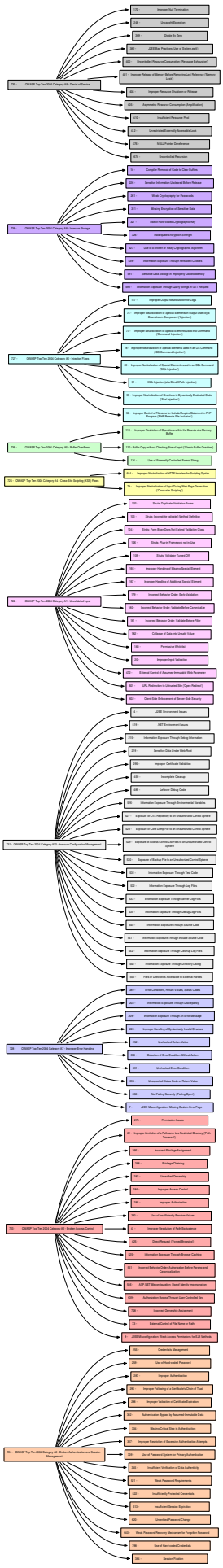
CWE/SIP Top Ten 2009 Category 0 - Insecure Interaction Between Components
170 - Improper Null Termination
248 - Uncaught Exception
390 - Errors By Item
460 - JSP/ASP Page Protections, Use of Sessions and
400 - Unnecessary Resource Consumption ("Resource Exhaustion")
401 - Improper Release of Memory Before Removing Last Reference ("Memory Leak")
243 - Improper Resource Shutdown or Release
245 - Asymmetric Resource Consumption (Amplification)
248 - Insufficient Resource Pool
412 - Unrestricted Externally Accessible Lock
476 - NULL Pointer Dereference
675 - Unsanitized Resources
CWE/SIP Top Ten 2009 Category 08 - Insecure Storage
312 - Cleartext Storage of Data in Clear Buffers
313 - Sensitive Information Uncleared Before Release
321 - Weak Cryptography for Passwords
317 - Missing Encryption of Sensitive Data
323 - Use of Hard-coded Cryptographic Key
326 - Inadequate Encryption Strength
327 - Use of a Broken or Risky Cryptographic Algorithm
403 - Information Exposure Through Persistent Cookies
311 - Sensitive Data Storage in Improperly Locked Memory
360 - Information Exposure Through Query Strings in GET Request
CWE/SIP Top Ten 2009 Category 06 - Injection Flaws
177 - Improper Output Neutralization for Logs
75 - Improper Neutralization of Special Elements in Output Used by a Downstream Component ("Injection")
77 - Improper Neutralization of Special Elements used in a Command ("Command Injection")
78 - Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection")
80 - Improper Neutralization of Special Elements used in an XSS Command ("XSS Injection")
91 - XML Injection (aka Blind XPath Injection)
89 - Improper Neutralization of Special Elements in Data Query Logic
90 - Improper Control of Resource Identifiers ("Resource Injection")
CWE/SIP Top Ten 2009 Category 05 - Buffer Overflows
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
CWE/SIP Top Ten 2009 Category 04 - Cross-Site Scripting (XSS) Flaws
644 - Improper Neutralization of HTTP Headers for Scripting Syntax
79 - Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")
CWE/SIP Top Ten 2009 Category 07 - Unvalidated Input
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
203 - Improper Handling of Missing Special Element
207 - Improper Handling of Additional Special Element
179 - Incorrect Behavior Order: Early Validation
180 - Incorrect Behavior Order: Validate Before Canonicalize
181 - Incorrect Behavior Order: Validate Before Filter
140 - Collapse of Data into Unsafe Value
185 - Permissive Whitelist
20 - Improper Input Validation
213 - Exposure of Sensitive Information Due to Incompatible Policies
601 - URL Redirection to Untrusted Site ("Open Redirect")
602 - Client-Side Enforcement of Server-Side Security
CWE/SIP Top Ten 2009 Category 10 - Insecure Configuration Management
2 - J2EE Environment Issues
219 - .NET Environment Issues
215 - Information Exposure Through Debug Information
219 - Sensitive Data Under Web Root
295 - Improper Certificate Validation
459 - Incomplete Cleanup
489 - Leftover Debug Code
526 - Information Exposure Through Environmental Variables
527 - Exposure of CVS Repository to an Unauthorized Control Sphere
528 - Exposure of Core Dump File to an Unauthorized Control Sphere
530 - Exposure of Backup File to an Unauthorized Control Sphere
531 - Information Exposure Through Test Code
532 - Information Exposure Through Log Files
533 - Information Exposure Through Server Log Files
534 - Information Exposure Through Debug Log Files
540 - Information Exposure Through Source Code
547 - Information Exposure Through Include Source Code
552 - Information Exposure Through Charset Log Files
589 - Information Exposure Through Directory Listing
602 - Files or Directories Accessible to External Parties
CWE/SIP Top Ten 2009 Category 07 - Improper Error Handling
209 - Error Conditions, Return Values, Status Codes
210 - Information Exposure Through Discrepancy
211 - Information Exposure Through an Error Message
224 - Improper Handling of Syntactically Invalid Structure
252 - Unchecked Return Value
390 - Detection of Error Condition Without Action
391 - Unchecked Error Condition
393 - Unexpected Status Code or Return Value
636 - Not Failing Securely ("Failing Open")
7 - J2EE Misconfiguration: Missing Custom Error Page
CWE/SIP Top Ten 2009 Category 02 - Broken Access Control
285 - Permission Issues
302 - Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")
230 - Improper Privilege Management
269 - Privilege Creeping
283 - Unverified Ownership
284 - Improper Access Control
285 - Improper Authorization
330 - Use of Insufficiently Random Values
17 - Improper Restriction of Path Equivalence
224 - Obfuscated Security Elements
351 - Information Exposure Through Browser Caching
367 - Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
302 - J2EE MVC Misconfiguration: Use of Identity Impersonation
603 - Authorization Bypass Through User-Controlled Key
708 - Incorrect Ownership Assignment
73 - External Control of File Name or Path
76 - J2EE Misconfiguration: Weak Access Permissions for EJB Methods
CWE/SIP Top Ten 2009 Category 03 - Broken Authentication and Session Management
255 - Credentials Management
259 - Use of Hard-coded Password
287 - Improper Authentication
289 - Improper Following of a Certificate's Chain of Trust
298 - Improper Validation of Certificate Expiration
302 - Authentication Bypass by Assumed-Immutable Data
306 - Missing Critical Step in Authentication
307 - Improper Restriction of Excessive Authentication Attempts
309 - Use of Password System for Primary Authentication
345 - Insufficient Verification of Data Authenticity
521 - Weak Password Requirements
522 - Insufficiently Protected Credentials
613 - Insufficient Session Expiration
620 - Unverified Password Change
640 - Weak Password Recovery Mechanism for Forgotten Password
798 - Use of Hard-coded Credentials
384 - Session Fixation