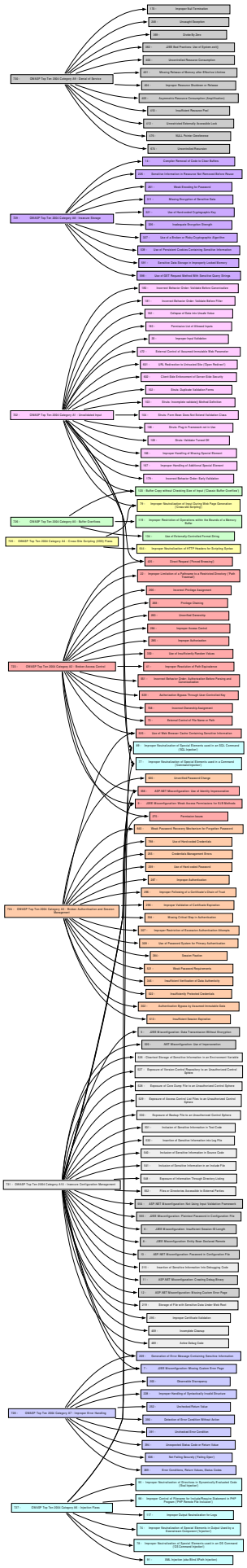
730 : OWASP Top Ten 2004 Category A9 - Denial of Service
119 : Improper Buf Termination
400 : Uncaught Exception
369 : Divide By Zero
382 : J2EE Bad Practices: Use of System.exit()
405 : Unconstrained Resource Consumption
231 : Missing Release of Memory after Effective Lifetime
404 : Improper Resource Shutdown or Release
834 : Excessive Resource Consumption (Amplification)
772 : Unclosed Resource Port
770 : Unrestricted Externally Accessible Lock
176 : NULL Pointer Dereference
833 : Unrestricted Resources
731 : 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
539 : Use of Persistent Cookies Containing Sensitive Information
257 : Storing Passwords in a Recoverable Format
312 : Cleartext Storage of Sensitive Information
732 : OWASP Top Ten 2004 Category A7 - Unvalidated Input
180 : Incorrect Behavior Order: Validate Before Canonicalize
181 : Incorrect Behavior Order: Validate Before Filter
184 : Collapse of Data into Unsafe Value
302 : Persistence Stor of Unsafe Inputs
20 : Improper Input Validation
552 : Files or Directories Accessible to External Parties
601 : URL Redirection to Untrusted Site (Open Redirect)
602 : Client-Side Enforcement of Server-Side Security
642 : Struts: Duplicate Validation Forms
103 : Struts: Incomplete validate() Method Definition
141 : Struts: Form Bean Does Not Extend Validation Class
108 : Struts: Plug-in Framework not in Use
109 : 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 CRLF Sequences in HTTP Headers for Scripting Syntax
785 : OWASP Top Ten 2004 Category A6 - Injection Flaws
784 : OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws
346 : Direct Request (Forced Browsing)
22 : Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")
733 : OWASP Top Ten 2004 Category A5 - Broken Access Control
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: Authorization Before Parsing and Canonicalization
219 : Authentication Bypass Through Upper Controlled Key
286 : Incorrect Ownership Assignment
73 : External Control of File Name or Path
527 : Use of Web Browser Cache Containing Sensitive Information
91 : Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection")
77 : Improper Neutralization of Special Elements used in a Command ("Command Injection")
262 : Unverified Password Change
304 : J2EE BST: Misconfiguration: Use of Identity Impersonation
5 : J2EE Misconfiguration: Weak Access Permissions for EJB Methods
215 : 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 Validation of a Certificate Chain of Trust
299 : Improper Validation of Certificate Expiration
304 : Missing Critical Step in Authentication
287 : Improper Restriction of Excessive Authentication Attempts
289 : Use of Password System for Primary Authentication
521 : Weak Password Requirements
345 : Insufficient Verification of Data Authenticity
522 : Insufficiently Protected Credentials
302 : Authentication Bypass by Assumed-Immutable Data
613 : Insufficient Session Expiration
734 : OWASP Top Ten 2004 Category A10 - Insecure Configuration Management
5 : J2EE Misconfiguration: Data Transmission Without Encryption
103 : BST Misconfiguration: Use of Impersonation
315 : Cleartext Storage of Sensitive Information in an Environment Variable
537 : Exposure of Sensitive Control Resources to an Unauthorized Control Sphere
538 : Exposure of Core Dump File to an Unauthorized Control Sphere
539 : Exposure of Access Control List Files to an Unauthorized Control Sphere
540 : Exposure of Backup File to an Unauthorized Control Sphere
651 : 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
303 : ASP.NET Misconfiguration: Not Using Input Validation Framework
315 : J2EE Misconfiguration: Plaintext Password in Configuration File
8 : J2EE Misconfiguration: Unsafe Session ID Length
9 : J2EE Misconfiguration: Entity Bean Declared Remote
12 : ASP.NET Misconfiguration: Password in Configuration File
215 : Insertion of Sensitive Information Into Debugging Code
117 : 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
489 : Leftover Debug Code
209 : Generation of Error Message Containing Sensitive Information
7 : J2EE Misconfiguration: Missing Custom Error Page
390 : Observable Discrepancy
248 : Improper Handling of Syntactically Invalid Structure
391 : Unchecked Error Value
395 : Detection of Error Condition Without Action
392 : Unchecked Error Condition
755 : Improper Handling of Exceptional Conditions
600 : Not Failing Securely ("Failing Open")
389 : Error Conditions, Return Values, Status Codes
96 : Improper Neutralization of Directives in Dynamically Evaluated Code (Deep Injection)
99 : Improper Control of Filename for Include/Require Statement in PHP Program (PHP Remote File Inclusion)
117 : Improper Output Neutralization for Logs
75 : 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")
89 : SQL Injection (aka Blind SPrint Injection)