

top 25 des erreurs de programmation ouvrant des failles de sécurité

le site CWE (Common Weakness Enumeration, c'est à dire Enumeration des faiblesses communes) publie une synthèse et un rapport détaillé sur les 25 erreurs de programmation qui ouvrent des failles de sécurité. Fortement orienté Web, cela reste utile dans les autres contextes de programmations:

Ce top 25 se divise en trois catégories : - les interactions non sécurisées: 9 erreurs ayant trait au nettoyage des entrées (data sanitization)- Gestion hasardeuse des ressources: 9 erreurs, tel que buffer overflow- Défenses poreuses: 7 erreurs, mot de passe unique, faiblesse des contrôles d'accès ACL..

on retrouve parmi celles-ci les classiques tels que SQL Injection, Code Injection, Cross-site Scripting, OS Command Injection, Race Condition... Lien: http://cwe.mitre.org/top25/archive/2009/2009_cwe_sans_top25.html