
922 - Insecure Storage of Sensitive Information
834 - Excessive Iteration
835 - Loop with Unreachable Exit Condition
755 - Improper Handling of Exceptional Conditions
697 - Incorrect Comparison
704 - Incorrect Type Conversion or Cast
681 - Incorrect Conversion between Numeric Types
843 - Access of Resource Using Incompatible Type
674 - Uncontrolled Recursion
776 - Improper Restriction of Recursive Entity References in DTDs
662 - Improper Synchronization
667 - Improper Locking
863 - Incorrect Authorization
639 - Authorization Bypass Through User-Controlled Key
670 - Always-Incorrect Control Flow Implementation
617 - Reachable Assertion
436 - Interpretation Conflict
444 - Inconsistent Interpretation of HTTP Requests
862 - Missing Authorization
425 - Direct Request
415 - Double Free
672 - Operation on a Resource after Expiration or Release
416 - Use After Free
613 - DEPRECATED: Insufficient Session Expiration
401 - Missing Release of Memory after Effective Lifetime
404 - Improper Resource Shutdown or Release
459 - Incomplete Cleanup
763 - Release of Invalid Pointer or Reference
772 - Missing Release of Resource after Effective Lifetime
400 - Uncontrolled Resource Consumption
770 - Allocation of Resources Without Limits or Throttling
920 - Improper Restriction of Power Consumption
363 - Concurrent Execution using Shared Resource with Improper Synchronization
367 - Time-of-check Time-of-use (TOCTOU) Race Condition
346 - Origin Validation Error
347 - Improper Verification of Cryptographic Signature
345 - Insufficient Verification of Data Authenticity
352 - Cross-Site Request Forgery
354 - Improper Validation of Integrity Check Value
924 - Improper Enforcement of Message Integrity During Transmission in a Communication Channel
331 - Insufficient Entropy
330 - Use of Insufficiently Random Values
335 - Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)
338 - Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)
327 - Use of a Broken or Risky Cryptographic Algorithm
916 - Use of Password Hash With Insufficient Computational Effort
326 - Inadequate Encryption Strength
312 - Cleartext Storage of Sensitive Information
311 - Missing Encryption of Sensitive Data
319 - Cleartext Transmission of Sensitive Information
290 - Authentication Bypass by Spoofing
294 - Authentication Bypass by Capture-replay
295 - Improper Certificate Validation
306 - Missing Authentication for Critical Function
287 - Improper Authentication
307 - Improper Restriction of Excessive Authentication Attempts
521 - Weak Password Requirements
522 - Insufficiently Protected Credentials
640 - Weak Password Recovery Mechanism for Forgotten Password
798 - Use of Hard-coded Credentials
732 - Incorrect Permission Assignment for Critical Resource
276 - Incorrect Default Permissions
281 - Improper Preservation of Permissions
269 - Improper Privilege Management
252 - Unchecked Return Value
754 - Improper Check for Unusual or Exceptional Conditions
273 - Improper Check for Dropped Privileges
476 - NULL Pointer Dereference
212 - Improper Removal of Sensitive Information Before Storage or Transfer
434 - Unrestricted Upload of File with Dangerous Type
669 - Incorrect Resource Transfer Between Spheres
494 - Download of Code Without Integrity Check
565 - Reliance on Cookies without Validation and Integrity Checking
829 - Inclusion of Functionality from Untrusted Control Sphere
203 - Observable Discrepancy
200 - Exposure of Sensitive Information to an Unauthorized Actor
209 - Generation of Error Message Containing Sensitive Information
532 - Insertion of Sensitive Information into Log File
178 - Improper Handling of Case Sensitivity
706 - Use of Incorrectly-Resolved Name or Reference
22 - Improper Limitation of a Pathname to a Restricted Directory
59 - Improper Link Resolution Before File Access
134 - Use of Externally-Controlled Format String
426 - Untrusted Search Path
427 - Uncontrolled Search Path Element
428 - Unquoted Search Path or Element
552 - Files or Directories Accessible to External Parties
407 - Inefficient Algorithmic Complexity
1333 - Inefficient Regular Expression Complexity
1321 - Improperly Controlled Modification of Object Prototype Attributes
915 - Improper Control of Dynamically-Managed Code Resources
470 - Use of Externally-Controlled Input to Select Classes or Code
502 - Deserialization of Untrusted Data
131 - Incorrect Calculation of Buffer Size
190 - Integer Overflow or Wraparound
682 - Incorrect Calculation
191 - Integer Underflow (Wrap or Wraparound)
193 - Off-by-one Error
369 - Divide By Zero
1284 - Improper Validation of Specified Quantity in Input
20 - Improper Input Validation
129 - Improper Validation of Array Index
1236 - Improper Neutralization of Formula Elements in a CSV File
77 - Improper Neutralization of Special Elements used in a Command
78 - Improper Neutralization of Special Elements used in an OS Command
79 - Improper Neutralization of Input During Web Page Generation
88 - Improper Neutralization of Argument Delimiters in a Command
89 - Improper Neutralization of Special Elements used in an SQL Command
74 - Improper Neutralization of Special Elements in Output Used by a Downstream Component
91 - XML Injection
917 - Improper Neutralization of Special Elements used in an Expression Language Statement
94 - Improper Control of Generation of Code
120 - Buffer Copy without Checking Size of Input
119 - Improper Restriction of Operations within the Bounds of a Memory Buffer
125 - Out-of-bounds Read
787 - Out-of-bounds Write
824 - Access of Uninitialized Pointer
1188 - Initialization of a Resource with an Insecure Default
665 - Improper Initialization
908 - Use of Uninitialized Resource
909 - Missing Initialization of Resource
116 - Improper Encoding or Escaping of Output
838 - Inappropriate Encoding for Output Context
1021 - Improper Restriction of Rendered UI Layers or Frames
384 - Session Fixation
610 - Externally Controlled Reference to a Resource in Another Sphere
601 - URL Redirection to Untrusted Site
611 - Improper Restriction of XML External Entity Reference
918 - Server-Side Request Forgery