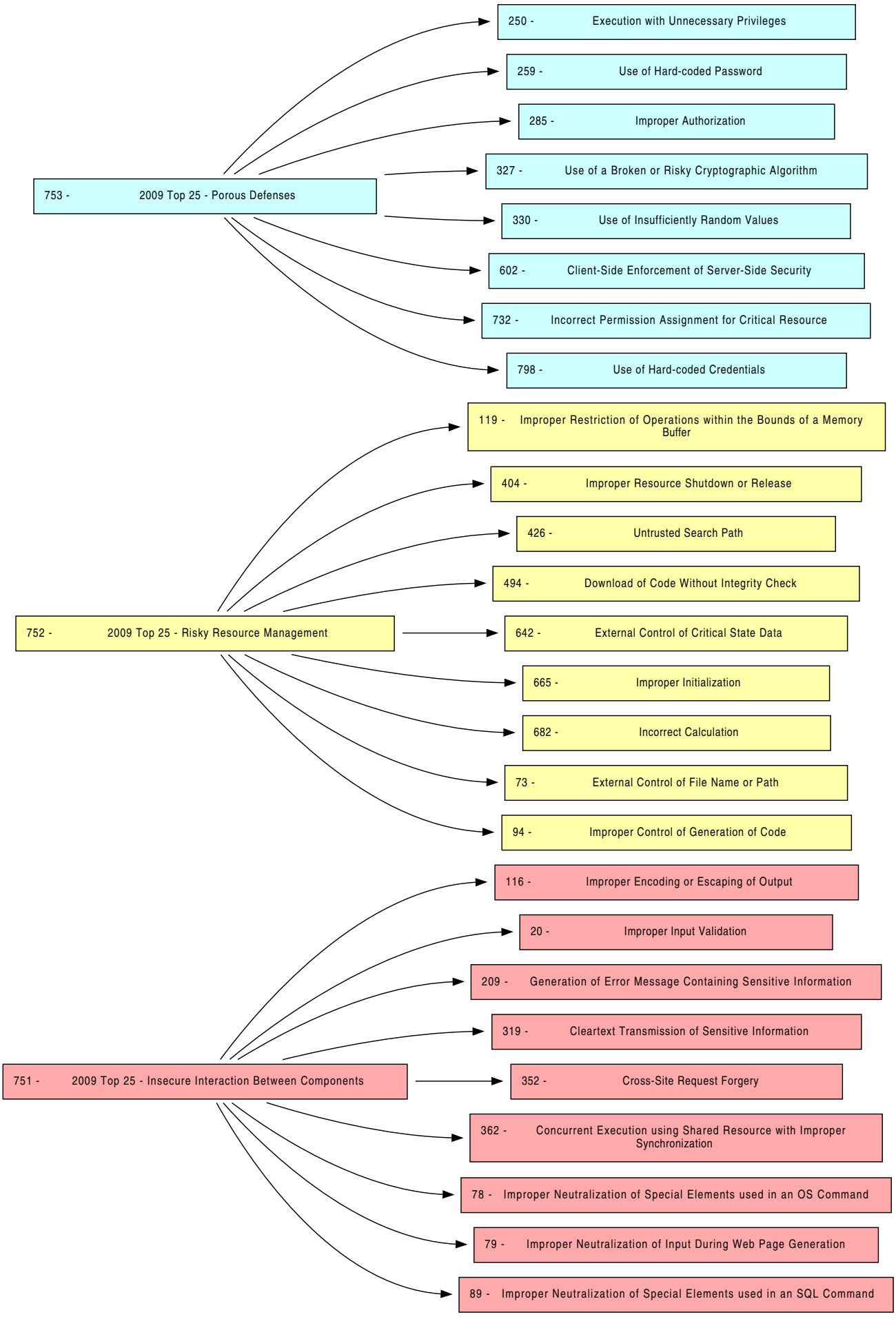

753 - 2009 Top 25 - Porous Defenses
250 - Execution with Unnecessary Privileges
259 - Use of Hard-coded Password
285 - Improper Authorization
327 - Use of a Broken or Risky Cryptographic Algorithm
330 - Use of Insufficiently Random Values
602 - Client-Side Enforcement of Server-Side Security
732 - Incorrect Permission Assignment for Critical Resource
798 - Use of Hard-coded Credentials
752 - 2009 Top 25 - Risky Resource Management
119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
404 - Improper Resource Shutdown or Release
426 - Untrusted Search Path
494 - Download of Code Without Integrity Check
642 - External Control of Critical State Data
665 - Improper Initialization
682 - Incorrect Calculation
73 - External Control of File Name or Path
94 - Improper Control of Generation of Code
751 - 2009 Top 25 - Insecure Interaction Between Components
116 - Improper Encoding or Escaping of Output
20 - Improper Input Validation
209 - Generation of Error Message Containing Sensitive Information
319 - Cleartext Transmission of Sensitive Information
352 - Cross-Site Request Forgery
362 - Concurrent Execution using Shared Resource with Improper Synchronization
78 - Improper Neutralization of Special Elements used in an OS Command
79 - Improper Neutralization of Input During Web Page Generation
89 - Improper Neutralization of Special Elements used in an SQL Command