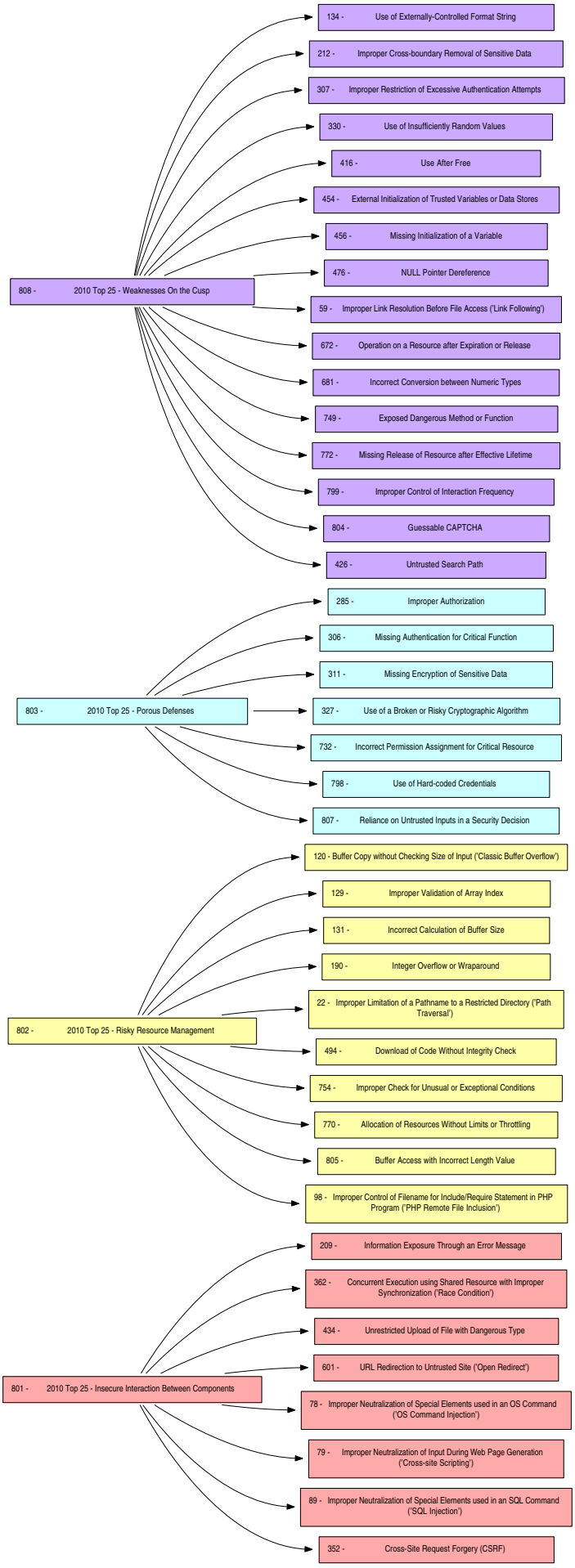
808 - 2010 Top 25 - Weaknesses On the Cusp
134 - Use of Externally-Controlled Format String
212 - Improper Cross-boundary Removal of Sensitive Data
307 - Improper Restriction of Excessive Authentication Attempts
330 - Use of Insufficiently Random Values
416 - Use After Free
454 - External Initialization of Trusted Variables or Data Stores
456 - Missing Initialization of a Variable
476 - NULL Pointer Dereference
59 - Improper Link Resolution Before File Access ('Link Following')
672 - Operation on a Resource after Expiration or Release
681 - Incorrect Conversion between Numeric Types
749 - Exposed Dangerous Method or Function
772 - Missing Release of Resource after Effective Lifetime
799 - Improper Control of Interaction Frequency
804 - Guessable CAPTCHA
426 - Untrusted Search Path
803 - 2010 Top 25 - Porous Defenses
285 - Improper Authorization
306 - Missing Authentication for Critical Function
311 - Missing Encryption of Sensitive Data
327 - Use of a Broken or Risky Cryptographic Algorithm
732 - Incorrect Permission Assignment for Critical Resource
798 - Use of Hard-coded Credentials
807 - Reliance on Untrusted Inputs in a Security Decision
802 - 2010 Top 25 - Risky Resource Management
120 - Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
129 - Improper Validation of Array Index
131 - Incorrect Calculation of Buffer Size
190 - Integer Overflow or Wraparound
22 - Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
494 - Download of Code Without Integrity Check
754 - Improper Check for Unusual or Exceptional Conditions
770 - Allocation of Resources Without Limits or Throttling
805 - Buffer Access with Incorrect Length Value
98 - Improper Control of Filename for Include/Require Statement in PHP Program ("PHP Remote File Inclusion")
801 - 2010 Top 25 - Insecure Interaction Between Components
209 - Information Exposure Through an Error Message
362 - Concurrent Execution using Shared Resource with Improper Synchronization ("Race Condition")
434 - Unrestricted Upload of File with Dangerous Type
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")
89 - Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection")
352 - Cross-Site Request Forgery (CSRF)