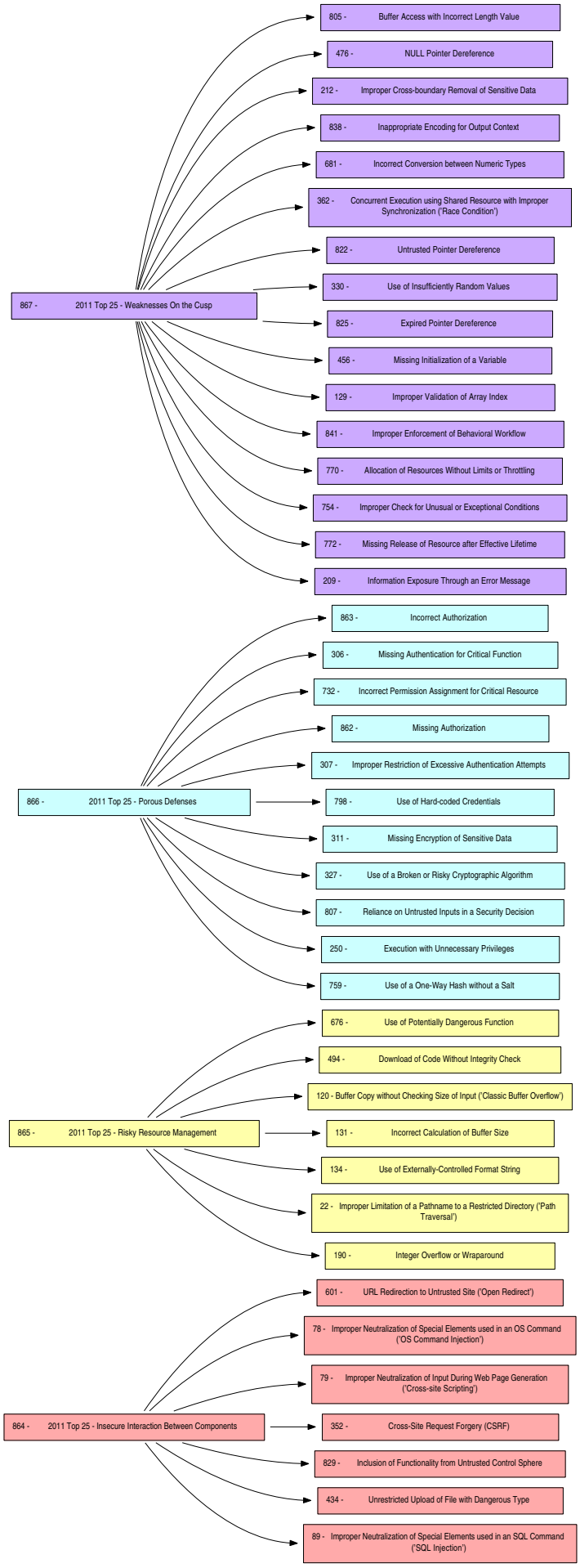
867 - 2011 Top 25 - Weaknesses On the Cusp
805 - Buffer Access with Incorrect Length Value
476 - NULL Pointer Dereference
212 - Improper Cross-boundary Removal of Sensitive Data
838 - Inappropriate Encoding for Output Context
681 - Incorrect Conversion between Numeric Types
362 - Concurrent Execution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