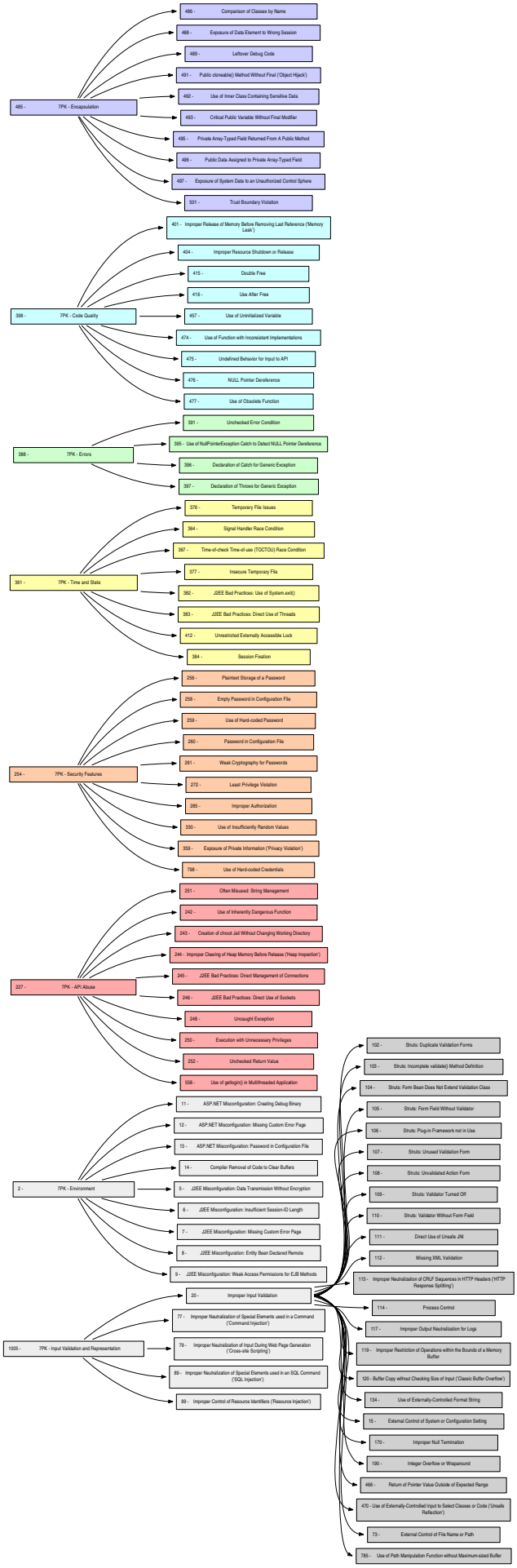
485 - 7PK - Encapsulation
486 - Comparison of Classes by Name
488 - Exposure of Data Element to Wrong Session
489 - Leftover Debug Code
491 - Public cloneable() Method Without Final ('Object Hijack')
492 - Use of Inner Class Containing Sensitive Data
493 - Critical Public Variable Without Final Modifier
495 - Private Array-Typed Field Returned From A Public Method
496 - Public Data Assigned to Private Array-Typed Field
497 - Exposure of System Data to an Unauthorized Control Sphere
501 - Trust Boundary Violation
398 - 7PK - Code Quality
401 - Improper Release of Memory Before Removing Last Reference ('Memory Leak')
404 - Improper Resource Shutdown or Release
415 - Double Free
416 - Use After Free
457 - Use of Uninitialized Variable
474 - Use of Function with Inconsistent Implementations
475 - Undefined Behavior for Input to API
476 - NULL Pointer Dereference
477 - Use of Obsolete Function
388 - 7PK - Errors
391 - Unchecked Error Condition
395 - Use of NullPointerException Catch to Detect NULL Pointer Dereference
396 - Declaration of Catch for Generic Exception
397 - Declaration of Throws for Generic Exception
361 - 7PK - Time and State
376 - Temporary File Issues
364 - Signal Handler Race Condition
367 - Time-of-check Time-of-use (TOCTOU) Race Condition
377 - Insecure Temporary File
382 - J2EE Bad Practices: Use of System.exit()
383 - J2EE Bad Practices: Direct Use of Threads
412 - Unrestricted Externally Accessible Lock
384 - Session Fixation
254 - 7PK - Security Features
256 - Plaintext Storage of a Password
258 - Empty Password in Configuration File
259 - Use of Hard-coded Password
260 - Password in Configuration File
261 - Weak Cryptography for Passwords
272 - Least Privilege Violation
285 - Improper Authorization
330 - Use of Insufficiently Random Values
359 - Exposure of Private Information ('Privacy Violation')
798 - Use of Hard-coded Credentials
227 - 7PK - API Abuse
251 - Often Misused: String Management
242 - Use of Inherently Dangerous Function
243 - Creation of chroot Jail Without Changing Working Directory
244 - Improper Clearing of Heap Memory Before Release ('Heap Inspection')
245 - J2EE Bad Practices: Direct Management of Connections
246 - J2EE Bad Practices: Direct Use of Sockets
248 - Uncaught Exception
250 - Execution with Unnecessary Privileges
252 - Unchecked Return Value
558 - Use of getlogin() in Multithreaded Application
2 - 7PK - Environment
11 - ASP.NET Misconfiguration: Creating Debug Binary
12 - ASP.NET Misconfiguration: Missing Custom Error Page
13 - ASP.NET Misconfiguration: Password in Configuration File
14 - Compiler Removal of Code to Clear Buffers
5 - J2EE Misconfiguration: Data Transmission Without Encryption
6 - J2EE Misconfiguration: Insufficient Session-ID Length
7 - J2EE Misconfiguration: Missing Custom Error Page
8 - J2EE Misconfiguration: Entity Bean Declared Remote
9 - J2EE Misconfiguration: Weak Access Permissions for EJB Methods
1005 - 7PK - Input Validation and Representation
20 - Improper Input Validation
77 - Improper Neutralization of Special Elements used in a Command ('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')
99 - Improper Control of Resource Identifiers ('Resource Injection')
102 - Struts: Duplicate Validation Forms
103 - Struts: Incomplete validate() Method Definition
104 - Struts: Form Bean Does Not Extend Validation Class
105 - Struts: Form Field Without Validator
106 - Struts: Plug-in Framework not in Use
107 - Struts: Unused Validation Form
108 - Struts: Unvalidated Action Form
109 - Struts: Validator Turned Off
110 - Struts: Validator Without Form Field
111 - Direct Use of Unsafe JNI
112 - Missing XML Validation
113 - Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting')
114 - Process Control
117 - Improper Output Neutralization for Logs
119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
120 - Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
134 - Use of Externally-Controlled Format String
15 - External Control of System or Configuration Setting
170 - Improper Null Termination
190 - Integer Overflow or Wraparound
466 - Return of Pointer Value Outside of Expected Range
470 - Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')
73 - External Control of File Name or Path
785 - Use of Path Manipulation Function without Maximum-sized Buffer