
730 - OWASP Top Ten 2004 Category A9 - Denial of Service
170 - Improper Null Termination
248 - Uncaught Exception
369 - Divide By Zero
382 - J2EE Bad Practices: Use of System.exit()
400 - Uncontrolled Resource Consumption
401 - Missing Release of Memory after Effective Lifetime
404 - Improper Resource Shutdown or Release
405 - Asymmetric Resource Consumption (Amplification)
410 - Insufficient Resource Pool
412 - Unrestricted Externally Accessible Lock
476 - NULL Pointer Dereference
674 - Uncontrolled Recursion
729 - OWASP Top Ten 2004 Category A8 - Insecure Storage
14 - Compiler Removal of Code to Clear Buffers
226 - 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
591 - Sensitive Data Storage in Improperly Locked Memory
598 - Use of HTTP Request With Sensitive Query String
722 - OWASP Top Ten 2004 Category A1 - Unvalidated Input
180 - Incorrect Behavior Order: Validate Before Canonicalize
181 - Incorrect Behavior Order: Validate Before Filter
182 - Collapse of Data into Unsafe Value
183 - Permissive List of Allowed Inputs
20 - Improper Input Validation
472 - External Control of Assumed-Immutable Web Parameter
601 - URL Redirection to Untrusted Site
602 - 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
106 - 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
726 - OWASP Top Ten 2004 Category A5 - Buffer Overflows
120 - Buffer Copy without Checking Size of Input
119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
134 - Use of Externally-Controlled Format String
725 - OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws
79 - Improper Neutralization of Input During Web Page Generation
644 - Improper Neutralization of HTTP Headers for Scripting Syntax
723 - OWASP Top Ten 2004 Category A2 - Broken Access Control
425 - Direct Request
22 - Improper Limitation of a Pathname to a Restricted Directory
266 - Incorrect Privilege Assignment
268 - Privilege Chaining
283 - Unverified Ownership
284 - Improper Access Control
285 - Improper Authorization
330 - Use of Insufficiently Random Values
41 - Improper Resolution of Path Equivalence
551 - Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
639 - Authorization Bypass Through User-Controlled Key
708 - Incorrect Ownership Assignment
73 - External Control of File Name or Path
525 - Use of Web Browser Cache Containing Sensitive Information
89 - Improper Neutralization of Special Elements used in an SQL Command
77 - Improper Neutralization of Special Elements used in a Command
620 - Unverified Password Change
556 - ASP.NET Misconfiguration: Use of Identity Impersonation
9 - J2EE Misconfiguration: Weak Access Permissions for EJB Methods
275 - Permission Issues
724 - OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management
640 - Weak Password Recovery Mechanism for Forgotten Password
798 - Use of Hard-coded Credentials
255 - Credentials Management Errors
259 - Use of Hard-coded Password
287 - Improper Authentication
296 - Improper Following of a Certificate's Chain of Trust
298 - 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
384 - Session Fixation
521 - Weak Password Requirements
345 - Insufficient Verification of Data Authenticity
522 - Insufficiently Protected Credentials
302 - Authentication Bypass by Assumed-Immutable Data
613 - DEPRECATED: Insufficient Session Expiration
731 - OWASP Top Ten 2004 Category A10 - Insecure Configuration Management
5 - J2EE Misconfiguration: Data Transmission Without Encryption
520 - .NET Misconfiguration: Use of Impersonation
526 - 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
554 - ASP.NET Misconfiguration: Not Using Input Validation Framework
555 - J2EE Misconfiguration: Plaintext Password in Configuration File
6 - J2EE Misconfiguration: Insufficient Session-ID Length
8 - J2EE Misconfiguration: Entity Bean Declared Remote
13 - ASP.NET Misconfiguration: Password in Configuration File
215 - Insertion of Sensitive Information Into Debugging Code
11 - ASP.NET Misconfiguration: Creating Debug Binary
12 - ASP.NET Misconfiguration: Missing Custom Error Page
219 - Storage of File with Sensitive Data Under Web Root
295 - Improper Certificate Validation
459 - Incomplete Cleanup
489 - Active Debug Code
728 - OWASP Top Ten 2004 Category A7 - Improper Error Handling
209 - Generation of Error Message Containing Sensitive Information
7 - J2EE Misconfiguration: Missing Custom Error Page
203 - Observable Discrepancy
228 - Improper Handling of Syntactically Invalid Structure
252 - Unchecked Return Value
390 - Detection of Error Condition Without Action
391 - DEPRECATED: Unchecked Error Condition
394 - Unexpected Status Code or Return Value
636 - Not Failing Securely
389 - Error Conditions, Return Values, Status Codes
727 - OWASP Top Ten 2004 Category A6 - Injection Flaws
95 - Improper Neutralization of Directives in Dynamically Evaluated Code
98 - Improper Control of Filename for Include/Require Statement in PHP Program
117 - Improper Output Neutralization for Logs
74 - Improper Neutralization of Special Elements in Output Used by a Downstream Component
78 - Improper Neutralization of Special Elements used in an OS Command
91 - XML Injection