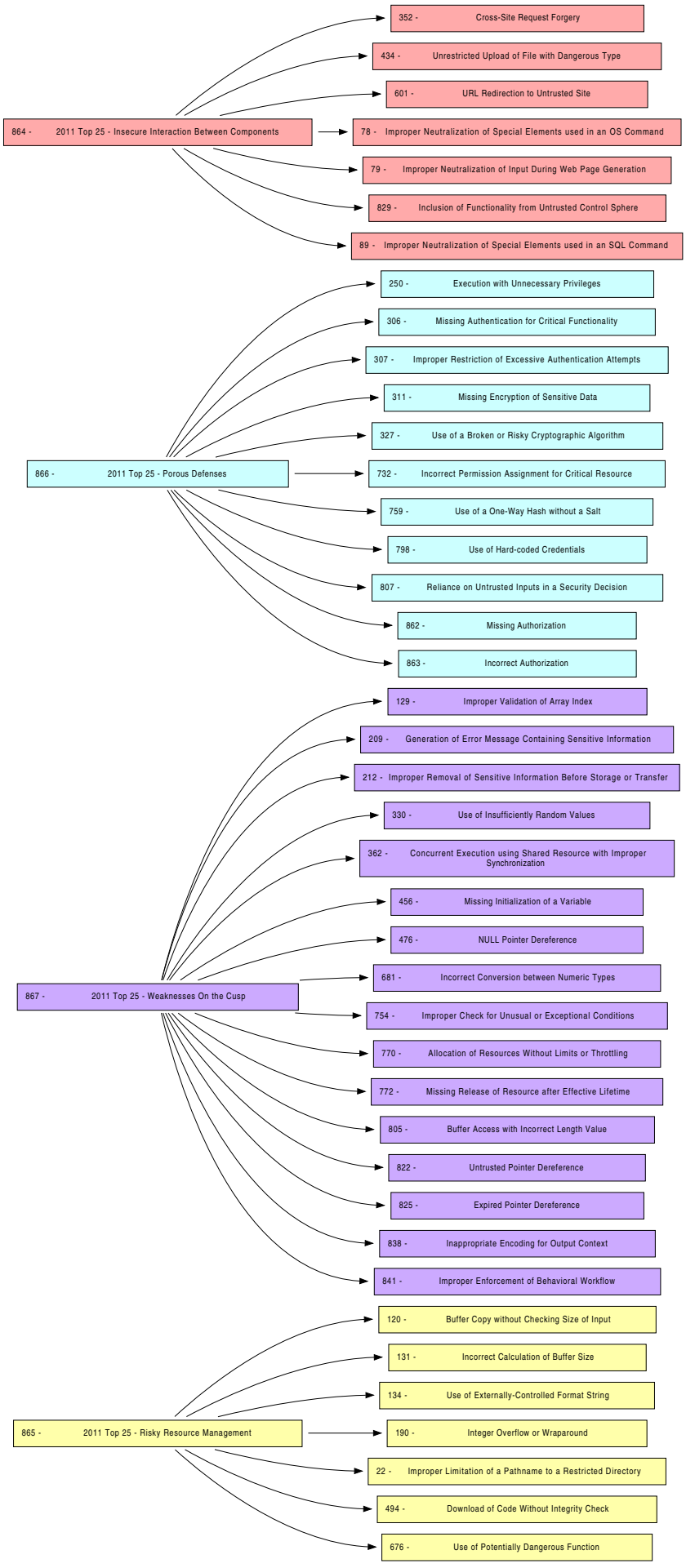

864 - 2011 Top 25 - Insecure Interaction Between Components
352 - Cross-Site Request Forgery
434 - Unrestricted Upload of File with Dangerous Type
601 - URL Redirection to Untrusted Site
78 - Improper Neutralization of Special Elements used in an OS Command
79 - Improper Neutralization of Input During Web Page Generation
829 - Inclusion of Functionality from Untrusted Control Sphere
89 - Improper Neutralization of Special Elements used in an SQL Command
866 - 2011 Top 25 - Porous Defenses
250 - Execution with Unnecessary Privileges
306 - Missing Authentication for Critical Functionality
307 - Improper Restriction of Excessive Authentication Attempts
311 - Missing Encryption of Sensitive Data
327 - Use of a Broken or Risky Cryptographic Algorithm
732 - Incorrect Permission Assignment for Critical Resource
759 - Use of a One-Way Hash without a Salt
798 - Use of Hard-coded Credentials
807 - Reliance on Untrusted Inputs in a Security Decision
862 - Missing Authorization
863 - Incorrect Authorization
867 - 2011 Top 25 - Weaknesses On the Cusp
129 - Improper Validation of Array Index
209 - Generation of Error Message Containing Sensitive Information
212 - Improper Removal of Sensitive Information Before Storage or Transfer
330 - Use of Insufficiently Random Values
362 - Concurrent Execution using Shared Resource with Improper Synchronization
456 - Missing Initialization of a Variable
476 - NULL Pointer Dereference
681 - Incorrect Conversion between Numeric Types
754 - Improper Check for Unusual or Exceptional Conditions
770 - Allocation of Resources Without Limits or Throttling
772 - Missing Release of Resource after Effective Lifetime
805 - Buffer Access with Incorrect Length Value
822 - Untrusted Pointer Dereference
825 - Expired Pointer Dereference
838 - Inappropriate Encoding for Output Context
841 - Improper Enforcement of Behavioral Workflow
865 - 2011 Top 25 - Risky Resource Management
120 - Buffer Copy without Checking Size of Input
131 - Incorrect Calculation of Buffer Size
134 - Use of Externally-Controlled Format String
190 - Integer Overflow or Wraparound
22 - Improper Limitation of a Pathname to a Restricted Directory
494 - Download of Code Without Integrity Check
676 - Use of Potentially Dangerous Function