Parasoft Support for CWE Top 25 + On the Cusp 2022 in C/C++test 2022.2

The following table shows how 2022 CWE Top 25 Most Dangerous Software Errors and Weaknesses On the Cusp (CWE Top 25 + On the Cusp 2022) maps to Parasoft's static analysis rules for C/C++.

ID	Kind	Name/description	Parasoft rule ID(s)
CWE-787	Top 25	Out-of-bounds Write	CWE-787-a, CWE-787-b, CWE-787-c, CWE-787-d, CWE-787-e, CWE-787-f, CWE-787-g
CWE-79	Top 25	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	N/A
CWE-89	Top 25	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	CWE-89-a
CWE-20	Top 25	Improper Input Validation	CWE-20-a, CWE-20-b, CWE-20-c, CWE-20-d, CWE-20-e, CWE-20-f, CWE-20-g, CWE-20-h, CWE-20-i, CWE-20-j
CWE-125	Top 25	Out-of-bounds Read	CWE-125-a, CWE-125-b, CWE-125-c, CWE-125-d
CWE-78	Top 25	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	CWE-78-a
CWE-416	Top 25	Use After Free	CWE-416-a, CWE-416-b, CWE-416-c
CWE-22	Top 25	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	CWE-22-a
CWE-352	Top 25	Cross-Site Request Forgery (CSRF)	N/A
CWE-434	Top 25	Unrestricted Upload of File with Dangerous Type	N/A
CWE-476	Top 25	NULL Pointer Dereference	CWE-476-a, CWE-476-b
CWE-502	Top 25	Deserialization of Untrusted Data	N/A
CWE-190	Top 25	Integer Overflow or Wraparound	CWE-190-a, CWE-190-b, CWE-190-c, CWE-190-d, CWE-190-e, CWE-190-f, CWE-190-g
CWE-287	Top 25	Improper Authentication	CWE-287-a
CWE-798	Top 25	Use of Hard-coded Credentials	CWE-798-a
CWE-862	Top 25	Missing Authorization	N/A
CWE-77	Top 25	Improper Neutralization of Special Elements used in a Command ('Command Injection')	CWE-77-a
CWE-306	Top 25	Missing Authentication for Critical Function	N/A

CWE-119	Top 25	Improper Restriction of Operations within the Bounds of a Memory Buffer	CWE-119-a, CWE-119-b, CWE-119-c, CWE-119-d, CWE-119-e, CWE-119-f, CWE-119-g, CWE-119-h, CWE-119-i, CWE-119-j, CWE-119-k
CWE-276	Top 25	Incorrect Default Permissions	N/A
CWE-918	Top 25	Server-Side Request Forgery (SSRF)	N/A
CWE-362	Top 25	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	CWE-362-a, CWE-362-b, CWE-362-c, CWE-362-d, CWE-362-e
CWE-400	Top 25	Uncontrolled Resource Consumption	CWE-400-a
CWE-611	Top 25	Improper Restriction of XML External Entity Reference	CWE-611-a
CWE-94	Top 25	Improper Control of Generation of Code ('Code Injection')	N/A
CWE-295	On the Cusp	Improper Certificate Validation	N/A
CWE-427	On the Cusp	Uncontrolled Search Path Element	CWE-427-a
CWE-863	On the Cusp	Incorrect Authorization	CWE-863-a
CWE-269	On the Cusp	Improper Privilege Management	CWE-269-a, CWE-269-b
CWE-732	On the Cusp	Incorrect Permission Assignment for Critical Resource	CWE-732-a, CWE-732-b
CWE-843	On the Cusp	Access of Resource Using Incompatible Type ('Type Confusion')	CWE-843-a
CWE-668	On the Cusp	Exposure of Resource to Wrong Sphere	CWE-668-a
CWE-200	On the Cusp	Exposure of Sensitive Information to an Unauthorized Actor	CWE-200-a
CWE-1321	On the Cusp	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')	N/A
CWE-601	On the Cusp	URL Redirection to Untrusted Site ('Open Redirect')	N/A
CWE-401	On the Cusp	Missing Release of Memory after Effective Lifetime	CWE-401-a
CWE-59	On the Cusp	Improper Link Resolution Before File Access ('Link Following')	CWE-59-a
CWE-522	On the Cusp	Insufficiently Protected Credentials	N/A
CWE-319	On the Cusp	Cleartext Transmission of Sensitive Information	N/A
CWE-312	On the Cusp	Cleartext Storage of Sensitive Information	CWE-312-a

Generated from cwe_top25_onthecusp_2022.csv d7d52b3 on 2022-11-18, 13:43