SYNOPSYS®

Coverity Support for CWE/SANS Top 25

CWE/SANS Top 25 (2011)	CWE	Java	C#	C/C++	Obj-C/Clang	JavaScript	Node.js	Android	Swift	Python 2.7	PHP	Scala	VB.NET	Ruby
1. Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	89	●	●	●	●	●	●	●	●	●	●		●	●
2. Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	78	●	●	●	●	●	●	●		●	●			●
3. Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	120			●	●									
4. Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	79	●	●			●	●	●		●	●		●	●
5. Missing Authentication for Critical Function	306													
6. Missing Authorization	862	●						●						●
7. Use of Hard-coded Credentials	798	●	●	●	●	●	●	●	●	●	●		●	●
8. Missing Encryption of Sensitive Data	311	●	●	●	●	●	●	●	●	●	●		●	
9. Unrestricted Upload of File with Dangerous Type	434													
10. Reliance on Untrusted Inputs in a Security Decision	807	●	●	●	●			●						
11. Execution with Unnecessary Privileges	250													
12. Cross-Site Request Forgery (CSRF)	352	●	●			●	●	●			●		●	●
13. Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22	●	●	●	●	●	●	●	●	●	●		●	●
14. Download of Code Without Integrity Check	494													
15. Incorrect Authorization	863	●	●					●						
16. Inclusion of Functionality from Untrusted Control Sphere	829	●				●	●	●	●					
17. Incorrect Permission Assignment for Critical Resource	732													
18. Use of Potentially Dangerous Function	676	●		●	●			●						
19. Use of a Broken or Risky Cryptographic Algorithm	327	●	●	●	●	●	●	●	●				●	
20. Incorrect Calculation of Buffer Size	131			●	●									
21. Improper Restriction of Excessive Authentication Attempts	307													●
22. URL Redirection to Untrusted Site ('Open Redirect')	601	●	●			●	●	●		●	●		●	●
23. Uncontrolled Format String	134			●	●									
24. Integer Overflow or Wraparound	190	●	●	●	●			●				●		
25. Use of a One-Way Hash without a Salt	759	●	●	●	●			●					●	