Vulnerability taxonomy

With the increase in the number of technologies over the past few years, there have been various attempts to introduce the best taxonomy that could categorize all the common sets of vulnerabilities. However, no single taxonomy has been produced to represent all the common coding mistakes that may affect the system's security. This is due to the fact that a single vulnerability might fall into more than one category or class. Additionally, every system platform has its own base for connectivity, complexity, and extensibility to interact with its environment. Thus, the taxonomy standards that are presented in the following table will help you identify most of the security glitches, whenever possible. Note that most of these taxonomies have already been implemented in a number of security assessment tools to investigate the software security problems in real time.

Security taxonomy	Resource link
HP Software security	http://www.hpenterprisesecurity.com/vulncat/en/vulncat/index.html
Seven pernicious kingdoms	http://www.cigital.com/papers/download/bsi11-taxonomy.pdf
Common Weakness Enumeration	http://cwe.mitre.org/data/index.html
OWASP Top 10	http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
Klocwork	http://www.klocwork.com/products/documentation/Insight-9.1/Taxonomy
GrammaTech	http://www.grammatech.com
WASC Threat Classification	http://projects.webappsec.org/Threat-Classification

The primary function of each of these taxonomies is to organize sets of security vulnerabilities that can be used by the security practitioners and developers to identify the specific errors that may have an impact on the system's security. Thus, no single taxonomy should be considered complete and accurate.