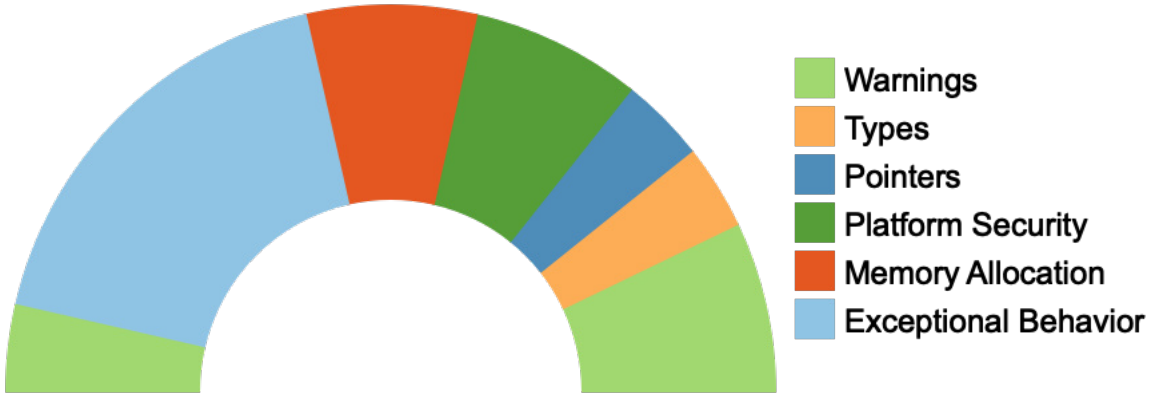
The CWE Top 25 Most Dangerous Software Weaknesses identifies the currently most common and impactful software weaknesses. These weaknesses are often easy to find and exploit and can allow adversaries to completely take over a system, steal data, or prevent applications from working.

Uncovering the root causes of these vulnerabilities serves as a powerful guide for investments, policies, and practices to prevent these vulnerabilities from occurring in the first place.

https://cwe.mitre.org/top25/

Checks by Tags



Checks

Check ID	Check Name	Supported
CWE-20	Improper Input Validation	No
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	No
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	Yes
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('Command Injection')	Yes
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	No
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	No
CWE-94	Improper Control of Generation of Code ('Code Injection')(Partial)	Yes
CWE-119A	Improper Restriction of Operations within the Bounds of a Memory Buffer(Part A: Read)	Yes
CWE-119B	Improper Restriction of Operations within the Bounds	Yes

	of a Memory Buffer(Part B: Write)	
CWE-125	Out-of-bounds Read	Yes
CWE-190	Integer Overflow or Wraparound	Yes
CWE-269	Improper Privilege Management	No
CWE-276	Incorrect Default Permissions	No
CWE-287	Improper Authentication	No
CWE-306	Missing Authentication for Critical Function (Partial)	Yes
CWE-352	Cross-Site Request Forgery (CSRF)	No
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')(Partial)	Yes
CWE-416	Use After Free	No
CWE-434	Unrestricted Upload of File with Dangerous Type	No
CWE-476	NULL Pointer Dereference	Yes
CWE-502	Deserialization of Untrusted Data (Partial)	Yes
CWE-787	Out-of-bounds Write	Yes
CWE-798	Use of Hard-coded Credentials (Partial)	Yes
CWE-862	Missing Authorization	No
CWE-863	Incorrect Authorization	No
CWE-918	Server-Side Request Forgery (SSRF)	No