE.284.MLVP, CWE.284.PWDPROP, CWE.284.USC, CWE.284.UTAX, CWE.284.PWDXML, CWE.284.TDPASSWD, CWE.284.UPWD, CWE.284.PCCF, CWE.284.PTPT, CWE.284.WCPWD, CWE.284.WPWD, CWE.284.SSM, CWE.284.PBFA, CWE.284.CKTS
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.CONSEN, CWE.532.SENSLOG
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	CWE.362.DCL, CWE.362.TOCTOU
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')	CWE.601.TDNET, CWE.601.TDRESP, CWE.601.UCO, CWE.601.VRD
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')	CWE.835.AIL, CWE.835.PCIF
CWE-704	Incorrect Type Conversion or Cast	CWE.704.AGBPT, CWE.704.CPTS, CWE.704.IDCD, CWE.704.CLP
CWE-415	Double Free	N/A
CWE-770	Allocation of Resources Without Limits or Throttling	CWE.770.ISTART, CWE.770.TDALLOC
CWE-59	Improper Link Resolution Before File Access ('Link Following')	CWE.59.LNK, CWE.59.FOLLOW