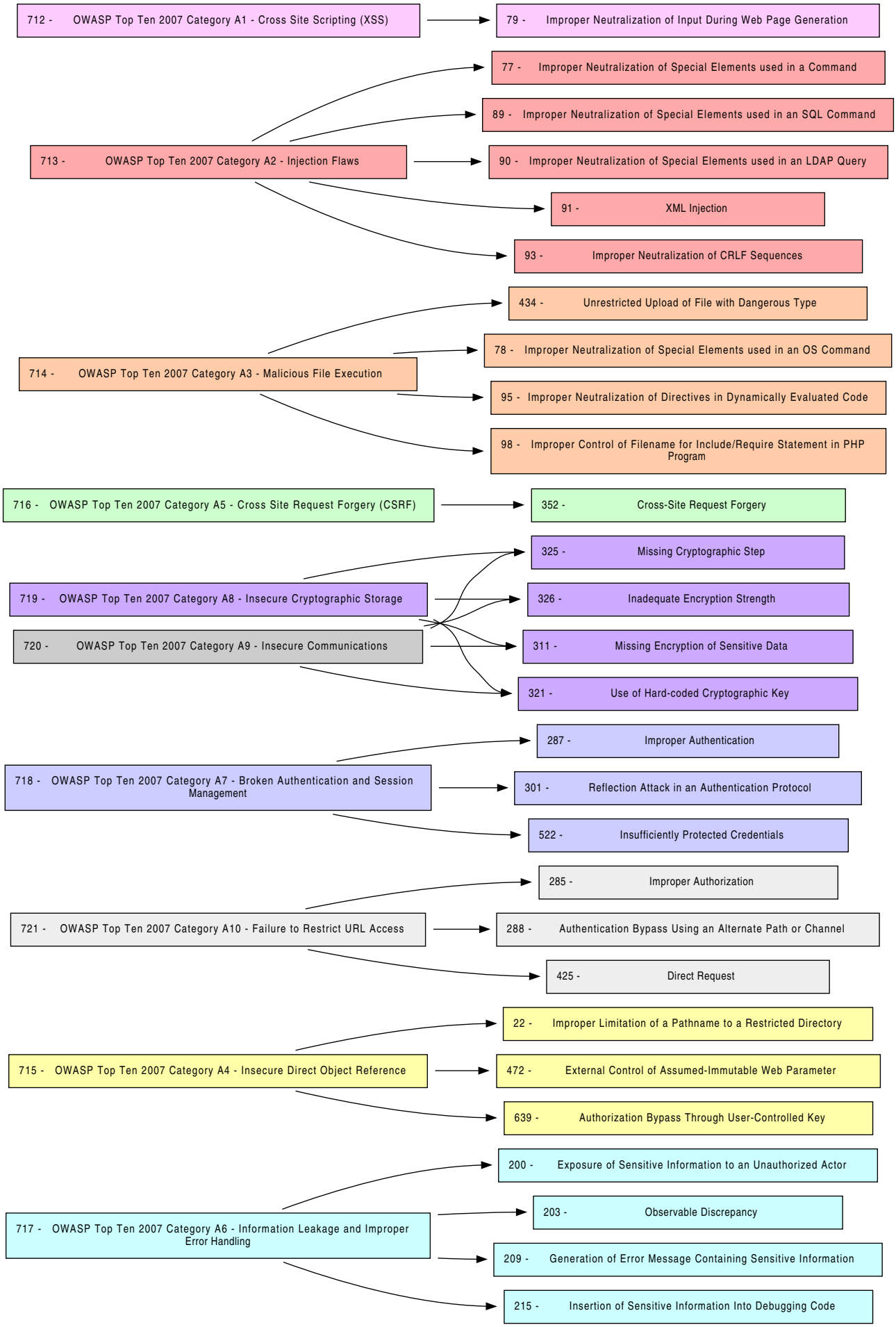

712 - OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS)
79 - Improper Neutralization of Input During Web Page Generation
77 - Improper Neutralization of Special Elements used in a Command
89 - Improper Neutralization of Special Elements used in an SQL Command
713 - OWASP Top Ten 2007 Category A2 - Injection Flaws
90 - Improper Neutralization of Special Elements used in an LDAP Query
91 - XML Injection
93 - Improper Neutralization of CRLF Sequences
434 - Unrestricted Upload of File with Dangerous Type
78 - Improper Neutralization of Special Elements used in an OS Command
714 - OWASP Top Ten 2007 Category A3 - Malicious File Execution
95 - Improper Neutralization of Directives in Dynamically Evaluated Code
98 - Improper Control of Filename for Include/Require Statement in PHP Program
716 - OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF)
352 - Cross-Site Request Forgery
325 - Missing Cryptographic Step
719 - OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage
326 - Inadequate Encryption Strength
720 - OWASP Top Ten 2007 Category A9 - Insecure Communications
311 - Missing Encryption of Sensitive Data
321 - Use of Hard-coded Cryptographic Key
287 - Improper Authentication
718 - OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management
301 - Reflection Attack in an Authentication Protocol
522 - Insufficiently Protected Credentials
285 - Improper Authorization
721 - OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access
288 - Authentication Bypass Using an Alternate Path or Channel
425 - Direct Request
22 - Improper Limitation of a Pathname to a Restricted Directory
715 - OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference
472 - External Control of Assumed-Immutable Web Parameter
639 - Authorization Bypass Through User-Controlled Key
200 - Exposure of Sensitive Information to an Unauthorized Actor
203 - Observable Discrepancy
717 - OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling
209 - Generation of Error Message Containing Sensitive Information
215 - Insertion of Sensitive Information Into Debugging Code