730 OWASP Top Ten 2004 Category 30 - Denial of Service
705 Improper Null Termination
248 Uncaught Exception
369 Divide By Zero
382 J2EE Bad Practices: Use of System.exit()
400 Uncontrolled Resource Consumption ("Resource Exhaustion")
401 Failure to Release Memory Before Removing Last Reference ("Memory Leak")
250 Improper Resource Shutdown or Release
405 Asymmetric Resource Consumption (Amplification)
410 Insufficient Resource Pool
412 Unrestricted Externally Accessible Lock
476 NULL Pointer Dereference
400 Uncontrolled Recursion
359 OWASP Top Ten 2004 Category A8 - Insecure Storage
12 Cryptic Removal of Code in Client Buffers
256 Sensitive Information Uncovered Before Release
261 Weak Cryptography for Passwords
317 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
329 Predictable Lack Through Persistent Counter
347 Sensitive Data Storage in Improperly Locked Memory
365 Information Leak Through Query Strings in GET Request
201 OWASP Top Ten 2004 Category A6 - Injection Flaws
117 Improper Output Sanitization for Logs
74 Failure to Sanitize Data into a Different Plane ("Injection")
77 Improper Sanitization of Special Elements used in a Command ("Command Injection")
78 Improper Sanitization of Special Elements used in an OS Command ("OS Command Injection")
89 Improper Sanitization of Special Elements used in an SQL Command ("SQL Injection")
91 XML Injection (aka Blind XPath Injection)
95 Improper Sanitization of Directives in Dynamically Evaluated Code ("Eval Injection")
96 Improper Control of Filename for Include/Require Statement in PHP Program ("PHP File Inclusion")
119 Failure to Constrain Operations within the Bounds of a Memory Buffer
120 Buffer Copy without Checking Size of Input ("Classic Buffer Overflow")
134 Uncontrolled Format String
352 Improper Neutralization of HTTP Headers for Scripting Syntax
79 Failure to Preserve Web Page Structure ("Cross-site Scripting")
730 OWASP Top Ten 2004 Category A1 - 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
180 Improper Handling of Missing Special Element
181 Improper Handling of Additional Special Element
179 Incorrect Behavior Order: Early Validation
183 Incorrect Behavior Order: Validate Before Canonicalize
187 Incorrect Behavior Order: Validate Before Filter
191 Collapse of Data Into Unsafe Value
192 Numeric Widening
20 Improper Input Validation
114 External Control of Assumed-Immutable Web Parameter
601 URL Redirection to Untrusted Site ("Open Redirect")
602 Client-Side Enforcement of Server-Side Security
389 Error Handling
203 Information Exposure Through Discrepancy
209 Information Exposure Through an Error Message
524 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
394 Not Following Redirects ("Failing Open")
395 J2EE Misconfiguration: Missing Custom Error Page
285 Permission Issues
22 Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal")
248 Incorrect Privilege Assignment
286 Privilege Chaining
287 Improper Authentication
263 Access Control (Authorization) Issues
285 Improper Access Control (Authorization)
233 Use of Insufficiently Random Values
17 Improper Resolution of Path Equivalence
351 Cross-Request ("Forced Browsing")
200 Information Leak Through Browser Caching
311 Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
132 ASP.NET Misconfiguration: Use of Identity Impersonation
302 Access Control Bypass Through User-Controlled Key
250 Incorrect Ownership Assignment
73 External Control of File Name or Path
71 J2EE Misconfiguration: Weak Access Permissions for EJB Methods
256 Credentials Management
259 Use of Hard-coded Password
287 Improper Authentication
295 Improper Following of Chain of Trust for Certificate Validation
296 Improper Validation of Certificate Expiration
287 Authentication Bypass by Assumed-Immutable Data
304 Missing Critical Step in Authentication
307 Improper Restriction of Excessive Authentication Attempts
309 Use of Password System for Primary Authentication
303 Insufficient Verification of Data Authenticity
521 Weak Password Requirements
523 Insufficiently Protected Credentials
305 Authentication Bypass Issues
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
732 OWASP Top Ten 2004 Category A10 - Insecure Configuration Management
10 ASP.NET Environment Issues
295 Certificate Issues
11 J2EE Environment Issues
213 Information Leak Through Debug Information
219 Sensitive Data Under Web Root
489 Incomplete Cleanup
489 Leftover Debug Code
200 Information Leak Through Environmental Variables
607 Exposure of CGI: Repository on an Unauthorized Control Sphere
608 Exposure of Core Dump File to an Unauthorized Control Sphere
609 Exposure of Source Control List Files to an Unauthorized Control Sphere
610 Exposure of Backup File to an Unauthorized Control Sphere
531 Information Leak Through Test Code
532 Information Leak Through Log Files
533 Information Leak Through Server Log Files
534 Information Leak Through Debug Log Files
540 Information Leak Through Source Code
541 Information Leak Through Include Source Code
542 Information Leak Through Cleanup Log Files
548 Information Leak Through Directory Listing
552 Files or Directories Accessible to External Parties