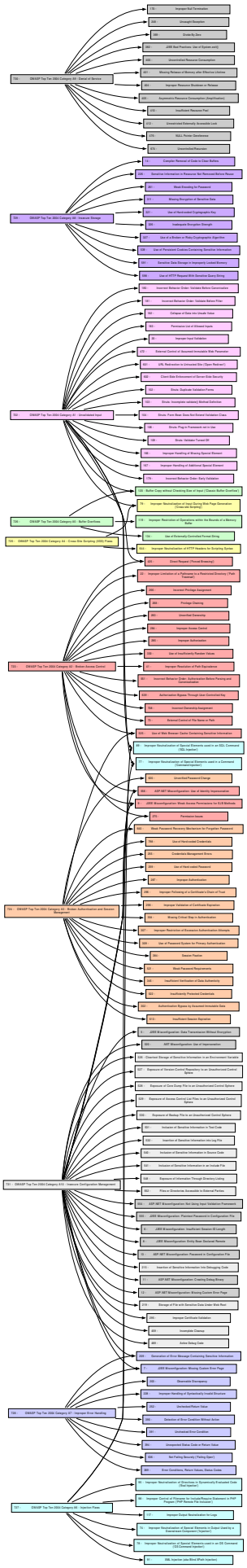
730 : OWASP Top Ten 2004 Category A9 - Denial of Service
125 : Improper Null Termination
400 : Uncaught Exception
369 : Divide By Zero
382 : J2EE Bad Practices: Use of System.exit()
405 : Unconstrained Resource Consumption
231 : Missing Release of Memory after Effective Lifetime
404 : Improper Resource Shutdown or Release
405 : Asymmetric Resource Consumption (Amplification)
772 : Unreleased Resource Pool
770 : Unconstrained Externally Accessible Load
119 : NULL Pointer Dereference
771 : Unconstrained Resources
729 : OWASP Top Ten 2004 Category A8 - Insecure Storage
11 : Compiler Removal of Code to Clear Buffers
524 : Sensitive Information in Resource Not Removed Before Reuse
261 : Weak Encoding for Password
311 : Missing Encryption of Sensitive Data
321 : Use of Hard-coded Cryptographic Key
326 : Inadequate Encryption Strength
327 : Use of a Broken or Risky Cryptographic Algorithm
256 : Use of Persistent Cookies Containing Sensitive Information
257 : Sensitive Data Storage in Improperly Locked Memory
358 : Use of HTTP Request With Sensitive Query String
732 : OWASP Top Ten 2004 Category A1 - Unvalidated Input
180 : Incorrect Behavior Order: Validate Before Canonicalize
181 : Incorrect Behavior Order: Validate Before Filter
184 : Collapse of Data into Unsafe Value
242 : Persistence Ind of Unsafe Inputs
20 : Improper Input Validation
552 : External Control of Assumed-Immutable Web Parameter
601 : URL Redirection to Untrusted Site (Open Redirect)
642 : Client-Side Enforcement of Server-Side Security
102 : Struts: Duplicate Validation Forms
103 : Struts: Incomplete validate() Method Definition
104 : Struts: Form Bean Does Not Extend Validation Class
105 : Struts: Plug-in Framework not in Use
106 : Struts: Validator Turned Off
166 : Improper Handling of Missing Special Element
167 : Improper Handling of Additional Special Element
179 : Incorrect Behavior Order: Early Validation
120 : Buffer Copy without Checking Size of Input ("Classic Buffer Overflow")
79 : Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")
119 : Improper Restriction of Operations within the Bounds of a Memory Buffer
184 : Use of Externally-Controlled Format String
113 : Improper Neutralization of HTTP Headers for Scripting Syntax
248 : Direct Request ("Forced Browsing")
22 : Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")
266 : Incorrect Privilege Assignment
269 : Privilege Chaining
282 : Unverified Ownership
285 : Improper Access Control
285 : Improper Authorization
286 : Use of Insufficiently Random Values
21 : Improper Resolution of Path Equivalence
287 : Incorrect Behavior Order: Authentication Before Parsing and Interpretation
319 : Authentication Bypass Through Use Controlled Key
286 : Incorrect Ownership Assignment
73 : External Control of File Name or Path
359 : Use of Web Browser Cache Containing Sensitive Information
80 : Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection")
81 : Improper Neutralization of Special Elements used in a Command ("Command Injection")
262 : Unverified Password Change
264 : J2EE MET: Misconfiguration: Use of Identity Impersonation
8 : J2EE Misconfiguration: Weak Access Permissions for EJB Methods
255 : Permission Issues
640 : Weak Password Recovery Mechanism for Forgotten Password
798 : Use of Hard-coded Credentials
315 : Cleartext Storage of Sensitive Information in a Cookie
259 : Use of Hard-coded Password
287 : Improper Authentication
298 : Improper Following of a Certificate's Chain of Trust
299 : Improper Validation of Certificate Expiration
304 : Missing Critical Step in Authentication
307 : Improper Restriction of Excessive Authentication Attempts
309 : Use of Password System for Primary Authentication
521 : Weak Password Requirements
522 : Insufficiently Protected Credentials
523 : Unprotected Transport of Credentials
287 : Authentication Bypass by Assumed-Immutable Data
613 : Insufficient Session Expiration
5 : J2EE Misconfiguration: Data Transmission Without Encryption
103 : J2EE Misconfiguration: Use of Impersonation
732 : OWASP Top Ten 2004 Category A10 - Insecure Configuration Management
315 : Cleartext Storage of Sensitive Information in an Environment Variable
527 : Exposure of Version Control Repository to an Unauthorized Control Sphere
528 : Exposure of Core Dump File to an Unauthorized Control Sphere
529 : Exposure of Access Control List Files to an Unauthorized Control Sphere
530 : Exposure of Backup File to an Unauthorized Control Sphere
531 : Inclusion of Sensitive Information in Test Code
532 : Insertion of Sensitive Information into Log File
540 : Inclusion of Sensitive Information in Source Code
541 : Inclusion of Sensitive Information in an Include File
548 : Exposure of Information Through Directory Listing
552 : Files or Directories Accessible to External Parties
233 : ASP.NET Misconfiguration: Not Using Input Validation Framework
315 : J2EE Misconfiguration: Plaintext Password in Configuration File
3 : J2EE Misconfiguration: Unofficial Session ID Length
8 : J2EE Misconfiguration: Entity Bean Declared Remote
12 : ASP.NET Misconfiguration: Password in Configuration File
215 : Insertion of Sensitive Information Into Debugging Code
217 : ASP.NET Misconfiguration: Creating Debug Binary
2 : ASP.NET Misconfiguration: Missing Custom Error Page
219 : Storage of File with Sensitive Data Under Web Root
295 : Improper Certificate Validation
297 : Improper Hostname Verification
489 : Active Debug Code
209 : Generation of Error Message Containing Sensitive Information
7 : J2EE Misconfiguration: Missing Custom Error Page
390 : Observable Discrepancy
228 : Improper Handling of Syntactically Invalid Structure
251 : Unchecked Return Value
390 : Detection of Error Condition Without Action
391 : Unchecked Error Condition
392 : Unreported Status Code or Return Value
393 : Not Failing Securely ("Failing Open")
394 : Error Conditions, Return Values, Status Codes
734 : OWASP Top Ten 2004 Category A3 - Improper Error Handling
95 : Improper Neutralization of Directives in Dynamically Evaluated Code ("Eval Injection")
96 : Improper Control of Filename for Include/Require Statement in PHP Program ("PHP Remote File Inclusion")
117 : Improper Output Neutralization for Logs
76 : Improper Neutralization of Special Elements in Output Used by a Downstream Component ("Injection")
78 : Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection")
91 : XML Injection (aka Blind XPath Injection)
737 : OWASP Top Ten 2004 Category A6 - Injection Flaws