

- B CWE-645: Overly Restrictive Account Lockout Mechanism (p.1432)
- G CWE-346: Origin Validation Error (p.860)
- V CWE-1385: Missing Origin Validation in WebSockets (p.2271)
- B CWE-940: Improper Verification of Source of a Communication Channel (p.1852)
- V CWE-925: Improper Verification of Intent by Broadcast Receiver (p.1841)
- B CWE-749: Exposed Dangerous Method or Function (p.1572)
- V CWE-618: Exposed Unsafe ActiveX Method (p.1389)
- V CWE-782: Exposed IOCTL with Insufficient Access Control (p.1657)
- G CWE-923: Improper Restriction of Communication Channel to Intended Endpoints (p.1836)
- V CWE-1275: Sensitive Cookie with Improper SameSite Attribute (p.2123)
- V CWE-291: Reliance on IP Address for Authentication (p.715)
- V CWE-297: Improper Validation of Certificate with Host Mismatch (p.729)
- G CWE-300: Channel Accessible by Non-Endpoint (p.737)
- B CWE-419: Unprotected Primary Channel (p.1024)
- B CWE-420: Unprotected Alternate Channel (p.1025)
- B CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface (p.2174)
- B CWE-421: Race Condition During Access to Alternate Channel (p.1028)
- V CWE-422: Unprotected Windows Messaging Channel ('Shatter') (p.1029)
- B CWE-940: Improper Verification of Source of a Communication Channel (p.1852)
- V CWE-925: Improper Verification of Intent by Broadcast Receiver (p.1841)
- B CWE-941: Incorrectly Specified Destination in a Communication Channel (p.1855)
- V CWE-942: Permissive Cross-domain Policy with Untrusted Domains (p.1857)
- P CWE-435: Improper Interaction Between Multiple Correctly-Behaving Entities (p.1063)
- G CWE-1038: Insecure Automated Optimizations (p.1881)
- B CWE-1037: Processor Optimization Removal or Modification of Security-critical Code (p.1879)
- B CWE-733: Compiler Optimization Removal or Modification of Security-critical Code (p.1570)
- V CWE-14: Compiler Removal of Code to Clear Buffers (p.14)
- B CWE-188: Reliance on Data/Memory Layout (p.476)
- V CWE-198: Use of Incorrect Byte Ordering (p.510)
- G CWE-436: Interpretation Conflict (p.1065)
- V CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') (p.277)
- B CWE-115: Misinterpretation of Input (p.286)
- B CWE-437: Incomplete Model of Endpoint Features (p.1067)
- B CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') (p.1075)
- V CWE-626: Null Byte Interaction Error (Poison Null Byte) (p.1403)
- V CWE-650: Trusting HTTP Permission Methods on the Server Side (p.1441)
- V CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages (p.194)
- B CWE-439: Behavioral Change in New Version or Environment (p.1068)
- P CWE-664: Improper Control of a Resource Through its Lifetime (p.1463)
- G CWE-118: Incorrect Access of Indexable Resource ('Range Error') (p.298)
- G CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
- B CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
- V CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer (p.1664)
- B CWE-125: Out-of-bounds Read (p.336)
- V CWE-126: Buffer Over-read (p.340)
- V CWE-127: Buffer Under-read (p.343)
- B CWE-466: Return of Pointer Value Outside of Expected Range (p.1117)
- B CWE-786: Access of Memory Location Before Start of Buffer (p.1666)
- B CWE-124: Buffer Underwrite ('Buffer Underflow') (p.332)
- V CWE-127: Buffer Under-read (p.343)
- B CWE-787: Out-of-bounds Write (p.1669)
- V CWE-121: Stack-based Buffer Overflow (p.320)
- V CWE-122: Heap-based Buffer Overflow (p.324)
- B CWE-123: Write-what-where Condition (p.329)

- B CWE-124: Buffer Underwrite ('Buffer Underflow') (p.332)
- B CWE-788: Access of Memory Location After End of Buffer (p.1678)
- V CWE-121: Stack-based Buffer Overflow (p.320)
- V CWE-122: Heap-based Buffer Overflow (p.324)
- V CWE-126: Buffer Over-read (p.340)
- B CWE-805: Buffer Access with Incorrect Length Value (p.1711)
- V CWE-806: Buffer Access Using Size of Source Buffer (p.1719)
- B CWE-822: Untrusted Pointer Dereference (p.1732)
- B CWE-823: Use of Out-of-range Pointer Offset (p.1735)
- B CWE-824: Access of Uninitialized Pointer (p.1738)
- B CWE-825: Expired Pointer Dereference (p.1741)
- V CWE-415: Double Free (p.1015)
- V CWE-416: Use After Free (p.1019)
- C CWE-1229: Creation of Emergent Resource (p.2016)
- C CWE-514: Covert Channel (p.1227)
- B CWE-385: Covert Timing Channel (p.947)
- B CWE-515: Covert Storage Channel (p.1229)
- B CWE-1250: Improper Preservation of Consistency Between Independent Representations of Shared State (p.2064)
- B CWE-1249: Application-Level Admin Tool with Inconsistent View of Underlying Operating System (p.2062)
- B CWE-1251: Mirrored Regions with Different Values (p.2065)
- B CWE-1329: Reliance on Component That is Not Updateable (p.2231)
- B CWE-1277: Firmware Not Updateable (p.2128)
- B CWE-1310: Missing Ability to Patch ROM Code (p.2191)
- C CWE-221: Information Loss or Omission (p.563)
- B CWE-222: Truncation of Security-relevant Information (p.565)
- B CWE-223: Omission of Security-relevant Information (p.566)
- B CWE-778: Insufficient Logging (p.1647)
- B CWE-224: Obscured Security-relevant Information by Alternate Name (p.568)
- B CWE-356: Product UI does not Warn User of Unsafe Actions (p.886)
- B CWE-396: Declaration of Catch for Generic Exception (p.966)
- B CWE-397: Declaration of Throws for Generic Exception (p.968)
- C CWE-451: User Interface (UI) Misrepresentation of Critical Information (p.1087)
- B CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User (p.1866)
- B CWE-1021: Improper Restriction of Rendered UI Layers or Frames (p.1869)
- B CWE-372: Incomplete Internal State Distinction (p.926)
- C CWE-400: Uncontrolled Resource Consumption (p.971)
- B CWE-1235: Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations (p.2029)
- B CWE-1246: Improper Write Handling in Limited-write Non-Volatile Memories (p.2054)
- C CWE-405: Asymmetric Resource Consumption (Amplification) (p.993)
- B CWE-1050: Excessive Platform Resource Consumption within a Loop (p.1895)
- B CWE-1072: Data Resource Access without Use of Connection Pooling (p.1921)
- B CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses (p.1922)
- B CWE-1084: Invokable Control Element with Excessive File or Data Access Operations (p.1933)
- B CWE-1089: Large Data Table with Excessive Number of Indices (p.1938)
- B CWE-1094: Excessive Index Range Scan for a Data Resource (p.1943)
- C CWE-1176: Inefficient CPU Computation (p.1980)
- V CWE-1042: Static Member Data Element outside of a Singleton Class Element (p.1886)
- B CWE-1046: Creation of Immutable Text Using String Concatenation (p.1890)
- B CWE-1049: Excessive Data Query Operations in a Large Data Table (p.1894)
- B CWE-1063: Creation of Class Instance within a Static Code Block (p.1910)
- B CWE-1067: Excessive Execution of Sequential Searches of Data Resource (p.1914)

- G CWE-406: Insufficient Control of Network Message Volume (Network Amplification) (p.997)
- G CWE-407: Inefficient Algorithmic Complexity (p.999)
- B CWE-1333: Inefficient Regular Expression Complexity (p.2243)
- B CWE-408: Incorrect Behavior Order: Early Amplification (p.1002)
- B CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) (p.1004)
- B CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') (p.1642)
- B CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
- B CWE-1325: Improperly Controlled Sequential Memory Allocation (p.2222)
- V CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling (p.1639)
- V CWE-789: Memory Allocation with Excessive Size Value (p.1683)
- B CWE-771: Missing Reference to Active Allocated Resource (p.1631)
- V CWE-773: Missing Reference to Active File Descriptor or Handle (p.1638)
- B CWE-779: Logging of Excessive Data (p.1651)
- B CWE-920: Improper Restriction of Power Consumption (p.1832)
- G CWE-404: Improper Resource Shutdown or Release (p.987)
- B CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device (p.2104)
- B CWE-299: Improper Check for Certificate Revocation (p.734)
- V CWE-370: Missing Check for Certificate Revocation after Initial Check (p.924)
- B CWE-459: Incomplete Cleanup (p.1106)
- B CWE-226: Sensitive Information in Resource Not Removed Before Reuse (p.569)
 - V CWE-1239: Improper Zeroization of Hardware Register (p.2033)
 - B CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition (p.2116)
 - B CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component (p.2183)
 - V CWE-1330: Remanent Data Readable after Memory Erase (p.2234)
 - B CWE-1342: Information Exposure through Microarchitectural State after Transient Execution (p.2262)
 - V CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') (p.598)
- B CWE-460: Improper Cleanup on Thrown Exception (p.1109)
- V CWE-568: finalize() Method Without super.finalize() (p.1299)
- B CWE-763: Release of Invalid Pointer or Reference (p.1608)
 - V CWE-761: Free of Pointer not at Start of Buffer (p.1601)
 - V CWE-762: Mismatched Memory Management Routines (p.1605)
 - V CWE-590: Free of Memory not on the Heap (p.1335)
- B CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
- B CWE-1091: Use of Object without Invoking Destructor Method (p.1940)
- V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
- V CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
- B CWE-410: Insufficient Resource Pool (p.1005)
- B CWE-471: Modification of Assumed-Immutable Data (MAID) (p.1129)
 - V CWE-291: Reliance on IP Address for Authentication (p.715)
- B CWE-472: External Control of Assumed-Immutable Web Parameter (p.1131)
- V CWE-473: PHP External Variable Modification (p.1134)
- V CWE-607: Public Static Final Field References Mutable Object (p.1368)
- B CWE-487: Reliance on Package-level Scope (p.1175)
- V CWE-495: Private Data Structure Returned From A Public Method (p.1197)
- V CWE-496: Public Data Assigned to Private Array-Typed Field (p.1199)
- B CWE-501: Trust Boundary Violation (p.1210)
- V CWE-580: clone() Method Without super.clone() (p.1319)
- G CWE-610: Externally Controlled Reference to a Resource in Another Sphere (p.1373)
 - B CWE-15: External Control of System or Configuration Setting (p.17)
- B CWE-384: Session Fixation (p.943)
- G CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') (p.1072)

- B CWE-1021: Improper Restriction of Rendered UI Layers or Frames (p.1869)
- B CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
- B CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (p.1125)
- B CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (p.1353)
- B CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
- B CWE-73: External Control of File Name or Path (p.133)
- C CWE-114: Process Control (p.283)
- C CWE-662: Improper Synchronization (p.1457)
 - B CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)
 - B CWE-663: Use of a Non-reentrant Function in a Concurrent Context (p.1461)
 - V CWE-479: Signal Handler Use of a Non-reentrant Function (p.1154)
 - V CWE-558: Use of getlogin() in Multithreaded Application (p.1281)
 - C CWE-667: Improper Locking (p.1472)
 - B CWE-1232: Improper Lock Behavior After Power State Transition (p.2021)
 - B CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection (p.2023)
 - B CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks (p.2026)
 - B CWE-412: Unrestricted Externally Accessible Lock (p.1007)
 - B CWE-413: Improper Resource Locking (p.1010)
 - V CWE-591: Sensitive Data Storage in Improperly Locked Memory (p.1338)
 - B CWE-414: Missing Lock Check (p.1014)
 - B CWE-609: Double-Checked Locking (p.1371)
 - B CWE-764: Multiple Locks of a Critical Resource (p.1613)
 - B CWE-765: Multiple Unlocks of a Critical Resource (p.1614)
 - B CWE-832: Unlock of a Resource that is not Locked (p.1761)
 - B CWE-833: Deadlock (p.1762)
 - B CWE-820: Missing Synchronization (p.1729)
 - V CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)
 - V CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context (p.1263)
 - B CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
 - B CWE-821: Incorrect Synchronization (p.1731)
 - B CWE-1088: Synchronous Access of Remote Resource without Timeout (p.1937)
 - B CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels (p.2098)
 - V CWE-572: Call to Thread run() instead of start() (p.1305)
 - V CWE-574: EJB Bad Practices: Use of Synchronization Primitives (p.1308)
- C CWE-665: Improper Initialization (p.1465)
 - B CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready (p.2132)
 - C CWE-1419: Incorrect Initialization of Resource (p.2292)
 - B CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data (p.1896)
 - B CWE-1052: Excessive Use of Hard-Coded Literals in Initialization (p.1897)
 - B CWE-1188: Initialization of a Resource with an Insecure Default (p.1983)
 - V CWE-453: Insecure Default Variable Initialization (p.1091)
 - B CWE-1221: Incorrect Register Defaults or Module Parameters (p.2005)
 - B CWE-454: External Initialization of Trusted Variables or Data Stores (p.1092)
 - B CWE-455: Non-exit on Failed Initialization (p.1095)
 - B CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
 - B CWE-1325: Improperly Controlled Sequential Memory Allocation (p.2222)
 - V CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling (p.1639)
 - V CWE-789: Memory Allocation with Excessive Size Value (p.1683)
 - B CWE-908: Use of Uninitialized Resource (p.1802)
 - V CWE-457: Use of Uninitialized Variable (p.1102)
 - C CWE-909: Missing Initialization of Resource (p.1806)

- B CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings (p.2115)
- V CWE-456: Missing Initialization of a Variable (p.1096)
- G CWE-666: Operation on Resource in Wrong Phase of Lifetime (p.1471)
 - V CWE-415: Double Free (p.1015)
 - V CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created (p.1339)
 - V CWE-605: Multiple Binds to the Same Port (p.1364)
 - G CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 - V CWE-298: Improper Validation of Certificate Expiration (p.733)
 - B CWE-324: Use of a Key Past its Expiration Date (p.799)
 - B CWE-613: Insufficient Session Expiration (p.1380)
 - B CWE-825: Expired Pointer Dereference (p.1741)
 - V CWE-415: Double Free (p.1015)
 - V CWE-416: Use After Free (p.1019)
 - B CWE-910: Use of Expired File Descriptor (p.1809)
 - B CWE-826: Premature Release of Resource During Expected Lifetime (p.1743)
- G CWE-668: Exposure of Resource to Wrong Sphere (p.1478)
 - B CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) (p.1985)
 - B CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
 - B CWE-1282: Assumed-Immutable Data is Stored in Writable Memory (p.2139)
 - B CWE-1327: Binding to an Unrestricted IP Address (p.2227)
 - B CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) (p.2237)
 - B CWE-134: Use of Externally-Controlled Format String (p.371)
 - G CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
 - B CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information (p.2082)
 - B CWE-1273: Device Unlock Credential Sharing (p.2119)
 - B CWE-1295: Debug Messages Revealing Unnecessary Information (p.2164)
 - B CWE-201: Insertion of Sensitive Information Into Sent Data (p.521)
 - V CWE-598: Use of GET Request Method With Sensitive Query Strings (p.1349)
 - B CWE-203: Observable Discrepancy (p.525)
 - B CWE-1300: Improper Protection of Physical Side Channels (p.2177)
 - V CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks (p.2073)
 - B CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
 - B CWE-204: Observable Response Discrepancy (p.530)
 - B CWE-205: Observable Behavioral Discrepancy (p.533)
 - V CWE-206: Observable Internal Behavioral Discrepancy (p.534)
 - V CWE-207: Observable Behavioral Discrepancy With Equivalent Products (p.535)
 - B CWE-208: Observable Timing Discrepancy (p.537)
 - B CWE-1254: Incorrect Comparison Logic Granularity (p.2071)
 - B CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
 - B CWE-210: Self-generated Error Message Containing Sensitive Information (p.546)
 - B CWE-211: Externally-Generated Error Message Containing Sensitive Information (p.548)
 - V CWE-535: Exposure of Information Through Shell Error Message (p.1253)
 - V CWE-536: Servlet Runtime Error Message Containing Sensitive Information (p.1254)
 - V CWE-537: Java Runtime Error Message Containing Sensitive Information (p.1255)
 - V CWE-550: Server-generated Error Message Containing Sensitive Information (p.1272)
 - B CWE-213: Exposure of Sensitive Information Due to Incompatible Policies (p.555)
 - B CWE-215: Insertion of Sensitive Information Into Debugging Code (p.558)
 - B CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
 - B CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere (p.1201)
 - B CWE-214: Invocation of Process Using Visible Sensitive Information (p.556)

- V CWE-548: Exposure of Information Through Directory Listing (p.1269)
- B CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory (p.1257)
- B CWE-532: Insertion of Sensitive Information into Log File (p.1250)
- B CWE-540: Inclusion of Sensitive Information in Source Code (p.1260)
 - V CWE-531: Inclusion of Sensitive Information in Test Code (p.1249)
 - V CWE-541: Inclusion of Sensitive Information in an Include File (p.1262)
 - V CWE-615: Inclusion of Sensitive Information in Source Code Comments (p.1383)
 - V CWE-651: Exposure of WSDL File Containing Sensitive Information (p.1442)
- B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 - B CWE-23: Relative Path Traversal (p.46)
 - V CWE-24: Path Traversal: '../filedir' (p.53)
 - V CWE-25: Path Traversal: '/../filedir' (p.55)
 - V CWE-26: Path Traversal: '/dir../filename' (p.57)
 - V CWE-27: Path Traversal: 'dir../filename' (p.58)
 - V CWE-28: Path Traversal: '..filedir' (p.60)
 - V CWE-29: Path Traversal: '..filename' (p.62)
 - V CWE-30: Path Traversal: 'dir..filename' (p.64)
 - V CWE-31: Path Traversal: 'dir..\filename' (p.65)
 - V CWE-32: Path Traversal: '...' (Triple Dot) (p.67)
 - V CWE-33: Path Traversal: '....' (Multiple Dot) (p.69)
 - V CWE-34: Path Traversal: '.../' (p.71)
 - V CWE-35: Path Traversal: '.../...' (p.73)
 - B CWE-36: Absolute Path Traversal (p.75)
 - V CWE-37: Path Traversal: '/absolute/pathname/here' (p.79)
 - V CWE-38: Path Traversal: '\absolute\pathname\here' (p.81)
 - V CWE-39: Path Traversal: 'C:dirname' (p.83)
 - V CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) (p.86)
- B CWE-374: Passing Mutable Objects to an Untrusted Method (p.927)
- B CWE-375: Returning a Mutable Object to an Untrusted Caller (p.930)
- C CWE-377: Insecure Temporary File (p.932)
 - B CWE-378: Creation of Temporary File With Insecure Permissions (p.935)
 - B CWE-379: Creation of Temporary File in Directory with Insecure Permissions (p.937)
- C CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') (p.984)
 - B CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') (p.985)
 - B CWE-619: Dangling Database Cursor ('Cursor Injection') (p.1391)
- B CWE-427: Uncontrolled Search Path Element (p.1040)
- B CWE-428: Unquoted Search Path or Element (p.1047)
- B CWE-488: Exposure of Data Element to Wrong Session (p.1176)
- V CWE-491: Public cloneable() Method Without Final ('Object Hijack') (p.1181)
- V CWE-492: Use of Inner Class Containing Sensitive Data (p.1183)
- V CWE-493: Critical Public Variable Without Final Modifier (p.1190)
- V CWE-500: Public Static Field Not Marked Final (p.1208)
- V CWE-498: Cloneable Class Containing Sensitive Information (p.1204)
- V CWE-499: Serializable Class Containing Sensitive Data (p.1206)
- C CWE-522: Insufficiently Protected Credentials (p.1234)
 - B CWE-256: Plaintext Storage of a Password (p.622)
 - B CWE-257: Storing Passwords in a Recoverable Format (p.625)
 - B CWE-260: Password in Configuration File (p.636)
 - V CWE-13: ASP.NET Misconfiguration: Password in Configuration File (p.13)
 - V CWE-258: Empty Password in Configuration File (p.628)
 - V CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File (p.1279)
 - B CWE-261: Weak Encoding for Password (p.638)
 - B CWE-523: Unprotected Transport of Credentials (p.1239)

- B CWE-549: Missing Password Field Masking (p.1271)
- B CWE-524: Use of Cache Containing Sensitive Information (p.1240)
- V CWE-525: Use of Web Browser Cache Containing Sensitive Information (p.1242)
- B CWE-552: Files or Directories Accessible to External Parties (p.1274)
 - V CWE-219: Storage of File with Sensitive Data Under Web Root (p.560)
 - V CWE-433: Unparsed Raw Web Content Delivery (p.1053)
 - V CWE-220: Storage of File With Sensitive Data Under FTP Root (p.562)
 - V CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere (p.1245)
 - V CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere (p.1246)
 - V CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere (p.1247)
 - V CWE-530: Exposure of Backup File to an Unauthorized Control Sphere (p.1248)
 - V CWE-539: Use of Persistent Cookies Containing Sensitive Information (p.1259)
 - V CWE-553: Command Shell in Externally Accessible Directory (p.1277)
- V CWE-582: Array Declared Public, Final, and Static (p.1322)
- V CWE-583: finalize() Method Declared Public (p.1324)
- V CWE-608: Struts: Non-private Field in ActionForm Class (p.1369)
- G CWE-642: External Control of Critical State Data (p.1422)
 - B CWE-15: External Control of System or Configuration Setting (p.17)
 - B CWE-426: Untrusted Search Path (p.1035)
 - B CWE-472: External Control of Assumed-Immutable Web Parameter (p.1131)
 - B CWE-565: Reliance on Cookies without Validation and Integrity Checking (p.1292)
 - V CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision (p.1662)
 - B CWE-73: External Control of File Name or Path (p.133)
 - G CWE-114: Process Control (p.283)
- G CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
 - V CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag (p.1863)
 - B CWE-276: Incorrect Default Permissions (p.672)
 - V CWE-277: Insecure Inherited Permissions (p.675)
 - V CWE-278: Insecure Preserved Inherited Permissions (p.676)
 - V CWE-279: Incorrect Execution-Assigned Permissions (p.678)
 - B CWE-281: Improper Preservation of Permissions (p.681)
 - B CWE-766: Critical Data Element Declared Public (p.1615)
- B CWE-767: Access to Critical Private Variable via Public Method (p.1619)
- V CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote (p.6)
- V CWE-927: Use of Implicit Intent for Sensitive Communication (p.1846)
- G CWE-669: Incorrect Resource Transfer Between Spheres (p.1480)
 - B CWE-1420: Exposure of Sensitive Information during Transient Execution (p.2297)
 - B CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution (p.2304)
 - B CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution (p.2310)
 - B CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution (p.2316)
 - B CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer (p.551)
 - B CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information (p.2082)
 - B CWE-226: Sensitive Information in Resource Not Removed Before Reuse (p.569)
 - V CWE-1239: Improper Zeroization of Hardware Register (p.2033)
 - B CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition (p.2116)
 - B CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component (p.2183)
 - V CWE-1330: Remanent Data Readable after Memory Erase (p.2234)

- B CWE-1342: Information Exposure through Microarchitectural State after Transient Execution (p.2262)
- V CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') (p.598)
- V CWE-243: Creation of chroot Jail Without Changing Working Directory (p.596)
- B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
- B CWE-494: Download of Code Without Integrity Check (p.1192)
- B CWE-829: Inclusion of Functionality from Untrusted Control Sphere (p.1750)
 - V CWE-827: Improper Control of Document Type Definition (p.1745)
 - V CWE-830: Inclusion of Web Functionality from an Untrusted Source (p.1756)
 - V CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') (p.242)
- C CWE-673: External Influence of Sphere Definition (p.1492)
- B CWE-426: Untrusted Search Path (p.1035)
- C CWE-704: Incorrect Type Conversion or Cast (p.1547)
 - B CWE-1389: Incorrect Parsing of Numbers with Different Radices (p.2275)
 - V CWE-588: Attempt to Access Child of a Non-structure Pointer (p.1332)
 - B CWE-681: Incorrect Conversion between Numeric Types (p.1504)
 - V CWE-192: Integer Coercion Error (p.489)
 - V CWE-194: Unexpected Sign Extension (p.498)
 - V CWE-195: Signed to Unsigned Conversion Error (p.501)
 - V CWE-196: Unsigned to Signed Conversion Error (p.505)
 - B CWE-197: Numeric Truncation Error (p.507)
 - B CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') (p.1785)
- C CWE-706: Use of Incorrectly-Resolved Name or Reference (p.1553)
- B CWE-178: Improper Handling of Case Sensitivity (p.451)
- B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 - B CWE-23: Relative Path Traversal (p.46)
 - V CWE-24: Path Traversal: '../filedir' (p.53)
 - V CWE-25: Path Traversal: './filedir' (p.55)
 - V CWE-26: Path Traversal: '/dir../filename' (p.57)
 - V CWE-27: Path Traversal: 'dir../filename' (p.58)
 - V CWE-28: Path Traversal: '..filedir' (p.60)
 - V CWE-29: Path Traversal: '..filename' (p.62)
 - V CWE-30: Path Traversal: 'dir..\filename' (p.64)
 - V CWE-31: Path Traversal: 'dir..\filename' (p.65)
 - V CWE-32: Path Traversal: '...' (Triple Dot) (p.67)
 - V CWE-33: Path Traversal: '...' (Multiple Dot) (p.69)
 - V CWE-34: Path Traversal: '.../' (p.71)
 - V CWE-35: Path Traversal: '.../' (p.73)
 - B CWE-36: Absolute Path Traversal (p.75)
 - V CWE-37: Path Traversal: '/absolute/pathname/here' (p.79)
 - V CWE-38: Path Traversal: '\absolute\pathname\here' (p.81)
 - V CWE-39: Path Traversal: 'C:dirname' (p.83)
 - V CWE-40: Path Traversal: '\\UNC\share\name' (Windows UNC Share) (p.86)
- B CWE-386: Symbolic Name not Mapping to Correct Object (p.949)
- B CWE-41: Improper Resolution of Path Equivalence (p.87)
 - V CWE-42: Path Equivalence: 'filename.' (Trailing Dot) (p.93)
 - V CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) (p.94)
 - V CWE-44: Path Equivalence: 'file.name' (Internal Dot) (p.95)
 - V CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) (p.96)
 - V CWE-46: Path Equivalence: 'filename ' (Trailing Space) (p.97)
 - V CWE-47: Path Equivalence: ' filename' (Leading Space) (p.98)
 - V CWE-48: Path Equivalence: 'file name' (Internal Whitespace) (p.99)
 - V CWE-49: Path Equivalence: 'filename/' (Trailing Slash) (p.100)
 - V CWE-50: Path Equivalence: '//multiple/leading/slash' (p.101)

- V CWE-51: Path Equivalence: '/multiple//internal/slash' (p.103)
- V CWE-52: Path Equivalence: '/multiple/trailing/slash/' (p.104)
- V CWE-53: Path Equivalence: '\multiple\internal\backslashslash' (p.105)
- V CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) (p.106)
- V CWE-55: Path Equivalence: './.' (Single Dot Directory) (p.107)
- V CWE-56: Path Equivalence: 'filedir*' (Wildcard) (p.108)
- V CWE-57: Path Equivalence: 'fakedir../readdir/filename' (p.109)
- V CWE-58: Path Equivalence: Windows 8.3 Filename (p.111)
- B CWE-59: Improper Link Resolution Before File Access ('Link Following') (p.112)
- B CWE-1386: Insecure Operation on Windows Junction / Mount Point (p.2273)
- C CWE-61: UNIX Symbolic Link (Symlink) Following (p.117)
- V CWE-62: UNIX Hard Link (p.120)
- V CWE-64: Windows Shortcut Following (.LNK) (p.122)
- V CWE-65: Windows Hard Link (p.124)
- B CWE-66: Improper Handling of File Names that Identify Virtual Resources (p.125)
- V CWE-67: Improper Handling of Windows Device Names (p.127)
- V CWE-69: Improper Handling of Windows ::DATA Alternate Data Stream (p.130)
- V CWE-72: Improper Handling of Apple HFS+ Alternate Data Stream Path (p.131)
- V CWE-827: Improper Control of Document Type Definition (p.1745)
- V CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') (p.242)
- B CWE-911: Improper Update of Reference Count (p.1811)
- C CWE-913: Improper Control of Dynamically-Managed Code Resources (p.1814)
- B CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (p.1125)
- B CWE-502: Deserialization of Untrusted Data (p.1212)
- B CWE-914: Improper Control of Dynamically-Identified Variables (p.1816)
- V CWE-621: Variable Extraction Error (p.1394)
- V CWE-627: Dynamic Variable Evaluation (p.1405)
- B CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes (p.1818)
- V CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (p.2216)
- B CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
- B CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine (p.2250)
- V CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (p.232)
- B CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') (p.238)
- V CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page (p.241)
- C CWE-922: Insecure Storage of Sensitive Information (p.1835)
- B CWE-312: Cleartext Storage of Sensitive Information (p.771)
- V CWE-313: Cleartext Storage in a File or on Disk (p.777)
- V CWE-314: Cleartext Storage in the Registry (p.779)
- V CWE-315: Cleartext Storage of Sensitive Information in a Cookie (p.781)
- V CWE-316: Cleartext Storage of Sensitive Information in Memory (p.782)
- V CWE-317: Cleartext Storage of Sensitive Information in GUI (p.784)
- V CWE-318: Cleartext Storage of Sensitive Information in Executable (p.785)
- V CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable (p.1243)
- B CWE-921: Storage of Sensitive Data in a Mechanism without Access Control (p.1834)
- P CWE-682: Incorrect Calculation (p.1507)
- B CWE-128: Wrap-around Error (p.345)
- B CWE-131: Incorrect Calculation of Buffer Size (p.361)
- V CWE-467: Use of sizeof() on a Pointer Type (p.1118)
- B CWE-1335: Incorrect Bitwise Shift of Integer (p.2247)

- B CWE-1339: Insufficient Precision or Accuracy of a Real Number (p.2254)
- B CWE-135: Incorrect Calculation of Multi-Byte String Length (p.377)
- B CWE-190: Integer Overflow or Wraparound (p.478)
- B CWE-680: Integer Overflow to Buffer Overflow (p.1502)
- B CWE-191: Integer Underflow (Wrap or Wraparound) (p.487)
- B CWE-193: Off-by-one Error (p.493)
- B CWE-369: Divide By Zero (p.920)
- B CWE-468: Incorrect Pointer Scaling (p.1121)
- B CWE-469: Use of Pointer Subtraction to Determine Size (p.1123)
- P CWE-691: Insufficient Control Flow Management (p.1525)
- B CWE-1265: Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls (p.2100)
- B CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready (p.2132)
- B CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior (p.2136)
- C CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
 - B CWE-1223: Race Condition for Write-Once Attributes (p.2011)
 - B CWE-1298: Hardware Logic Contains Race Conditions (p.2170)
 - B CWE-364: Signal Handler Race Condition (p.905)
 - B CWE-432: Dangerous Signal Handler not Disabled During Sensitive Operations (p.1052)
 - V CWE-828: Signal Handler with Functionality that is not Asynchronous-Safe (p.1746)
 - V CWE-479: Signal Handler Use of a Non-reentrant Function (p.1154)
 - V CWE-831: Signal Handler Function Associated with Multiple Signals (p.1758)
 - B CWE-366: Race Condition within a Thread (p.910)
 - B CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition (p.913)
 - B CWE-363: Race Condition Enabling Link Following (p.904)
 - B CWE-368: Context Switching Race Condition (p.918)
 - B CWE-421: Race Condition During Access to Alternate Channel (p.1028)
 - B CWE-689: Permission Race Condition During Resource Copy (p.1521)
- B CWE-430: Deployment of Wrong Handler (p.1049)
- B CWE-431: Missing Handler (p.1051)
- C CWE-662: Improper Synchronization (p.1457)
 - B CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)
 - B CWE-663: Use of a Non-reentrant Function in a Concurrent Context (p.1461)
 - V CWE-479: Signal Handler Use of a Non-reentrant Function (p.1154)
 - V CWE-558: Use of getlogin() in Multithreaded Application (p.1281)
 - C CWE-667: Improper Locking (p.1472)
 - B CWE-1232: Improper Lock Behavior After Power State Transition (p.2021)
 - B CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection (p.2023)
 - B CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks (p.2026)
 - B CWE-412: Unrestricted Externally Accessible Lock (p.1007)
 - B CWE-413: Improper Resource Locking (p.1010)
 - V CWE-591: Sensitive Data Storage in Improperly Locked Memory (p.1338)
 - B CWE-414: Missing Lock Check (p.1014)
 - B CWE-609: Double-Checked Locking (p.1371)
 - B CWE-764: Multiple Locks of a Critical Resource (p.1613)
 - B CWE-765: Multiple Unlocks of a Critical Resource (p.1614)
 - B CWE-832: Unlock of a Resource that is not Locked (p.1761)
 - B CWE-833: Deadlock (p.1762)
 - B CWE-820: Missing Synchronization (p.1729)
 - V CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)
 - V CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context (p.1263)
 - B CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
 - B CWE-821: Incorrect Synchronization (p.1731)

- B CWE-1088: Synchronous Access of Remote Resource without Timeout (*p.1937*)
- B CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels (*p.2098*)
- V CWE-572: Call to Thread run() instead of start() (*p.1305*)
- V CWE-574: EJB Bad Practices: Use of Synchronization Primitives (*p.1308*)
- G CWE-670: Always-Incorrect Control Flow Implementation (*p.1484*)
- B CWE-480: Use of Incorrect Operator (*p.1157*)
- V CWE-481: Assigning instead of Comparing (*p.1161*)
- V CWE-482: Comparing instead of Assigning (*p.1165*)
- V CWE-597: Use of Wrong Operator in String Comparison (*p.1345*)
- B CWE-483: Incorrect Block Delimitation (*p.1167*)
- B CWE-484: Omitted Break Statement in Switch (*p.1169*)
- B CWE-617: Reachable Assertion (*p.1387*)
- B CWE-698: Execution After Redirect (EAR) (*p.1542*)
- B CWE-783: Operator Precedence Logic Error (*p.1659*)
- G CWE-696: Incorrect Behavior Order (*p.1535*)
- B CWE-1190: DMA Device Enabled Too Early in Boot Phase (*p.1987*)
- B CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control (*p.1995*)
- B CWE-1280: Access Control Check Implemented After Asset is Accessed (*p.2134*)
- B CWE-179: Incorrect Behavior Order: Early Validation (*p.454*)
- V CWE-180: Incorrect Behavior Order: Validate Before Canonicalize (*p.457*)
- V CWE-181: Incorrect Behavior Order: Validate Before Filter (*p.460*)
- B CWE-408: Incorrect Behavior Order: Early Amplification (*p.1002*)
- B CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization (*p.1273*)
- G CWE-705: Incorrect Control Flow Scoping (*p.1550*)
- B CWE-248: Uncaught Exception (*p.603*)
- V CWE-600: Uncaught Exception in Servlet (*p.1352*)
- V CWE-382: J2EE Bad Practices: Use of System.exit() (*p.940*)
- B CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference (*p.964*)
- B CWE-396: Declaration of Catch for Generic Exception (*p.966*)
- B CWE-397: Declaration of Throws for Generic Exception (*p.968*)
- B CWE-455: Non-exit on Failed Initialization (*p.1095*)
- B CWE-584: Return Inside Finally Block (*p.1325*)
- B CWE-698: Execution After Redirect (EAR) (*p.1542*)
- V CWE-768: Incorrect Short Circuit Evaluation (*p.1620*)
- G CWE-799: Improper Control of Interaction Frequency (*p.1708*)
- B CWE-307: Improper Restriction of Excessive Authentication Attempts (*p.754*)
- B CWE-837: Improper Enforcement of a Single, Unique Action (*p.1771*)
- G CWE-834: Excessive Iteration (*p.1763*)
- B CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context (*p.2219*)
- G CWE-674: Uncontrolled Recursion (*p.1493*)
- B CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') (*p.1642*)
- B CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') (*p.1766*)
- B CWE-841: Improper Enforcement of Behavioral Workflow (*p.1781*)
- P CWE-693: Protection Mechanism Failure (*p.1529*)
- G CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations (*p.1882*)
- B CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications (*p.2060*)
- B CWE-1253: Incorrect Selection of Fuse Values (*p.2069*)
- B CWE-1269: Product Released in Non-Release Configuration (*p.2110*)
- B CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques (*p.2131*)
- B CWE-1291: Public Key Re-Use for Signing both Debug and Production Code (*p.2157*)
- B CWE-1318: Missing Support for Security Features in On-chip Fabrics or Buses (*p.2209*)

- B CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) (p.2212)
- B CWE-1326: Missing Immutable Root of Trust in Hardware (p.2224)
- B CWE-1338: Improper Protections Against Hardware Overheating (p.2252)
- B CWE-182: Collapse of Data into Unsafe Value (p.462)
- B CWE-184: Incomplete List of Disallowed Inputs (p.466)
- B CWE-692: Incomplete Denylist to Cross-Site Scripting (p.1528)
- G CWE-311: Missing Encryption of Sensitive Data (p.764)
 - B CWE-312: Cleartext Storage of Sensitive Information (p.771)
 - V CWE-313: Cleartext Storage in a File or on Disk (p.777)
 - V CWE-314: Cleartext Storage in the Registry (p.779)
 - V CWE-315: Cleartext Storage of Sensitive Information in a Cookie (p.781)
 - V CWE-316: Cleartext Storage of Sensitive Information in Memory (p.782)
 - V CWE-317: Cleartext Storage of Sensitive Information in GUI (p.784)
 - V CWE-318: Cleartext Storage of Sensitive Information in Executable (p.785)
 - V CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable (p.1243)
 - B CWE-319: Cleartext Transmission of Sensitive Information (p.786)
 - V CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption (p.1)
 - V CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute (p.1382)
- G CWE-326: Inadequate Encryption Strength (p.803)
 - B CWE-328: Use of Weak Hash (p.813)
 - B CWE-916: Use of Password Hash With Insufficient Computational Effort (p.1822)
 - V CWE-759: Use of a One-Way Hash without a Salt (p.1593)
 - V CWE-760: Use of a One-Way Hash with a Predictable Salt (p.1598)
- G CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 - B CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation (p.2036)
 - B CWE-328: Use of Weak Hash (p.813)
 - B CWE-916: Use of Password Hash With Insufficient Computational Effort (p.1822)
 - V CWE-759: Use of a One-Way Hash without a Salt (p.1593)
 - V CWE-760: Use of a One-Way Hash with a Predictable Salt (p.1598)
 - V CWE-780: Use of RSA Algorithm without OAEP (p.1652)
- G CWE-330: Use of Insufficiently Random Values (p.821)
 - B CWE-1204: Generation of Weak Initialization Vector (IV) (p.1996)
 - V CWE-329: Generation of Predictable IV with CBC Mode (p.818)
 - B CWE-1241: Use of Predictable Algorithm in Random Number Generator (p.2042)
 - B CWE-331: Insufficient Entropy (p.828)
 - V CWE-332: Insufficient Entropy in PRNG (p.830)
 - V CWE-333: Improper Handling of Insufficient Entropy in TRNG (p.832)
 - B CWE-334: Small Space of Random Values (p.834)
 - V CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length (p.2)
 - B CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) (p.836)
 - V CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) (p.839)
 - V CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) (p.841)
 - V CWE-339: Small Seed Space in PRNG (p.847)
 - B CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (p.844)
 - G CWE-340: Generation of Predictable Numbers or Identifiers (p.849)
 - B CWE-341: Predictable from Observable State (p.850)
 - B CWE-342: Predictable Exact Value from Previous Values (p.852)
 - B CWE-343: Predictable Value Range from Previous Values (p.854)
 - B CWE-344: Use of Invariant Value in Dynamically Changing Context (p.856)
 - B CWE-323: Reusing a Nonce, Key Pair in Encryption (p.797)
 - V CWE-587: Assignment of a Fixed Address to a Pointer (p.1330)
 - B CWE-798: Use of Hard-coded Credentials (p.1699)
 - V CWE-259: Use of Hard-coded Password (p.630)
 - V CWE-321: Use of Hard-coded Cryptographic Key (p.792)
- G CWE-345: Insufficient Verification of Data Authenticity (p.858)
 - B CWE-1293: Missing Source Correlation of Multiple Independent Data (p.2161)

- G CWE-346: Origin Validation Error (p.860)
- V CWE-1385: Missing Origin Validation in WebSockets (p.2271)
- B CWE-940: Improper Verification of Source of a Communication Channel (p.1852)
- V CWE-925: Improper Verification of Intent by Broadcast Receiver (p.1841)
- B CWE-347: Improper Verification of Cryptographic Signature (p.864)
- B CWE-348: Use of Less Trusted Source (p.866)
- B CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data (p.868)
- B CWE-351: Insufficient Type Distinction (p.873)
- B CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
- B CWE-353: Missing Support for Integrity Check (p.881)
- B CWE-354: Improper Validation of Integrity Check Value (p.883)
- B CWE-360: Trust of System Event Data (p.894)
- V CWE-422: Unprotected Windows Messaging Channel ('Shatter') (p.1029)
- B CWE-494: Download of Code Without Integrity Check (p.1192)
- V CWE-616: Incomplete Identification of Uploaded File Variables (PHP) (p.1385)
- V CWE-646: Reliance on File Name or Extension of Externally-Supplied File (p.1434)
- B CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking (p.1439)
- B CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel (p.1839)
- B CWE-357: Insufficient UI Warning of Dangerous Operations (p.887)
- B CWE-450: Multiple Interpretations of UI Input (p.1085)
- B CWE-358: Improperly Implemented Security Check for Standard (p.888)
- G CWE-424: Improper Protection of Alternate Path (p.1031)
- B CWE-425: Direct Request ('Forced Browsing') (p.1032)
- G CWE-602: Client-Side Enforcement of Server-Side Security (p.1359)
- B CWE-565: Reliance on Cookies without Validation and Integrity Checking (p.1292)
- V CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision (p.1662)
- B CWE-603: Use of Client-Side Authentication (p.1363)
- G CWE-653: Improper Isolation or Compartmentalization (p.1445)
- B CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) (p.1985)
- B CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
- B CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) (p.2237)
- B CWE-654: Reliance on a Single Factor in a Security Decision (p.1448)
- B CWE-308: Use of Single-factor Authentication (p.759)
- B CWE-309: Use of Password System for Primary Authentication (p.761)
- G CWE-655: Insufficient Psychological Acceptability (p.1450)
- G CWE-656: Reliance on Security Through Obscurity (p.1452)
- B CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') (p.1589)
- B CWE-778: Insufficient Logging (p.1647)
- B CWE-807: Reliance on Untrusted Inputs in a Security Decision (p.1723)
- B CWE-302: Authentication Bypass by Assumed-Immutable Data (p.742)
- V CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action (p.870)
- V CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision (p.1662)
- P CWE-697: Incorrect Comparison (p.1538)
- G CWE-1023: Incomplete Comparison with Missing Factors (p.1874)
- B CWE-184: Incomplete List of Disallowed Inputs (p.466)
- B CWE-692: Incomplete Denylist to Cross-Site Scripting (p.1528)
- V CWE-187: Partial String Comparison (p.474)
- B CWE-478: Missing Default Case in Multiple Condition Expression (p.1149)
- B CWE-839: Numeric Range Comparison Without Minimum Check (p.1776)
- B CWE-1024: Comparison of Incompatible Types (p.1877)
- B CWE-1025: Comparison Using Wrong Factors (p.1878)
- V CWE-486: Comparison of Classes by Name (p.1172)
- V CWE-595: Comparison of Object References Instead of Object Contents (p.1342)

- V CWE-597: Use of Wrong Operator in String Comparison (p.1345)
- G CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations (p.1882)
- V CWE-1077: Floating Point Comparison with Incorrect Operator (p.1926)
- B CWE-1254: Incorrect Comparison Logic Granularity (p.2071)
- B CWE-183: Permissive List of Allowed Inputs (p.464)
- V CWE-942: Permissive Cross-domain Policy with Untrusted Domains (p.1857)
- G CWE-185: Incorrect Regular Expression (p.469)
- B CWE-186: Overly Restrictive Regular Expression (p.472)
- B CWE-625: Permissive Regular Expression (p.1400)
- V CWE-777: Regular Expression without Anchors (p.1645)
- V CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined (p.1321)
- P CWE-703: Improper Check or Handling of Exceptional Conditions (p.1544)
- G CWE-1384: Improper Handling of Physical or Environmental Conditions (p.2269)
- B CWE-1247: Improper Protection Against Voltage and Clock Glitches (p.2056)
- B CWE-1261: Improper Handling of Single Event Upsets (p.2091)
- B CWE-1332: Improper Handling of Faults that Lead to Instruction Skips (p.2240)
- B CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments (p.2265)
- G CWE-228: Improper Handling of Syntactically Invalid Structure (p.575)
- B CWE-166: Improper Handling of Missing Special Element (p.429)
- B CWE-167: Improper Handling of Additional Special Element (p.431)
- B CWE-168: Improper Handling of Inconsistent Special Elements (p.433)
- B CWE-229: Improper Handling of Values (p.577)
- V CWE-230: Improper Handling of Missing Values (p.578)
- V CWE-231: Improper Handling of Extra Values (p.579)
- V CWE-232: Improper Handling of Undefined Values (p.580)
- B CWE-233: Improper Handling of Parameters (p.581)
- V CWE-234: Failure to Handle Missing Parameter (p.583)
- V CWE-235: Improper Handling of Extra Parameters (p.585)
- V CWE-236: Improper Handling of Undefined Parameters (p.586)
- B CWE-237: Improper Handling of Structural Elements (p.587)
- V CWE-238: Improper Handling of Incomplete Structural Elements (p.588)
- V CWE-239: Failure to Handle Incomplete Element (p.589)
- B CWE-240: Improper Handling of Inconsistent Structural Elements (p.590)
- B CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
- B CWE-241: Improper Handling of Unexpected Data Type (p.591)
- B CWE-393: Return of Wrong Status Code (p.960)
- B CWE-397: Declaration of Throws for Generic Exception (p.968)
- G CWE-754: Improper Check for Unusual or Exceptional Conditions (p.1577)
- B CWE-252: Unchecked Return Value (p.613)
- B CWE-690: Unchecked Return Value to NULL Pointer Dereference (p.1523)
- B CWE-253: Incorrect Check of Function Return Value (p.620)
- B CWE-273: Improper Check for Dropped Privileges (p.667)
- B CWE-354: Improper Validation of Integrity Check Value (p.883)
- B CWE-391: Unchecked Error Condition (p.955)
- B CWE-394: Unexpected Status Code or Return Value (p.962)
- B CWE-476: NULL Pointer Dereference (p.1139)
- G CWE-755: Improper Handling of Exceptional Conditions (p.1585)
- B CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
- B CWE-210: Self-generated Error Message Containing Sensitive Information (p.546)
- B CWE-211: Externally-Generated Error Message Containing Sensitive Information (p.548)
- V CWE-535: Exposure of Information Through Shell Error Message (p.1253)
- V CWE-536: Servlet Runtime Error Message Containing Sensitive Information (p.1254)
- V CWE-537: Java Runtime Error Message Containing Sensitive Information (p.1255)
- V CWE-550: Server-generated Error Message Containing Sensitive Information (p.1272)

- B CWE-248: Uncaught Exception (p.603)
- V CWE-600: Uncaught Exception in Servlet (p.1352)
- B CWE-274: Improper Handling of Insufficient Privileges (p.670)
- B CWE-280: Improper Handling of Insufficient Permissions or Privileges (p.679)
- V CWE-333: Improper Handling of Insufficient Entropy in TRNG (p.832)
- B CWE-390: Detection of Error Condition Without Action (p.950)
- B CWE-392: Missing Report of Error Condition (p.958)
- B CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference (p.964)
- B CWE-396: Declaration of Catch for Generic Exception (p.966)
- B CWE-460: Improper Cleanup on Thrown Exception (p.1109)
- B CWE-544: Missing Standardized Error Handling Mechanism (p.1265)
- G CWE-636: Not Failing Securely ('Failing Open') (p.1409)
- B CWE-455: Non-exit on Failed Initialization (p.1095)
- B CWE-756: Missing Custom Error Page (p.1588)
- V CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page (p.11)
- V CWE-7: J2EE Misconfiguration: Missing Custom Error Page (p.4)
- P CWE-707: Improper Neutralization (p.1554)
- G CWE-116: Improper Encoding or Escaping of Output (p.287)
- B CWE-117: Improper Output Neutralization for Logs (p.294)
- V CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax (p.1430)
- B CWE-838: Inappropriate Encoding for Output Context (p.1773)
- G CWE-138: Improper Neutralization of Special Elements (p.379)
- B CWE-140: Improper Neutralization of Delimiters (p.382)
- V CWE-141: Improper Neutralization of Parameter/Argument Delimiters (p.384)
- V CWE-142: Improper Neutralization of Value Delimiters (p.386)
- V CWE-143: Improper Neutralization of Record Delimiters (p.387)
- V CWE-144: Improper Neutralization of Line Delimiters (p.389)
- V CWE-145: Improper Neutralization of Section Delimiters (p.391)
- V CWE-146: Improper Neutralization of Expression/Command Delimiters (p.393)
- V CWE-147: Improper Neutralization of Input Terminators (p.395)
- V CWE-626: Null Byte Interaction Error (Poison Null Byte) (p.1403)
- V CWE-148: Improper Neutralization of Input Leaders (p.397)
- V CWE-149: Improper Neutralization of Quoting Syntax (p.398)
- V CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences (p.400)
- V CWE-151: Improper Neutralization of Comment Delimiters (p.402)
- V CWE-152: Improper Neutralization of Macro Symbols (p.404)
- V CWE-153: Improper Neutralization of Substitution Characters (p.406)
- V CWE-154: Improper Neutralization of Variable Name Delimiters (p.407)
- V CWE-155: Improper Neutralization of Wildcards or Matching Symbols (p.409)
- V CWE-56: Path Equivalence: 'filedir*' (Wildcard) (p.108)
- V CWE-156: Improper Neutralization of Whitespace (p.411)
- V CWE-157: Failure to Sanitize Paired Delimiters (p.413)
- V CWE-158: Improper Neutralization of Null Byte or NUL Character (p.415)
- G CWE-159: Improper Handling of Invalid Use of Special Elements (p.417)
- B CWE-166: Improper Handling of Missing Special Element (p.429)
- B CWE-167: Improper Handling of Additional Special Element (p.431)
- B CWE-168: Improper Handling of Inconsistent Special Elements (p.433)
- V CWE-160: Improper Neutralization of Leading Special Elements (p.419)
- V CWE-161: Improper Neutralization of Multiple Leading Special Elements (p.421)
- V CWE-50: Path Equivalence: '//multiple/leading/slash' (p.101)
- V CWE-37: Path Traversal: '/absolute/pathname/here' (p.79)
- V CWE-162: Improper Neutralization of Trailing Special Elements (p.423)
- V CWE-163: Improper Neutralization of Multiple Trailing Special Elements (p.425)
- V CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) (p.94)
- V CWE-52: Path Equivalence: '/multiple/trailing/slash/' (p.104)

- V CWE-42: Path Equivalence: 'filename.' (Trailing Dot) (p.93)
- V CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) (p.94)
- V CWE-46: Path Equivalence: 'filename ' (Trailing Space) (p.97)
- V CWE-49: Path Equivalence: 'filename/' (Trailing Slash) (p.100)
- V CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) (p.106)
- V CWE-164: Improper Neutralization of Internal Special Elements (p.426)
- V CWE-165: Improper Neutralization of Multiple Internal Special Elements (p.428)
 - V CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) (p.96)
 - V CWE-53: Path Equivalence: '\\multiple\\internal\\backslash' (p.105)
- B CWE-464: Addition of Data Structure Sentinel (p.1115)
- G CWE-790: Improper Filtering of Special Elements (p.1687)
 - B CWE-791: Incomplete Filtering of Special Elements (p.1689)
 - V CWE-792: Incomplete Filtering of One or More Instances of Special Elements (p.1690)
 - V CWE-793: Only Filtering One Instance of a Special Element (p.1692)
 - V CWE-794: Incomplete Filtering of Multiple Instances of Special Elements (p.1693)
 - B CWE-795: Only Filtering Special Elements at a Specified Location (p.1694)
 - V CWE-796: Only Filtering Special Elements Relative to a Marker (p.1696)
 - V CWE-797: Only Filtering Special Elements at an Absolute Position (p.1698)
- B CWE-1426: Improper Validation of Generative AI Output (p.2321)
- B CWE-170: Improper Null Termination (p.434)
- G CWE-172: Encoding Error (p.439)
 - V CWE-173: Improper Handling of Alternate Encoding (p.441)
 - V CWE-174: Double Decoding of the Same Data (p.443)
 - V CWE-175: Improper Handling of Mixed Encoding (p.445)
 - V CWE-176: Improper Handling of Unicode Encoding (p.446)
 - V CWE-177: Improper Handling of URL Encoding (Hex Encoding) (p.449)
- G CWE-20: Improper Input Validation (p.20)
 - B CWE-1173: Improper Use of Validation Framework (p.1978)
 - V CWE-102: Struts: Duplicate Validation Forms (p.252)
 - V CWE-105: Struts: Form Field Without Validator (p.259)
 - V CWE-106: Struts: Plug-in Framework not in Use (p.262)
 - V CWE-108: Struts: Unvalidated Action Form (p.267)
 - V CWE-109: Struts: Validator Turned Off (p.269)
 - V CWE-1174: ASP.NET Misconfiguration: Improper Model Validation (p.1979)
 - V CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework (p.1278)
 - B CWE-1284: Improper Validation of Specified Quantity in Input (p.2142)
 - B CWE-606: Unchecked Input for Loop Condition (p.1366)
 - B CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input (p.2144)
 - V CWE-129: Improper Validation of Array Index (p.347)
 - V CWE-781: Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code (p.1654)
 - B CWE-1286: Improper Validation of Syntactic Correctness of Input (p.2148)
 - B CWE-112: Missing XML Validation (p.275)
 - B CWE-1287: Improper Validation of Specified Type of Input (p.2150)
 - B CWE-1288: Improper Validation of Consistency within Input (p.2151)
 - B CWE-1289: Improper Validation of Unsafe Equivalence in Input (p.2153)
 - B CWE-179: Incorrect Behavior Order: Early Validation (p.454)
 - V CWE-180: Incorrect Behavior Order: Validate Before Canonicalize (p.457)
 - V CWE-181: Incorrect Behavior Order: Validate Before Filter (p.460)
 - V CWE-622: Improper Validation of Function Hook Arguments (p.1396)
- G CWE-228: Improper Handling of Syntactically Invalid Structure (p.575)
 - B CWE-166: Improper Handling of Missing Special Element (p.429)
 - B CWE-167: Improper Handling of Additional Special Element (p.431)
 - B CWE-168: Improper Handling of Inconsistent Special Elements (p.433)
 - B CWE-229: Improper Handling of Values (p.577)
 - V CWE-230: Improper Handling of Missing Values (p.578)




- V CWE-231: Improper Handling of Extra Values (p.579)
- V CWE-232: Improper Handling of Undefined Values (p.580)
- B CWE-233: Improper Handling of Parameters (p.581)
- V CWE-234: Failure to Handle Missing Parameter (p.583)
- V CWE-235: Improper Handling of Extra Parameters (p.585)
- V CWE-236: Improper Handling of Undefined Parameters (p.586)
- B CWE-237: Improper Handling of Structural Elements (p.587)
- V CWE-238: Improper Handling of Incomplete Structural Elements (p.588)
- V CWE-239: Failure to Handle Incomplete Element (p.589)
- B CWE-240: Improper Handling of Inconsistent Structural Elements (p.590)
- B CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
- B CWE-241: Improper Handling of Unexpected Data Type (p.591)
- B CWE-240: Improper Handling of Inconsistent Structural Elements (p.590)
- B CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
- B CWE-463: Deletion of Data Structure Sentinel (p.1113)
- G CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (p.138)
- B CWE-1236: Improper Neutralization of Formula Elements in a CSV File (p.2031)
- G CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) (p.145)
- B CWE-76: Improper Neutralization of Equivalent Special Elements (p.146)
- G CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
- B CWE-1427: Improper Neutralization of Input Used for LLM Prompting (p.2324)
- B CWE-624: Executable Regular Expression Error (p.1399)
- B CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
- B CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
- B CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
- B CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
- V CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) (p.182)
- V CWE-81: Improper Neutralization of Script in an Error Message Web Page (p.184)
- V CWE-83: Improper Neutralization of Script in Attributes in a Web Page (p.188)
- V CWE-82: Improper Neutralization of Script in Attributes of IMG Tags in a Web Page (p.186)
- V CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page (p.190)
- V CWE-85: Doubled Character XSS Manipulations (p.192)
- V CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages (p.194)
- V CWE-87: Improper Neutralization of Alternate XSS Syntax (p.196)
- B CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
- B CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
- B CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)
- B CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') (p.222)
- V CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') (p.277)
- B CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
- B CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine (p.2250)
- V CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (p.232)
- B CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') (p.238)

- V CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page (p.241)
- C CWE-943: Improper Neutralization of Special Elements in Data Query Logic (p.1860)
- B CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
- B CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)
- B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
- V CWE-564: SQL Injection: Hibernate (p.1290)
- B CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
- C CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
- B CWE-641: Improper Restriction of Names for Files and Other Resources (p.1421)
- B CWE-694: Use of Multiple Resources with Duplicate Identifier (p.1531)
- V CWE-102: Struts: Duplicate Validation Forms (p.252)
- V CWE-462: Duplicate Key in Associative List (Alist) (p.1111)
- B CWE-914: Improper Control of Dynamically-Identified Variables (p.1816)
- V CWE-621: Variable Extraction Error (p.1394)
- V CWE-627: Dynamic Variable Evaluation (p.1405)
- P CWE-710: Improper Adherence to Coding Standards (p.1558)
- B CWE-1041: Use of Redundant Code (p.1884)
- B CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range (p.1888)
- B CWE-1048: Invokable Control Element with Large Number of Outward Calls (p.1892)
- C CWE-1059: Insufficient Technical Documentation (p.1904)
- B CWE-1053: Missing Documentation for Design (p.1898)
- B CWE-1110: Incomplete Design Documentation (p.1959)
- B CWE-1111: Incomplete I/O Documentation (p.1960)
- B CWE-1112: Incomplete Documentation of Program Execution (p.1961)
- B CWE-1118: Insufficient Documentation of Error Handling Techniques (p.1967)
- C CWE-1061: Insufficient Encapsulation (p.1907)
- B CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer (p.1899)
- B CWE-1057: Data Access Operations Outside of Expected Data Manager Component (p.1902)
- B CWE-1062: Parent Class with References to Child Class (p.1909)
- B CWE-1083: Data Access from Outside Expected Data Manager Component (p.1932)
- B CWE-1090: Method Containing Access of a Member Element from Another Class (p.1939)
- B CWE-1100: Insufficient Isolation of System-Dependent Functions (p.1949)
- B CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality (p.1954)
- B CWE-188: Reliance on Data/Memory Layout (p.476)
- V CWE-198: Use of Incorrect Byte Ordering (p.510)
- B CWE-766: Critical Data Element Declared Public (p.1615)
- B CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers (p.1912)
- B CWE-1066: Missing Serialization Control Element (p.1913)
- B CWE-1068: Inconsistency Between Implementation and Documented Design (p.1915)
- C CWE-1076: Insufficient Adherence to Expected Conventions (p.1925)
- B CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor (p.1889)
- B CWE-1070: Serializable Data Element Containing non-Serializable Item Elements (p.1918)
- C CWE-1078: Inappropriate Source Code Style or Formatting (p.1927)
- B CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code (p.1934)
- B CWE-1099: Inconsistent Naming Conventions for Identifiers (p.1948)
- B CWE-1106: Insufficient Use of Symbolic Constants (p.1955)
- B CWE-1107: Insufficient Isolation of Symbolic Constant Definitions (p.1956)
- B CWE-1109: Use of Same Variable for Multiple Purposes (p.1958)
- B CWE-1113: Inappropriate Comment Style (p.1962)

- B CWE-1114: Inappropriate Whitespace Style (*p.1963*)
- B CWE-1115: Source Code Element without Standard Prologue (*p.1963*)
- B CWE-1116: Inaccurate Comments (*p.1964*)
- B CWE-1117: Callable with Insufficient Behavioral Summary (*p.1966*)
- V CWE-546: Suspicious Comment (*p.1266*)
- B CWE-547: Use of Hard-coded, Security-relevant Constants (*p.1267*)
- B CWE-1079: Parent Class without Virtual Destructor Method (*p.1929*)
- B CWE-1082: Class Instance Self Destruction Control Element (*p.1931*)
- B CWE-1087: Class with Virtual Method without a Virtual Destructor (*p.1936*)
- B CWE-1091: Use of Object without Invoking Destructor Method (*p.1940*)
- B CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element (*p.1946*)
- B CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element (*p.1947*)
- B CWE-1108: Excessive Reliance on Global Variables (*p.1957*)
- B CWE-586: Explicit Call to Finalize() (*p.1329*)
- V CWE-594: J2EE Framework: Saving Unserializable Objects to Disk (*p.1341*)
- B CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers (*p.1941*)
- G CWE-1093: Excessively Complex Data Representation (*p.1942*)
- B CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements (*p.1887*)
- B CWE-1055: Multiple Inheritance from Concrete Classes (*p.1900*)
- B CWE-1074: Class with Excessively Deep Inheritance (*p.1923*)
- B CWE-1086: Class with Excessive Number of Child Classes (*p.1935*)
- B CWE-1101: Reliance on Runtime Component in Generated Code (*p.1950*)
- G CWE-1120: Excessive Code Complexity (*p.1969*)
- B CWE-1047: Modules with Circular Dependencies (*p.1891*)
- B CWE-1056: Invokable Control Element with Variadic Parameters (*p.1901*)
- B CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses (*p.1906*)
- B CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters (*p.1911*)
- B CWE-1075: Unconditional Control Flow Transfer outside of Switch Block (*p.1924*)
- B CWE-1080: Source Code File with Excessive Number of Lines of Code (*p.1930*)
- B CWE-1095: Loop Condition Value Update within the Loop (*p.1944*)
- B CWE-1119: Excessive Use of Unconditional Branching (*p.1968*)
- B CWE-1121: Excessive McCabe Cyclomatic Complexity (*p.1970*)
- B CWE-1122: Excessive Halstead Complexity (*p.1971*)
- B CWE-1123: Excessive Use of Self-Modifying Code (*p.1972*)
- B CWE-1124: Excessively Deep Nesting (*p.1973*)
- B CWE-1125: Excessive Attack Surface (*p.1974*)
- B CWE-1126: Declaration of Variable with Unnecessarily Wide Scope (*p.1975*)
- B CWE-1127: Compilation with Insufficient Warnings or Errors (*p.1976*)
- G CWE-1164: Irrelevant Code (*p.1976*)
- V CWE-107: Struts: Unused Validation Form (*p.265*)
- B CWE-1071: Empty Code Block (*p.1919*)
- V CWE-1069: Empty Exception Block (*p.1916*)
- V CWE-585: Empty Synchronized Block (*p.1327*)
- V CWE-110: Struts: Validator Without Form Field (*p.270*)
- B CWE-561: Dead Code (*p.1283*)
- B CWE-563: Assignment to Variable without Use (*p.1289*)
- G CWE-1177: Use of Prohibited Code (*p.1981*)
- B CWE-242: Use of Inherently Dangerous Function (*p.593*)
- B CWE-676: Use of Potentially Dangerous Function (*p.1498*)
- V CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer (*p.1664*)
- B CWE-1209: Failure to Disable Reserved Bits (*p.2000*)
- G CWE-1357: Reliance on Insufficiently Trustworthy Component (*p.2266*)

- B CWE-1104: Use of Unmaintained Third Party Components (p.1953)
- B CWE-1329: Reliance on Component That is Not Updateable (p.2231)
- B CWE-1277: Firmware Not Updateable (p.2128)
- B CWE-1310: Missing Ability to Patch ROM Code (p.2191)
- B CWE-476: NULL Pointer Dereference (p.1139)
- B CWE-477: Use of Obsolete Function (p.1146)
- B CWE-484: Omitted Break Statement in Switch (p.1169)
- B CWE-489: Active Debug Code (p.1178)
- V CWE-11: ASP.NET Misconfiguration: Creating Debug Binary (p.9)
- B CWE-570: Expression is Always False (p.1300)
- B CWE-571: Expression is Always True (p.1303)
- G CWE-573: Improper Following of Specification by Caller (p.1307)
- V CWE-103: Struts: Incomplete validate() Method Definition (p.254)
- V CWE-104: Struts: Form Bean Does Not Extend Validation Class (p.257)
- V CWE-243: Creation of chroot Jail Without Changing Working Directory (p.596)
- B CWE-253: Incorrect Check of Function Return Value (p.620)
- B CWE-296: Improper Following of a Certificate's Chain of Trust (p.726)
- B CWE-304: Missing Critical Step in Authentication (p.745)
- B CWE-325: Missing Cryptographic Step (p.801)
- V CWE-329: Generation of Predictable IV with CBC Mode (p.818)
- B CWE-358: Improperly Implemented Security Check for Standard (p.888)
- B CWE-475: Undefined Behavior for Input to API (p.1138)
- V CWE-568: finalize() Method Without super.finalize() (p.1299)
- V CWE-577: EJB Bad Practices: Use of Sockets (p.1314)
- V CWE-578: EJB Bad Practices: Use of Class Loader (p.1316)
- V CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session (p.1318)
- V CWE-580: clone() Method Without super.clone() (p.1319)
- V CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined (p.1321)
- B CWE-628: Function Call with Incorrectly Specified Arguments (p.1407)
- V CWE-683: Function Call With Incorrect Order of Arguments (p.1512)
- V CWE-685: Function Call With Incorrect Number of Arguments (p.1516)
- V CWE-686: Function Call With Incorrect Argument Type (p.1517)
- V CWE-687: Function Call With Incorrectly Specified Argument Value (p.1518)
- V CWE-560: Use of umask() with chmod-style Argument (p.1282)
- V CWE-688: Function Call With Incorrect Variable or Reference as Argument (p.1520)
- G CWE-675: Multiple Operations on Resource in Single-Operation Context (p.1496)
- B CWE-1341: Multiple Releases of Same Resource or Handle (p.2258)
- V CWE-415: Double Free (p.1015)
- V CWE-174: Double Decoding of the Same Data (p.443)
- V CWE-605: Multiple Binds to the Same Port (p.1364)
- B CWE-764: Multiple Locks of a Critical Resource (p.1613)
- B CWE-765: Multiple Unlocks of a Critical Resource (p.1614)
- B CWE-694: Use of Multiple Resources with Duplicate Identifier (p.1531)
- V CWE-102: Struts: Duplicate Validation Forms (p.252)
- V CWE-462: Duplicate Key in Associative List (Alist) (p.1111)
- B CWE-695: Use of Low-Level Functionality (p.1533)
- V CWE-111: Direct Use of Unsafe JNI (p.272)
- V CWE-245: J2EE Bad Practices: Direct Management of Connections (p.599)
- V CWE-246: J2EE Bad Practices: Direct Use of Sockets (p.601)
- V CWE-383: J2EE Bad Practices: Direct Use of Threads (p.942)
- V CWE-574: EJB Bad Practices: Use of Synchronization Primitives (p.1308)
- V CWE-575: EJB Bad Practices: Use of AWT Swing (p.1310)
- V CWE-576: EJB Bad Practices: Use of Java I/O (p.1312)
- G CWE-657: Violation of Secure Design Principles (p.1454)
- B CWE-1192: Improper Identifier for IP Block used in System-On-Chip (SOC) (p.1994)

- C CWE-1395: Dependency on Vulnerable Third-Party Component (p.2289)
- B CWE-250: Execution with Unnecessary Privileges (p.606)
- C CWE-636: Not Failing Securely ('Failing Open') (p.1409)
- B CWE-455: Non-exit on Failed Initialization (p.1095)
- C CWE-637: Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism') (p.1411)
- C CWE-638: Not Using Complete Mediation (p.1413)
- C CWE-424: Improper Protection of Alternate Path (p.1031)
- B CWE-425: Direct Request ('Forced Browsing') (p.1032)
- C CWE-653: Improper Isolation or Compartmentalization (p.1445)
- B CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) (p.1985)
- B CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
- B CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) (p.2237)
- B CWE-654: Reliance on a Single Factor in a Security Decision (p.1448)
- B CWE-308: Use of Single-factor Authentication (p.759)
- B CWE-309: Use of Password System for Primary Authentication (p.761)
- C CWE-655: Insufficient Psychological Acceptability (p.1450)
- C CWE-656: Reliance on Security Through Obscurity (p.1452)
- C CWE-671: Lack of Administrator Control over Security (p.1487)
- B CWE-447: Unimplemented or Unsupported Feature in UI (p.1082)
- B CWE-798: Use of Hard-coded Credentials (p.1699)
- V CWE-259: Use of Hard-coded Password (p.630)
- V CWE-321: Use of Hard-coded Cryptographic Key (p.792)
- C CWE-684: Incorrect Provision of Specified Functionality (p.1514)
- B CWE-1245: Improper Finite State Machines (FSMs) in Hardware Logic (p.2052)
- B CWE-392: Missing Report of Error Condition (p.958)
- B CWE-393: Return of Wrong Status Code (p.960)
- B CWE-440: Expected Behavior Violation (p.1069)
- C CWE-446: UI Discrepancy for Security Feature (p.1081)
- B CWE-447: Unimplemented or Unsupported Feature in UI (p.1082)
- B CWE-448: Obsolete Feature in UI (p.1083)
- B CWE-449: The UI Performs the Wrong Action (p.1084)
- C CWE-451: User Interface (UI) Misrepresentation of Critical Information (p.1087)
- B CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User (p.1866)
- B CWE-1021: Improper Restriction of Rendered UI Layers or Frames (p.1869)
- C CWE-912: Hidden Functionality (p.1812)
- C CWE-506: Embedded Malicious Code (p.1218)
- B CWE-507: Trojan Horse (p.1220)
- B CWE-508: Non-Replicating Malicious Code (p.1221)
- B CWE-509: Replicating Malicious Code (Virus or Worm) (p.1222)
- B CWE-510: Trapdoor (p.1223)
- B CWE-511: Logic/Time Bomb (p.1225)
- B CWE-512: Spyware (p.1226)
- C CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
- C CWE-1038: Insecure Automated Optimizations (p.1881)
- B CWE-1037: Processor Optimization Removal or Modification of Security-critical Code (p.1879)
- B CWE-733: Compiler Optimization Removal or Modification of Security-critical Code (p.1570)
- V CWE-14: Compiler Removal of Code to Clear Buffers (p.14)
- B CWE-1102: Reliance on Machine-Dependent Data Representation (p.1951)
- B CWE-1103: Use of Platform-Dependent Third Party Components (p.1952)
- B CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality (p.1954)
- B CWE-188: Reliance on Data/Memory Layout (p.476)
- V CWE-198: Use of Incorrect Byte Ordering (p.510)
- B CWE-474: Use of Function with Inconsistent Implementations (p.1136)
- V CWE-589: Call to Non-ubiquitous API (p.1333)

-  CWE-562: Return of Stack Variable Address (*p. 1287*)
-  CWE-587: Assignment of a Fixed Address to a Pointer (*p. 1330*)
-  CWE-588: Attempt to Access Child of a Non-structure Pointer (*p. 1332*)

Graph View: CWE-1003: Weaknesses for Simplified Mapping of Published Vulnerabilities

- C CWE-20: Improper Input Validation (p.20)
- B CWE-1284: Improper Validation of Specified Quantity in Input (p.2142)
- V CWE-129: Improper Validation of Array Index (p.347)
- C CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (p.138)
 - B CWE-1236: Improper Neutralization of Formula Elements in a CSV File (p.2031)
 - C CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
 - B CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 - B CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
 - B CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
 - B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
 - B CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
 - B CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
 - B CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
- C CWE-116: Improper Encoding or Escaping of Output (p.287)
 - B CWE-838: Inappropriate Encoding for Output Context (p.1773)
- C CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
 - B CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
 - B CWE-125: Out-of-bounds Read (p.336)
 - B CWE-787: Out-of-bounds Write (p.1669)
 - B CWE-824: Access of Uninitialized Pointer (p.1738)
- C CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
 - B CWE-203: Observable Discrepancy (p.525)
 - B CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
 - B CWE-532: Insertion of Sensitive Information into Log File (p.1250)
- C CWE-269: Improper Privilege Management (p.653)
- C CWE-287: Improper Authentication (p.699)
 - B CWE-290: Authentication Bypass by Spoofing (p.712)
 - B CWE-294: Authentication Bypass by Capture-replay (p.719)
 - B CWE-295: Improper Certificate Validation (p.721)
 - B CWE-306: Missing Authentication for Critical Function (p.748)
 - B CWE-307: Improper Restriction of Excessive Authentication Attempts (p.754)
 - B CWE-521: Weak Password Requirements (p.1231)
 - C CWE-522: Insufficiently Protected Credentials (p.1234)
 - B CWE-640: Weak Password Recovery Mechanism for Forgotten Password (p.1418)
 - B CWE-798: Use of Hard-coded Credentials (p.1699)
- C CWE-311: Missing Encryption of Sensitive Data (p.764)
 - B CWE-312: Cleartext Storage of Sensitive Information (p.771)
 - B CWE-319: Cleartext Transmission of Sensitive Information (p.786)
- C CWE-326: Inadequate Encryption Strength (p.803)
- C CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 - B CWE-916: Use of Password Hash With Insufficient Computational Effort (p.1822)
- C CWE-330: Use of Insufficiently Random Values (p.821)
 - B CWE-331: Insufficient Entropy (p.828)
 - B CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) (p.836)
 - B CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (p.844)
- C CWE-345: Insufficient Verification of Data Authenticity (p.858)
 - C CWE-346: Origin Validation Error (p.860)
 - B CWE-347: Improper Verification of Cryptographic Signature (p.864)

- B CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
- B CWE-354: Improper Validation of Integrity Check Value (p.883)
- B CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel (p.1839)
- C CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
 - B CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition (p.913)
- C CWE-400: Uncontrolled Resource Consumption (p.971)
 - B CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
 - B CWE-920: Improper Restriction of Power Consumption (p.1832)
- C CWE-404: Improper Resource Shutdown or Release (p.987)
 - V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
 - B CWE-459: Incomplete Cleanup (p.1106)
 - B CWE-763: Release of Invalid Pointer or Reference (p.1608)
 - B CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
- C CWE-407: Inefficient Algorithmic Complexity (p.999)
 - B CWE-1333: Inefficient Regular Expression Complexity (p.2243)
- C CWE-436: Interpretation Conflict (p.1065)
 - B CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') (p.1075)
- C CWE-610: Externally Controlled Reference to a Resource in Another Sphere (p.1373)
 - B CWE-1021: Improper Restriction of Rendered UI Layers or Frames (p.1869)
 - B CWE-384: Session Fixation (p.943)
 - B CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (p.1353)
 - B CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
 - B CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
- C CWE-662: Improper Synchronization (p.1457)
 - C CWE-667: Improper Locking (p.1472)
- C CWE-665: Improper Initialization (p.1465)
 - B CWE-1188: Initialization of a Resource with an Insecure Default (p.1983)
 - B CWE-908: Use of Uninitialized Resource (p.1802)
 - C CWE-909: Missing Initialization of Resource (p.1806)
- C CWE-668: Exposure of Resource to Wrong Sphere (p.1478)
 - B CWE-134: Use of Externally-Controlled Format String (p.371)
 - B CWE-426: Untrusted Search Path (p.1035)
 - B CWE-427: Uncontrolled Search Path Element (p.1040)
 - B CWE-428: Unquoted Search Path or Element (p.1047)
 - B CWE-552: Files or Directories Accessible to External Parties (p.1274)
- C CWE-669: Incorrect Resource Transfer Between Spheres (p.1480)
 - B CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer (p.551)
 - B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
 - B CWE-494: Download of Code Without Integrity Check (p.1192)
 - B CWE-565: Reliance on Cookies without Validation and Integrity Checking (p.1292)
 - B CWE-829: Inclusion of Functionality from Untrusted Control Sphere (p.1750)
- C CWE-670: Always-Incorrect Control Flow Implementation (p.1484)
 - B CWE-617: Reachable Assertion (p.1387)
- C CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 - V CWE-415: Double Free (p.1015)
 - V CWE-416: Use After Free (p.1019)
 - B CWE-613: Insufficient Session Expiration (p.1380)
- C CWE-674: Uncontrolled Recursion (p.1493)
 - B CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') (p.1642)
- P CWE-682: Incorrect Calculation (p.1507)
 - B CWE-131: Incorrect Calculation of Buffer Size (p.361)
 - B CWE-190: Integer Overflow or Wraparound (p.478)




















































- B CWE-191: Integer Underflow (Wrap or Wraparound) (p.487)
- B CWE-193: Off-by-one Error (p.493)
- B CWE-369: Divide By Zero (p.920)
- P CWE-697: Incorrect Comparison (p.1538)
- G CWE-704: Incorrect Type Conversion or Cast (p.1547)
- B CWE-681: Incorrect Conversion between Numeric Types (p.1504)
- B CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') (p.1785)
- G CWE-706: Use of Incorrectly-Resolved Name or Reference (p.1553)
- B CWE-178: Improper Handling of Case Sensitivity (p.451)
- B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
- B CWE-59: Improper Link Resolution Before File Access ('Link Following') (p.112)
- G CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
- B CWE-276: Incorrect Default Permissions (p.672)
- B CWE-281: Improper Preservation of Permissions (p.681)
- G CWE-754: Improper Check for Unusual or Exceptional Conditions (p.1577)
- B CWE-252: Unchecked Return Value (p.613)
- B CWE-273: Improper Check for Dropped Privileges (p.667)
- B CWE-476: NULL Pointer Dereference (p.1139)
- G CWE-755: Improper Handling of Exceptional Conditions (p.1585)
- G CWE-834: Excessive Iteration (p.1763)
- B CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') (p.1766)
- G CWE-862: Missing Authorization (p.1789)
- B CWE-425: Direct Request ('Forced Browsing') (p.1032)
- G CWE-863: Incorrect Authorization (p.1796)
- B CWE-639: Authorization Bypass Through User-Controlled Key (p.1415)
- G CWE-913: Improper Control of Dynamically-Managed Code Resources (p.1814)
- V CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (p.2216)
- B CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (p.1125)
- B CWE-502: Deserialization of Untrusted Data (p.1212)
- G CWE-922: Insecure Storage of Sensitive Information (p.1835)

Graph View: CWE-1008: Architectural Concepts

- C** CWE-1009: Audit (p.2445)
 - B** CWE-117: Improper Output Neutralization for Logs (p.294)
 - B** CWE-223: Omission of Security-relevant Information (p.566)
 - B** CWE-224: Obscured Security-relevant Information by Alternate Name (p.568)
 - B** CWE-532: Insertion of Sensitive Information into Log File (p.1250)
 - B** CWE-778: Insufficient Logging (p.1647)
 - B** CWE-779: Logging of Excessive Data (p.1651)
- C** CWE-1010: Authenticate Actors (p.2445)
 - V** CWE-258: Empty Password in Configuration File (p.628)
 - V** CWE-259: Use of Hard-coded Password (p.630)
 - B** CWE-262: Not Using Password Aging (p.640)
 - B** CWE-263: Password Aging with Long Expiration (p.643)
 - G** CWE-287: Improper Authentication (p.699)
 - B** CWE-288: Authentication Bypass Using an Alternate Path or Channel (p.707)
 - B** CWE-289: Authentication Bypass by Alternate Name (p.710)
 - B** CWE-290: Authentication Bypass by Spoofing (p.712)
 - V** CWE-291: Reliance on IP Address for Authentication (p.715)
 - V** CWE-293: Using Referer Field for Authentication (p.717)
 - B** CWE-294: Authentication Bypass by Capture-replay (p.719)
 - B** CWE-301: Reflection Attack in an Authentication Protocol (p.740)
 - B** CWE-302: Authentication Bypass by Assumed-Immutable Data (p.742)
 - B** CWE-303: Incorrect Implementation of Authentication Algorithm (p.744)
 - B** CWE-304: Missing Critical Step in Authentication (p.745)
 - B** CWE-305: Authentication Bypass by Primary Weakness (p.747)
 - B** CWE-306: Missing Authentication for Critical Function (p.748)
 - B** CWE-307: Improper Restriction of Excessive Authentication Attempts (p.754)
 - B** CWE-308: Use of Single-factor Authentication (p.759)
 - B** CWE-322: Key Exchange without Entity Authentication (p.795)
 - B** CWE-521: Weak Password Requirements (p.1231)
 - V** CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created (p.1339)
 - B** CWE-603: Use of Client-Side Authentication (p.1363)
 - B** CWE-620: Unverified Password Change (p.1392)
 - B** CWE-640: Weak Password Recovery Mechanism for Forgotten Password (p.1418)
 - B** CWE-798: Use of Hard-coded Credentials (p.1699)
 - B** CWE-836: Use of Password Hash Instead of Password for Authentication (p.1770)
 - B** CWE-916: Use of Password Hash With Insufficient Computational Effort (p.1822)
- C** CWE-1011: Authorize Actors (p.2446)
 - G** CWE-114: Process Control (p.283)
 - B** CWE-15: External Control of System or Configuration Setting (p.17)
 - V** CWE-219: Storage of File with Sensitive Data Under Web Root (p.560)
 - V** CWE-220: Storage of File With Sensitive Data Under FTP Root (p.562)
 - B** CWE-266: Incorrect Privilege Assignment (p.645)
 - B** CWE-267: Privilege Defined With Unsafe Actions (p.648)
 - B** CWE-268: Privilege Chaining (p.651)
 - G** CWE-269: Improper Privilege Management (p.653)
 - B** CWE-270: Privilege Context Switching Error (p.659)
 - G** CWE-271: Privilege Dropping / Lowering Errors (p.660)
 - B** CWE-272: Least Privilege Violation (p.663)
 - B** CWE-273: Improper Check for Dropped Privileges (p.667)
 - B** CWE-274: Improper Handling of Insufficient Privileges (p.670)
 - B** CWE-276: Incorrect Default Permissions (p.672)
 - V** CWE-277: Insecure Inherited Permissions (p.675)
















































- V CWE-279: Incorrect Execution-Assigned Permissions (p.678)
- B CWE-280: Improper Handling of Insufficient Permissions or Privileges (p.679)
- B CWE-281: Improper Preservation of Permissions (p.681)
- C CWE-282: Improper Ownership Management (p.683)
- B CWE-283: Unverified Ownership (p.685)
- P CWE-284: Improper Access Control (p.687)
- C CWE-285: Improper Authorization (p.691)
- C CWE-286: Incorrect User Management (p.698)
- C CWE-300: Channel Accessible by Non-Endpoint (p.737)
- B CWE-341: Predictable from Observable State (p.850)
- B CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
- B CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') (p.985)
- B CWE-419: Unprotected Primary Channel (p.1024)
- B CWE-420: Unprotected Alternate Channel (p.1025)
- B CWE-425: Direct Request ('Forced Browsing') (p.1032)
- B CWE-426: Untrusted Search Path (p.1035)
- B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
- V CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere (p.1245)
- V CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere (p.1246)
- V CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere (p.1247)
- V CWE-530: Exposure of Backup File to an Unauthorized Control Sphere (p.1248)
- B CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory (p.1257)
- B CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization (p.1273)
- B CWE-552: Files or Directories Accessible to External Parties (p.1274)
- V CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key (p.1294)
- B CWE-639: Authorization Bypass Through User-Controlled Key (p.1415)
- C CWE-642: External Control of Critical State Data (p.1422)
- V CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions (p.1435)
- C CWE-653: Improper Isolation or Compartmentalization (p.1445)
- C CWE-656: Reliance on Security Through Obscurity (p.1452)
- C CWE-668: Exposure of Resource to Wrong Sphere (p.1478)
- C CWE-669: Incorrect Resource Transfer Between Spheres (p.1480)
- C CWE-671: Lack of Administrator Control over Security (p.1487)
- C CWE-673: External Influence of Sphere Definition (p.1492)
- B CWE-708: Incorrect Ownership Assignment (p.1556)
- C CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
- B CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
- V CWE-782: Exposed IOCTL with Insufficient Access Control (p.1657)
- V CWE-827: Improper Control of Document Type Definition (p.1745)
- C CWE-862: Missing Authorization (p.1789)
- C CWE-863: Incorrect Authorization (p.1796)
- B CWE-921: Storage of Sensitive Data in a Mechanism without Access Control (p.1834)
- C CWE-923: Improper Restriction of Communication Channel to Intended Endpoints (p.1836)
- B CWE-939: Improper Authorization in Handler for Custom URL Scheme (p.1849)
- V CWE-942: Permissive Cross-domain Policy with Untrusted Domains (p.1857)
- C CWE-1012: Cross Cutting (p.2448)
- B CWE-208: Observable Timing Discrepancy (p.537)
- B CWE-392: Missing Report of Error Condition (p.958)
- B CWE-460: Improper Cleanup on Thrown Exception (p.1109)
- B CWE-544: Missing Standardized Error Handling Mechanism (p.1265)
- C CWE-602: Client-Side Enforcement of Server-Side Security (p.1359)
- P CWE-703: Improper Check or Handling of Exceptional Conditions (p.1544)
- C CWE-754: Improper Check for Unusual or Exceptional Conditions (p.1577)

- V CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision (p.1662)
- B CWE-807: Reliance on Untrusted Inputs in a Security Decision (p.1723)
- C CWE-1013: Encrypt Data (p.2449)
 - B CWE-256: Plaintext Storage of a Password (p.622)
 - B CWE-257: Storing Passwords in a Recoverable Format (p.625)
 - B CWE-260: Password in Configuration File (p.636)
 - B CWE-261: Weak Encoding for Password (p.638)
 - C CWE-311: Missing Encryption of Sensitive Data (p.764)
 - B CWE-312: Cleartext Storage of Sensitive Information (p.771)
 - V CWE-313: Cleartext Storage in a File or on Disk (p.777)
 - V CWE-314: Cleartext Storage in the Registry (p.779)
 - V CWE-315: Cleartext Storage of Sensitive Information in a Cookie (p.781)
 - V CWE-316: Cleartext Storage of Sensitive Information in Memory (p.782)
 - V CWE-317: Cleartext Storage of Sensitive Information in GUI (p.784)
 - V CWE-318: Cleartext Storage of Sensitive Information in Executable (p.785)
 - B CWE-319: Cleartext Transmission of Sensitive Information (p.786)
 - V CWE-321: Use of Hard-coded Cryptographic Key (p.792)
 - B CWE-323: Reusing a Nonce, Key Pair in Encryption (p.797)
 - B CWE-324: Use of a Key Past its Expiration Date (p.799)
 - B CWE-325: Missing Cryptographic Step (p.801)
 - C CWE-326: Inadequate Encryption Strength (p.803)
 - C CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 - B CWE-328: Use of Weak Hash (p.813)
 - C CWE-330: Use of Insufficiently Random Values (p.821)
 - B CWE-331: Insufficient Entropy (p.828)
 - V CWE-332: Insufficient Entropy in PRNG (p.830)
 - V CWE-333: Improper Handling of Insufficient Entropy in TRNG (p.832)
 - B CWE-334: Small Space of Random Values (p.834)
 - B CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) (p.836)
 - V CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) (p.839)
 - V CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) (p.841)
 - B CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (p.844)
 - V CWE-339: Small Seed Space in PRNG (p.847)
 - B CWE-347: Improper Verification of Cryptographic Signature (p.864)
 - C CWE-522: Insufficiently Protected Credentials (p.1234)
 - B CWE-523: Unprotected Transport of Credentials (p.1239)
 - B CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') (p.1589)
 - V CWE-759: Use of a One-Way Hash without a Salt (p.1593)
 - V CWE-760: Use of a One-Way Hash with a Predictable Salt (p.1598)
 - V CWE-780: Use of RSA Algorithm without OAEP (p.1652)
 - C CWE-922: Insecure Storage of Sensitive Information (p.1835)
- C CWE-1014: Identify Actors (p.2450)
 - B CWE-295: Improper Certificate Validation (p.721)
 - B CWE-296: Improper Following of a Certificate's Chain of Trust (p.726)
 - V CWE-297: Improper Validation of Certificate with Host Mismatch (p.729)
 - V CWE-298: Improper Validation of Certificate Expiration (p.733)
 - B CWE-299: Improper Check for Certificate Revocation (p.734)
 - C CWE-345: Insufficient Verification of Data Authenticity (p.858)
 - C CWE-346: Origin Validation Error (p.860)
 - V CWE-370: Missing Check for Certificate Revocation after Initial Check (p.924)
 - C CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') (p.1072)
 - V CWE-599: Missing Validation of OpenSSL Certificate (p.1350)
 - B CWE-940: Improper Verification of Source of a Communication Channel (p.1852)

-  CWE-941: Incorrectly Specified Destination in a Communication Channel (p.1855)
-  CWE-1015: Limit Access (p.2451)
 -  CWE-201: Insertion of Sensitive Information Into Sent Data (p.521)
 -  CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
 -  CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer (p.551)
 -  CWE-243: Creation of chroot Jail Without Changing Working Directory (p.596)
 -  CWE-250: Execution with Unnecessary Privileges (p.606)
 -  CWE-610: Externally Controlled Reference to a Resource in Another Sphere (p.1373)
 -  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
 -  CWE-73: External Control of File Name or Path (p.133)
-  CWE-1016: Limit Exposure (p.2452)
 -  CWE-210: Self-generated Error Message Containing Sensitive Information (p.546)
 -  CWE-211: Externally-Generated Error Message Containing Sensitive Information (p.548)
 -  CWE-214: Invocation of Process Using Visible Sensitive Information (p.556)
 -  CWE-550: Server-generated Error Message Containing Sensitive Information (p.1272)
 -  CWE-829: Inclusion of Functionality from Untrusted Control Sphere (p.1750)
 -  CWE-830: Inclusion of Web Functionality from an Untrusted Source (p.1756)
-  CWE-1017: Lock Computer (p.2452)
 -  CWE-645: Overly Restrictive Account Lockout Mechanism (p.1432)
-  CWE-1018: Manage User Sessions (p.2453)
 -  CWE-384: Session Fixation (p.943)
 -  CWE-488: Exposure of Data Element to Wrong Session (p.1176)
 -  CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session (p.1318)
 -  CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length (p.2)
 -  CWE-613: Insufficient Session Expiration (p.1380)
 -  CWE-841: Improper Enforcement of Behavioral Workflow (p.1781)
-  CWE-1019: Validate Inputs (p.2454)
 -  CWE-138: Improper Neutralization of Special Elements (p.379)
 -  CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences (p.400)
 -  CWE-20: Improper Input Validation (p.20)
 -  CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data (p.868)
 -  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
 -  CWE-472: External Control of Assumed-Immutable Web Parameter (p.1131)
 -  CWE-473: PHP External Variable Modification (p.1134)
 -  CWE-502: Deserialization of Untrusted Data (p.1212)
 -  CWE-59: Improper Link Resolution Before File Access ('Link Following') (p.112)
 -  CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (p.1353)
 -  CWE-641: Improper Restriction of Names for Files and Other Resources (p.1421)
 -  CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
 -  CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)
 -  CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (p.138)
 -  CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) (p.145)
 -  CWE-76: Improper Neutralization of Equivalent Special Elements (p.146)
 -  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
 -  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 -  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
 -  CWE-790: Improper Filtering of Special Elements (p.1687)
 -  CWE-791: Incomplete Filtering of Special Elements (p.1689)
 -  CWE-792: Incomplete Filtering of One or More Instances of Special Elements (p.1690)
 -  CWE-793: Only Filtering One Instance of a Special Element (p.1692)
 -  CWE-794: Incomplete Filtering of Multiple Instances of Special Elements (p.1693)

- B CWE-795: Only Filtering Special Elements at a Specified Location (p.1694)
- V CWE-796: Only Filtering Special Elements Relative to a Marker (p.1696)
- V CWE-797: Only Filtering Special Elements at an Absolute Position (p.1698)
- B CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
- B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
- B CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
- B CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
- B CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') (p.222)
- B CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
- C CWE-943: Improper Neutralization of Special Elements in Data Query Logic (p.1860)
- V CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (p.232)
- B CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') (p.238)
- V CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page (p.241)
- V CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') (p.242)
- C CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
- C CWE-1020: Verify Message Integrity (p.2455)
- B CWE-353: Missing Support for Integrity Check (p.881)
- B CWE-354: Improper Validation of Integrity Check Value (p.883)
- B CWE-390: Detection of Error Condition Without Action (p.950)
- B CWE-391: Unchecked Error Condition (p.955)
- B CWE-494: Download of Code Without Integrity Check (p.1192)
- B CWE-565: Reliance on Cookies without Validation and Integrity Checking (p.1292)
- B CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking (p.1439)
- P CWE-707: Improper Neutralization (p.1554)
- C CWE-755: Improper Handling of Exceptional Conditions (p.1585)
- B CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel (p.1839)

Graph View: CWE-1026: Weaknesses in OWASP Top Ten (2017)

-  CWE-1027: OWASP Top Ten 2017 Category A1 - Injection (p.2456)
 -  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
 -  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 -  CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
 -  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
 -  CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
 -  CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
 -  CWE-564: SQL Injection: Hibernate (p.1290)
 -  CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
 -  CWE-943: Improper Neutralization of Special Elements in Data Query Logic (p.1860)
-  CWE-1028: OWASP Top Ten 2017 Category A2 - Broken Authentication (p.2457)
 -  CWE-287: Improper Authentication (p.699)
 -  CWE-256: Plaintext Storage of a Password (p.622)
 -  CWE-308: Use of Single-factor Authentication (p.759)
 -  CWE-384: Session Fixation (p.943)
 -  CWE-522: Insufficiently Protected Credentials (p.1234)
 -  CWE-523: Unprotected Transport of Credentials (p.1239)
 -  CWE-613: Insufficient Session Expiration (p.1380)
 -  CWE-620: Unverified Password Change (p.1392)
 -  CWE-640: Weak Password Recovery Mechanism for Forgotten Password (p.1418)
-  CWE-1029: OWASP Top Ten 2017 Category A3 - Sensitive Data Exposure (p.2457)
 -  CWE-220: Storage of File With Sensitive Data Under FTP Root (p.562)
 -  CWE-295: Improper Certificate Validation (p.721)
 -  CWE-311: Missing Encryption of Sensitive Data (p.764)
 -  CWE-312: Cleartext Storage of Sensitive Information (p.771)
 -  CWE-319: Cleartext Transmission of Sensitive Information (p.786)
 -  CWE-320: Key Management Errors (p.2340)
 -  CWE-325: Missing Cryptographic Step (p.801)
 -  CWE-326: Inadequate Encryption Strength (p.803)
 -  CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 -  CWE-328: Use of Weak Hash (p.813)
 -  CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
-  CWE-1030: OWASP Top Ten 2017 Category A4 - XML External Entities (XXE) (p.2458)
 -  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
 -  CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') (p.1642)
-  CWE-1031: OWASP Top Ten 2017 Category A5 - Broken Access Control (p.2458)
 -  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 -  CWE-284: Improper Access Control (p.687)
 -  CWE-285: Improper Authorization (p.691)
 -  CWE-425: Direct Request ('Forced Browsing') (p.1032)
 -  CWE-639: Authorization Bypass Through User-Controlled Key (p.1415)
-  CWE-1032: OWASP Top Ten 2017 Category A6 - Security Misconfiguration (p.2459)
 -  CWE-16: Configuration (p.2330)
 -  CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
 -  CWE-548: Exposure of Information Through Directory Listing (p.1269)
-  CWE-1033: OWASP Top Ten 2017 Category A7 - Cross-Site Scripting (XSS) (p.2459)
 -  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)

- C CWE-1034: OWASP Top Ten 2017 Category A8 - Insecure Deserialization (p.2459)
 - B CWE-502: Deserialization of Untrusted Data (p.1212)
- C CWE-1035: OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities (p.2460)
- C CWE-1036: OWASP Top Ten 2017 Category A10 - Insufficient Logging & Monitoring (p.2460)
 - B CWE-223: Omission of Security-relevant Information (p.566)
 - B CWE-778: Insufficient Logging (p.1647)

Graph View: CWE-1128: CISQ Quality Measures (2016)

-  CWE-1129: CISQ Quality Measures (2016) - Reliability (p.2461)
 -  CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
 -  CWE-252: Unchecked Return Value (p.613)
 -  CWE-396: Declaration of Catch for Generic Exception (p.966)
 -  CWE-397: Declaration of Throws for Generic Exception (p.968)
 -  CWE-456: Missing Initialization of a Variable (p.1096)
 -  CWE-674: Uncontrolled Recursion (p.1493)
 -  CWE-704: Incorrect Type Conversion or Cast (p.1547)
 -  CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
 -  CWE-788: Access of Memory Location After End of Buffer (p.1678)
 -  CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor (p.1889)
 -  CWE-1047: Modules with Circular Dependencies (p.1891)
 -  CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data (p.1896)
 -  CWE-1056: Invokable Control Element with Variadic Parameters (p.1901)
 -  CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)
 -  CWE-1062: Parent Class with References to Child Class (p.1909)
 -  CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers (p.1912)
 -  CWE-1066: Missing Serialization Control Element (p.1913)
 -  CWE-1069: Empty Exception Block (p.1916)
 -  CWE-1070: Serializable Data Element Containing non-Serializable Item Elements (p.1918)
 -  CWE-1077: Floating Point Comparison with Incorrect Operator (p.1926)
 -  CWE-1079: Parent Class without Virtual Destructor Method (p.1929)
 -  CWE-1082: Class Instance Self Destruction Control Element (p.1931)
 -  CWE-1083: Data Access from Outside Expected Data Manager Component (p.1932)
 -  CWE-1087: Class with Virtual Method without a Virtual Destructor (p.1936)
 -  CWE-1088: Synchronous Access of Remote Resource without Timeout (p.1937)
 -  CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element (p.1946)
 -  CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)
 -  CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element (p.1947)
-  CWE-1130: CISQ Quality Measures (2016) - Maintainability (p.2462)
 -  CWE-561: Dead Code (p.1283)
 -  CWE-1041: Use of Redundant Code (p.1884)
 -  CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range (p.1888)
 -  CWE-1047: Modules with Circular Dependencies (p.1891)
 -  CWE-1048: Invokable Control Element with Large Number of Outward Calls (p.1892)
 -  CWE-1052: Excessive Use of Hard-Coded Literals in Initialization (p.1897)
 -  CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer (p.1899)
 -  CWE-1055: Multiple Inheritance from Concrete Classes (p.1900)
 -  CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters (p.1911)
 -  CWE-1074: Class with Excessively Deep Inheritance (p.1923)
 -  CWE-1075: Unconditional Control Flow Transfer outside of Switch Block (p.1924)
 -  CWE-1080: Source Code File with Excessive Number of Lines of Code (p.1930)
 -  CWE-766: Critical Data Element Declared Public (p.1615)
 -  CWE-1084: Invokable Control Element with Excessive File or Data Access Operations (p.1933)
 -  CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code (p.1934)
 -  CWE-1086: Class with Excessive Number of Child Classes (p.1935)
 -  CWE-1090: Method Containing Access of a Member Element from Another Class (p.1939)
 -  CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers (p.1941)

- B CWE-1095: Loop Condition Value Update within the Loop (p.1944)
- B CWE-1121: Excessive McCabe Cyclomatic Complexity (p.1970)
- C CWE-1131: CISQ Quality Measures (2016) - Security (p.2463)
 - B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 - B CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 - B CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
 - B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
 - C CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
 - B CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
 - V CWE-129: Improper Validation of Array Index (p.347)
 - B CWE-134: Use of Externally-Controlled Format String (p.371)
 - B CWE-252: Unchecked Return Value (p.613)
 - C CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 - B CWE-396: Declaration of Catch for Generic Exception (p.966)
 - B CWE-397: Declaration of Throws for Generic Exception (p.968)
 - B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
 - V CWE-456: Missing Initialization of a Variable (p.1096)
 - B CWE-606: Unchecked Input for Loop Condition (p.1366)
 - C CWE-667: Improper Locking (p.1472)
 - C CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 - B CWE-681: Incorrect Conversion between Numeric Types (p.1504)
 - B CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
 - V CWE-789: Memory Allocation with Excessive Size Value (p.1683)
 - B CWE-798: Use of Hard-coded Credentials (p.1699)
 - B CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') (p.1766)
- C CWE-1132: CISQ Quality Measures (2016) - Performance Efficiency (p.2464)
 - V CWE-1042: Static Member Data Element outside of a Singleton Class Element (p.1886)
 - B CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements (p.1887)
 - B CWE-1046: Creation of Immutable Text Using String Concatenation (p.1890)
 - B CWE-1049: Excessive Data Query Operations in a Large Data Table (p.1894)
 - B CWE-1050: Excessive Platform Resource Consumption within a Loop (p.1895)
 - B CWE-1057: Data Access Operations Outside of Expected Data Manager Component (p.1902)
 - B CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses (p.1906)
 - B CWE-1063: Creation of Class Instance within a Static Code Block (p.1910)
 - B CWE-1067: Excessive Execution of Sequential Searches of Data Resource (p.1914)
 - B CWE-1072: Data Resource Access without Use of Connection Pooling (p.1921)
 - B CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses (p.1922)
 - B CWE-1089: Large Data Table with Excessive Number of Indices (p.1938)
 - B CWE-1091: Use of Object without Invoking Destructor Method (p.1940)
 - B CWE-1094: Excessive Index Range Scan for a Data Resource (p.1943)




















































Graph View: CWE-1133: Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java






















































- C** CWE-1134: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 00. Input Validation and Data Sanitization (IDS) (p.2465)
 - G** CWE-116: Improper Encoding or Escaping of Output (p.287)
 - V** CWE-180: Incorrect Behavior Order: Validate Before Canonicalize (p.457)
 - B** CWE-289: Authentication Bypass by Alternate Name (p.710)
 - B** CWE-117: Improper Output Neutralization for Logs (p.294)
 - V** CWE-144: Improper Neutralization of Line Delimiters (p.389)
 - V** CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences (p.400)
 - B** CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) (p.1004)
 - B** CWE-134: Use of Externally-Controlled Format String (p.371)
 - B** CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 - B** CWE-182: Collapse of Data into Unsafe Value (p.462)
- C** CWE-1135: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 01. Declarations and Initialization (DCL) (p.2465)
 - G** CWE-665: Improper Initialization (p.1465)
- C** CWE-1136: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 02. Expressions (EXP) (p.2466)
 - B** CWE-252: Unchecked Return Value (p.613)
 - B** CWE-476: NULL Pointer Dereference (p.1139)
 - V** CWE-597: Use of Wrong Operator in String Comparison (p.1345)
 - V** CWE-595: Comparison of Object References Instead of Object Contents (p.1342)
- C** CWE-1137: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 03. Numeric Types and Operations (NUM) (p.2466)
 - B** CWE-190: Integer Overflow or Wraparound (p.478)
 - B** CWE-191: Integer Underflow (Wrap or Wraparound) (p.487)
 - B** CWE-197: Numeric Truncation Error (p.507)
 - B** CWE-369: Divide By Zero (p.920)
 - B** CWE-681: Incorrect Conversion between Numeric Types (p.1504)
 - P** CWE-682: Incorrect Calculation (p.1507)
- C** CWE-1138: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 04. Characters and Strings (STR) (p.2467)
 - B** CWE-838: Inappropriate Encoding for Output Context (p.1773)
- C** CWE-1139: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 05. Object Orientation (OBJ) (p.2467)
 - B** CWE-374: Passing Mutable Objects to an Untrusted Method (p.927)
 - B** CWE-375: Returning a Mutable Object to an Untrusted Caller (p.930)
 - V** CWE-486: Comparison of Classes by Name (p.1172)
 - V** CWE-491: Public cloneable() Method Without Final ('Object Hijack') (p.1181)
 - V** CWE-492: Use of Inner Class Containing Sensitive Data (p.1183)
 - V** CWE-498: Cloneable Class Containing Sensitive Information (p.1204)
 - V** CWE-500: Public Static Field Not Marked Final (p.1208)
 - B** CWE-766: Critical Data Element Declared Public (p.1615)
- C** CWE-1140: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 06. Methods (MET) (p.2468)
 - B** CWE-617: Reachable Assertion (p.1387)
 - V** CWE-589: Call to Non-ubiquitous API (p.1333)
 - P** CWE-697: Incorrect Comparison (p.1538)
 - V** CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined (p.1321)
 - G** CWE-573: Improper Following of Specification by Caller (p.1307)
 - B** CWE-586: Explicit Call to Finalize() (p.1329)
 - V** CWE-583: finalize() Method Declared Public (p.1324)
 - V** CWE-568: finalize() Method Without super.finalize() (p.1299)

- C** CWE-1141: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 07. Exceptional Behavior (ERR) (p.2469)
 - B** CWE-460: Improper Cleanup on Thrown Exception (p.1109)
 - B** CWE-584: Return Inside Finally Block (p.1325)
 - B** CWE-459: Incomplete Cleanup (p.1106)
 - B** CWE-248: Uncaught Exception (p.603)
 - C** CWE-705: Incorrect Control Flow Scoping (p.1550)
 - C** CWE-754: Improper Check for Unusual or Exceptional Conditions (p.1577)
 - P** CWE-703: Improper Check or Handling of Exceptional Conditions (p.1544)
 - B** CWE-397: Declaration of Throws for Generic Exception (p.968)
 - V** CWE-382: J2EE Bad Practices: Use of System.exit() (p.940)
- C** CWE-1142: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 08. Visibility and Atomicity (VNA) (p.2469)
 - C** CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
 - B** CWE-366: Race Condition within a Thread (p.910)
 - B** CWE-413: Improper Resource Locking (p.1010)
 - B** CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
 - C** CWE-662: Improper Synchronization (p.1457)
 - C** CWE-667: Improper Locking (p.1472)
- C** CWE-1143: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 09. Locking (LCK) (p.2470)
 - B** CWE-412: Unrestricted Externally Accessible Lock (p.1007)
 - B** CWE-609: Double-Checked Locking (p.1371)
 - C** CWE-667: Improper Locking (p.1472)
 - B** CWE-820: Missing Synchronization (p.1729)
- C** CWE-1144: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 10. Thread APIs (THI) (p.2470)
 - V** CWE-572: Call to Thread run() instead of start() (p.1305)
- C** CWE-1145: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 11. Thread Pools (TPS) (p.2471)
 - B** CWE-392: Missing Report of Error Condition (p.958)
 - C** CWE-405: Asymmetric Resource Consumption (Amplification) (p.993)
 - B** CWE-410: Insufficient Resource Pool (p.1005)
- C** CWE-1146: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 12. Thread-Safety Miscellaneous (TSM) (p.2471)
- C** CWE-1147: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 13. Input Output (FIO) (p.2471)
 - V** CWE-67: Improper Handling of Windows Device Names (p.127)
 - V** CWE-180: Incorrect Behavior Order: Validate Before Canonicalize (p.457)
 - V** CWE-198: Use of Incorrect Byte Ordering (p.510)
 - B** CWE-276: Incorrect Default Permissions (p.672)
 - V** CWE-279: Incorrect Execution-Assigned Permissions (p.678)
 - B** CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
 - C** CWE-377: Insecure Temporary File (p.932)
 - C** CWE-404: Improper Resource Shutdown or Release (p.987)
 - C** CWE-405: Asymmetric Resource Consumption (Amplification) (p.993)
 - B** CWE-459: Incomplete Cleanup (p.1106)
 - B** CWE-532: Insertion of Sensitive Information into Log File (p.1250)
 - V** CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions (p.1435)
 - C** CWE-705: Incorrect Control Flow Scoping (p.1550)
 - C** CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
 - B** CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
- C** CWE-1148: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 14. Serialization (SER) (p.2472)
 - B** CWE-319: Cleartext Transmission of Sensitive Information (p.786)
 - C** CWE-400: Uncontrolled Resource Consumption (p.971)

- V CWE-499: Serializable Class Containing Sensitive Data (p.1206)
- B CWE-502: Deserialization of Untrusted Data (p.1212)
- B CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
- C CWE-1149: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 15. Platform Security (SEC) (p.2473)
- B CWE-266: Incorrect Privilege Assignment (p.645)
- B CWE-272: Least Privilege Violation (p.663)
- G CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
- C CWE-1150: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 16. Runtime Environment (ENV) (p.2473)
- B CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data (p.868)
- G CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
- C CWE-1151: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 17. Java Native Interface (JNI) (p.2474)
- V CWE-111: Direct Use of Unsafe JNI (p.272)
- C CWE-1152: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 49. Miscellaneous (MSC) (p.2474)
- V CWE-259: Use of Hard-coded Password (p.630)
- G CWE-311: Missing Encryption of Sensitive Data (p.764)
- G CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
- G CWE-330: Use of Insufficiently Random Values (p.821)
- V CWE-332: Insufficient Entropy in PRNG (p.830)
- V CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) (p.839)
- V CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) (p.841)
- G CWE-400: Uncontrolled Resource Consumption (p.971)
- V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
- B CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
- B CWE-798: Use of Hard-coded Credentials (p.1699)
- C CWE-1153: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 50. Android (DRD) (p.2475)
- C CWE-1175: SEI CERT Oracle Secure Coding Standard for Java - Guidelines 18. Concurrency (CON) (p.2485)






































Graph View: CWE-1154: Weaknesses Addressed by the SEI CERT C Coding Standard

-  CWE-1155: SEI CERT C Coding Standard - Guidelines 01. Preprocessor (PRE) (p.2475)
-  CWE-1156: SEI CERT C Coding Standard - Guidelines 02. Declarations and Initialization (DCL) (p.2476)
 -  CWE-562: Return of Stack Variable Address (p.1287)
-  CWE-1157: SEI CERT C Coding Standard - Guidelines 03. Expressions (EXP) (p.2476)
 -  CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
 -  CWE-908: Use of Uninitialized Resource (p.1802)
 -  CWE-476: NULL Pointer Dereference (p.1139)
 -  CWE-690: Unchecked Return Value to NULL Pointer Dereference (p.1523)
 -  CWE-628: Function Call with Incorrectly Specified Arguments (p.1407)
 -  CWE-685: Function Call With Incorrect Number of Arguments (p.1516)
 -  CWE-686: Function Call With Incorrect Argument Type (p.1517)
 -  CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') (p.1785)
 -  CWE-704: Incorrect Type Conversion or Cast (p.1547)
 -  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
 -  CWE-125: Out-of-bounds Read (p.336)
 -  CWE-480: Use of Incorrect Operator (p.1157)
 -  CWE-481: Assigning instead of Comparing (p.1161)
-  CWE-1158: SEI CERT C Coding Standard - Guidelines 04. Integers (INT) (p.2477)
 -  CWE-190: Integer Overflow or Wraparound (p.478)
 -  CWE-131: Incorrect Calculation of Buffer Size (p.361)
 -  CWE-191: Integer Underflow (Wrap or Wraparound) (p.487)
 -  CWE-680: Integer Overflow to Buffer Overflow (p.1502)
 -  CWE-192: Integer Coercion Error (p.489)
 -  CWE-197: Numeric Truncation Error (p.507)
 -  CWE-681: Incorrect Conversion between Numeric Types (p.1504)
 -  CWE-704: Incorrect Type Conversion or Cast (p.1547)
 -  CWE-194: Unexpected Sign Extension (p.498)
 -  CWE-195: Signed to Unsigned Conversion Error (p.501)
 -  CWE-369: Divide By Zero (p.920)
 -  CWE-682: Incorrect Calculation (p.1507)
 -  CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
 -  CWE-587: Assignment of a Fixed Address to a Pointer (p.1330)
-  CWE-1159: SEI CERT C Coding Standard - Guidelines 05. Floating Point (FLP) (p.2478)
 -  CWE-682: Incorrect Calculation (p.1507)
 -  CWE-391: Unchecked Error Condition (p.955)
 -  CWE-681: Incorrect Conversion between Numeric Types (p.1504)
 -  CWE-197: Numeric Truncation Error (p.507)
-  CWE-1160: SEI CERT C Coding Standard - Guidelines 06. Arrays (ARR) (p.2478)
 -  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
 -  CWE-129: Improper Validation of Array Index (p.347)
 -  CWE-786: Access of Memory Location Before Start of Buffer (p.1666)
 -  CWE-123: Write-what-where Condition (p.329)
 -  CWE-125: Out-of-bounds Read (p.336)
 -  CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
 -  CWE-469: Use of Pointer Subtraction to Determine Size (p.1123)
 -  CWE-121: Stack-based Buffer Overflow (p.320)
 -  CWE-805: Buffer Access with Incorrect Length Value (p.1711)
 -  CWE-468: Incorrect Pointer Scaling (p.1121)
-  CWE-1161: SEI CERT C Coding Standard - Guidelines 07. Characters and Strings (STR) (p.2479)
 -  CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
 -  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)

-  CWE-121: Stack-based Buffer Overflow (p.320)
-  CWE-122: Heap-based Buffer Overflow (p.324)
-  CWE-123: Write-what-where Condition (p.329)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-676: Use of Potentially Dangerous Function (p.1498)
-  CWE-170: Improper Null Termination (p.434)
-  CWE-704: Incorrect Type Conversion or Cast (p.1547)
-  CWE-1162: SEI CERT C Coding Standard - Guidelines 08. Memory Management (MEM) (p.2479)
 -  CWE-416: Use After Free (p.1019)
 -  CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 -  CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
 -  CWE-666: Operation on Resource in Wrong Phase of Lifetime (p.1471)
 -  CWE-415: Double Free (p.1015)
 -  CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
 -  CWE-404: Improper Resource Shutdown or Release (p.987)
 -  CWE-459: Incomplete Cleanup (p.1106)
 -  CWE-771: Missing Reference to Active Allocated Resource (p.1631)
 -  CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
 -  CWE-590: Free of Memory not on the Heap (p.1335)
 -  CWE-131: Incorrect Calculation of Buffer Size (p.361)
 -  CWE-680: Integer Overflow to Buffer Overflow (p.1502)
 -  CWE-467: Use of sizeof() on a Pointer Type (p.1118)
 -  CWE-789: Memory Allocation with Excessive Size Value (p.1683)
 -  CWE-190: Integer Overflow or Wraparound (p.478)
-  CWE-1163: SEI CERT C Coding Standard - Guidelines 09. Input Output (FIO) (p.2480)
 -  CWE-134: Use of Externally-Controlled Format String (p.371)
 -  CWE-20: Improper Input Validation (p.20)
 -  CWE-67: Improper Handling of Windows Device Names (p.127)
 -  CWE-197: Numeric Truncation Error (p.507)
 -  CWE-241: Improper Handling of Unexpected Data Type (p.591)
 -  CWE-664: Improper Control of a Resource Through its Lifetime (p.1463)
 -  CWE-404: Improper Resource Shutdown or Release (p.987)
 -  CWE-459: Incomplete Cleanup (p.1106)
 -  CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
 -  CWE-773: Missing Reference to Active File Descriptor or Handle (p.1638)
 -  CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
 -  CWE-771: Missing Reference to Active Allocated Resource (p.1631)
 -  CWE-910: Use of Expired File Descriptor (p.1809)
 -  CWE-666: Operation on Resource in Wrong Phase of Lifetime (p.1471)
 -  CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 -  CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
 -  CWE-686: Function Call With Incorrect Argument Type (p.1517)
 -  CWE-685: Function Call With Incorrect Number of Arguments (p.1516)
-  CWE-1165: SEI CERT C Coding Standard - Guidelines 10. Environment (ENV) (p.2481)
 -  CWE-705: Incorrect Control Flow Scoping (p.1550)
 -  CWE-676: Use of Potentially Dangerous Function (p.1498)
 -  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 -  CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
-  CWE-1166: SEI CERT C Coding Standard - Guidelines 11. Signals (SIG) (p.2481)
 -  CWE-479: Signal Handler Use of a Non-reentrant Function (p.1154)
 -  CWE-662: Improper Synchronization (p.1457)
-  CWE-1167: SEI CERT C Coding Standard - Guidelines 12. Error Handling (ERR) (p.2482)
 -  CWE-456: Missing Initialization of a Variable (p.1096)

- B CWE-391: Unchecked Error Condition (p.955)
- B CWE-252: Unchecked Return Value (p.613)
- B CWE-253: Incorrect Check of Function Return Value (p.620)
- B CWE-676: Use of Potentially Dangerous Function (p.1498)
- C CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
- C CWE-1168: SEI CERT C Coding Standard - Guidelines 13. Application Programming Interfaces (API) (p.2483)
- C CWE-1169: SEI CERT C Coding Standard - Guidelines 14. Concurrency (CON) (p.2483)
 - C CWE-667: Improper Locking (p.1472)
 - B CWE-366: Race Condition within a Thread (p.910)
 - B CWE-676: Use of Potentially Dangerous Function (p.1498)
 - C CWE-330: Use of Insufficiently Random Values (p.821)
 - C CWE-377: Insecure Temporary File (p.932)
- C CWE-1170: SEI CERT C Coding Standard - Guidelines 48. Miscellaneous (MSC) (p.2484)
 - C CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 - C CWE-330: Use of Insufficiently Random Values (p.821)
 - B CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (p.844)
 - B CWE-676: Use of Potentially Dangerous Function (p.1498)
 - B CWE-331: Insufficient Entropy (p.828)
 - C CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
- C CWE-1171: SEI CERT C Coding Standard - Guidelines 50. POSIX (POS) (p.2484)
 - B CWE-170: Improper Null Termination (p.434)
 - B CWE-242: Use of Inherently Dangerous Function (p.593)
 - B CWE-363: Race Condition Enabling Link Following (p.904)
 - C CWE-696: Incorrect Behavior Order (p.1535)
 - B CWE-273: Improper Check for Dropped Privileges (p.667)
 - C CWE-667: Improper Locking (p.1472)
 - B CWE-391: Unchecked Error Condition (p.955)
 - B CWE-252: Unchecked Return Value (p.613)
 - B CWE-253: Incorrect Check of Function Return Value (p.620)
- C CWE-1172: SEI CERT C Coding Standard - Guidelines 51. Microsoft Windows (WIN) (p.2485)
 - V CWE-762: Mismatched Memory Management Routines (p.1605)
 - V CWE-590: Free of Memory not on the Heap (p.1335)

Graph View: CWE-1178: Weaknesses Addressed by the SEI CERT Perl Coding Standard

-  CWE-1179: SEI CERT Perl Coding Standard - Guidelines 01. Input Validation and Data Sanitization (IDS) (p.2486)
 -  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 -  CWE-134: Use of Externally-Controlled Format String (p.371)
 -  CWE-129: Improper Validation of Array Index (p.347)
 -  CWE-789: Memory Allocation with Excessive Size Value (p.1683)
 -  CWE-116: Improper Encoding or Escaping of Output (p.287)
 -  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
 -  CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (p.232)
-  CWE-1180: SEI CERT Perl Coding Standard - Guidelines 02. Declarations and Initialization (DCL) (p.2486)
 -  CWE-628: Function Call with Incorrectly Specified Arguments (p.1407)
 -  CWE-456: Missing Initialization of a Variable (p.1096)
 -  CWE-457: Use of Uninitialized Variable (p.1102)
 -  CWE-477: Use of Obsolete Function (p.1146)
-  CWE-1181: SEI CERT Perl Coding Standard - Guidelines 03. Expressions (EXP) (p.2487)
 -  CWE-394: Unexpected Status Code or Return Value (p.962)
 -  CWE-783: Operator Precedence Logic Error (p.1659)
 -  CWE-477: Use of Obsolete Function (p.1146)
 -  CWE-248: Uncaught Exception (p.603)
 -  CWE-391: Unchecked Error Condition (p.955)
 -  CWE-460: Improper Cleanup on Thrown Exception (p.1109)
 -  CWE-705: Incorrect Control Flow Scoping (p.1550)
 -  CWE-754: Improper Check for Unusual or Exceptional Conditions (p.1577)
 -  CWE-252: Unchecked Return Value (p.613)
 -  CWE-690: Unchecked Return Value to NULL Pointer Dereference (p.1523)
 -  CWE-628: Function Call with Incorrectly Specified Arguments (p.1407)
 -  CWE-375: Returning a Mutable Object to an Untrusted Caller (p.930)
 -  CWE-597: Use of Wrong Operator in String Comparison (p.1345)
-  CWE-1182: SEI CERT Perl Coding Standard - Guidelines 04. Integers (INT) (p.2487)
 -  CWE-189: Numeric Errors (p.2333)
-  CWE-1183: SEI CERT Perl Coding Standard - Guidelines 05. Strings (STR) (p.2488)
-  CWE-1184: SEI CERT Perl Coding Standard - Guidelines 06. Object-Oriented Programming (OOP) (p.2488)
 -  CWE-767: Access to Critical Private Variable via Public Method (p.1619)
-  CWE-1185: SEI CERT Perl Coding Standard - Guidelines 07. File Input and Output (FIO) (p.2489)
 -  CWE-59: Improper Link Resolution Before File Access ('Link Following') (p.112)
-  CWE-1186: SEI CERT Perl Coding Standard - Guidelines 50. Miscellaneous (MSC) (p.2489)
 -  CWE-561: Dead Code (p.1283)
 -  CWE-563: Assignment to Variable without Use (p.1289)


























Graph View: CWE-1194: Hardware Design

- C** CWE-1195: Manufacturing and Life Cycle Management Concerns (p.2490)
 - G** CWE-1059: Insufficient Technical Documentation (p.1904)
 - B** CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications (p.2060)
 - B** CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device (p.2104)
 - B** CWE-1269: Product Released in Non-Release Configuration (p.2110)
 - B** CWE-1273: Device Unlock Credential Sharing (p.2119)
 - B** CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT Vendors (p.2168)
- C** CWE-1196: Security Flow Issues (p.2490)
 - B** CWE-1190: DMA Device Enabled Too Early in Boot Phase (p.1987)
 - B** CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control (p.1995)
 - B** CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels (p.2098)
 - B** CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code (p.2121)
 - B** CWE-1283: Mutable Attestation or Measurement Reporting Data (p.2140)
 - B** CWE-1310: Missing Ability to Patch ROM Code (p.2191)
 - B** CWE-1326: Missing Immutable Root of Trust in Hardware (p.2224)
 - B** CWE-1328: Security Version Number Mutable to Older Versions (p.2229)
- C** CWE-1197: Integration Issues (p.2491)
 - B** CWE-1276: Hardware Child Block Incorrectly Connected to Parent System (p.2125)
- C** CWE-1198: Privilege Separation and Access Control Issues (p.2491)
 - B** CWE-276: Incorrect Default Permissions (p.672)
 - G** CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') (p.1072)
 - B** CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) (p.1985)
 - B** CWE-1192: Improper Identifier for IP Block used in System-On-Chip (SOC) (p.1994)
 - B** CWE-1220: Insufficient Granularity of Access Control (p.2002)
 - V** CWE-1222: Insufficient Granularity of Address Regions Protected by Register Locks (p.2010)
 - B** CWE-1242: Inclusion of Undocumented Features or Chicken Bits (p.2044)
 - B** CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges (p.2087)
 - B** CWE-1262: Improper Access Control for Register Interface (p.2093)
 - B** CWE-1267: Policy Uses Obsolete Encoding (p.2105)
 - B** CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents (p.2107)
 - B** CWE-1280: Access Control Check Implemented After Asset is Accessed (p.2134)
 - G** CWE-1294: Insecure Security Identifier Mechanism (p.2162)
 - B** CWE-1259: Improper Restriction of Security Token Assignment (p.2085)
 - B** CWE-1270: Generation of Incorrect Security Tokens (p.2113)
 - B** CWE-1290: Incorrect Decoding of Security Identifiers (p.2155)
 - B** CWE-1292: Incorrect Conversion of Security Identifiers (p.2159)
 - B** CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface (p.2174)
 - B** CWE-1302: Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC) (p.2185)
 - B** CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
 - B** CWE-1314: Missing Write Protection for Parametric Data Values (p.2199)
 - B** CWE-1318: Missing Support for Security Features in On-chip Fabrics or Buses (p.2209)
 - B** CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy (p.2246)
 - B** CWE-1420: Exposure of Sensitive Information during Transient Execution (p.2297)
 - B** CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution (p.2304)
 - B** CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution (p.2310)
 - B** CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution (p.2316)
- C** CWE-1199: General Circuit and Logic Design Concerns (p.2492)
 - B** CWE-1209: Failure to Disable Reserved Bits (p.2000)
 - B** CWE-1221: Incorrect Register Defaults or Module Parameters (p.2005)

- B CWE-1223: Race Condition for Write-Once Attributes (p.2011)
- B CWE-1224: Improper Restriction of Write-Once Bit Fields (p.2014)
- B CWE-1231: Improper Prevention of Lock Bit Modification (p.2018)
- B CWE-1232: Improper Lock Behavior After Power State Transition (p.2021)
- B CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection (p.2023)
- B CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks (p.2026)
- B CWE-1245: Improper Finite State Machines (FSMs) in Hardware Logic (p.2052)
- B CWE-1250: Improper Preservation of Consistency Between Independent Representations of Shared State (p.2064)
- B CWE-1253: Incorrect Selection of Fuse Values (p.2069)
- B CWE-1254: Incorrect Comparison Logic Granularity (p.2071)
- B CWE-1261: Improper Handling of Single Event Upsets (p.2091)
- B CWE-1298: Hardware Logic Contains Race Conditions (p.2170)
- C CWE-1201: Core and Compute Issues (p.2492)
 - B CWE-1252: CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations (p.2068)
 - B CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior (p.2136)
 - B CWE-1342: Information Exposure through Microarchitectural State after Transient Execution (p.2262)
 - B CWE-1420: Exposure of Sensitive Information during Transient Execution (p.2297)
 - B CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution (p.2304)
 - B CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution (p.2310)
 - B CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution (p.2316)
- C CWE-1202: Memory and Storage Issues (p.2493)
 - B CWE-226: Sensitive Information in Resource Not Removed Before Reuse (p.569)
 - V CWE-1239: Improper Zeroization of Hardware Register (p.2033)
 - B CWE-1342: Information Exposure through Microarchitectural State after Transient Execution (p.2262)
 - B CWE-1246: Improper Write Handling in Limited-write Non-Volatile Memories (p.2054)
 - B CWE-1251: Mirrored Regions with Different Values (p.2065)
 - B CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions (p.2079)
 - B CWE-1282: Assumed-Immutable Data is Stored in Writable Memory (p.2139)
 - B CWE-1420: Exposure of Sensitive Information during Transient Execution (p.2297)
 - B CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution (p.2304)
 - B CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution (p.2310)
 - B CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution (p.2316)
- C CWE-1203: Peripherals, On-chip Fabric, and Interface/IO Problems (p.2493)
 - B CWE-1311: Improper Translation of Security Attributes by Fabric Bridge (p.2194)
 - B CWE-1312: Missing Protection for Mirrored Regions in On-Chip Fabric Firewall (p.2196)
 - B CWE-1315: Improper Setting of Bus Controlling Capability in Fabric End-point (p.2202)
 - B CWE-1316: Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges (p.2204)
 - B CWE-1317: Improper Access Control in Fabric Bridge (p.2206)
 - B CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) (p.2237)
- C CWE-1205: Security Primitives and Cryptography Issues (p.2494)
 - B CWE-203: Observable Discrepancy (p.525)
 - B CWE-1300: Improper Protection of Physical Side Channels (p.2177)
 - B CWE-325: Missing Cryptographic Step (p.801)
 - B CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation (p.2036)
 - B CWE-1241: Use of Predictable Algorithm in Random Number Generator (p.2042)
 - B CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready (p.2132)
 - B CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments (p.2265)

- C CWE-1206: Power, Clock, Thermal, and Reset Concerns (p.2494)
 - B CWE-1232: Improper Lock Behavior After Power State Transition (p.2021)
 - B CWE-1247: Improper Protection Against Voltage and Clock Glitches (p.2056)
 - B CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications (p.2060)
 - V CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks (p.2073)
 - B CWE-1256: Improper Restriction of Software Interfaces to Hardware Features (p.2076)
 - B CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings (p.2115)
 - B CWE-1304: Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation (p.2188)
 - B CWE-1314: Missing Write Protection for Parametric Data Values (p.2199)
 - B CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals (p.2214)
 - B CWE-1332: Improper Handling of Faults that Lead to Instruction Skips (p.2240)
 - B CWE-1338: Improper Protections Against Hardware Overheating (p.2252)
- C CWE-1207: Debug and Test Problems (p.2495)
 - B CWE-1191: On-Chip Debug and Test Interface With Improper Access Control (p.1989)
 - B CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks (p.2026)
 - B CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug (p.2046)
 - B CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State (p.2048)
 - B CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information (p.2082)
 - B CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition (p.2116)
 - B CWE-1291: Public Key Re-Use for Signing both Debug and Production Code (p.2157)
 - B CWE-1295: Debug Messages Revealing Unnecessary Information (p.2164)
 - B CWE-1296: Incorrect Chaining or Granularity of Debug Components (p.2166)
 - B CWE-1313: Hardware Allows Activation of Test or Debug Logic at Runtime (p.2198)
 - B CWE-1323: Improper Management of Sensitive Trace Data (p.2220)
 - B CWE-319: Cleartext Transmission of Sensitive Information (p.786)
- C CWE-1208: Cross-Cutting Problems (p.2495)
 - B CWE-440: Expected Behavior Violation (p.1069)
 - B CWE-1053: Missing Documentation for Design (p.1898)
 - C CWE-1059: Insufficient Technical Documentation (p.1904)
 - C CWE-1263: Improper Physical Access Control (p.2097)
 - B CWE-1277: Firmware Not Updateable (p.2128)
 - B CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component (p.2183)
 - V CWE-1330: Remanent Data Readable after Memory Erase (p.2234)
 - B CWE-1329: Reliance on Component That is Not Updateable (p.2231)
 - C CWE-1357: Reliance on Insufficiently Trustworthy Component (p.2266)
- C CWE-1388: Physical Access Issues and Concerns (p.2539)
 - C CWE-1384: Improper Handling of Physical or Environmental Conditions (p.2269)
 - B CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) (p.2212)
 - B CWE-1247: Improper Protection Against Voltage and Clock Glitches (p.2056)
 - B CWE-1261: Improper Handling of Single Event Upsets (p.2091)
 - B CWE-1332: Improper Handling of Faults that Lead to Instruction Skips (p.2240)
 - B CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments (p.2265)
 - B CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques (p.2131)
 - V CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks (p.2073)
 - B CWE-1300: Improper Protection of Physical Side Channels (p.2177)
 - B CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications (p.2060)

Graph View: CWE-1200: Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors

-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (*p.299*)
-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (*p.168*)
-  CWE-20: Improper Input Validation (*p.20*)
-  CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (*p.511*)
-  CWE-125: Out-of-bounds Read (*p.336*)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (*p.206*)
-  CWE-416: Use After Free (*p.1019*)
-  CWE-190: Integer Overflow or Wraparound (*p.478*)
-  CWE-352: Cross-Site Request Forgery (CSRF) (*p.875*)
-  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (*p.33*)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (*p.155*)
-  CWE-787: Out-of-bounds Write (*p.1669*)
-  CWE-287: Improper Authentication (*p.699*)
-  CWE-476: NULL Pointer Dereference (*p.1139*)
-  CWE-732: Incorrect Permission Assignment for Critical Resource (*p.1559*)
-  CWE-434: Unrestricted Upload of File with Dangerous Type (*p.1055*)
-  CWE-611: Improper Restriction of XML External Entity Reference (*p.1376*)
-  CWE-94: Improper Control of Generation of Code ('Code Injection') (*p.225*)
-  CWE-798: Use of Hard-coded Credentials (*p.1699*)
-  CWE-400: Uncontrolled Resource Consumption (*p.971*)
-  CWE-772: Missing Release of Resource after Effective Lifetime (*p.1632*)
-  CWE-426: Untrusted Search Path (*p.1035*)
-  CWE-502: Deserialization of Untrusted Data (*p.1212*)
-  CWE-269: Improper Privilege Management (*p.653*)
-  CWE-295: Improper Certificate Validation (*p.721*)

Graph View: CWE-1305: CISQ Quality Measures (2020)


























- CWE-1306: CISQ Quality Measures - Reliability (p.2504)
 - G CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
 - B CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
 - B CWE-123: Write-what-where Condition (p.329)
 - B CWE-125: Out-of-bounds Read (p.336)
 - B CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
 - B CWE-786: Access of Memory Location Before Start of Buffer (p.1666)
 - B CWE-787: Out-of-bounds Write (p.1669)
 - B CWE-788: Access of Memory Location After End of Buffer (p.1678)
 - B CWE-805: Buffer Access with Incorrect Length Value (p.1711)
 - B CWE-822: Untrusted Pointer Dereference (p.1732)
 - B CWE-823: Use of Out-of-range Pointer Offset (p.1735)
 - B CWE-824: Access of Uninitialized Pointer (p.1738)
 - B CWE-825: Expired Pointer Dereference (p.1741)
 - B CWE-170: Improper Null Termination (p.434)
 - B CWE-252: Unchecked Return Value (p.613)
 - B CWE-390: Detection of Error Condition Without Action (p.950)
 - B CWE-394: Unexpected Status Code or Return Value (p.962)
 - G CWE-404: Improper Resource Shutdown or Release (p.987)
 - V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
 - B CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
 - V CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
 - G CWE-424: Improper Protection of Alternate Path (p.1031)
 - B CWE-459: Incomplete Cleanup (p.1106)
 - B CWE-476: NULL Pointer Dereference (p.1139)
 - B CWE-480: Use of Incorrect Operator (p.1157)
 - B CWE-484: Omitted Break Statement in Switch (p.1169)
 - B CWE-562: Return of Stack Variable Address (p.1287)
 - V CWE-595: Comparison of Object References Instead of Object Contents (p.1342)
 - B CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element (p.1946)
 - V CWE-597: Use of Wrong Operator in String Comparison (p.1345)
 - G CWE-662: Improper Synchronization (p.1457)
 - B CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)
 - V CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)
 - B CWE-366: Race Condition within a Thread (p.910)
 - V CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context (p.1263)
 - B CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
 - G CWE-667: Improper Locking (p.1472)
 - B CWE-764: Multiple Locks of a Critical Resource (p.1613)
 - B CWE-820: Missing Synchronization (p.1729)
 - B CWE-821: Incorrect Synchronization (p.1731)
 - B CWE-833: Deadlock (p.1762)
 - G CWE-665: Improper Initialization (p.1465)
 - V CWE-456: Missing Initialization of a Variable (p.1096)
 - V CWE-457: Use of Uninitialized Variable (p.1102)
 - G CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 - V CWE-415: Double Free (p.1015)
 - V CWE-416: Use After Free (p.1019)
 - B CWE-681: Incorrect Conversion between Numeric Types (p.1504)
 - V CWE-194: Unexpected Sign Extension (p.498)
 - V CWE-195: Signed to Unsigned Conversion Error (p.501)

- V CWE-196: Unsigned to Signed Conversion Error (p.505)
- B CWE-197: Numeric Truncation Error (p.507)
- P| CWE-682: Incorrect Calculation (p.1507)
- B CWE-131: Incorrect Calculation of Buffer Size (p.361)
- B CWE-369: Divide By Zero (p.920)
- P| CWE-703: Improper Check or Handling of Exceptional Conditions (p.1544)
- B CWE-248: Uncaught Exception (p.603)
- B CWE-391: Unchecked Error Condition (p.955)
- B CWE-392: Missing Report of Error Condition (p.958)
- G CWE-704: Incorrect Type Conversion or Cast (p.1547)
- G CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p.1591)
- B CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') (p.1766)
- B CWE-908: Use of Uninitialized Resource (p.1802)
- B CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor (p.1889)
- B CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data (p.1896)
- B CWE-1066: Missing Serialization Control Element (p.1913)
- B CWE-1070: Serializable Data Element Containing non-Serializable Item Elements (p.1918)
- V CWE-1077: Floating Point Comparison with Incorrect Operator (p.1926)
- B CWE-1079: Parent Class without Virtual Destructor Method (p.1929)
- B CWE-1082: Class Instance Self Destruction Control Element (p.1931)
- B CWE-1083: Data Access from Outside Expected Data Manager Component (p.1932)
- B CWE-1087: Class with Virtual Method without a Virtual Destructor (p.1936)
- B CWE-1088: Synchronous Access of Remote Resource without Timeout (p.1937)
- B CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element (p.1947)
- C CWE-1307: CISQ Quality Measures - Maintainability (p.2505)
- G CWE-407: Inefficient Algorithmic Complexity (p.999)
- B CWE-478: Missing Default Case in Multiple Condition Expression (p.1149)
- B CWE-480: Use of Incorrect Operator (p.1157)
- B CWE-484: Omitted Break Statement in Switch (p.1169)
- B CWE-561: Dead Code (p.1283)
- B CWE-570: Expression is Always False (p.1300)
- B CWE-571: Expression is Always True (p.1303)
- B CWE-783: Operator Precedence Logic Error (p.1659)
- B CWE-1041: Use of Redundant Code (p.1884)
- B CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor (p.1889)
- B CWE-1047: Modules with Circular Dependencies (p.1891)
- B CWE-1048: Invokable Control Element with Large Number of Outward Calls (p.1892)
- B CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data (p.1896)
- B CWE-1052: Excessive Use of Hard-Coded Literals in Initialization (p.1897)
- B CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer (p.1899)
- B CWE-1055: Multiple Inheritance from Concrete Classes (p.1900)
- B CWE-1062: Parent Class with References to Child Class (p.1909)
- B CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters (p.1911)
- B CWE-1074: Class with Excessively Deep Inheritance (p.1923)
- B CWE-1075: Unconditional Control Flow Transfer outside of Switch Block (p.1924)
- B CWE-1079: Parent Class without Virtual Destructor Method (p.1929)
- B CWE-1080: Source Code File with Excessive Number of Lines of Code (p.1930)
- B CWE-1084: Invokable Control Element with Excessive File or Data Access Operations (p.1933)
- B CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code (p.1934)
- B CWE-1086: Class with Excessive Number of Child Classes (p.1935)
- B CWE-1087: Class with Virtual Method without a Virtual Destructor (p.1936)
- B CWE-1090: Method Containing Access of a Member Element from Another Class (p.1939)




















































- B CWE-1095: Loop Condition Value Update within the Loop (p.1944)
- C CWE-1308: CISQ Quality Measures - Security (p.2506)
- B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 - B CWE-23: Relative Path Traversal (p.46)
 - B CWE-36: Absolute Path Traversal (p.75)
- C CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
 - B CWE-624: Executable Regular Expression Error (p.1399)
 - B CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 - B CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
 - B CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
- B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
 - V CWE-564: SQL Injection: Hibernate (p.1290)
- B CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
- B CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
- C CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
- C CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
 - B CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
 - B CWE-123: Write-what-where Condition (p.329)
 - B CWE-125: Out-of-bounds Read (p.336)
 - B CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
 - B CWE-786: Access of Memory Location Before Start of Buffer (p.1666)
 - B CWE-787: Out-of-bounds Write (p.1669)
 - B CWE-788: Access of Memory Location After End of Buffer (p.1678)
 - B CWE-805: Buffer Access with Incorrect Length Value (p.1711)
 - B CWE-822: Untrusted Pointer Dereference (p.1732)
 - B CWE-823: Use of Out-of-range Pointer Offset (p.1735)
 - B CWE-824: Access of Uninitialized Pointer (p.1738)
 - B CWE-825: Expired Pointer Dereference (p.1741)
- V CWE-129: Improper Validation of Array Index (p.347)
- B CWE-134: Use of Externally-Controlled Format String (p.371)
- B CWE-252: Unchecked Return Value (p.613)
- C CWE-404: Improper Resource Shutdown or Release (p.987)
 - V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
 - B CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
 - V CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
- C CWE-424: Improper Protection of Alternate Path (p.1031)
- B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
- B CWE-477: Use of Obsolete Function (p.1146)
- B CWE-480: Use of Incorrect Operator (p.1157)
- B CWE-502: Deserialization of Untrusted Data (p.1212)
- B CWE-570: Expression is Always False (p.1300)
- B CWE-571: Expression is Always True (p.1303)
- B CWE-606: Unchecked Input for Loop Condition (p.1366)
- B CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
- B CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
- B CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)
- C CWE-662: Improper Synchronization (p.1457)
 - B CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)

- V CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)
- B CWE-366: Race Condition within a Thread (p.910)
- V CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context (p.1263)
- B CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
- G CWE-667: Improper Locking (p.1472)
- B CWE-764: Multiple Locks of a Critical Resource (p.1613)
- B CWE-820: Missing Synchronization (p.1729)
- B CWE-821: Incorrect Synchronization (p.1731)
- B CWE-833: Deadlock (p.1762)
- G CWE-665: Improper Initialization (p.1465)
- V CWE-456: Missing Initialization of a Variable (p.1096)
- V CWE-457: Use of Uninitialized Variable (p.1102)
- G CWE-672: Operation on a Resource after Expiration or Release (p.1488)
- V CWE-415: Double Free (p.1015)
- V CWE-416: Use After Free (p.1019)
- B CWE-681: Incorrect Conversion between Numeric Types (p.1504)
- V CWE-194: Unexpected Sign Extension (p.498)
- V CWE-195: Signed to Unsigned Conversion Error (p.501)
- V CWE-196: Unsigned to Signed Conversion Error (p.505)
- B CWE-197: Numeric Truncation Error (p.507)
- P CWE-682: Incorrect Calculation (p.1507)
- B CWE-131: Incorrect Calculation of Buffer Size (p.361)
- B CWE-369: Divide By Zero (p.920)
- G CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
- B CWE-778: Insufficient Logging (p.1647)
- B CWE-783: Operator Precedence Logic Error (p.1659)
- V CWE-789: Memory Allocation with Excessive Size Value (p.1683)
- B CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
- B CWE-798: Use of Hard-coded Credentials (p.1699)
- V CWE-259: Use of Hard-coded Password (p.630)
- V CWE-321: Use of Hard-coded Cryptographic Key (p.792)
- B CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') (p.1766)
- C CWE-1309: CISQ Quality Measures - Efficiency (p.2507)
- G CWE-404: Improper Resource Shutdown or Release (p.987)
- V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
- B CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
- V CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
- G CWE-424: Improper Protection of Alternate Path (p.1031)
- V CWE-1042: Static Member Data Element outside of a Singleton Class Element (p.1886)
- B CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements (p.1887)
- B CWE-1046: Creation of Immutable Text Using String Concatenation (p.1890)
- B CWE-1049: Excessive Data Query Operations in a Large Data Table (p.1894)
- B CWE-1050: Excessive Platform Resource Consumption within a Loop (p.1895)
- B CWE-1057: Data Access Operations Outside of Expected Data Manager Component (p.1902)
- B CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses (p.1906)
- B CWE-1067: Excessive Execution of Sequential Searches of Data Resource (p.1914)
- B CWE-1072: Data Resource Access without Use of Connection Pooling (p.1921)
- B CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses (p.1922)
- B CWE-1089: Large Data Table with Excessive Number of Indices (p.1938)
- B CWE-1091: Use of Object without Invoking Destructor Method (p.1940)
- B CWE-1094: Excessive Index Range Scan for a Data Resource (p.1943)

Graph View: CWE-1337: Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses



































-  CWE-787: Out-of-bounds Write (p.1669)
-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-20: Improper Input Validation (p.20)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
-  CWE-416: Use After Free (p.1019)
-  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
-  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
-  CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
-  CWE-306: Missing Authentication for Critical Function (p.748)
-  CWE-190: Integer Overflow or Wraparound (p.478)
-  CWE-502: Deserialization of Untrusted Data (p.1212)
-  CWE-287: Improper Authentication (p.699)
-  CWE-476: NULL Pointer Dereference (p.1139)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-862: Missing Authorization (p.1789)
-  CWE-276: Incorrect Default Permissions (p.672)
-  CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
-  CWE-522: Insufficiently Protected Credentials (p.1234)
-  CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
-  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
-  CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
-  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)

Graph View: CWE-1340: CISQ Data Protection Measures





















































-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
-  CWE-123: Write-what-where Condition (p.329)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
-  CWE-786: Access of Memory Location Before Start of Buffer (p.1666)
-  CWE-787: Out-of-bounds Write (p.1669)
-  CWE-788: Access of Memory Location After End of Buffer (p.1678)
-  CWE-805: Buffer Access with Incorrect Length Value (p.1711)
-  CWE-822: Untrusted Pointer Dereference (p.1732)
-  CWE-823: Use of Out-of-range Pointer Offset (p.1735)
-  CWE-824: Access of Uninitialized Pointer (p.1738)
-  CWE-825: Expired Pointer Dereference (p.1741)
-  CWE-672: Operation on a Resource after Expiration or Release (p.1488)
-  CWE-415: Double Free (p.1015)
-  CWE-416: Use After Free (p.1019)
-  CWE-665: Improper Initialization (p.1465)
-  CWE-456: Missing Initialization of a Variable (p.1096)
-  CWE-457: Use of Uninitialized Variable (p.1102)
-  CWE-404: Improper Resource Shutdown or Release (p.987)
-  CWE-761: Free of Pointer not at Start of Buffer (p.1601)
-  CWE-762: Mismatched Memory Management Routines (p.1605)
-  CWE-763: Release of Invalid Pointer or Reference (p.1608)
-  CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
-  CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
-  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
-  CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
-  CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)
-  CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
-  CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
-  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
-  CWE-624: Executable Regular Expression Error (p.1399)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
-  CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
-  CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
-  CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
-  CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data (p.1896)
-  CWE-424: Improper Protection of Alternate Path (p.1031)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-259: Use of Hard-coded Password (p.630)
-  CWE-321: Use of Hard-coded Cryptographic Key (p.792)
-  CWE-681: Incorrect Conversion between Numeric Types (p.1504)
-  CWE-194: Unexpected Sign Extension (p.498)
-  CWE-195: Signed to Unsigned Conversion Error (p.501)
-  CWE-196: Unsigned to Signed Conversion Error (p.505)
-  CWE-197: Numeric Truncation Error (p.507)
-  CWE-662: Improper Synchronization (p.1457)
-  CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)
-  CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)

- B CWE-366: Race Condition within a Thread (p.910)
- V CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context (p.1263)
- B CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
- C CWE-667: Improper Locking (p.1472)
- B CWE-764: Multiple Locks of a Critical Resource (p.1613)
- B CWE-820: Missing Synchronization (p.1729)
- B CWE-821: Incorrect Synchronization (p.1731)
- C CWE-704: Incorrect Type Conversion or Cast (p.1547)
- B CWE-562: Return of Stack Variable Address (p.1287)
- B CWE-170: Improper Null Termination (p.434)
- V CWE-129: Improper Validation of Array Index (p.347)
- B CWE-134: Use of Externally-Controlled Format String (p.371)
- B CWE-606: Unchecked Input for Loop Condition (p.1366)
- B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 - B CWE-23: Relative Path Traversal (p.46)
 - B CWE-36: Absolute Path Traversal (p.75)
- B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
- P CWE-703: Improper Check or Handling of Exceptional Conditions (p.1544)
 - B CWE-248: Uncaught Exception (p.603)
 - B CWE-391: Unchecked Error Condition (p.955)
 - B CWE-392: Missing Report of Error Condition (p.958)
- B CWE-908: Use of Uninitialized Resource (p.1802)
- P CWE-682: Incorrect Calculation (p.1507)
 - B CWE-131: Incorrect Calculation of Buffer Size (p.361)
 - B CWE-369: Divide By Zero (p.920)
- C CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
- B CWE-502: Deserialization of Untrusted Data (p.1212)
- B CWE-213: Exposure of Sensitive Information Due to Incompatible Policies (p.555)
- B CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes (p.1818)
- C CWE-311: Missing Encryption of Sensitive Data (p.764)
- B CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
- P CWE-284: Improper Access Control (p.687)
 - C CWE-285: Improper Authorization (p.691)
 - C CWE-287: Improper Authentication (p.699)
 - B CWE-288: Authentication Bypass Using an Alternate Path or Channel (p.707)
 - B CWE-639: Authorization Bypass Through User-Controlled Key (p.1415)
 - C CWE-862: Missing Authorization (p.1789)
 - C CWE-863: Incorrect Authorization (p.1796)

Graph View: CWE-1344: Weaknesses in OWASP Top Ten (2021)

-  CWE-1345: OWASP Top Ten 2021 Category A01:2021 - Broken Access Control (p.2508)
 -  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
 -  CWE-23: Relative Path Traversal (p.46)
 -  CWE-35: Path Traversal: '..'/'..'/' (p.73)
 -  CWE-59: Improper Link Resolution Before File Access ('Link Following') (p.112)
 -  CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
 -  CWE-201: Insertion of Sensitive Information Into Sent Data (p.521)
 -  CWE-219: Storage of File with Sensitive Data Under Web Root (p.560)
 -  CWE-264: Permissions, Privileges, and Access Controls (p.2337)
 -  CWE-275: Permission Issues (p.2339)
 -  CWE-276: Incorrect Default Permissions (p.672)
 -  CWE-284: Improper Access Control (p.687)
 -  CWE-285: Improper Authorization (p.691)
 -  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
 -  CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
 -  CWE-377: Insecure Temporary File (p.932)
 -  CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') (p.984)
 -  CWE-425: Direct Request ('Forced Browsing') (p.1032)
 -  CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') (p.1072)
 -  CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere (p.1201)
 -  CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory (p.1257)
 -  CWE-540: Inclusion of Sensitive Information in Source Code (p.1260)
 -  CWE-548: Exposure of Information Through Directory Listing (p.1269)
 -  CWE-552: Files or Directories Accessible to External Parties (p.1274)
 -  CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key (p.1294)
 -  CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (p.1353)
 -  CWE-639: Authorization Bypass Through User-Controlled Key (p.1415)
 -  CWE-651: Exposure of WSDL File Containing Sensitive Information (p.1442)
 -  CWE-668: Exposure of Resource to Wrong Sphere (p.1478)
 -  CWE-706: Use of Incorrectly-Resolved Name or Reference (p.1553)
 -  CWE-862: Missing Authorization (p.1789)
 -  CWE-863: Incorrect Authorization (p.1796)
 -  CWE-913: Improper Control of Dynamically-Managed Code Resources (p.1814)
 -  CWE-922: Insecure Storage of Sensitive Information (p.1835)
 -  CWE-1275: Sensitive Cookie with Improper SameSite Attribute (p.2123)
-  CWE-1346: OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures (p.2509)
 -  CWE-261: Weak Encoding for Password (p.638)
 -  CWE-296: Improper Following of a Certificate's Chain of Trust (p.726)
 -  CWE-310: Cryptographic Issues (p.2339)
 -  CWE-319: Cleartext Transmission of Sensitive Information (p.786)
 -  CWE-321: Use of Hard-coded Cryptographic Key (p.792)
 -  CWE-322: Key Exchange without Entity Authentication (p.795)
 -  CWE-323: Reusing a Nonce, Key Pair in Encryption (p.797)
 -  CWE-324: Use of a Key Past its Expiration Date (p.799)
 -  CWE-325: Missing Cryptographic Step (p.801)
 -  CWE-326: Inadequate Encryption Strength (p.803)
 -  CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 -  CWE-328: Use of Weak Hash (p.813)
 -  CWE-329: Generation of Predictable IV with CBC Mode (p.818)
 -  CWE-330: Use of Insufficiently Random Values (p.821)
 -  CWE-331: Insufficient Entropy (p.828)


























- B CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) (p.836)
- V CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) (p.839)
- V CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) (p.841)
- B CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (p.844)
- C CWE-340: Generation of Predictable Numbers or Identifiers (p.849)
- B CWE-347: Improper Verification of Cryptographic Signature (p.864)
- B CWE-523: Unprotected Transport of Credentials (p.1239)
- C CWE-720: OWASP Top Ten 2007 Category A9 - Insecure Communications (p.2354)
- B CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') (p.1589)
- V CWE-759: Use of a One-Way Hash without a Salt (p.1593)
- V CWE-760: Use of a One-Way Hash with a Predictable Salt (p.1598)
- V CWE-780: Use of RSA Algorithm without OAEP (p.1652)
- C CWE-818: OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection (p.2381)
- B CWE-916: Use of Password Hash With Insufficient Computational Effort (p.1822)
- C CWE-1347: OWASP Top Ten 2021 Category A03:2021 - Injection (p.2511)
- C CWE-20: Improper Input Validation (p.20)
- C CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (p.138)
- C CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) (p.145)
- C CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
- B CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
- B CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
- V CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) (p.182)
- V CWE-83: Improper Neutralization of Script in Attributes in a Web Page (p.188)
- V CWE-87: Improper Neutralization of Alternate XSS Syntax (p.196)
- B CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
- B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
- B CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
- B CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
- B CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') (p.222)
- B CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
- V CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (p.232)
- B CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') (p.238)
- V CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page (p.241)
- V CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') (p.242)
- C CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
- V CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') (p.277)
- C CWE-116: Improper Encoding or Escaping of Output (p.287)
- C CWE-138: Improper Neutralization of Special Elements (p.379)
- B CWE-184: Incomplete List of Disallowed Inputs (p.466)
- B CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (p.1125)
- B CWE-471: Modification of Assumed-Immutable Data (MAID) (p.1129)
- V CWE-564: SQL Injection: Hibernate (p.1290)
- C CWE-610: Externally Controlled Reference to a Resource in Another Sphere (p.1373)
- B CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
- V CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax (p.1430)
- B CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)

-  CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
-  CWE-1348: OWASP Top Ten 2021 Category A04:2021 - Insecure Design (p.2512)
 -  CWE-73: External Control of File Name or Path (p.133)
 -  CWE-183: Permissive List of Allowed Inputs (p.464)
 -  CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
 -  CWE-213: Exposure of Sensitive Information Due to Incompatible Policies (p.555)
 -  CWE-235: Improper Handling of Extra Parameters (p.585)
 -  CWE-256: Plaintext Storage of a Password (p.622)
 -  CWE-257: Storing Passwords in a Recoverable Format (p.625)
 -  CWE-266: Incorrect Privilege Assignment (p.645)
 -  CWE-269: Improper Privilege Management (p.653)
 -  CWE-280: Improper Handling of Insufficient Permissions or Privileges (p.679)
 -  CWE-311: Missing Encryption of Sensitive Data (p.764)
 -  CWE-312: Cleartext Storage of Sensitive Information (p.771)
 -  CWE-313: Cleartext Storage in a File or on Disk (p.777)
 -  CWE-316: Cleartext Storage of Sensitive Information in Memory (p.782)
 -  CWE-419: Unprotected Primary Channel (p.1024)
 -  CWE-430: Deployment of Wrong Handler (p.1049)
 -  CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
 -  CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') (p.1075)
 -  CWE-451: User Interface (UI) Misrepresentation of Critical Information (p.1087)
 -  CWE-472: External Control of Assumed-Immutable Web Parameter (p.1131)
 -  CWE-501: Trust Boundary Violation (p.1210)
 -  CWE-522: Insufficiently Protected Credentials (p.1234)
 -  CWE-525: Use of Web Browser Cache Containing Sensitive Information (p.1242)
 -  CWE-539: Use of Persistent Cookies Containing Sensitive Information (p.1259)
 -  CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session (p.1318)
 -  CWE-598: Use of GET Request Method With Sensitive Query Strings (p.1349)
 -  CWE-602: Client-Side Enforcement of Server-Side Security (p.1359)
 -  CWE-642: External Control of Critical State Data (p.1422)
 -  CWE-646: Reliance on File Name or Extension of Externally-Supplied File (p.1434)
 -  CWE-650: Trusting HTTP Permission Methods on the Server Side (p.1441)
 -  CWE-653: Improper Isolation or Compartmentalization (p.1445)
 -  CWE-656: Reliance on Security Through Obscurity (p.1452)
 -  CWE-657: Violation of Secure Design Principles (p.1454)
 -  CWE-799: Improper Control of Interaction Frequency (p.1708)
 -  CWE-807: Reliance on Untrusted Inputs in a Security Decision (p.1723)
 -  CWE-840: Business Logic Errors (p.2381)
 -  CWE-841: Improper Enforcement of Behavioral Workflow (p.1781)
 -  CWE-927: Use of Implicit Intent for Sensitive Communication (p.1846)
 -  CWE-1021: Improper Restriction of Rendered UI Layers or Frames (p.1869)
 -  CWE-1173: Improper Use of Validation Framework (p.1978)
 -  CWE-1349: OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration (p.2514)
 -  CWE-2: 7PK - Environment (p.2329)
 -  CWE-11: ASP.NET Misconfiguration: Creating Debug Binary (p.9)
 -  CWE-13: ASP.NET Misconfiguration: Password in Configuration File (p.13)
 -  CWE-15: External Control of System or Configuration Setting (p.17)
 -  CWE-16: Configuration (p.2330)
 -  CWE-260: Password in Configuration File (p.636)
 -  CWE-315: Cleartext Storage of Sensitive Information in a Cookie (p.781)
 -  CWE-520: .NET Misconfiguration: Use of Impersonation (p.1230)
 -  CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable (p.1243)

- V CWE-537: Java Runtime Error Message Containing Sensitive Information (p.1255)
- V CWE-541: Inclusion of Sensitive Information in an Include File (p.1262)
- B CWE-547: Use of Hard-coded, Security-relevant Constants (p.1267)
- B CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
- V CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute (p.1382)
- B CWE-756: Missing Custom Error Page (p.1588)
- B CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') (p.1642)
- V CWE-942: Permissive Cross-domain Policy with Untrusted Domains (p.1857)
- V CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag (p.1863)
- C CWE-1032: OWASP Top Ten 2017 Category A6 - Security Misconfiguration (p.2459)
- V CWE-1174: ASP.NET Misconfiguration: Improper Model Validation (p.1979)
- C CWE-1352: OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components (p.2515)
- C CWE-937: OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities (p.2413)
- C CWE-1035: OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities (p.2460)
- B CWE-1104: Use of Unmaintained Third Party Components (p.1953)
- C CWE-1353: OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures (p.2515)
- C CWE-255: Credentials Management Errors (p.2336)
- V CWE-259: Use of Hard-coded Password (p.630)
- C CWE-287: Improper Authentication (p.699)
- B CWE-288: Authentication Bypass Using an Alternate Path or Channel (p.707)
- B CWE-290: Authentication Bypass by Spoofing (p.712)
- B CWE-294: Authentication Bypass by Capture-replay (p.719)
- B CWE-295: Improper Certificate Validation (p.721)
- V CWE-297: Improper Validation of Certificate with Host Mismatch (p.729)
- C CWE-300: Channel Accessible by Non-Endpoint (p.737)
- B CWE-302: Authentication Bypass by Assumed-Immutable Data (p.742)
- B CWE-304: Missing Critical Step in Authentication (p.745)
- B CWE-306: Missing Authentication for Critical Function (p.748)
- B CWE-307: Improper Restriction of Excessive Authentication Attempts (p.754)
- C CWE-346: Origin Validation Error (p.860)
- B CWE-384: Session Fixation (p.943)
- B CWE-521: Weak Password Requirements (p.1231)
- B CWE-613: Insufficient Session Expiration (p.1380)
- B CWE-620: Unverified Password Change (p.1392)
- B CWE-640: Weak Password Recovery Mechanism for Forgotten Password (p.1418)
- B CWE-798: Use of Hard-coded Credentials (p.1699)
- B CWE-940: Improper Verification of Source of a Communication Channel (p.1852)
- C CWE-1216: Lockout Mechanism Errors (p.2499)
- C CWE-1354: OWASP Top Ten 2021 Category A08:2021 - Software and Data Integrity Failures (p.2516)
- C CWE-345: Insufficient Verification of Data Authenticity (p.858)
- B CWE-353: Missing Support for Integrity Check (p.881)
- B CWE-426: Untrusted Search Path (p.1035)
- B CWE-494: Download of Code Without Integrity Check (p.1192)
- B CWE-502: Deserialization of Untrusted Data (p.1212)
- B CWE-565: Reliance on Cookies without Validation and Integrity Checking (p.1292)
- V CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision (p.1662)
- B CWE-829: Inclusion of Functionality from Untrusted Control Sphere (p.1750)
- V CWE-830: Inclusion of Web Functionality from an Untrusted Source (p.1756)
- B CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes (p.1818)
- C CWE-1355: OWASP Top Ten 2021 Category A09:2021 - Security Logging and Monitoring Failures (p.2517)
- B CWE-117: Improper Output Neutralization for Logs (p.294)

- B CWE-223: Omission of Security-relevant Information (p.566)
- B CWE-532: Insertion of Sensitive Information into Log File (p.1250)
- B CWE-778: Insufficient Logging (p.1647)
- C CWE-1356: OWASP Top Ten 2021 Category A10:2021 - Server-Side Request Forgery (SSRF) (p.2518)
- B CWE-918: Server-Side Request Forgery (SSRF) (p.1829)

Graph View: CWE-1350: Weaknesses in the 2020 CWE Top 25 Most Dangerous Software Weaknesses

-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
-  CWE-787: Out-of-bounds Write (p.1669)
-  CWE-20: Improper Input Validation (p.20)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
-  CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
-  CWE-416: Use After Free (p.1019)
-  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
-  CWE-190: Integer Overflow or Wraparound (p.478)
-  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
-  CWE-476: NULL Pointer Dereference (p.1139)
-  CWE-287: Improper Authentication (p.699)
-  CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
-  CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
-  CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
-  CWE-522: Insufficiently Protected Credentials (p.1234)
-  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-502: Deserialization of Untrusted Data (p.1212)
-  CWE-269: Improper Privilege Management (p.653)
-  CWE-400: Uncontrolled Resource Consumption (p.971)
-  CWE-306: Missing Authentication for Critical Function (p.748)
-  CWE-862: Missing Authorization (p.1789)


























Appendix A - Graph Views: CWE-1358: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS

CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) (p.841)



















- B CWE-341: Predictable from Observable State (p.850)
- B CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data (p.868)
- B CWE-358: Improperly Implemented Security Check for Standard (p.888)
- C CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
- C CWE-377: Insecure Temporary File (p.932)
- B CWE-384: Session Fixation (p.943)
- B CWE-648: Incorrect Use of Privileged APIs (p.1437)
- B CWE-787: Out-of-bounds Write (p.1669)
- B CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) (p.1985)
- B CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
- B CWE-1393: Use of Default Password (p.2286)
- C CWE-1360: ICS Dependencies (& Architecture) (p.2519)
 - C CWE-1367: ICS Dependencies (& Architecture): External Physical Systems (p.2525)
 - B CWE-1247: Improper Protection Against Voltage and Clock Glitches (p.2056)
 - B CWE-1338: Improper Protections Against Hardware Overheating (p.2252)
 - C CWE-1357: Reliance on Insufficiently Trustworthy Component (p.2266)
 - C CWE-1384: Improper Handling of Physical or Environmental Conditions (p.2269)
 - C CWE-1368: ICS Dependencies (& Architecture): External Digital Systems (p.2526)
 - B CWE-15: External Control of System or Configuration Setting (p.17)
 - C CWE-287: Improper Authentication (p.699)
 - B CWE-306: Missing Authentication for Critical Function (p.748)
 - B CWE-308: Use of Single-factor Authentication (p.759)
 - B CWE-312: Cleartext Storage of Sensitive Information (p.771)
 - B CWE-440: Expected Behavior Violation (p.1069)
 - B CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (p.1125)
 - B CWE-603: Use of Client-Side Authentication (p.1363)
 - C CWE-610: Externally Controlled Reference to a Resource in Another Sphere (p.1373)
 - C CWE-638: Not Using Complete Mediation (p.1413)
 - C CWE-1059: Insufficient Technical Documentation (p.1904)
 - B CWE-1068: Inconsistency Between Implementation and Documented Design (p.1915)
 - B CWE-1104: Use of Unmaintained Third Party Components (p.1953)
 - B CWE-1329: Reliance on Component That is Not Updateable (p.2231)
 - C CWE-1357: Reliance on Insufficiently Trustworthy Component (p.2266)
 - B CWE-1393: Use of Default Password (p.2286)
- C CWE-1361: ICS Supply Chain (p.2520)
 - C CWE-1369: ICS Supply Chain: IT/OT Convergence/Expansion (p.2527)
 - C CWE-636: Not Failing Securely ('Failing Open') (p.1409)
 - P CWE-284: Improper Access Control (p.687)
 - C CWE-1370: ICS Supply Chain: Common Mode Frailties (p.2528)
 - P CWE-664: Improper Control of a Resource Through its Lifetime (p.1463)
 - P CWE-707: Improper Neutralization (p.1554)
 - P CWE-710: Improper Adherence to Coding Standards (p.1558)
 - C CWE-1357: Reliance on Insufficiently Trustworthy Component (p.2266)
 - V CWE-329: Generation of Predictable IV with CBC Mode (p.818)
 - P CWE-693: Protection Mechanism Failure (p.1529)
 - C CWE-1371: ICS Supply Chain: Poorly Documented or Undocumented Features (p.2529)
 - B CWE-489: Active Debug Code (p.1178)
 - C CWE-912: Hidden Functionality (p.1812)
 - C CWE-1059: Insufficient Technical Documentation (p.1904)
 - B CWE-1242: Inclusion of Undocumented Features or Chicken Bits (p.2044)
 - C CWE-1372: ICS Supply Chain: OT Counterfeit and Malicious Corruption (p.2530)
 - B CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques (p.2131)


- C CWE-1198: Privilege Separation and Access Control Issues (p.2491)
- B CWE-1231: Improper Prevention of Lock Bit Modification (p.2018)
- B CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection (p.2023)
- P CWE-284: Improper Access Control (p.687)
- C CWE-1362: ICS Engineering (Constructions/Deployment) (p.2520)
- C CWE-1373: ICS Engineering (Construction/Deployment): Trust Model Problems (p.2531)
 - G CWE-269: Improper Privilege Management (p.653)
 - B CWE-807: Reliance on Untrusted Inputs in a Security Decision (p.1723)
 - B CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data (p.868)
- C CWE-1374: ICS Engineering (Construction/Deployment): Maker Breaker Blindness (p.2531)
- C CWE-1375: ICS Engineering (Construction/Deployment): Gaps in Details/Data (p.2532)
 - G CWE-1059: Insufficient Technical Documentation (p.1904)
 - B CWE-1110: Incomplete Design Documentation (p.1959)
 - P CWE-710: Improper Adherence to Coding Standards (p.1558)
 - B CWE-1053: Missing Documentation for Design (p.1898)
 - B CWE-1111: Incomplete I/O Documentation (p.1960)
- C CWE-1376: ICS Engineering (Construction/Deployment): Security Gaps in Commissioning (p.2533)
 - B CWE-276: Incorrect Default Permissions (p.672)
 - G CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
 - B CWE-1393: Use of Default Password (p.2286)
- C CWE-1377: ICS Engineering (Construction/Deployment): Inherent Predictability in Design (p.2534)
 - B CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques (p.2131)
- C CWE-1363: ICS Operations (& Maintenance) (p.2521)
 - C CWE-1378: ICS Operations (& Maintenance): Gaps in obligations and training (p.2534)
 - C CWE-1379: ICS Operations (& Maintenance): Human factors in ICS environments (p.2535)
 - G CWE-655: Insufficient Psychological Acceptability (p.1450)
 - G CWE-451: User Interface (UI) Misrepresentation of Critical Information (p.1087)
 - C CWE-1380: ICS Operations (& Maintenance): Post-analysis changes (p.2536)
 - C CWE-1381: ICS Operations (& Maintenance): Exploitable Standard Operational Procedures (p.2537)
 - C CWE-1382: ICS Operations (& Maintenance): Emerging Energy Technologies (p.2538)
 - G CWE-20: Improper Input Validation (p.20)
 - G CWE-285: Improper Authorization (p.691)
 - B CWE-295: Improper Certificate Validation (p.721)
 - B CWE-296: Improper Following of a Certificate's Chain of Trust (p.726)
 - G CWE-346: Origin Validation Error (p.860)
 - G CWE-406: Insufficient Control of Network Message Volume (Network Amplification) (p.997)
 - B CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (p.1353)
 - C CWE-1383: ICS Operations (& Maintenance): Compliance/Conformance with Regulatory Requirements (p.2538)
 - P CWE-710: Improper Adherence to Coding Standards (p.1558)

Graph View: CWE-1387: Weaknesses in the 2022 CWE Top 25 Most Dangerous Software Weaknesses

-  CWE-787: Out-of-bounds Write (p.1669)
-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
-  CWE-20: Improper Input Validation (p.20)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
-  CWE-416: Use After Free (p.1019)
-  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
-  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
-  CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
-  CWE-476: NULL Pointer Dereference (p.1139)
-  CWE-502: Deserialization of Untrusted Data (p.1212)
-  CWE-190: Integer Overflow or Wraparound (p.478)
-  CWE-287: Improper Authentication (p.699)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-862: Missing Authorization (p.1789)
-  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
-  CWE-306: Missing Authentication for Critical Function (p.748)
-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-276: Incorrect Default Permissions (p.672)
-  CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
-  CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
-  CWE-400: Uncontrolled Resource Consumption (p.971)
-  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
-  CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)


Graph View: CWE-1400: Comprehensive Categorization for Software Assurance Trends

-  CWE-1396: Comprehensive Categorization: Access Control (p.2540)
 -  CWE-9: J2EE Misconfiguration: Weak Access Permissions for EJB Methods (p.8)
 -  CWE-13: ASP.NET Misconfiguration: Password in Configuration File (p.13)
 -  CWE-202: Exposure of Sensitive Information Through Data Queries (p.523)
 -  CWE-256: Plaintext Storage of a Password (p.622)
 -  CWE-257: Storing Passwords in a Recoverable Format (p.625)
 -  CWE-258: Empty Password in Configuration File (p.628)
 -  CWE-259: Use of Hard-coded Password (p.630)
 -  CWE-260: Password in Configuration File (p.636)
 -  CWE-261: Weak Encoding for Password (p.638)
 -  CWE-262: Not Using Password Aging (p.640)
 -  CWE-263: Password Aging with Long Expiration (p.643)
 -  CWE-266: Incorrect Privilege Assignment (p.645)
 -  CWE-267: Privilege Defined With Unsafe Actions (p.648)
 -  CWE-268: Privilege Chaining (p.651)
 -  CWE-269: Improper Privilege Management (p.653)
 -  CWE-270: Privilege Context Switching Error (p.659)
 -  CWE-271: Privilege Dropping / Lowering Errors (p.660)
 -  CWE-272: Least Privilege Violation (p.663)
 -  CWE-273: Improper Check for Dropped Privileges (p.667)
 -  CWE-274: Improper Handling of Insufficient Privileges (p.670)
 -  CWE-276: Incorrect Default Permissions (p.672)
 -  CWE-277: Insecure Inherited Permissions (p.675)
 -  CWE-278: Insecure Preserved Inherited Permissions (p.676)
 -  CWE-279: Incorrect Execution-Assigned Permissions (p.678)
 -  CWE-280: Improper Handling of Insufficient Permissions or Privileges (p.679)
 -  CWE-281: Improper Preservation of Permissions (p.681)
 -  CWE-282: Improper Ownership Management (p.683)
 -  CWE-283: Unverified Ownership (p.685)
 -  CWE-284: Improper Access Control (p.687)
 -  CWE-285: Improper Authorization (p.691)
 -  CWE-286: Incorrect User Management (p.698)
 -  CWE-287: Improper Authentication (p.699)
 -  CWE-288: Authentication Bypass Using an Alternate Path or Channel (p.707)
 -  CWE-289: Authentication Bypass by Alternate Name (p.710)
 -  CWE-290: Authentication Bypass by Spoofing (p.712)
 -  CWE-291: Reliance on IP Address for Authentication (p.715)
 -  CWE-293: Using Referer Field for Authentication (p.717)
 -  CWE-294: Authentication Bypass by Capture-replay (p.719)
 -  CWE-295: Improper Certificate Validation (p.721)
 -  CWE-296: Improper Following of a Certificate's Chain of Trust (p.726)
 -  CWE-297: Improper Validation of Certificate with Host Mismatch (p.729)
 -  CWE-298: Improper Validation of Certificate Expiration (p.733)
 -  CWE-299: Improper Check for Certificate Revocation (p.734)
 -  CWE-300: Channel Accessible by Non-Endpoint (p.737)
 -  CWE-301: Reflection Attack in an Authentication Protocol (p.740)
 -  CWE-302: Authentication Bypass by Assumed-Immutable Data (p.742)
 -  CWE-303: Incorrect Implementation of Authentication Algorithm (p.744)
 -  CWE-304: Missing Critical Step in Authentication (p.745)
 -  CWE-305: Authentication Bypass by Primary Weakness (p.747)














































-  CWE-306: Missing Authentication for Critical Function (p.748)
-  CWE-307: Improper Restriction of Excessive Authentication Attempts (p.754)
-  CWE-308: Use of Single-factor Authentication (p.759)
-  CWE-309: Use of Password System for Primary Authentication (p.761)
-  CWE-321: Use of Hard-coded Cryptographic Key (p.792)
-  CWE-322: Key Exchange without Entity Authentication (p.795)
-  CWE-350: Reliance on Reverse DNS Resolution for a Security-Critical Action (p.870)
-  CWE-370: Missing Check for Certificate Revocation after Initial Check (p.924)
-  CWE-384: Session Fixation (p.943)
-  CWE-419: Unprotected Primary Channel (p.1024)
-  CWE-420: Unprotected Alternate Channel (p.1025)
-  CWE-421: Race Condition During Access to Alternate Channel (p.1028)
-  CWE-422: Unprotected Windows Messaging Channel ('Shatter') (p.1029)
-  CWE-425: Direct Request ('Forced Browsing') (p.1032)
-  CWE-441: Unintended Proxy or Intermediary ('Confused Deputy') (p.1072)
-  CWE-520: .NET Misconfiguration: Use of Impersonation (p.1230)
-  CWE-521: Weak Password Requirements (p.1231)
-  CWE-522: Insufficiently Protected Credentials (p.1234)
-  CWE-523: Unprotected Transport of Credentials (p.1239)
-  CWE-549: Missing Password Field Masking (p.1271)
-  CWE-551: Incorrect Behavior Order: Authorization Before Parsing and Canonicalization (p.1273)
-  CWE-555: J2EE Misconfiguration: Plaintext Password in Configuration File (p.1279)
-  CWE-556: ASP.NET Misconfiguration: Use of Identity Impersonation (p.1280)
-  CWE-566: Authorization Bypass Through User-Controlled SQL Primary Key (p.1294)
-  CWE-593: Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created (p.1339)
-  CWE-599: Missing Validation of OpenSSL Certificate (p.1350)
-  CWE-601: URL Redirection to Untrusted Site ('Open Redirect') (p.1353)
-  CWE-603: Use of Client-Side Authentication (p.1363)
-  CWE-611: Improper Restriction of XML External Entity Reference (p.1376)
-  CWE-612: Improper Authorization of Index Containing Sensitive Information (p.1379)
-  CWE-613: Insufficient Session Expiration (p.1380)
-  CWE-620: Unverified Password Change (p.1392)
-  CWE-623: Unsafe ActiveX Control Marked Safe For Scripting (p.1397)
-  CWE-639: Authorization Bypass Through User-Controlled Key (p.1415)
-  CWE-640: Weak Password Recovery Mechanism for Forgotten Password (p.1418)
-  CWE-645: Overly Restrictive Account Lockout Mechanism (p.1432)
-  CWE-647: Use of Non-Canonical URL Paths for Authorization Decisions (p.1435)
-  CWE-648: Incorrect Use of Privileged APIs (p.1437)
-  CWE-708: Incorrect Ownership Assignment (p.1556)
-  CWE-732: Incorrect Permission Assignment for Critical Resource (p.1559)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-804: Guessable CAPTCHA (p.1710)
-  CWE-836: Use of Password Hash Instead of Password for Authentication (p.1770)
-  CWE-842: Placement of User into Incorrect Group (p.1784)
-  CWE-862: Missing Authorization (p.1789)
-  CWE-863: Incorrect Authorization (p.1796)
-  CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
-  CWE-921: Storage of Sensitive Data in a Mechanism without Access Control (p.1834)
-  CWE-923: Improper Restriction of Communication Channel to Intended Endpoints (p.1836)
-  CWE-925: Improper Verification of Intent by Broadcast Receiver (p.1841)
-  CWE-926: Improper Export of Android Application Components (p.1843)
-  CWE-927: Use of Implicit Intent for Sensitive Communication (p.1846)
-  CWE-939: Improper Authorization in Handler for Custom URL Scheme (p.1849)

-  CWE-940: Improper Verification of Source of a Communication Channel (p.1852)
-  CWE-941: Incorrectly Specified Destination in a Communication Channel (p.1855)
-  CWE-942: Permissive Cross-domain Policy with Untrusted Domains (p.1857)
-  CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag (p.1863)
-  CWE-1021: Improper Restriction of Rendered UI Layers or Frames (p.1869)
-  CWE-1022: Use of Web Link to Untrusted Target with window.opener Access (p.1872)
-  CWE-1191: On-Chip Debug and Test Interface With Improper Access Control (p.1989)
-  CWE-1220: Insufficient Granularity of Access Control (p.2002)
-  CWE-1222: Insufficient Granularity of Address Regions Protected by Register Locks (p.2010)
-  CWE-1224: Improper Restriction of Write-Once Bit Fields (p.2014)
-  CWE-1230: Exposure of Sensitive Information Through Metadata (p.2017)
-  CWE-1231: Improper Prevention of Lock Bit Modification (p.2018)
-  CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection (p.2023)
-  CWE-1242: Inclusion of Undocumented Features or Chicken Bits (p.2044)
-  CWE-1243: Sensitive Non-Volatile Information Not Protected During Debug (p.2046)
-  CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State (p.2048)
-  CWE-1252: CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations (p.2068)
-  CWE-1256: Improper Restriction of Software Interfaces to Hardware Features (p.2076)
-  CWE-1257: Improper Access Control Applied to Mirrored or Aliased Memory Regions (p.2079)
-  CWE-1259: Improper Restriction of Security Token Assignment (p.2085)
-  CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges (p.2087)
-  CWE-1262: Improper Access Control for Register Interface (p.2093)
-  CWE-1263: Improper Physical Access Control (p.2097)
-  CWE-1267: Policy Uses Obsolete Encoding (p.2105)
-  CWE-1268: Policy Privileges are not Assigned Consistently Between Control and Data Agents (p.2107)
-  CWE-1270: Generation of Incorrect Security Tokens (p.2113)
-  CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code (p.2121)
-  CWE-1275: Sensitive Cookie with Improper SameSite Attribute (p.2123)
-  CWE-1276: Hardware Child Block Incorrectly Connected to Parent System (p.2125)
-  CWE-1283: Mutable Attestation or Measurement Reporting Data (p.2140)
-  CWE-1290: Incorrect Decoding of Security Identifiers (p.2155)
-  CWE-1292: Incorrect Conversion of Security Identifiers (p.2159)
-  CWE-1294: Insecure Security Identifier Mechanism (p.2162)
-  CWE-1296: Incorrect Chaining or Granularity of Debug Components (p.2166)
-  CWE-1297: Unprotected Confidential Information on Device is Accessible by OSAT Vendors (p.2168)
-  CWE-1299: Missing Protection Mechanism for Alternate Hardware Interface (p.2174)
-  CWE-1302: Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC) (p.2185)
-  CWE-1304: Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation (p.2188)
-  CWE-1311: Improper Translation of Security Attributes by Fabric Bridge (p.2194)
-  CWE-1312: Missing Protection for Mirrored Regions in On-Chip Fabric Firewall (p.2196)
-  CWE-1313: Hardware Allows Activation of Test or Debug Logic at Runtime (p.2198)
-  CWE-1314: Missing Write Protection for Parametric Data Values (p.2199)
-  CWE-1315: Improper Setting of Bus Controlling Capability in Fabric End-point (p.2202)
-  CWE-1316: Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges (p.2204)
-  CWE-1317: Improper Access Control in Fabric Bridge (p.2206)
-  CWE-1320: Improper Protection for Outbound Error Messages and Alert Signals (p.2214)
-  CWE-1323: Improper Management of Sensitive Trace Data (p.2220)
-  CWE-1328: Security Version Number Mutable to Older Versions (p.2229)
-  CWE-1334: Unauthorized Error Injection Can Degrade Hardware Redundancy (p.2246)
-  CWE-1390: Weak Authentication (p.2279)

- C CWE-1391: Use of Weak Credentials (p.2281)
- B CWE-1392: Use of Default Credentials (p.2284)
- B CWE-1393: Use of Default Password (p.2286)
- B CWE-1394: Use of Default Cryptographic Key (p.2288)
- C CWE-1397: Comprehensive Categorization: Comparison (p.2544)
- B CWE-183: Permissive List of Allowed Inputs (p.464)
- C CWE-185: Incorrect Regular Expression (p.469)
- B CWE-186: Overly Restrictive Regular Expression (p.472)
- V CWE-187: Partial String Comparison (p.474)
- B CWE-478: Missing Default Case in Multiple Condition Expression (p.1149)
- V CWE-486: Comparison of Classes by Name (p.1172)
- V CWE-595: Comparison of Object References Instead of Object Contents (p.1342)
- V CWE-597: Use of Wrong Operator in String Comparison (p.1345)
- B CWE-625: Permissive Regular Expression (p.1400)
- P CWE-697: Incorrect Comparison (p.1538)
- V CWE-777: Regular Expression without Anchors (p.1645)
- B CWE-839: Numeric Range Comparison Without Minimum Check (p.1776)
- C CWE-1023: Incomplete Comparison with Missing Factors (p.1874)
- B CWE-1024: Comparison of Incompatible Types (p.1877)
- B CWE-1025: Comparison Using Wrong Factors (p.1878)
- V CWE-1077: Floating Point Comparison with Incorrect Operator (p.1926)
- C CWE-1398: Comprehensive Categorization: Component Interaction (p.2545)
- V CWE-14: Compiler Removal of Code to Clear Buffers (p.14)
- B CWE-115: Misinterpretation of Input (p.286)
- P CWE-435: Improper Interaction Between Multiple Correctly-Behaving Entities (p.1063)
- C CWE-436: Interpretation Conflict (p.1065)
- B CWE-437: Incomplete Model of Endpoint Features (p.1067)
- B CWE-439: Behavioral Change in New Version or Environment (p.1068)
- B CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') (p.1075)
- V CWE-650: Trusting HTTP Permission Methods on the Server Side (p.1441)
- B CWE-733: Compiler Optimization Removal or Modification of Security-critical Code (p.1570)
- B CWE-1037: Processor Optimization Removal or Modification of Security-critical Code (p.1879)
- C CWE-1038: Insecure Automated Optimizations (p.1881)
- C CWE-1401: Comprehensive Categorization: Concurrency (p.2547)
- C CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
- B CWE-363: Race Condition Enabling Link Following (p.904)
- B CWE-364: Signal Handler Race Condition (p.905)
- B CWE-366: Race Condition within a Thread (p.910)
- B CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition (p.913)
- B CWE-368: Context Switching Race Condition (p.918)
- B CWE-412: Unrestricted Externally Accessible Lock (p.1007)
- B CWE-413: Improper Resource Locking (p.1010)
- B CWE-414: Missing Lock Check (p.1014)
- B CWE-432: Dangerous Signal Handler not Disabled During Sensitive Operations (p.1052)
- V CWE-479: Signal Handler Use of a Non-reentrant Function (p.1154)
- V CWE-543: Use of Singleton Pattern Without Synchronization in a Multithreaded Context (p.1263)
- V CWE-558: Use of getlogin() in Multithreaded Application (p.1281)
- B CWE-567: Unsynchronized Access to Shared Data in a Multithreaded Context (p.1296)
- V CWE-572: Call to Thread run() instead of start() (p.1305)
- V CWE-574: EJB Bad Practices: Use of Synchronization Primitives (p.1308)
- V CWE-591: Sensitive Data Storage in Improperly Locked Memory (p.1338)
- B CWE-609: Double-Checked Locking (p.1371)

-  CWE-663: Use of a Non-reentrant Function in a Concurrent Context (p.1461)
-  CWE-667: Improper Locking (p.1472)
-  CWE-689: Permission Race Condition During Resource Copy (p.1521)
-  CWE-764: Multiple Locks of a Critical Resource (p.1613)
-  CWE-765: Multiple Unlocks of a Critical Resource (p.1614)
-  CWE-820: Missing Synchronization (p.1729)
-  CWE-821: Incorrect Synchronization (p.1731)
-  CWE-828: Signal Handler with Functionality that is not Asynchronous-Safe (p.1746)
-  CWE-831: Signal Handler Function Associated with Multiple Signals (p.1758)
-  CWE-832: Unlock of a Resource that is not Locked (p.1761)
-  CWE-833: Deadlock (p.1762)
-  CWE-1058: Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element (p.1903)
-  CWE-1088: Synchronous Access of Remote Resource without Timeout (p.1937)
-  CWE-1096: Singleton Class Instance Creation without Proper Locking or Synchronization (p.1945)
-  CWE-1223: Race Condition for Write-Once Attributes (p.2011)
-  CWE-1232: Improper Lock Behavior After Power State Transition (p.2021)
-  CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks (p.2026)
-  CWE-1264: Hardware Logic with Insecure De-Synchronization between Control and Data Channels (p.2098)
-  CWE-1298: Hardware Logic Contains Race Conditions (p.2170)
-  CWE-1402: Comprehensive Categorization: Encryption (p.2548)
 -  CWE-5: J2EE Misconfiguration: Data Transmission Without Encryption (p.1)
 -  CWE-311: Missing Encryption of Sensitive Data (p.764)
 -  CWE-312: Cleartext Storage of Sensitive Information (p.771)
 -  CWE-313: Cleartext Storage in a File or on Disk (p.777)
 -  CWE-314: Cleartext Storage in the Registry (p.779)
 -  CWE-315: Cleartext Storage of Sensitive Information in a Cookie (p.781)
 -  CWE-316: Cleartext Storage of Sensitive Information in Memory (p.782)
 -  CWE-317: Cleartext Storage of Sensitive Information in GUI (p.784)
 -  CWE-318: Cleartext Storage of Sensitive Information in Executable (p.785)
 -  CWE-319: Cleartext Transmission of Sensitive Information (p.786)
 -  CWE-324: Use of a Key Past its Expiration Date (p.799)
 -  CWE-325: Missing Cryptographic Step (p.801)
 -  CWE-326: Inadequate Encryption Strength (p.803)
 -  CWE-327: Use of a Broken or Risky Cryptographic Algorithm (p.806)
 -  CWE-328: Use of Weak Hash (p.813)
 -  CWE-347: Improper Verification of Cryptographic Signature (p.864)
 -  CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute (p.1382)
 -  CWE-759: Use of a One-Way Hash without a Salt (p.1593)
 -  CWE-760: Use of a One-Way Hash with a Predictable Salt (p.1598)
 -  CWE-780: Use of RSA Algorithm without OAEP (p.1652)
 -  CWE-916: Use of Password Hash With Insufficient Computational Effort (p.1822)
 -  CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation (p.2036)
-  CWE-1403: Comprehensive Categorization: Exposed Resource (p.2549)
 -  CWE-8: J2EE Misconfiguration: Entity Bean Declared Remote (p.6)
 -  CWE-15: External Control of System or Configuration Setting (p.17)
 -  CWE-73: External Control of File Name or Path (p.133)
 -  CWE-114: Process Control (p.283)
 -  CWE-219: Storage of File with Sensitive Data Under Web Root (p.560)
 -  CWE-220: Storage of File With Sensitive Data Under FTP Root (p.562)
 -  CWE-374: Passing Mutable Objects to an Untrusted Method (p.927)
 -  CWE-375: Returning a Mutable Object to an Untrusted Caller (p.930)
 -  CWE-377: Insecure Temporary File (p.932)





















































- B CWE-378: Creation of Temporary File With Insecure Permissions (p.935)
- B CWE-379: Creation of Temporary File in Directory with Insecure Permissions (p.937)
- C CWE-402: Transmission of Private Resources into a New Sphere ('Resource Leak') (p.984)
- B CWE-403: Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak') (p.985)
- B CWE-426: Untrusted Search Path (p.1035)
- B CWE-427: Uncontrolled Search Path Element (p.1040)
- B CWE-428: Unquoted Search Path or Element (p.1047)
- V CWE-433: Unparsed Raw Web Content Delivery (p.1053)
- B CWE-472: External Control of Assumed-Immutable Web Parameter (p.1131)
- B CWE-488: Exposure of Data Element to Wrong Session (p.1176)
- V CWE-491: Public cloneable() Method Without Final ('Object Hijack') (p.1181)
- V CWE-492: Use of Inner Class Containing Sensitive Data (p.1183)
- V CWE-493: Critical Public Variable Without Final Modifier (p.1190)
- V CWE-498: Cloneable Class Containing Sensitive Information (p.1204)
- V CWE-499: Serializable Class Containing Sensitive Data (p.1206)
- V CWE-500: Public Static Field Not Marked Final (p.1208)
- B CWE-524: Use of Cache Containing Sensitive Information (p.1240)
- V CWE-525: Use of Web Browser Cache Containing Sensitive Information (p.1242)
- V CWE-527: Exposure of Version-Control Repository to an Unauthorized Control Sphere (p.1245)
- V CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere (p.1246)
- V CWE-529: Exposure of Access Control List Files to an Unauthorized Control Sphere (p.1247)
- V CWE-530: Exposure of Backup File to an Unauthorized Control Sphere (p.1248)
- V CWE-539: Use of Persistent Cookies Containing Sensitive Information (p.1259)
- B CWE-552: Files or Directories Accessible to External Parties (p.1274)
- V CWE-553: Command Shell in Externally Accessible Directory (p.1277)
- B CWE-565: Reliance on Cookies without Validation and Integrity Checking (p.1292)
- V CWE-582: Array Declared Public, Final, and Static (p.1322)
- V CWE-583: finalize() Method Declared Public (p.1324)
- V CWE-608: Struts: Non-private Field in ActionForm Class (p.1369)
- B CWE-619: Dangling Database Cursor ('Cursor Injection') (p.1391)
- C CWE-642: External Control of Critical State Data (p.1422)
- C CWE-668: Exposure of Resource to Wrong Sphere (p.1478)
- B CWE-767: Access to Critical Private Variable via Public Method (p.1619)
- V CWE-784: Reliance on Cookies without Validation and Integrity Checking in a Security Decision (p.1662)
- B CWE-1282: Assumed-Immutable Data is Stored in Writable Memory (p.2139)
- B CWE-1327: Binding to an Unrestricted IP Address (p.2227)
- C CWE-1404: Comprehensive Categorization: File Handling (p.2550)
- B CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
- B CWE-23: Relative Path Traversal (p.46)
- V CWE-24: Path Traversal: '../filedir' (p.53)
- V CWE-25: Path Traversal: '/../filedir' (p.55)
- V CWE-26: Path Traversal: '/dir/../filename' (p.57)
- V CWE-27: Path Traversal: 'dir/../filename' (p.58)
- V CWE-28: Path Traversal: '..filedir' (p.60)
- V CWE-29: Path Traversal: '\\.filename' (p.62)
- V CWE-30: Path Traversal: 'dir\\.filename' (p.64)
- V CWE-31: Path Traversal: 'dir\\.\\.filename' (p.65)
- V CWE-32: Path Traversal: '...' (Triple Dot) (p.67)
- V CWE-33: Path Traversal: '....' (Multiple Dot) (p.69)
- V CWE-34: Path Traversal: '..../' (p.71)
- V CWE-35: Path Traversal: '....//' (p.73)
- B CWE-36: Absolute Path Traversal (p.75)
- V CWE-37: Path Traversal: '/absolute/pathname/here' (p.79)

-  CWE-38: Path Traversal: '\absolute\pathname\here' (p.81)
-  CWE-39: Path Traversal: 'C:dirname' (p.83)
-  CWE-40: Path Traversal: '\\UNC\share\name\' (Windows UNC Share) (p.86)
-  CWE-41: Improper Resolution of Path Equivalence (p.87)
-  CWE-42: Path Equivalence: 'filename.' (Trailing Dot) (p.93)
-  CWE-43: Path Equivalence: 'filename....' (Multiple Trailing Dot) (p.94)
-  CWE-44: Path Equivalence: 'file.name' (Internal Dot) (p.95)
-  CWE-45: Path Equivalence: 'file...name' (Multiple Internal Dot) (p.96)
-  CWE-46: Path Equivalence: 'filename ' (Trailing Space) (p.97)
-  CWE-47: Path Equivalence: ' filename' (Leading Space) (p.98)
-  CWE-48: Path Equivalence: 'file name' (Internal Whitespace) (p.99)
-  CWE-49: Path Equivalence: 'filename/' (Trailing Slash) (p.100)
-  CWE-50: Path Equivalence: '//multiple/leading/slash' (p.101)
-  CWE-51: Path Equivalence: '/multiple/internal/slash' (p.103)
-  CWE-52: Path Equivalence: '/multiple/trailing/slash/' (p.104)
-  CWE-53: Path Equivalence: '\multiple\internal\backslash' (p.105)
-  CWE-54: Path Equivalence: 'filedir\' (Trailing Backslash) (p.106)
-  CWE-55: Path Equivalence: './.' (Single Dot Directory) (p.107)
-  CWE-56: Path Equivalence: 'filedir*' (Wildcard) (p.108)
-  CWE-57: Path Equivalence: 'fakedir/./readdir/filename' (p.109)
-  CWE-58: Path Equivalence: Windows 8.3 Filename (p.111)
-  CWE-59: Improper Link Resolution Before File Access ('Link Following') (p.112)
-  CWE-61: UNIX Symbolic Link (Symlink) Following (p.117)
-  CWE-62: UNIX Hard Link (p.120)
-  CWE-64: Windows Shortcut Following (.LNK) (p.122)
-  CWE-65: Windows Hard Link (p.124)
-  CWE-66: Improper Handling of File Names that Identify Virtual Resources (p.125)
-  CWE-67: Improper Handling of Windows Device Names (p.127)
-  CWE-69: Improper Handling of Windows ::DATA Alternate Data Stream (p.130)
-  CWE-72: Improper Handling of Apple HFS+ Alternate Data Stream Path (p.131)
-  CWE-1405: Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions (p.2552)
-  CWE-7: J2EE Misconfiguration: Missing Custom Error Page (p.4)
-  CWE-12: ASP.NET Misconfiguration: Missing Custom Error Page (p.11)
-  CWE-252: Unchecked Return Value (p.613)
-  CWE-390: Detection of Error Condition Without Action (p.950)
-  CWE-391: Unchecked Error Condition (p.955)
-  CWE-394: Unexpected Status Code or Return Value (p.962)
-  CWE-544: Missing Standardized Error Handling Mechanism (p.1265)
-  CWE-703: Improper Check or Handling of Exceptional Conditions (p.1544)
-  CWE-754: Improper Check for Unusual or Exceptional Conditions (p.1577)
-  CWE-755: Improper Handling of Exceptional Conditions (p.1585)
-  CWE-756: Missing Custom Error Page (p.1588)
-  CWE-1247: Improper Protection Against Voltage and Clock Glitches (p.2056)
-  CWE-1261: Improper Handling of Single Event Upsets (p.2091)
-  CWE-1332: Improper Handling of Faults that Lead to Instruction Skips (p.2240)
-  CWE-1351: Improper Handling of Hardware Behavior in Exceptionally Cold Environments (p.2265)
-  CWE-1384: Improper Handling of Physical or Environmental Conditions (p.2269)
-  CWE-1406: Comprehensive Categorization: Improper Input Validation (p.2552)
-  CWE-20: Improper Input Validation (p.20)
-  CWE-105: Struts: Form Field Without Validator (p.259)
-  CWE-106: Struts: Plug-in Framework not in Use (p.262)
-  CWE-108: Struts: Unvalidated Action Form (p.267)
-  CWE-109: Struts: Validator Turned Off (p.269)





















































- B CWE-112: Missing XML Validation (p.275)
- V CWE-554: ASP.NET Misconfiguration: Not Using Input Validation Framework (p.1278)
- B CWE-606: Unchecked Input for Loop Condition (p.1366)
- V CWE-622: Improper Validation of Function Hook Arguments (p.1396)
- V CWE-781: Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code (p.1654)
- B CWE-1173: Improper Use of Validation Framework (p.1978)
- V CWE-1174: ASP.NET Misconfiguration: Improper Model Validation (p.1979)
- B CWE-1284: Improper Validation of Specified Quantity in Input (p.2142)
- B CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input (p.2144)
- B CWE-1286: Improper Validation of Syntactic Correctness of Input (p.2148)
- B CWE-1287: Improper Validation of Specified Type of Input (p.2150)
- B CWE-1288: Improper Validation of Consistency within Input (p.2151)
- B CWE-1289: Improper Validation of Unsafe Equivalence in Input (p.2153)
- C CWE-1407: Comprehensive Categorization: Improper Neutralization (p.2553)
 - G CWE-116: Improper Encoding or Escaping of Output (p.287)
 - B CWE-117: Improper Output Neutralization for Logs (p.294)
 - B CWE-130: Improper Handling of Length Parameter Inconsistency (p.357)
 - G CWE-138: Improper Neutralization of Special Elements (p.379)
 - B CWE-140: Improper Neutralization of Delimiters (p.382)
 - V CWE-141: Improper Neutralization of Parameter/Argument Delimiters (p.384)
 - V CWE-142: Improper Neutralization of Value Delimiters (p.386)
 - V CWE-143: Improper Neutralization of Record Delimiters (p.387)
 - V CWE-144: Improper Neutralization of Line Delimiters (p.389)
 - V CWE-145: Improper Neutralization of Section Delimiters (p.391)
 - V CWE-146: Improper Neutralization of Expression/Command Delimiters (p.393)
 - V CWE-147: Improper Neutralization of Input Terminators (p.395)
 - V CWE-148: Improper Neutralization of Input Leaders (p.397)
 - V CWE-149: Improper Neutralization of Quoting Syntax (p.398)
 - V CWE-150: Improper Neutralization of Escape, Meta, or Control Sequences (p.400)
 - V CWE-151: Improper Neutralization of Comment Delimiters (p.402)
 - V CWE-152: Improper Neutralization of Macro Symbols (p.404)
 - V CWE-153: Improper Neutralization of Substitution Characters (p.406)
 - V CWE-154: Improper Neutralization of Variable Name Delimiters (p.407)
 - V CWE-155: Improper Neutralization of Wildcards or Matching Symbols (p.409)
 - V CWE-156: Improper Neutralization of Whitespace (p.411)
 - V CWE-157: Failure to Sanitize Paired Delimiters (p.413)
 - V CWE-158: Improper Neutralization of Null Byte or NUL Character (p.415)
 - G CWE-159: Improper Handling of Invalid Use of Special Elements (p.417)
 - V CWE-160: Improper Neutralization of Leading Special Elements (p.419)
 - V CWE-161: Improper Neutralization of Multiple Leading Special Elements (p.421)
 - V CWE-162: Improper Neutralization of Trailing Special Elements (p.423)
 - V CWE-163: Improper Neutralization of Multiple Trailing Special Elements (p.425)
 - V CWE-164: Improper Neutralization of Internal Special Elements (p.426)
 - V CWE-165: Improper Neutralization of Multiple Internal Special Elements (p.428)
 - B CWE-166: Improper Handling of Missing Special Element (p.429)
 - B CWE-167: Improper Handling of Additional Special Element (p.431)
 - B CWE-168: Improper Handling of Inconsistent Special Elements (p.433)
 - B CWE-170: Improper Null Termination (p.434)
 - G CWE-172: Encoding Error (p.439)
 - V CWE-173: Improper Handling of Alternate Encoding (p.441)
 - V CWE-174: Double Decoding of the Same Data (p.443)
 - V CWE-175: Improper Handling of Mixed Encoding (p.445)
 - V CWE-176: Improper Handling of Unicode Encoding (p.446)
 - V CWE-177: Improper Handling of URL Encoding (Hex Encoding) (p.449)

-  CWE-228: Improper Handling of Syntactically Invalid Structure (p.575)
-  CWE-229: Improper Handling of Values (p.577)
-  CWE-230: Improper Handling of Missing Values (p.578)
-  CWE-231: Improper Handling of Extra Values (p.579)
-  CWE-232: Improper Handling of Undefined Values (p.580)
-  CWE-233: Improper Handling of Parameters (p.581)
-  CWE-234: Failure to Handle Missing Parameter (p.583)
-  CWE-235: Improper Handling of Extra Parameters (p.585)
-  CWE-236: Improper Handling of Undefined Parameters (p.586)
-  CWE-237: Improper Handling of Structural Elements (p.587)
-  CWE-238: Improper Handling of Incomplete Structural Elements (p.588)
-  CWE-239: Failure to Handle Incomplete Element (p.589)
-  CWE-240: Improper Handling of Inconsistent Structural Elements (p.590)
-  CWE-241: Improper Handling of Unexpected Data Type (p.591)
-  CWE-463: Deletion of Data Structure Sentinel (p.1113)
-  CWE-464: Addition of Data Structure Sentinel (p.1115)
-  CWE-626: Null Byte Interaction Error (Poison Null Byte) (p.1403)
-  CWE-644: Improper Neutralization of HTTP Headers for Scripting Syntax (p.1430)
-  CWE-707: Improper Neutralization (p.1554)
-  CWE-790: Improper Filtering of Special Elements (p.1687)
-  CWE-791: Incomplete Filtering of Special Elements (p.1689)
-  CWE-792: Incomplete Filtering of One or More Instances of Special Elements (p.1690)
-  CWE-793: Only Filtering One Instance of a Special Element (p.1692)
-  CWE-794: Incomplete Filtering of Multiple Instances of Special Elements (p.1693)
-  CWE-795: Only Filtering Special Elements at a Specified Location (p.1694)
-  CWE-796: Only Filtering Special Elements Relative to a Marker (p.1696)
-  CWE-797: Only Filtering Special Elements at an Absolute Position (p.1698)
-  CWE-838: Inappropriate Encoding for Output Context (p.1773)
-  CWE-1408: Comprehensive Categorization: Incorrect Calculation (p.2555)
 -  CWE-128: Wrap-around Error (p.345)
 -  CWE-135: Incorrect Calculation of Multi-Byte String Length (p.377)
 -  CWE-190: Integer Overflow or Wraparound (p.478)
 -  CWE-191: Integer Underflow (Wrap or Wraparound) (p.487)
 -  CWE-193: Off-by-one Error (p.493)
 -  CWE-369: Divide By Zero (p.920)
 -  CWE-467: Use of sizeof() on a Pointer Type (p.1118)
 -  CWE-468: Incorrect Pointer Scaling (p.1121)
 -  CWE-469: Use of Pointer Subtraction to Determine Size (p.1123)
 -  CWE-682: Incorrect Calculation (p.1507)
 -  CWE-1335: Incorrect Bitwise Shift of Integer (p.2247)
 -  CWE-1339: Insufficient Precision or Accuracy of a Real Number (p.2254)
-  CWE-1409: Comprehensive Categorization: Injection (p.2556)
 -  CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') (p.138)
 -  CWE-75: Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) (p.145)
 -  CWE-76: Improper Neutralization of Equivalent Special Elements (p.146)
 -  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
 -  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
 -  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
 -  CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) (p.182)
 -  CWE-81: Improper Neutralization of Script in an Error Message Web Page (p.184)
 -  CWE-82: Improper Neutralization of Script in Attributes of IMG Tags in a Web Page (p.186)

- V CWE-83: Improper Neutralization of Script in Attributes in a Web Page (p.188)
- V CWE-84: Improper Neutralization of Encoded URI Schemes in a Web Page (p.190)
- V CWE-85: Doubled Character XSS Manipulations (p.192)
- V CWE-86: Improper Neutralization of Invalid Characters in Identifiers in Web Pages (p.194)
- V CWE-87: Improper Neutralization of Alternate XSS Syntax (p.196)
- B CWE-88: Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') (p.198)
- B CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
- B CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection') (p.217)
- B CWE-91: XML Injection (aka Blind XPath Injection) (p.220)
- B CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection') (p.222)
- B CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
- V CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (p.232)
- B CWE-96: Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') (p.238)
- V CWE-97: Improper Neutralization of Server-Side Includes (SSI) Within a Web Page (p.241)
- G CWE-99: Improper Control of Resource Identifiers ('Resource Injection') (p.249)
- V CWE-102: Struts: Duplicate Validation Forms (p.252)
- V CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting') (p.277)
- V CWE-564: SQL Injection: Hibernate (p.1290)
- V CWE-621: Variable Extraction Error (p.1394)
- B CWE-624: Executable Regular Expression Error (p.1399)
- V CWE-627: Dynamic Variable Evaluation (p.1405)
- B CWE-641: Improper Restriction of Names for Files and Other Resources (p.1421)
- B CWE-643: Improper Neutralization of Data within XPath Expressions ('XPath Injection') (p.1428)
- B CWE-652: Improper Neutralization of Data within XQuery Expressions ('XQuery Injection') (p.1444)
- G CWE-692: Incomplete Denylist to Cross-Site Scripting (p.1528)
- B CWE-694: Use of Multiple Resources with Duplicate Identifier (p.1531)
- B CWE-914: Improper Control of Dynamically-Identified Variables (p.1816)
- B CWE-917: Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection') (p.1827)
- G CWE-943: Improper Neutralization of Special Elements in Data Query Logic (p.1860)
- B CWE-1236: Improper Neutralization of Formula Elements in a CSV File (p.2031)
- B CWE-1336: Improper Neutralization of Special Elements Used in a Template Engine (p.2250)
- B CWE-1426: Improper Validation of Generative AI Output (p.2321)
- B CWE-1427: Improper Neutralization of Input Used for LLM Prompting (p.2324)
- C CWE-1410: Comprehensive Categorization: Insufficient Control Flow Management (p.2557)
- B CWE-179: Incorrect Behavior Order: Early Validation (p.454)
- V CWE-180: Incorrect Behavior Order: Validate Before Canonicalize (p.457)
- V CWE-181: Incorrect Behavior Order: Validate Before Filter (p.460)
- B CWE-248: Uncaught Exception (p.603)
- V CWE-382: J2EE Bad Practices: Use of System.exit() (p.940)
- B CWE-395: Use of NullPointerException Catch to Detect NULL Pointer Dereference (p.964)
- B CWE-396: Declaration of Catch for Generic Exception (p.966)
- B CWE-397: Declaration of Throws for Generic Exception (p.968)
- B CWE-408: Incorrect Behavior Order: Early Amplification (p.1002)
- B CWE-430: Deployment of Wrong Handler (p.1049)
- B CWE-431: Missing Handler (p.1051)
- B CWE-455: Non-exit on Failed Initialization (p.1095)
- B CWE-480: Use of Incorrect Operator (p.1157)
- V CWE-481: Assigning instead of Comparing (p.1161)
- V CWE-482: Comparing instead of Assigning (p.1165)
- B CWE-483: Incorrect Block Delimitation (p.1167)

-  CWE-584: Return Inside Finally Block (p.1325)
-  CWE-600: Uncaught Exception in Servlet (p.1352)
-  CWE-617: Reachable Assertion (p.1387)
-  CWE-670: Always-Incorrect Control Flow Implementation (p.1484)
-  CWE-674: Uncontrolled Recursion (p.1493)
-  CWE-691: Insufficient Control Flow Management (p.1525)
-  CWE-696: Incorrect Behavior Order (p.1535)
-  CWE-698: Execution After Redirect (EAR) (p.1542)
-  CWE-705: Incorrect Control Flow Scoping (p.1550)
-  CWE-768: Incorrect Short Circuit Evaluation (p.1620)
-  CWE-783: Operator Precedence Logic Error (p.1659)
-  CWE-799: Improper Control of Interaction Frequency (p.1708)
-  CWE-834: Excessive Iteration (p.1763)
-  CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') (p.1766)
-  CWE-837: Improper Enforcement of a Single, Unique Action (p.1771)
-  CWE-841: Improper Enforcement of Behavioral Workflow (p.1781)
-  CWE-1190: DMA Device Enabled Too Early in Boot Phase (p.1987)
-  CWE-1193: Power-On of Untrusted Execution Core Before Enabling Fabric Access Control (p.1995)
-  CWE-1265: Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls (p.2100)
-  CWE-1280: Access Control Check Implemented After Asset is Accessed (p.2134)
-  CWE-1281: Sequence of Processor Instructions Leads to Unexpected Behavior (p.2136)
-  CWE-1322: Use of Blocking Code in Single-threaded, Non-blocking Context (p.2219)
-  CWE-1411: Comprehensive Categorization: Insufficient Verification of Data Authenticity (p.2559)
-  CWE-345: Insufficient Verification of Data Authenticity (p.858)
-  CWE-346: Origin Validation Error (p.860)
-  CWE-348: Use of Less Trusted Source (p.866)
-  CWE-349: Acceptance of Extraneous Untrusted Data With Trusted Data (p.868)
-  CWE-351: Insufficient Type Distinction (p.873)
-  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
-  CWE-353: Missing Support for Integrity Check (p.881)
-  CWE-354: Improper Validation of Integrity Check Value (p.883)
-  CWE-360: Trust of System Event Data (p.894)
-  CWE-494: Download of Code Without Integrity Check (p.1192)
-  CWE-616: Incomplete Identification of Uploaded File Variables (PHP) (p.1385)
-  CWE-646: Reliance on File Name or Extension of Externally-Supplied File (p.1434)
-  CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking (p.1439)
-  CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel (p.1839)
-  CWE-1293: Missing Source Correlation of Multiple Independent Data (p.2161)
-  CWE-1385: Missing Origin Validation in WebSockets (p.2271)
-  CWE-1399: Comprehensive Categorization: Memory Safety (p.2546)
-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') (p.310)
-  CWE-121: Stack-based Buffer Overflow (p.320)
-  CWE-122: Heap-based Buffer Overflow (p.324)
-  CWE-123: Write-what-where Condition (p.329)
-  CWE-124: Buffer Underwrite ('Buffer Underflow') (p.332)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-126: Buffer Over-read (p.340)
-  CWE-127: Buffer Under-read (p.343)
-  CWE-129: Improper Validation of Array Index (p.347)
-  CWE-131: Incorrect Calculation of Buffer Size (p.361)
-  CWE-134: Use of Externally-Controlled Format String (p.371)





















































- B CWE-188: Reliance on Data/Memory Layout (p.476)
- V CWE-198: Use of Incorrect Byte Ordering (p.510)
- V CWE-244: Improper Clearing of Heap Memory Before Release ('Heap Inspection') (p.598)
- V CWE-401: Missing Release of Memory after Effective Lifetime (p.980)
- V CWE-415: Double Free (p.1015)
- V CWE-416: Use After Free (p.1019)
- B CWE-466: Return of Pointer Value Outside of Expected Range (p.1117)
- B CWE-562: Return of Stack Variable Address (p.1287)
- V CWE-587: Assignment of a Fixed Address to a Pointer (p.1330)
- V CWE-590: Free of Memory not on the Heap (p.1335)
- C CWE-680: Integer Overflow to Buffer Overflow (p.1502)
- C CWE-690: Unchecked Return Value to NULL Pointer Dereference (p.1523)
- V CWE-761: Free of Pointer not at Start of Buffer (p.1601)
- V CWE-762: Mismatched Memory Management Routines (p.1605)
- B CWE-763: Release of Invalid Pointer or Reference (p.1608)
- B CWE-786: Access of Memory Location Before Start of Buffer (p.1666)
- B CWE-787: Out-of-bounds Write (p.1669)
- B CWE-788: Access of Memory Location After End of Buffer (p.1678)
- V CWE-789: Memory Allocation with Excessive Size Value (p.1683)
- B CWE-805: Buffer Access with Incorrect Length Value (p.1711)
- V CWE-806: Buffer Access Using Size of Source Buffer (p.1719)
- B CWE-822: Untrusted Pointer Dereference (p.1732)
- B CWE-823: Use of Out-of-range Pointer Offset (p.1735)
- B CWE-824: Access of Uninitialized Pointer (p.1738)
- B CWE-825: Expired Pointer Dereference (p.1741)
- C CWE-1412: Comprehensive Categorization: Poor Coding Practices (p.2559)
- V CWE-11: ASP.NET Misconfiguration: Creating Debug Binary (p.9)
- V CWE-103: Struts: Incomplete validate() Method Definition (p.254)
- V CWE-104: Struts: Form Bean Does Not Extend Validation Class (p.257)
- V CWE-107: Struts: Unused Validation Form (p.265)
- V CWE-110: Struts: Validator Without Form Field (p.270)
- V CWE-111: Direct Use of Unsafe JNI (p.272)
- B CWE-242: Use of Inherently Dangerous Function (p.593)
- V CWE-245: J2EE Bad Practices: Direct Management of Connections (p.599)
- V CWE-246: J2EE Bad Practices: Direct Use of Sockets (p.601)
- B CWE-253: Incorrect Check of Function Return Value (p.620)
- B CWE-358: Improperly Implemented Security Check for Standard (p.888)
- V CWE-383: J2EE Bad Practices: Direct Use of Threads (p.942)
- B CWE-392: Missing Report of Error Condition (p.958)
- B CWE-393: Return of Wrong Status Code (p.960)
- B CWE-440: Expected Behavior Violation (p.1069)
- C CWE-446: UI Discrepancy for Security Feature (p.1081)
- B CWE-448: Obsolete Feature in UI (p.1083)
- B CWE-449: The UI Performs the Wrong Action (p.1084)
- C CWE-451: User Interface (UI) Misrepresentation of Critical Information (p.1087)
- V CWE-462: Duplicate Key in Associative List (Alist) (p.1111)
- B CWE-474: Use of Function with Inconsistent Implementations (p.1136)
- B CWE-475: Undefined Behavior for Input to API (p.1138)
- B CWE-476: NULL Pointer Dereference (p.1139)
- B CWE-477: Use of Obsolete Function (p.1146)
- B CWE-484: Omitted Break Statement in Switch (p.1169)
- B CWE-489: Active Debug Code (p.1178)
- C CWE-506: Embedded Malicious Code (p.1218)
- B CWE-507: Trojan Horse (p.1220)

-  CWE-508: Non-Replicating Malicious Code (p. 1221)
-  CWE-509: Replicating Malicious Code (Virus or Worm) (p. 1222)
-  CWE-510: Trapdoor (p. 1223)
-  CWE-511: Logic/Time Bomb (p. 1225)
-  CWE-512: Spyware (p. 1226)
-  CWE-546: Suspicious Comment (p. 1266)
-  CWE-547: Use of Hard-coded, Security-relevant Constants (p. 1267)
-  CWE-560: Use of umask() with chmod-style Argument (p. 1282)
-  CWE-561: Dead Code (p. 1283)
-  CWE-563: Assignment to Variable without Use (p. 1289)
-  CWE-570: Expression is Always False (p. 1300)
-  CWE-571: Expression is Always True (p. 1303)
-  CWE-573: Improper Following of Specification by Caller (p. 1307)
-  CWE-575: EJB Bad Practices: Use of AWT Swing (p. 1310)
-  CWE-576: EJB Bad Practices: Use of Java I/O (p. 1312)
-  CWE-577: EJB Bad Practices: Use of Sockets (p. 1314)
-  CWE-578: EJB Bad Practices: Use of Class Loader (p. 1316)
-  CWE-579: J2EE Bad Practices: Non-serializable Object Stored in Session (p. 1318)
-  CWE-581: Object Model Violation: Just One of Equals and Hashcode Defined (p. 1321)
-  CWE-585: Empty Synchronized Block (p. 1327)
-  CWE-586: Explicit Call to Finalize() (p. 1329)
-  CWE-589: Call to Non-ubiquitous API (p. 1333)
-  CWE-594: J2EE Framework: Saving Unserializable Objects to Disk (p. 1341)
-  CWE-605: Multiple Binds to the Same Port (p. 1364)
-  CWE-628: Function Call with Incorrectly Specified Arguments (p. 1407)
-  CWE-675: Multiple Operations on Resource in Single-Operation Context (p. 1496)
-  CWE-676: Use of Potentially Dangerous Function (p. 1498)
-  CWE-683: Function Call With Incorrect Order of Arguments (p. 1512)
-  CWE-684: Incorrect Provision of Specified Functionality (p. 1514)
-  CWE-685: Function Call With Incorrect Number of Arguments (p. 1516)
-  CWE-686: Function Call With Incorrect Argument Type (p. 1517)
-  CWE-687: Function Call With Incorrectly Specified Argument Value (p. 1518)
-  CWE-688: Function Call With Incorrect Variable or Reference as Argument (p. 1520)
-  CWE-695: Use of Low-Level Functionality (p. 1533)
-  CWE-710: Improper Adherence to Coding Standards (p. 1558)
-  CWE-758: Reliance on Undefined, Unspecified, or Implementation-Defined Behavior (p. 1591)
-  CWE-766: Critical Data Element Declared Public (p. 1615)
-  CWE-785: Use of Path Manipulation Function without Maximum-sized Buffer (p. 1664)
-  CWE-912: Hidden Functionality (p. 1812)
-  CWE-1007: Insufficient Visual Distinction of Homoglyphs Presented to User (p. 1866)
-  CWE-1041: Use of Redundant Code (p. 1884)
-  CWE-1043: Data Element Aggregating an Excessively Large Number of Non-Primitive Elements (p. 1887)
-  CWE-1044: Architecture with Number of Horizontal Layers Outside of Expected Range (p. 1888)
-  CWE-1045: Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor (p. 1889)
-  CWE-1047: Modules with Circular Dependencies (p. 1891)
-  CWE-1048: Invokable Control Element with Large Number of Outward Calls (p. 1892)
-  CWE-1053: Missing Documentation for Design (p. 1898)
-  CWE-1054: Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer (p. 1899)
-  CWE-1055: Multiple Inheritance from Concrete Classes (p. 1900)
-  CWE-1056: Invokable Control Element with Variadic Parameters (p. 1901)
-  CWE-1057: Data Access Operations Outside of Expected Data Manager Component (p. 1902)
-  CWE-1059: Insufficient Technical Documentation (p. 1904)

-  CWE-1060: Excessive Number of Inefficient Server-Side Data Accesses (p.1906)
-  CWE-1061: Insufficient Encapsulation (p.1907)
-  CWE-1062: Parent Class with References to Child Class (p.1909)
-  CWE-1064: Invokable Control Element with Signature Containing an Excessive Number of Parameters (p.1911)
-  CWE-1065: Runtime Resource Management Control Element in a Component Built to Run on Application Servers (p.1912)
-  CWE-1066: Missing Serialization Control Element (p.1913)
-  CWE-1068: Inconsistency Between Implementation and Documented Design (p.1915)
-  CWE-1069: Empty Exception Block (p.1916)
-  CWE-1070: Serializable Data Element Containing non-Serializable Item Elements (p.1918)
-  CWE-1071: Empty Code Block (p.1919)
-  CWE-1074: Class with Excessively Deep Inheritance (p.1923)
-  CWE-1075: Unconditional Control Flow Transfer outside of Switch Block (p.1924)
-  CWE-1076: Insufficient Adherence to Expected Conventions (p.1925)
-  CWE-1078: Inappropriate Source Code Style or Formatting (p.1927)
-  CWE-1079: Parent Class without Virtual Destructor Method (p.1929)
-  CWE-1080: Source Code File with Excessive Number of Lines of Code (p.1930)
-  CWE-1082: Class Instance Self Destruction Control Element (p.1931)
-  CWE-1083: Data Access from Outside Expected Data Manager Component (p.1932)
-  CWE-1085: Invokable Control Element with Excessive Volume of Commented-out Code (p.1934)
-  CWE-1086: Class with Excessive Number of Child Classes (p.1935)
-  CWE-1087: Class with Virtual Method without a Virtual Destructor (p.1936)
-  CWE-1090: Method Containing Access of a Member Element from Another Class (p.1939)
-  CWE-1092: Use of Same Invokable Control Element in Multiple Architectural Layers (p.1941)
-  CWE-1093: Excessively Complex Data Representation (p.1942)
-  CWE-1095: Loop Condition Value Update within the Loop (p.1944)
-  CWE-1097: Persistent Storable Data Element without Associated Comparison Control Element (p.1946)
-  CWE-1098: Data Element containing Pointer Item without Proper Copy Control Element (p.1947)
-  CWE-1099: Inconsistent Naming Conventions for Identifiers (p.1948)
-  CWE-1100: Insufficient Isolation of System-Dependent Functions (p.1949)
-  CWE-1101: Reliance on Runtime Component in Generated Code (p.1950)
-  CWE-1102: Reliance on Machine-Dependent Data Representation (p.1951)
-  CWE-1103: Use of Platform-Dependent Third Party Components (p.1952)
-  CWE-1105: Insufficient Encapsulation of Machine-Dependent Functionality (p.1954)
-  CWE-1106: Insufficient Use of Symbolic Constants (p.1955)
-  CWE-1107: Insufficient Isolation of Symbolic Constant Definitions (p.1956)
-  CWE-1108: Excessive Reliance on Global Variables (p.1957)
-  CWE-1109: Use of Same Variable for Multiple Purposes (p.1958)
-  CWE-1110: Incomplete Design Documentation (p.1959)
-  CWE-1111: Incomplete I/O Documentation (p.1960)
-  CWE-1112: Incomplete Documentation of Program Execution (p.1961)
-  CWE-1113: Inappropriate Comment Style (p.1962)
-  CWE-1114: Inappropriate Whitespace Style (p.1963)
-  CWE-1115: Source Code Element without Standard Prologue (p.1963)
-  CWE-1116: Inaccurate Comments (p.1964)
-  CWE-1117: Callable with Insufficient Behavioral Summary (p.1966)
-  CWE-1118: Insufficient Documentation of Error Handling Techniques (p.1967)
-  CWE-1119: Excessive Use of Unconditional Branching (p.1968)
-  CWE-1120: Excessive Code Complexity (p.1969)
-  CWE-1121: Excessive McCabe Cyclomatic Complexity (p.1970)
-  CWE-1122: Excessive Halstead Complexity (p.1971)
-  CWE-1123: Excessive Use of Self-Modifying Code (p.1972)

-  CWE-1124: Excessively Deep Nesting (*p.1973*)
-  CWE-1125: Excessive Attack Surface (*p.1974*)
-  CWE-1126: Declaration of Variable with Unnecessarily Wide Scope (*p.1975*)
-  CWE-1127: Compilation with Insufficient Warnings or Errors (*p.1976*)
-  CWE-1164: Irrelevant Code (*p.1976*)
-  CWE-1177: Use of Prohibited Code (*p.1981*)
-  CWE-1209: Failure to Disable Reserved Bits (*p.2000*)
-  CWE-1245: Improper Finite State Machines (FSMs) in Hardware Logic (*p.2052*)
-  CWE-1341: Multiple Releases of Same Resource or Handle (*p.2258*)
-  CWE-1357: Reliance on Insufficiently Trustworthy Component (*p.2266*)
-  CWE-1413: Comprehensive Categorization: Protection Mechanism Failure (*p.2563*)
 -  CWE-182: Collapse of Data into Unsafe Value (*p.462*)
 -  CWE-184: Incomplete List of Disallowed Inputs (*p.466*)
 -  CWE-222: Truncation of Security-relevant Information (*p.565*)
 -  CWE-223: Omission of Security-relevant Information (*p.566*)
 -  CWE-224: Obscured Security-relevant Information by Alternate Name (*p.568*)
 -  CWE-356: Product UI does not Warn User of Unsafe Actions (*p.886*)
 -  CWE-357: Insufficient UI Warning of Dangerous Operations (*p.887*)
 -  CWE-450: Multiple Interpretations of UI Input (*p.1085*)
 -  CWE-602: Client-Side Enforcement of Server-Side Security (*p.1359*)
 -  CWE-693: Protection Mechanism Failure (*p.1529*)
 -  CWE-757: Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') (*p.1589*)
 -  CWE-778: Insufficient Logging (*p.1647*)
 -  CWE-807: Reliance on Untrusted Inputs in a Security Decision (*p.1723*)
 -  CWE-1039: Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations (*p.1882*)
 -  CWE-1248: Semiconductor Defects in Hardware Logic with Security-Sensitive Implications (*p.2060*)
 -  CWE-1253: Incorrect Selection of Fuse Values (*p.2069*)
 -  CWE-1269: Product Released in Non-Release Configuration (*p.2110*)
 -  CWE-1278: Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques (*p.2131*)
 -  CWE-1291: Public Key Re-Use for Signing both Debug and Production Code (*p.2157*)
 -  CWE-1318: Missing Support for Security Features in On-chip Fabrics or Buses (*p.2209*)
 -  CWE-1319: Improper Protection against Electromagnetic Fault Injection (EM-FI) (*p.2212*)
 -  CWE-1326: Missing Immutable Root of Trust in Hardware (*p.2224*)
 -  CWE-1338: Improper Protections Against Hardware Overheating (*p.2252*)
-  CWE-1414: Comprehensive Categorization: Randomness (*p.2564*)
 -  CWE-6: J2EE Misconfiguration: Insufficient Session-ID Length (*p.2*)
 -  CWE-323: Reusing a Nonce, Key Pair in Encryption (*p.797*)
 -  CWE-329: Generation of Predictable IV with CBC Mode (*p.818*)
 -  CWE-330: Use of Insufficiently Random Values (*p.821*)
 -  CWE-331: Insufficient Entropy (*p.828*)
 -  CWE-332: Insufficient Entropy in PRNG (*p.830*)
 -  CWE-333: Improper Handling of Insufficient Entropy in TRNG (*p.832*)
 -  CWE-334: Small Space of Random Values (*p.834*)
 -  CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG) (*p.836*)
 -  CWE-336: Same Seed in Pseudo-Random Number Generator (PRNG) (*p.839*)
 -  CWE-337: Predictable Seed in Pseudo-Random Number Generator (PRNG) (*p.841*)
 -  CWE-338: Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (*p.844*)
 -  CWE-339: Small Seed Space in PRNG (*p.847*)
 -  CWE-340: Generation of Predictable Numbers or Identifiers (*p.849*)
 -  CWE-341: Predictable from Observable State (*p.850*)
 -  CWE-342: Predictable Exact Value from Previous Values (*p.852*)
 -  CWE-343: Predictable Value Range from Previous Values (*p.854*)


























- B CWE-344: Use of Invariant Value in Dynamically Changing Context (p.856)
- B CWE-1204: Generation of Weak Initialization Vector (IV) (p.1996)
- B CWE-1241: Use of Predictable Algorithm in Random Number Generator (p.2042)
- C CWE-1415: Comprehensive Categorization: Resource Control (p.2565)
 - B CWE-385: Covert Timing Channel (p.947)
 - B CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') (p.1125)
 - V CWE-473: PHP External Variable Modification (p.1134)
 - B CWE-502: Deserialization of Untrusted Data (p.1212)
 - C CWE-514: Covert Channel (p.1227)
 - B CWE-515: Covert Storage Channel (p.1229)
 - C CWE-672: Operation on a Resource after Expiration or Release (p.1488)
 - B CWE-826: Premature Release of Resource During Expected Lifetime (p.1743)
 - B CWE-910: Use of Expired File Descriptor (p.1809)
 - B CWE-915: Improperly Controlled Modification of Dynamically-Determined Object Attributes (p.1818)
 - B CWE-1104: Use of Unmaintained Third Party Components (p.1953)
 - B CWE-1249: Application-Level Admin Tool with Inconsistent View of Underlying Operating System (p.2062)
 - B CWE-1251: Mirrored Regions with Different Values (p.2065)
 - B CWE-1277: Firmware Not Updateable (p.2128)
 - B CWE-1310: Missing Ability to Patch ROM Code (p.2191)
 - V CWE-1321: Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') (p.2216)
 - B CWE-1329: Reliance on Component That is Not Updateable (p.2231)
- C CWE-1416: Comprehensive Categorization: Resource Lifecycle Management (p.2566)
 - V CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') (p.242)
 - C CWE-118: Incorrect Access of Indexable Resource ('Range Error') (p.298)
 - B CWE-178: Improper Handling of Case Sensitivity (p.451)
 - V CWE-192: Integer Coercion Error (p.489)
 - V CWE-194: Unexpected Sign Extension (p.498)
 - V CWE-195: Signed to Unsigned Conversion Error (p.501)
 - V CWE-196: Unsigned to Signed Conversion Error (p.505)
 - B CWE-197: Numeric Truncation Error (p.507)
 - B CWE-212: Improper Removal of Sensitive Information Before Storage or Transfer (p.551)
 - C CWE-221: Information Loss or Omission (p.563)
 - B CWE-226: Sensitive Information in Resource Not Removed Before Reuse (p.569)
 - V CWE-243: Creation of chroot Jail Without Changing Working Directory (p.596)
 - B CWE-372: Incomplete Internal State Distinction (p.926)
 - B CWE-386: Symbolic Name not Mapping to Correct Object (p.949)
 - C CWE-400: Uncontrolled Resource Consumption (p.971)
 - C CWE-404: Improper Resource Shutdown or Release (p.987)
 - C CWE-405: Asymmetric Resource Consumption (Amplification) (p.993)
 - C CWE-406: Insufficient Control of Network Message Volume (Network Amplification) (p.997)
 - C CWE-407: Inefficient Algorithmic Complexity (p.999)
 - B CWE-409: Improper Handling of Highly Compressed Data (Data Amplification) (p.1004)
 - B CWE-410: Insufficient Resource Pool (p.1005)
 - B CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
 - V CWE-453: Insecure Default Variable Initialization (p.1091)
 - B CWE-454: External Initialization of Trusted Variables or Data Stores (p.1092)
 - V CWE-456: Missing Initialization of a Variable (p.1096)
 - V CWE-457: Use of Uninitialized Variable (p.1102)
 - B CWE-459: Incomplete Cleanup (p.1106)
 - B CWE-460: Improper Cleanup on Thrown Exception (p.1109)
 - B CWE-471: Modification of Assumed-Immutable Data (MAID) (p.1129)

-  CWE-487: Reliance on Package-level Scope (p.1175)
-  CWE-495: Private Data Structure Returned From A Public Method (p.1197)
-  CWE-496: Public Data Assigned to Private Array-Typed Field (p.1199)
-  CWE-501: Trust Boundary Violation (p.1210)
-  CWE-568: finalize() Method Without super.finalize() (p.1299)
-  CWE-580: clone() Method Without super.clone() (p.1319)
-  CWE-588: Attempt to Access Child of a Non-structure Pointer (p.1332)
-  CWE-607: Public Static Final Field References Mutable Object (p.1368)
-  CWE-610: Externally Controlled Reference to a Resource in Another Sphere (p.1373)
-  CWE-618: Exposed Unsafe ActiveX Method (p.1389)
-  CWE-662: Improper Synchronization (p.1457)
-  CWE-664: Improper Control of a Resource Through its Lifetime (p.1463)
-  CWE-665: Improper Initialization (p.1465)
-  CWE-666: Operation on Resource in Wrong Phase of Lifetime (p.1471)
-  CWE-669: Incorrect Resource Transfer Between Spheres (p.1480)
-  CWE-673: External Influence of Sphere Definition (p.1492)
-  CWE-681: Incorrect Conversion between Numeric Types (p.1504)
-  CWE-704: Incorrect Type Conversion or Cast (p.1547)
-  CWE-706: Use of Incorrectly-Resolved Name or Reference (p.1553)
-  CWE-749: Exposed Dangerous Method or Function (p.1572)
-  CWE-770: Allocation of Resources Without Limits or Throttling (p.1622)
-  CWE-771: Missing Reference to Active Allocated Resource (p.1631)
-  CWE-772: Missing Release of Resource after Effective Lifetime (p.1632)
-  CWE-773: Missing Reference to Active File Descriptor or Handle (p.1638)
-  CWE-774: Allocation of File Descriptors or Handles Without Limits or Throttling (p.1639)
-  CWE-775: Missing Release of File Descriptor or Handle after Effective Lifetime (p.1640)
-  CWE-776: Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion') (p.1642)
-  CWE-779: Logging of Excessive Data (p.1651)
-  CWE-782: Exposed IOCTL with Insufficient Access Control (p.1657)
-  CWE-827: Improper Control of Document Type Definition (p.1745)
-  CWE-829: Inclusion of Functionality from Untrusted Control Sphere (p.1750)
-  CWE-830: Inclusion of Web Functionality from an Untrusted Source (p.1756)
-  CWE-843: Access of Resource Using Incompatible Type ('Type Confusion') (p.1785)
-  CWE-908: Use of Uninitialized Resource (p.1802)
-  CWE-909: Missing Initialization of Resource (p.1806)
-  CWE-911: Improper Update of Reference Count (p.1811)
-  CWE-913: Improper Control of Dynamically-Managed Code Resources (p.1814)
-  CWE-920: Improper Restriction of Power Consumption (p.1832)
-  CWE-922: Insecure Storage of Sensitive Information (p.1835)
-  CWE-1042: Static Member Data Element outside of a Singleton Class Element (p.1886)
-  CWE-1046: Creation of Immutable Text Using String Concatenation (p.1890)
-  CWE-1049: Excessive Data Query Operations in a Large Data Table (p.1894)
-  CWE-1050: Excessive Platform Resource Consumption within a Loop (p.1895)
-  CWE-1051: Initialization with Hard-Coded Network Resource Configuration Data (p.1896)
-  CWE-1052: Excessive Use of Hard-Coded Literals in Initialization (p.1897)
-  CWE-1063: Creation of Class Instance within a Static Code Block (p.1910)
-  CWE-1067: Excessive Execution of Sequential Searches of Data Resource (p.1914)
-  CWE-1072: Data Resource Access without Use of Connection Pooling (p.1921)
-  CWE-1073: Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses (p.1922)
-  CWE-1084: Invokable Control Element with Excessive File or Data Access Operations (p.1933)
-  CWE-1089: Large Data Table with Excessive Number of Indices (p.1938)
-  CWE-1091: Use of Object without Invoking Destructor Method (p.1940)


























- B CWE-1094: Excessive Index Range Scan for a Data Resource (p.1943)
- C CWE-1176: Inefficient CPU Computation (p.1980)
- B CWE-1188: Initialization of a Resource with an Insecure Default (p.1983)
- B CWE-1221: Incorrect Register Defaults or Module Parameters (p.2005)
- C CWE-1229: Creation of Emergent Resource (p.2016)
- B CWE-1235: Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations (p.2029)
- V CWE-1239: Improper Zeroization of Hardware Register (p.2033)
- B CWE-1246: Improper Write Handling in Limited-write Non-Volatile Memories (p.2054)
- B CWE-1250: Improper Preservation of Consistency Between Independent Representations of Shared State (p.2064)
- B CWE-1258: Exposure of Sensitive System Information Due to Uncleared Debug Information (p.2082)
- B CWE-1266: Improper Scrubbing of Sensitive Data from Decommissioned Device (p.2104)
- B CWE-1271: Uninitialized Value on Reset for Registers Holding Security Settings (p.2115)
- B CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition (p.2116)
- B CWE-1279: Cryptographic Operations are run Before Supporting Units are Ready (p.2132)
- B CWE-1301: Insufficient or Incomplete Data Removal within Hardware Component (p.2183)
- B CWE-1325: Improperly Controlled Sequential Memory Allocation (p.2222)
- V CWE-1330: Remanent Data Readable after Memory Erase (p.2234)
- B CWE-1333: Inefficient Regular Expression Complexity (p.2243)
- B CWE-1342: Information Exposure through Microarchitectural State after Transient Execution (p.2262)
- B CWE-1386: Insecure Operation on Windows Junction / Mount Point (p.2273)
- B CWE-1389: Incorrect Parsing of Numbers with Different Radices (p.2275)
- C CWE-1419: Incorrect Initialization of Resource (p.2292)
- B CWE-1420: Exposure of Sensitive Information during Transient Execution (p.2297)
- B CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution (p.2304)
- B CWE-1422: Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution (p.2310)
- B CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution (p.2316)
- C CWE-1417: Comprehensive Categorization: Sensitive Information Exposure (p.2569)
- C CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
- B CWE-201: Insertion of Sensitive Information Into Sent Data (p.521)
- B CWE-203: Observable Discrepancy (p.525)
- B CWE-204: Observable Response Discrepancy (p.530)
- B CWE-205: Observable Behavioral Discrepancy (p.533)
- V CWE-206: Observable Internal Behavioral Discrepancy (p.534)
- V CWE-207: Observable Behavioral Discrepancy With Equivalent Products (p.535)
- B CWE-208: Observable Timing Discrepancy (p.537)
- B CWE-209: Generation of Error Message Containing Sensitive Information (p.540)
- B CWE-210: Self-generated Error Message Containing Sensitive Information (p.546)
- B CWE-211: Externally-Generated Error Message Containing Sensitive Information (p.548)
- B CWE-213: Exposure of Sensitive Information Due to Incompatible Policies (p.555)
- B CWE-214: Invocation of Process Using Visible Sensitive Information (p.556)
- B CWE-215: Insertion of Sensitive Information Into Debugging Code (p.558)
- B CWE-359: Exposure of Private Personal Information to an Unauthorized Actor (p.889)
- B CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere (p.1201)
- V CWE-526: Cleartext Storage of Sensitive Information in an Environment Variable (p.1243)
- V CWE-531: Inclusion of Sensitive Information in Test Code (p.1249)
- B CWE-532: Insertion of Sensitive Information into Log File (p.1250)
- V CWE-535: Exposure of Information Through Shell Error Message (p.1253)
- V CWE-536: Servlet Runtime Error Message Containing Sensitive Information (p.1254)
- V CWE-537: Java Runtime Error Message Containing Sensitive Information (p.1255)
- B CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory (p.1257)
- B CWE-540: Inclusion of Sensitive Information in Source Code (p.1260)

- V CWE-541: Inclusion of Sensitive Information in an Include File (p.1262)
- V CWE-548: Exposure of Information Through Directory Listing (p.1269)
- V CWE-550: Server-generated Error Message Containing Sensitive Information (p.1272)
- V CWE-598: Use of GET Request Method With Sensitive Query Strings (p.1349)
- V CWE-615: Inclusion of Sensitive Information in Source Code Comments (p.1383)
- V CWE-651: Exposure of WSDL File Containing Sensitive Information (p.1442)
- B CWE-1254: Incorrect Comparison Logic Granularity (p.2071)
- V CWE-1255: Comparison Logic is Vulnerable to Power Side-Channel Attacks (p.2073)
- B CWE-1273: Device Unlock Credential Sharing (p.2119)
- B CWE-1295: Debug Messages Revealing Unnecessary Information (p.2164)
- B CWE-1300: Improper Protection of Physical Side Channels (p.2177)
- C CWE-1418: Comprehensive Categorization: Violation of Secure Design Principles (p.2570)
- B CWE-250: Execution with Unnecessary Privileges (p.606)
- G CWE-424: Improper Protection of Alternate Path (p.1031)
- B CWE-447: Unimplemented or Unsupported Feature in UI (p.1082)
- G CWE-636: Not Failing Securely ('Failing Open') (p.1409)
- G CWE-637: Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism') (p.1411)
- G CWE-638: Not Using Complete Mediation (p.1413)
- G CWE-653: Improper Isolation or Compartmentalization (p.1445)
- B CWE-654: Reliance on a Single Factor in a Security Decision (p.1448)
- G CWE-655: Insufficient Psychological Acceptability (p.1450)
- G CWE-656: Reliance on Security Through Obscurity (p.1452)
- G CWE-657: Violation of Secure Design Principles (p.1454)
- G CWE-671: Lack of Administrator Control over Security (p.1487)
- B CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC) (p.1985)
- B CWE-1192: Improper Identifier for IP Block used in System-On-Chip (SOC) (p.1994)
- B CWE-1303: Non-Transparent Sharing of Microarchitectural Resources (p.2186)
- B CWE-1331: Improper Isolation of Shared Resources in Network On Chip (NoC) (p.2237)
- G CWE-1395: Dependency on Vulnerable Third-Party Component (p.2289)

Graph View: CWE-1425: Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses

-  CWE-787: Out-of-bounds Write (p.1669)
-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
-  CWE-416: Use After Free (p.1019)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
-  CWE-20: Improper Input Validation (p.20)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
-  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
-  CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
-  CWE-862: Missing Authorization (p.1789)
-  CWE-476: NULL Pointer Dereference (p.1139)
-  CWE-287: Improper Authentication (p.699)
-  CWE-190: Integer Overflow or Wraparound (p.478)
-  CWE-502: Deserialization of Untrusted Data (p.1212)
-  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
-  CWE-306: Missing Authentication for Critical Function (p.748)
-  CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (p.895)
-  CWE-269: Improper Privilege Management (p.653)
-  CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
-  CWE-863: Incorrect Authorization (p.1796)
-  CWE-276: Incorrect Default Permissions (p.672)

Graph View: CWE-1430: Weaknesses in the 2024 CWE Top 25 Most Dangerous Software Weaknesses

-  CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') (p.168)
-  CWE-787: Out-of-bounds Write (p.1669)
-  CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') (p.206)
-  CWE-352: Cross-Site Request Forgery (CSRF) (p.875)
-  CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') (p.33)
-  CWE-125: Out-of-bounds Read (p.336)
-  CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (p.155)
-  CWE-416: Use After Free (p.1019)
-  CWE-862: Missing Authorization (p.1789)
-  CWE-434: Unrestricted Upload of File with Dangerous Type (p.1055)
-  CWE-94: Improper Control of Generation of Code ('Code Injection') (p.225)
-  CWE-20: Improper Input Validation (p.20)
-  CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') (p.148)
-  CWE-287: Improper Authentication (p.699)
-  CWE-269: Improper Privilege Management (p.653)
-  CWE-502: Deserialization of Untrusted Data (p.1212)
-  CWE-200: Exposure of Sensitive Information to an Unauthorized Actor (p.511)
-  CWE-863: Incorrect Authorization (p.1796)
-  CWE-918: Server-Side Request Forgery (SSRF) (p.1829)
-  CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer (p.299)
-  CWE-476: NULL Pointer Dereference (p.1139)
-  CWE-798: Use of Hard-coded Credentials (p.1699)
-  CWE-190: Integer Overflow or Wraparound (p.478)
-  CWE-400: Uncontrolled Resource Consumption (p.971)
-  CWE-306: Missing Authentication for Critical Function (p.748)

Deprecated

CWE-1: DEPRECATED: Location

CWE ID : 1

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-3: DEPRECATED: Technology-specific Environment Issues

CWE ID : 3

Summary

This category has been deprecated. It was originally intended as a "catch-all" for environment issues for technologies that did not have their own CWE, but it introduced unnecessary depth and complexity to the Development View (CWE-699).

CWE-4: DEPRECATED: J2EE Environment Issues

CWE ID : 4

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-10: DEPRECATED: ASP.NET Environment Issues

CWE ID : 10

Summary

This category has been deprecated. It added unnecessary depth and complexity to its associated views.

CWE-17: DEPRECATED: Code

CWE ID : 17

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-18: DEPRECATED: Source Code

CWE ID : 18

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-21: DEPRECATED: Pathname Traversal and Equivalence Errors

CWE ID : 21

Summary

This category has been deprecated. It was originally used for organizing weaknesses involving file names, which enabled access to files outside of a restricted directory (path traversal) or to perform operations on files that would otherwise be restricted (path equivalence). Consider using either the File Handling Issues category (CWE-1219) or the class Use of Incorrectly-Resolved Name or Reference (CWE-706).

CWE-60: DEPRECATED: UNIX Path Link Problems

CWE ID : 60

Summary

This category has been deprecated. It covered a very low level of abstraction based on operating system, which was not useful for any existing view.

CWE-63: DEPRECATED: Windows Path Link Problems

CWE ID : 63

Summary

This category has been deprecated. It covered a very low level of abstraction based on operating system, which was not useful for any existing view.

CWE-68: DEPRECATED: Windows Virtual File Problems

CWE ID : 68

Summary

This category has been deprecated as it was found to be an unnecessary abstraction of platform specific details. Please refer to the category CWE-632 and weakness CWE-66 for relevant relationships.

CWE-70: DEPRECATED: Mac Virtual File Problems

CWE ID : 70

Summary

This category has been deprecated as it was found to be an unnecessary abstraction of platform specific details. Please refer to the category CWE-632 and weakness CWE-66 for relevant relationships.

CWE-71: DEPRECATED: Apple '.DS_Store'

CWE ID : 71

Description

This entry has been deprecated as it represents a specific observed example of a UNIX Hard Link weakness type rather than its own individual weakness type. Please refer to CWE-62.

CWE-92: DEPRECATED: Improper Sanitization of Custom Special Characters

CWE ID : 92

Description

This entry has been deprecated. It originally came from PLOVER, which sometimes defined "other" and "miscellaneous" categories in order to satisfy exhaustiveness requirements for taxonomies. Within the context of CWE, the use of a more abstract entry is preferred in mapping situations. CWE-75 is a more appropriate mapping.

CWE-100: DEPRECATED: Technology-Specific Input Validation Problems

CWE ID : 100

Summary

This category has been deprecated. It was originally intended as a "catch-all" for input validation problems in technologies that did not have their own CWE, but introduces unnecessary depth to the hierarchy.

CWE-101: DEPRECATED: Struts Validation Problems

CWE ID : 101

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-132: DEPRECATED: Miscalculated Null Termination

CWE ID : 132

CWE-71: DEPRECATED: Apple '.DS_Store'

Description

This entry has been deprecated because it was a duplicate of CWE-170. All content has been transferred to CWE-170.

CWE-139: DEPRECATED: General Special Element Problems

CWE ID : 139

Summary

This entry has been deprecated. It is a leftover from PLOVER, but CWE-138 is a more appropriate mapping.

CWE-169: DEPRECATED: Technology-Specific Special Elements

CWE ID : 169

Summary

This category has been deprecated. It was originally intended as a "catch-all" for input validation problems in technologies that did not have their own CWE, but introduces unnecessary depth to the hierarchy.

CWE-171: DEPRECATED: Cleansing, Canonicalization, and Comparison Errors

CWE ID : 171

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree. Weaknesses in this category were related to improper handling of data within protection mechanisms that attempt to perform neutralization for untrusted data. These weaknesses can be found in other similar categories.

CWE-216: DEPRECATED: Containment Errors (Container Errors)

CWE ID : 216

Description

This entry has been deprecated, as it was not effective as a weakness and was structured more like a category. In addition, the name is inappropriate, since the "container" term is widely understood by developers in different ways than originally intended by PLOVER, the original source for this entry.

CWE-217: DEPRECATED: Failure to Protect Stored Data from Modification

CWE ID : 217

Description

This entry has been deprecated because it incorporated and confused multiple weaknesses. The issues formerly covered in this entry can be found at CWE-766 and CWE-767.

CWE-218: DEPRECATED: Failure to provide confidentiality for stored data

CWE ID : 218

Description

This weakness has been deprecated because it was a duplicate of CWE-493. All content has been transferred to CWE-493.

CWE-225: DEPRECATED: General Information Management Problems

CWE ID : 225

Description

This weakness can be found at CWE-199.

CWE-247: DEPRECATED: Reliance on DNS Lookups in a Security Decision

CWE ID : 247

Description

This entry has been deprecated because it was a duplicate of CWE-350. All content has been transferred to CWE-350.

CWE-249: DEPRECATED: Often Misused: Path Manipulation

CWE ID : 249

Description

This entry has been deprecated because of name confusion and an accidental combination of multiple weaknesses. Most of its content has been transferred to CWE-785.

CWE-292: DEPRECATED: Trusting Self-reported DNS Name

CWE ID : 292

Description

This entry has been deprecated because it was a duplicate of CWE-350. All content has been transferred to CWE-350.

CWE-365: DEPRECATED: Race Condition in Switch

CWE ID : 365

Description

This entry has been deprecated. There are no documented cases in which a switch's control expression is evaluated more than once.

CWE-373: DEPRECATED: State Synchronization Error

CWE ID : 373

Description

This entry was deprecated because it overlapped the same concepts as race condition (CWE-362) and Improper Synchronization (CWE-662).

CWE-376: DEPRECATED: Temporary File Issues

CWE ID : 376

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree. Consider using the File Handling Issues category (CWE-1219).

CWE-380: DEPRECATED: Technology-Specific Time and State Issues

CWE ID : 380

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-381: DEPRECATED: J2EE Time and State Issues

CWE ID : 381

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-418: DEPRECATED: Channel Errors

CWE ID : 418

Summary

2762

This category has been deprecated because it redundant with the grouping provided by CWE-417.

CWE-423: DEPRECATED: Proxied Trusted Channel

CWE ID : 423

Description

This entry has been deprecated because it was a duplicate of CWE-441. All content has been transferred to CWE-441.

CWE-442: DEPRECATED: Web Problems

CWE ID : 442

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-443: DEPRECATED: HTTP response splitting

CWE ID : 443

Description

This weakness can be found at CWE-113.

CWE-445: DEPRECATED: User Interface Errors

CWE ID : 445

Summary

This weakness has been deprecated because it was a duplicate of CWE-355. All content has been transferred to CWE-355.

CWE-458: DEPRECATED: Incorrect Initialization

CWE ID : 458

Description

This weakness has been deprecated because its name and description did not match. The description duplicated CWE-454, while the name suggested a more abstract initialization problem. Please refer to CWE-665 for the more abstract problem.

CWE-461: DEPRECATED: Data Structure Issues

CWE ID : 461

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-490: DEPRECATED: Mobile Code Issues

CWE ID : 490

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-503: DEPRECATED: Byte/Object Code

CWE ID : 503

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-504: DEPRECATED: Motivation/Intent

CWE ID : 504

Summary

This category has been deprecated. It was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-505: DEPRECATED: Intentionally Introduced Weakness

CWE ID : 505

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-513: DEPRECATED: Intentionally Introduced Nonmalicious Weakness

CWE ID : 513

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-516: DEPRECATED: Covert Timing Channel

CWE ID : 516

Description

This weakness can be found at CWE-385.

CWE-517: DEPRECATED: Other Intentional, Nonmalicious Weakness

CWE ID : 517

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-518: DEPRECATED: Inadvertently Introduced Weakness

CWE ID : 518

Summary

This category has been deprecated as it was originally used for organizing the Development View (CWE-699), but it introduced unnecessary complexity and depth to the resulting tree.

CWE-519: DEPRECATED: .NET Environment Issues

CWE ID : 519

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-533: DEPRECATED: Information Exposure Through Server Log Files

CWE ID : 533

Description

This entry has been deprecated because its abstraction was too low-level. See CWE-532.

CWE-534: DEPRECATED: Information Exposure Through Debug Log Files

CWE ID : 534

Description

This entry has been deprecated because its abstraction was too low-level. See CWE-532.

CWE-542: DEPRECATED: Information Exposure Through Cleanup Log Files

CWE ID : 542

Description

This entry has been deprecated because its abstraction was too low-level. See CWE-532.

CWE-545: DEPRECATED: Use of Dynamic Class Loading

CWE ID : 545

Description

This weakness has been deprecated because it partially overlaps CWE-470, it describes legitimate programmer behavior, and other portions will need to be integrated into other entries.

CWE-559: DEPRECATED: Often Misused: Arguments and Parameters

CWE ID : 559

Summary

This entry has been deprecated. It was originally used for organizing the Development View (CWE-699) and some other views, but it introduced unnecessary complexity and depth to the resulting tree.

CWE-592: DEPRECATED: Authentication Bypass Issues

CWE ID : 592

Description

This weakness has been deprecated because it covered redundant concepts already described in CWE-287.

CWE-596: DEPRECATED: Incorrect Semantic Object Comparison

CWE ID : 596

Description

This weakness has been deprecated. It was poorly described and difficult to distinguish from other entries. It was also inappropriate to assign a separate ID solely because of domain-specific considerations. Its closest equivalent is CWE-1023.

CWE-630: DEPRECATED: Weaknesses Examined by SAMATE

CWE ID : 630

Objective

This view has been deprecated. It was only used for an early year of the NIST SAMATE project, and it did not represent any official or commonly-utilized list.

CWE-631: DEPRECATED: Resource-specific Weaknesses

CWE ID : 631

Objective

This view has been deprecated because it is not actively maintained and does not provide utility to stakeholders. It was originally created before CWE 1.0 as a simple example of how views could be structured within CWE.

CWE-632: DEPRECATED: Weaknesses that Affect Files or Directories

CWE ID : 632

Summary

This category has been deprecated. It was not actively maintained, and it was not useful to stakeholders. It was originally created before CWE 1.0 as part of view CWE-631, which was a simple example of how views could be structured within CWE.

CWE-633: DEPRECATED: Weaknesses that Affect Memory

CWE ID : 633

Summary

This category has been deprecated. It was not actively maintained, and it was not useful to stakeholders. It was originally created before CWE 1.0 as part of view CWE-631, which was a simple example of how views could be structured within CWE.

CWE-634: DEPRECATED: Weaknesses that Affect System Processes

CWE ID : 634

Summary

This category has been deprecated. It was not actively maintained, and it was not useful to stakeholders. It was originally created before CWE 1.0 as part of view CWE-631, which was a simple example of how views could be structured within CWE.

CWE-679: DEPRECATED: Chain Elements

CWE ID : 679

Objective

This view has been deprecated. It has limited utility for stakeholders, since all weaknesses can be links in a chain.

CWE-769: DEPRECATED: Uncontrolled File Descriptor Consumption

CWE ID : 769

Description

This entry has been deprecated because it was a duplicate of CWE-774. All content has been transferred to CWE-774.

CWE-999: DEPRECATED: Weaknesses without Software Fault Patterns

CWE ID : 999

Objective

This view has been deprecated. It was based on gaps in another view (CWE-888) related to research that is no longer updated, but was complete with respect to CWE at the time it was conducted.

CWE-1187: DEPRECATED: Use of Uninitialized Resource

CWE ID : 1187

Description

This entry has been deprecated because it was a duplicate of CWE-908. All content has been transferred to CWE-908.

CWE-1324: DEPRECATED: Sensitive Information Accessible by Physical Probing of JTAG Interface

CWE ID : 1324

Description

This entry has been deprecated because it was at a lower level of abstraction than supported by CWE. All relevant content has been integrated into CWE-319.

Glossary

Index

A

Absolute Path Traversal, 75
 Acceptance of Extraneous Untrusted Data With Trusted Data, 868
 Access Control Check Implemented After Asset is Accessed, 2134
 Access of Memory Location After End of Buffer, 1678
 Access of Memory Location Before Start of Buffer, 1666
 Access of Resource Using Incompatible Type ('Type Confusion'), 1785
 Access of Uninitialized Pointer, 1738
 Access to Critical Private Variable via Public Method, 1619
 Active Debug Code, 1178
 Addition of Data Structure Sentinel, 1115
 Allocation of File Descriptors or Handles Without Limits or Throttling, 1639
 Allocation of Resources Without Limits or Throttling, 1622
 Always-Incorrect Control Flow Implementation, 1484
 API / Function Errors, 2503
 Application-Level Admin Tool with Inconsistent View of Underlying Operating System, 2062
 Architectural Concepts, 2598(*Graph*: 2699)
 Architecture with Number of Horizontal Layers Outside of Expected Range, 1888
 Array Declared Public, Final, and Static, 1322
 ASP.NET Misconfiguration: Creating Debug Binary, 9
 ASP.NET Misconfiguration: Improper Model Validation, 1979
 ASP.NET Misconfiguration: Missing Custom Error Page, 11
 ASP.NET Misconfiguration: Not Using Input Validation Framework, 1278
 ASP.NET Misconfiguration: Password in Configuration File, 13
 ASP.NET Misconfiguration: Use of Identity Impersonation, 1280
 Assigning instead of Comparing, 1161
 Assignment of a Fixed Address to a Pointer, 1330
 Assignment to Variable without Use, 1289
 Assumed-Immutable Data is Stored in Writable Memory, 2139
 Asymmetric Resource Consumption (Amplification), 993
 Attempt to Access Child of a Non-structure Pointer, 1332
 Audit, 2445
 Audit / Logging Errors, 2496
 Authenticate Actors, 2445
 Authentication Bypass by Alternate Name, 710
 Authentication Bypass by Assumed-Immutable Data, 742
 Authentication Bypass by Capture-replay, 719
 Authentication Bypass by Primary Weakness, 747
 Authentication Bypass by Spoofing, 712
 Authentication Bypass Using an Alternate Path or Channel, 707
 Authentication Bypass: OpenSSL CTX Object Modified after SSL Objects are Created, 1339
 Authentication Errors, 2496
 Authorization Bypass Through User-Controlled Key, 1415
 Authorization Bypass Through User-Controlled SQL Primary Key, 1294
 Authorization Errors, 2497
 Authorize Actors, 2446
 Automated Recognition Mechanism with Inadequate Detection or Handling of Adversarial Input Perturbations, 1882

B

Bad Coding Practices, 2443

Behavioral Change in New Version or Environment, 1068
 Behavioral Problems, 2348
 Binding to an Unrestricted IP Address, 2227
 Buffer Access Using Size of Source Buffer, 1719
 Buffer Access with Incorrect Length Value, 1711
 Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'), 310
 Buffer Over-read, 340
 Buffer Under-read, 343
 Buffer Underwrite ('Buffer Underflow'), 332
 Business Logic Errors, 2381

C

Call to Non-ubiquitous API, 1333
 Call to Thread run() instead of start(), 1305
 Callable with Insufficient Behavioral Summary, 1966
 CERT C Secure Coding Standard (2008) Appendix - POSIX (POS), 2372
 CERT C Secure Coding Standard (2008) Chapter 10 - Input Output (FIO), 2368
 CERT C Secure Coding Standard (2008) Chapter 11 - Environment (ENV), 2369
 CERT C Secure Coding Standard (2008) Chapter 12 - Signals (SIG), 2370
 CERT C Secure Coding Standard (2008) Chapter 13 - Error Handling (ERR), 2371
 CERT C Secure Coding Standard (2008) Chapter 14 - Miscellaneous (MSC), 2371
 CERT C Secure Coding Standard (2008) Chapter 2 - Preprocessor (PRE), 2361
 CERT C Secure Coding Standard (2008) Chapter 3 - Declarations and Initialization (DCL), 2362
 CERT C Secure Coding Standard (2008) Chapter 4 - Expressions (EXP), 2362
 CERT C Secure Coding Standard (2008) Chapter 5 - Integers (INT), 2363
 CERT C Secure Coding Standard (2008) Chapter 6 - Floating Point (FLP), 2364
 CERT C Secure Coding Standard (2008) Chapter 7 - Arrays (ARR), 2365
 CERT C Secure Coding Standard (2008) Chapter 8 - Characters and Strings (STR), 2366
 CERT C Secure Coding Standard (2008) Chapter 9 - Memory Management (MEM), 2367
 CERT C++ Secure Coding Section 01 - Preprocessor (PRE), 2394
 CERT C++ Secure Coding Section 02 - Declarations and Initialization (DCL), 2395
 CERT C++ Secure Coding Section 03 - Expressions (EXP), 2395
 CERT C++ Secure Coding Section 04 - Integers (INT), 2395
 CERT C++ Secure Coding Section 05 - Floating Point Arithmetic (FLP), 2396
 CERT C++ Secure Coding Section 06 - Arrays and the STL (ARR), 2396
 CERT C++ Secure Coding Section 07 - Characters and Strings (STR), 2397
 CERT C++ Secure Coding Section 08 - Memory Management (MEM), 2398
 CERT C++ Secure Coding Section 09 - Input Output (FIO), 2398
 CERT C++ Secure Coding Section 10 - Environment (ENV), 2399
 CERT C++ Secure Coding Section 11 - Signals (SIG), 2400
 CERT C++ Secure Coding Section 12 - Exceptions and Error Handling (ERR), 2400

- CERT C++ Secure Coding Section 13 - Object Oriented Programming (OOP), 2401
- CERT C++ Secure Coding Section 14 - Concurrency (CON), 2401
- CERT C++ Secure Coding Section 49 - Miscellaneous (MSC), 2402
- Channel Accessible by Non-Endpoint, 737
- CISQ Data Protection Measures, 2611(*Graph: 2724*)
- CISQ Quality Measures (2016), 2602(*Graph: 2706*)
- CISQ Quality Measures (2016) - Maintainability, 2462
- CISQ Quality Measures (2016) - Performance Efficiency, 2464
- CISQ Quality Measures (2016) - Reliability, 2461
- CISQ Quality Measures (2016) - Security, 2463
- CISQ Quality Measures (2020), 2609(*Graph: 2719*)
- CISQ Quality Measures - Efficiency, 2507
- CISQ Quality Measures - Maintainability, 2505
- CISQ Quality Measures - Reliability, 2504
- CISQ Quality Measures - Security, 2506
- Class Instance Self Destruction Control Element, 1931
- Class with Excessive Number of Child Classes, 1935
- Class with Excessively Deep Inheritance, 1923
- Class with Virtual Method without a Virtual Destructor, 1936
- Cleartext Storage in a File or on Disk, 777
- Cleartext Storage in the Registry, 779
- Cleartext Storage of Sensitive Information, 771
- Cleartext Storage of Sensitive Information in a Cookie, 781
- Cleartext Storage of Sensitive Information in an Environment Variable, 1243
- Cleartext Storage of Sensitive Information in Executable, 785
- Cleartext Storage of Sensitive Information in GUI, 784
- Cleartext Storage of Sensitive Information in Memory, 782
- Cleartext Transmission of Sensitive Information, 786
- Client-Side Enforcement of Server-Side Security, 1359
- clone() Method Without super.clone(), 1319
- Cloneable Class Containing Sensitive Information, 1204
- Collapse of Data into Unsafe Value, 462
- Command Shell in Externally Accessible Directory, 1277
- Communication Channel Errors, 2347
- Comparing instead of Assigning, 1165
- Comparison Logic is Vulnerable to Power Side-Channel Attacks, 2073
- Comparison of Classes by Name, 1172
- Comparison of Incompatible Types, 1877
- Comparison of Object References Instead of Object Contents, 1342
- Comparison Using Wrong Factors, 1878
- Compilation with Insufficient Warnings or Errors, 1976
- Compiler Optimization Removal or Modification of Security-critical Code, 1570
- Compiler Removal of Code to Clear Buffers, 14
- Complexity Issues, 2502
- Composites, 2576
- Comprehensive Categorization for Software Assurance Trends, 2619(*Graph: 2736*)
- Comprehensive Categorization: Access Control, 2540
- Comprehensive Categorization: Comparison, 2544
- Comprehensive Categorization: Component Interaction, 2545
- Comprehensive Categorization: Concurrency, 2547
- Comprehensive Categorization: Encryption, 2548
- Comprehensive Categorization: Exposed Resource, 2549
- Comprehensive Categorization: File Handling, 2550
- Comprehensive Categorization: Improper Check or Handling of Exceptional Conditions, 2552
- Comprehensive Categorization: Improper Input Validation, 2552
- Comprehensive Categorization: Improper Neutralization, 2553
- Comprehensive Categorization: Incorrect Calculation, 2555
- Comprehensive Categorization: Injection, 2556
- Comprehensive Categorization: Insufficient Control Flow Management, 2557
- Comprehensive Categorization: Insufficient Verification of Data Authenticity, 2559
- Comprehensive Categorization: Memory Safety, 2546
- Comprehensive Categorization: Poor Coding Practices, 2559
- Comprehensive Categorization: Protection Mechanism Failure, 2563
- Comprehensive Categorization: Randomness, 2564
- Comprehensive Categorization: Resource Control, 2565
- Comprehensive Categorization: Resource Lifecycle Management, 2566
- Comprehensive Categorization: Sensitive Information Exposure, 2569
- Comprehensive Categorization: Violation of Secure Design Principles, 2570
- Comprehensive CWE Dictionary, 2624
- Concurrency Issues, 2350
- Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition'), 895
- Configuration, 2330
- Context Switching Race Condition, 918
- Core and Compute Issues, 2492
- Covert Channel, 1227
- Covert Storage Channel, 1229
- Covert Timing Channel, 947
- CPU Hardware Not Configured to Support Exclusivity of Write and Execute Operations, 2068
- Creation of chroot Jail Without Changing Working Directory, 596
- Creation of Class Instance within a Static Code Block, 1910
- Creation of Emergent Resource, 2016
- Creation of Immutable Text Using String Concatenation, 1890
- Creation of Temporary File in Directory with Insecure Permissions, 937
- Creation of Temporary File With Insecure Permissions, 935
- Credentials Management Errors, 2336
- Critical Data Element Declared Public, 1615
- Critical Public Variable Without Final Modifier, 1190
- Cross Cutting, 2448
- Cross-Cutting Problems, 2495
- Cross-Site Request Forgery (CSRF), 875
- Cryptographic Issues, 2339
- Cryptographic Operations are run Before Supporting Units are Ready, 2132
- CWE Cross-section, 2588
- ## D
- Dangerous Signal Handler not Disabled During Sensitive Operations, 1052
- Dangling Database Cursor ('Cursor Injection'), 1391
- Data Access from Outside Expected Data Manager Component, 1932
- Data Access Operations Outside of Expected Data Manager Component, 1902
- Data Element Aggregating an Excessively Large Number of Non-Primitive Elements, 1887
- Data Element containing Pointer Item without Proper Copy Control Element, 1947
- Data Integrity Issues, 2498
- Data Neutralization Issues, 2332
- Data Processing Errors, 2330

Data Resource Access without Use of Connection Pooling, 1921
 Data Validation Issues, 2499
 Dead Code, 1283
 Deadlock, 1762
 Debug and Test Problems, 2495
 Debug Messages Revealing Unnecessary Information, 2164
 Declaration of Catch for Generic Exception, 966
 Declaration of Throws for Generic Exception, 968
 Declaration of Variable with Unnecessarily Wide Scope, 1975
 Deletion of Data Structure Sentinel, 1113
 Dependency on Vulnerable Third-Party Component, 2289
 Deployment of Wrong Handler, 1049
 Deprecated Entries, 2571
 DEPRECATED: Apple '.DS_Store', 2759
 DEPRECATED: ASP.NET Environment Issues, 2757
 DEPRECATED: Authentication Bypass Issues, 2766
 DEPRECATED: Byte/Object Code, 2764
 DEPRECATED: Chain Elements, 2767
 DEPRECATED: Channel Errors, 2762
 DEPRECATED: Cleansing, Canonicalization, and Comparison Errors, 2760
 DEPRECATED: Code, 2757
 DEPRECATED: Containment Errors (Container Errors), 2760
 DEPRECATED: Covert Timing Channel, 2765
 DEPRECATED: Data Structure Issues, 2763
 DEPRECATED: Failure to Protect Stored Data from Modification, 2760
 DEPRECATED: Failure to provide confidentiality for stored data, 2761
 DEPRECATED: General Information Management Problems, 2761
 DEPRECATED: General Special Element Problems, 2760
 DEPRECATED: HTTP response splitting, 2763
 DEPRECATED: Improper Sanitization of Custom Special Characters, 2759
 DEPRECATED: Inadvertently Introduced Weakness, 2765
 DEPRECATED: Incorrect Initialization, 2763
 DEPRECATED: Incorrect Semantic Object Comparison, 2766
 DEPRECATED: Information Exposure Through Cleanup Log Files, 2766
 DEPRECATED: Information Exposure Through Debug Log Files, 2765
 DEPRECATED: Information Exposure Through Server Log Files, 2765
 DEPRECATED: Intentionally Introduced Nonmalicious Weakness, 2764
 DEPRECATED: Intentionally Introduced Weakness, 2764
 DEPRECATED: J2EE Environment Issues, 2757
 DEPRECATED: J2EE Time and State Issues, 2762
 DEPRECATED: Location, 2757
 DEPRECATED: Mac Virtual File Problems, 2758
 DEPRECATED: Miscalculated Null Termination, 2759
 DEPRECATED: Mobile Code Issues, 2764
 DEPRECATED: Motivation/Intent, 2764
 DEPRECATED: .NET Environment Issues, 2765
 DEPRECATED: Often Misused: Arguments and Parameters, 2766
 DEPRECATED: Often Misused: Path Manipulation, 2761
 DEPRECATED: Other Intentional, Nonmalicious Weakness, 2765
 DEPRECATED: Pathname Traversal and Equivalence Errors, 2758
 DEPRECATED: Proxied Trusted Channel, 2763
 DEPRECATED: Race Condition in Switch, 2761
 DEPRECATED: Reliance on DNS Lookups in a Security Decision, 2761
 DEPRECATED: Resource-specific Weaknesses, 2767 (*Graph: 2626*)
 DEPRECATED: Sensitive Information Accessible by Physical Probing of JTAG Interface, 2768
 DEPRECATED: Source Code, 2758
 DEPRECATED: State Synchronization Error, 2762
 DEPRECATED: Struts Validation Problems, 2759
 DEPRECATED: Technology-specific Environment Issues, 2757
 DEPRECATED: Technology-Specific Input Validation Problems, 2759
 DEPRECATED: Technology-Specific Special Elements, 2760
 DEPRECATED: Technology-Specific Time and State Issues, 2762
 DEPRECATED: Temporary File Issues, 2762
 DEPRECATED: Trusting Self-reported DNS Name, 2761
 DEPRECATED: Uncontrolled File Descriptor Consumption, 2768
 DEPRECATED: UNIX Path Link Problems, 2758
 DEPRECATED: Use of Dynamic Class Loading, 2766
 DEPRECATED: Use of Uninitialized Resource, 2768
 DEPRECATED: User Interface Errors, 2763
 DEPRECATED: Weaknesses Examined by SAMATE, 2767
 DEPRECATED: Weaknesses that Affect Files or Directories, 2767
 DEPRECATED: Weaknesses that Affect Memory, 2767
 DEPRECATED: Weaknesses that Affect System Processes, 2767
 DEPRECATED: Weaknesses without Software Fault Patterns, 2768
 DEPRECATED: Web Problems, 2763
 DEPRECATED: Windows Path Link Problems, 2758
 DEPRECATED: Windows Virtual File Problems, 2758
 Deserialization of Untrusted Data, 1212
 Detection of Error Condition Without Action, 950
 Device Unlock Credential Sharing, 2119
 Direct Request ('Forced Browsing'), 1032
 Direct Use of Unsafe JNI, 272
 Divide By Zero, 920
 DMA Device Enabled Too Early in Boot Phase, 1987
 Documentation Issues, 2501
 Double Decoding of the Same Data, 443
 Double Free, 1015
 Double-Checked Locking, 1371
 Doubled Character XSS Manipulations, 192
 Download of Code Without Integrity Check, 1192
 Duplicate Key in Associative List (Alist), 1111
 Dynamic Variable Evaluation, 1405

E

EJB Bad Practices: Use of AWT Swing, 1310
 EJB Bad Practices: Use of Class Loader, 1316
 EJB Bad Practices: Use of Java I/O, 1312
 EJB Bad Practices: Use of Sockets, 1314
 EJB Bad Practices: Use of Synchronization Primitives, 1308
 Embedded Malicious Code, 1218
 Empty Code Block, 1919
 Empty Exception Block, 1916
 Empty Password in Configuration File, 628
 Empty Synchronized Block, 1327
 Encapsulation Issues, 2502
 Encoding Error, 439
 Encrypt Data, 2449
 Entries with Maintenance Notes, 2601
 Error Conditions, Return Values, Status Codes, 2344

- Excessive Attack Surface, 1974
 - Excessive Code Complexity, 1969
 - Excessive Data Query Operations in a Large Data Table, 1894
 - Excessive Execution of Sequential Searches of Data Resource, 1914
 - Excessive Halstead Complexity, 1971
 - Excessive Index Range Scan for a Data Resource, 1943
 - Excessive Iteration, 1763
 - Excessive McCabe Cyclomatic Complexity, 1970
 - Excessive Number of Inefficient Server-Side Data Accesses, 1906
 - Excessive Platform Resource Consumption within a Loop, 1895
 - Excessive Reliance on Global Variables, 1957
 - Excessive Use of Hard-Coded Literals in Initialization, 1897
 - Excessive Use of Self-Modifying Code, 1972
 - Excessive Use of Unconditional Branching, 1968
 - Excessively Complex Data Representation, 1942
 - Excessively Deep Nesting, 1973
 - Executable Regular Expression Error, 1399
 - Execution After Redirect (EAR), 1542
 - Execution with Unnecessary Privileges, 606
 - Expected Behavior Violation, 1069
 - Expired Pointer Dereference, 1741
 - Explicit Call to Finalize(), 1329
 - Exposed Dangerous Method or Function, 1572
 - Exposed IOCTL with Insufficient Access Control, 1657
 - Exposed Unsafe ActiveX Method, 1389
 - Exposure of Access Control List Files to an Unauthorized Control Sphere, 1247
 - Exposure of Backup File to an Unauthorized Control Sphere, 1248
 - Exposure of Core Dump File to an Unauthorized Control Sphere, 1246
 - Exposure of Data Element to Wrong Session, 1176
 - Exposure of File Descriptor to Unintended Control Sphere ('File Descriptor Leak'), 985
 - Exposure of Information Through Directory Listing, 1269
 - Exposure of Information Through Shell Error Message, 1253
 - Exposure of Private Personal Information to an Unauthorized Actor, 889
 - Exposure of Resource to Wrong Sphere, 1478
 - Exposure of Sensitive Information caused by Incorrect Data Forwarding during Transient Execution, 2310
 - Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution, 2316
 - Exposure of Sensitive Information Due to Incompatible Policies, 555
 - Exposure of Sensitive Information during Transient Execution, 2297
 - Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution, 2304
 - Exposure of Sensitive Information Through Data Queries, 523
 - Exposure of Sensitive Information Through Metadata, 2017
 - Exposure of Sensitive Information to an Unauthorized Actor, 511
 - Exposure of Sensitive System Information Due to Uncleared Debug Information, 2082
 - Exposure of Sensitive System Information to an Unauthorized Control Sphere, 1201
 - Exposure of Version-Control Repository to an Unauthorized Control Sphere, 1245
 - Exposure of WSDL File Containing Sensitive Information, 1442
 - Expression is Always False, 1300
 - Expression is Always True, 1303
 - Expression Issues, 2351
 - External Control of Assumed-Immutable Web Parameter, 1131
 - External Control of Critical State Data, 1422
 - External Control of File Name or Path, 133
 - External Control of System or Configuration Setting, 17
 - External Influence of Sphere Definition, 1492
 - External Initialization of Trusted Variables or Data Stores, 1092
 - Externally Controlled Reference to a Resource in Another Sphere, 1373
 - Externally-Generated Error Message Containing Sensitive Information, 548
- ## F
- Fabric-Address Map Allows Programming of Unwarranted Overlaps of Protected and Unprotected Ranges, 2204
 - Failure to Disable Reserved Bits, 2000
 - Failure to Handle Incomplete Element, 589
 - Failure to Handle Missing Parameter, 583
 - Failure to Sanitize Paired Delimiters, 413
 - Failure to Sanitize Special Elements into a Different Plane (Special Element Injection), 145
 - File Handling Issues, 2501
 - Files or Directories Accessible to External Parties, 1274
 - finalize() Method Declared Public, 1324
 - finalize() Method Without super.finalize(), 1299
 - Firmware Not Updateable, 2128
 - Floating Point Comparison with Incorrect Operator, 1926
 - Free of Memory not on the Heap, 1335
 - Free of Pointer not at Start of Buffer, 1601
 - Function Call With Incorrect Argument Type, 1517
 - Function Call With Incorrect Number of Arguments, 1516
 - Function Call With Incorrect Order of Arguments, 1512
 - Function Call With Incorrect Variable or Reference as Argument, 1520
 - Function Call With Incorrectly Specified Argument Value, 1518
 - Function Call with Incorrectly Specified Arguments, 1407
- ## G
- General Circuit and Logic Design Concerns, 2492
 - Generation of Error Message Containing Sensitive Information, 540
 - Generation of Incorrect Security Tokens, 2113
 - Generation of Predictable IV with CBC Mode, 818
 - Generation of Predictable Numbers or Identifiers, 849
 - Generation of Weak Initialization Vector (IV), 1996
 - Guessable CAPTCHA, 1710
- ## H
- Handler Errors, 2347
 - Hardware Allows Activation of Test or Debug Logic at Runtime, 2198
 - Hardware Child Block Incorrectly Connected to Parent System, 2125
 - Hardware Design, 2607(*Graph*: 2715)
 - Hardware Internal or Debug Modes Allow Override of Locks, 2026
 - Hardware Logic Contains Race Conditions, 2170
 - Hardware Logic with Insecure De-Synchronization between Control and Data Channels, 2098
 - Heap-based Buffer Overflow, 324
 - Hidden Functionality, 1812
- ## I
- ICS Communications, 2518
 - ICS Communications: Frail Security in Protocols, 2524
 - ICS Communications: Unreliability, 2523

ICS Communications: Zone Boundary Failures, 2522
 ICS Dependencies (& Architecture), 2519
 ICS Dependencies (& Architecture): External Digital Systems, 2526
 ICS Dependencies (& Architecture): External Physical Systems, 2525
 ICS Engineering (Construction/Deployment): Gaps in Details/Data, 2532
 ICS Engineering (Construction/Deployment): Inherent Predictability in Design, 2534
 ICS Engineering (Construction/Deployment): Maker Breaker Blindness, 2531
 ICS Engineering (Construction/Deployment): Security Gaps in Commissioning, 2533
 ICS Engineering (Construction/Deployment): Trust Model Problems, 2531
 ICS Engineering (Constructions/Deployment), 2520
 ICS Operations (& Maintenance), 2521
 ICS Operations (& Maintenance): Compliance/Conformance with Regulatory Requirements, 2538
 ICS Operations (& Maintenance): Emerging Energy Technologies, 2538
 ICS Operations (& Maintenance): Exploitable Standard Operational Procedures, 2537
 ICS Operations (& Maintenance): Gaps in obligations and training, 2534
 ICS Operations (& Maintenance): Human factors in ICS environments, 2535
 ICS Operations (& Maintenance): Post-analysis changes, 2536
 ICS Supply Chain, 2520
 ICS Supply Chain: Common Mode Frailties, 2528
 ICS Supply Chain: IT/OT Convergence/Expansion, 2527
 ICS Supply Chain: OT Counterfeit and Malicious Corruption, 2530
 ICS Supply Chain: Poorly Documented or Undocumented Features, 2529
 Identify Actors, 2450
 Improper Access Control, 687
 Improper Access Control Applied to Mirrored or Aliased Memory Regions, 2079
 Improper Access Control for Register Interface, 2093
 Improper Access Control for Volatile Memory Containing Boot Code, 2121
 Improper Access Control in Fabric Bridge, 2206
 Improper Address Validation in IOCTL with METHOD_NEITHER I/O Control Code, 1654
 Improper Adherence to Coding Standards, 1558
 Improper Authentication, 699
 Improper Authorization, 691
 Improper Authorization in Handler for Custom URL Scheme, 1849
 Improper Authorization of Index Containing Sensitive Information, 1379
 Improper Certificate Validation, 721
 Improper Check for Certificate Revocation, 734
 Improper Check for Dropped Privileges, 667
 Improper Check for Unusual or Exceptional Conditions, 1577
 Improper Check or Handling of Exceptional Conditions, 1544
 Improper Cleanup on Thrown Exception, 1109
 Improper Clearing of Heap Memory Before Release ('Heap Inspection'), 598
 Improper Control of a Resource Through its Lifetime, 1463
 Improper Control of Document Type Definition, 1745
 Improper Control of Dynamically-Identified Variables, 1816
 Improper Control of Dynamically-Managed Code Resources, 1814
 Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion'), 242
 Improper Control of Generation of Code ('Code Injection'), 225
 Improper Control of Interaction Frequency, 1708
 Improper Control of Resource Identifiers ('Resource Injection'), 249
 Improper Encoding or Escaping of Output, 287
 Improper Enforcement of a Single, Unique Action, 1771
 Improper Enforcement of Behavioral Workflow, 1781
 Improper Enforcement of Message Integrity During Transmission in a Communication Channel, 1839
 Improper Export of Android Application Components, 1843
 Improper Filtering of Special Elements, 1687
 Improper Finite State Machines (FSMs) in Hardware Logic, 2052
 Improper Following of a Certificate's Chain of Trust, 726
 Improper Following of Specification by Caller, 1307
 Improper Handling of Additional Special Element, 431
 Improper Handling of Alternate Encoding, 441
 Improper Handling of Apple HFS+ Alternate Data Stream Path, 131
 Improper Handling of Case Sensitivity, 451
 Improper Handling of Exceptional Conditions, 1585
 Improper Handling of Extra Parameters, 585
 Improper Handling of Extra Values, 579
 Improper Handling of Faults that Lead to Instruction Skips, 2240
 Improper Handling of File Names that Identify Virtual Resources, 125
 Improper Handling of Hardware Behavior in Exceptionally Cold Environments, 2265
 Improper Handling of Highly Compressed Data (Data Amplification), 1004
 Improper Handling of Incomplete Structural Elements, 588
 Improper Handling of Inconsistent Special Elements, 433
 Improper Handling of Inconsistent Structural Elements, 590
 Improper Handling of Insufficient Entropy in TRNG, 832
 Improper Handling of Insufficient Permissions or Privileges, 679
 Improper Handling of Insufficient Privileges, 670
 Improper Handling of Invalid Use of Special Elements, 417
 Improper Handling of Length Parameter Inconsistency, 357
 Improper Handling of Missing Special Element, 429
 Improper Handling of Missing Values, 578
 Improper Handling of Mixed Encoding, 445
 Improper Handling of Overlap Between Protected Memory Ranges, 2087
 Improper Handling of Parameters, 581
 Improper Handling of Physical or Environmental Conditions, 2269
 Improper Handling of Single Event Upsets, 2091
 Improper Handling of Structural Elements, 587
 Improper Handling of Syntactically Invalid Structure, 575
 Improper Handling of Undefined Parameters, 586
 Improper Handling of Undefined Values, 580
 Improper Handling of Unexpected Data Type, 591
 Improper Handling of Unicode Encoding, 446
 Improper Handling of URL Encoding (Hex Encoding), 449
 Improper Handling of Values, 577
 Improper Handling of Windows ::DATA Alternate Data Stream, 130
 Improper Handling of Windows Device Names, 127
 Improper Identifier for IP Block used in System-On-Chip (SOC), 1994
 Improper Initialization, 1465
 Improper Input Validation, 20

- Improper Interaction Between Multiple Correctly-Behaving Entities, 1063
- Improper Isolation of Shared Resources in Network On Chip (NoC), 2237
- Improper Isolation of Shared Resources on System-on-a-Chip (SoC), 1985
- Improper Isolation or Compartmentalization, 1445
- Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), 33
- Improper Link Resolution Before File Access ('Link Following'), 112
- Improper Lock Behavior After Power State Transition, 2021
- Improper Locking, 1472
- Improper Management of Sensitive Trace Data, 2220
- Improper Neutralization, 1554
- Improper Neutralization of Alternate XSS Syntax, 196
- Improper Neutralization of Argument Delimiters in a Command ('Argument Injection'), 198
- Improper Neutralization of Comment Delimiters, 402
- Improper Neutralization of CRLF Sequences ('CRLF Injection'), 222
- Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting'), 277
- Improper Neutralization of Data within XPath Expressions ('XPath Injection'), 1428
- Improper Neutralization of Data within XQuery Expressions ('XQuery Injection'), 1444
- Improper Neutralization of Delimiters, 382
- Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection'), 232
- Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection'), 238
- Improper Neutralization of Encoded URI Schemes in a Web Page, 190
- Improper Neutralization of Equivalent Special Elements, 146
- Improper Neutralization of Escape, Meta, or Control Sequences, 400
- Improper Neutralization of Expression/Command Delimiters, 393
- Improper Neutralization of Formula Elements in a CSV File, 2031
- Improper Neutralization of HTTP Headers for Scripting Syntax, 1430
- Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), 168
- Improper Neutralization of Input Leaders, 397
- Improper Neutralization of Input Terminators, 395
- Improper Neutralization of Input Used for LLM Prompting, 2324
- Improper Neutralization of Internal Special Elements, 426
- Improper Neutralization of Invalid Characters in Identifiers in Web Pages, 194
- Improper Neutralization of Leading Special Elements, 419
- Improper Neutralization of Line Delimiters, 389
- Improper Neutralization of Macro Symbols, 404
- Improper Neutralization of Multiple Internal Special Elements, 428
- Improper Neutralization of Multiple Leading Special Elements, 421
- Improper Neutralization of Multiple Trailing Special Elements, 425
- Improper Neutralization of Null Byte or NUL Character, 415
- Improper Neutralization of Parameter/Argument Delimiters, 384
- Improper Neutralization of Quoting Syntax, 398
- Improper Neutralization of Record Delimiters, 387
- Improper Neutralization of Script in an Error Message Web Page, 184
- Improper Neutralization of Script in Attributes in a Web Page, 188
- Improper Neutralization of Script in Attributes of IMG Tags in a Web Page, 186
- Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS), 182
- Improper Neutralization of Section Delimiters, 391
- Improper Neutralization of Server-Side Includes (SSI) Within a Web Page, 241
- Improper Neutralization of Special Elements, 379
- Improper Neutralization of Special Elements in Data Query Logic, 1860
- Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), 138
- Improper Neutralization of Special Elements used in a Command ('Command Injection'), 148
- Improper Neutralization of Special Elements Used in a Template Engine, 2250
- Improper Neutralization of Special Elements used in an Expression Language Statement ('Expression Language Injection'), 1827
- Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection'), 217
- Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), 155
- Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), 206
- Improper Neutralization of Substitution Characters, 406
- Improper Neutralization of Trailing Special Elements, 423
- Improper Neutralization of Value Delimiters, 386
- Improper Neutralization of Variable Name Delimiters, 407
- Improper Neutralization of Whitespace, 411
- Improper Neutralization of Wildcards or Matching Symbols, 409
- Improper Null Termination, 434
- Improper Output Neutralization for Logs, 294
- Improper Ownership Management, 683
- Improper Physical Access Control, 2097
- Improper Preservation of Consistency Between Independent Representations of Shared State, 2064
- Improper Preservation of Permissions, 681
- Improper Prevention of Lock Bit Modification, 2018
- Improper Privilege Management, 653
- Improper Protection against Electromagnetic Fault Injection (EM-FI), 2212
- Improper Protection Against Voltage and Clock Glitches, 2056
- Improper Protection for Outbound Error Messages and Alert Signals, 2214
- Improper Protection of Alternate Path, 1031
- Improper Protection of Physical Side Channels, 2177
- Improper Protections Against Hardware Overheating, 2252
- Improper Removal of Sensitive Information Before Storage or Transfer, 551
- Improper Resolution of Path Equivalence, 87
- Improper Resource Locking, 1010
- Improper Resource Shutdown or Release, 987
- Improper Restriction of Communication Channel to Intended Endpoints, 1836
- Improper Restriction of Excessive Authentication Attempts, 754
- Improper Restriction of Names for Files and Other Resources, 1421
- Improper Restriction of Operations within the Bounds of a Memory Buffer, 299
- Improper Restriction of Power Consumption, 1832
- Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion'), 1642

Improper Restriction of Rendered UI Layers or Frames, 1869
 Improper Restriction of Security Token Assignment, 2085
 Improper Restriction of Software Interfaces to Hardware Features, 2076
 Improper Restriction of Write-Once Bit Fields, 2014
 Improper Restriction of XML External Entity Reference, 1376
 Improper Scrubbing of Sensitive Data from Decommissioned Device, 2104
 Improper Setting of Bus Controlling Capability in Fabric End-point, 2202
 Improper Synchronization, 1457
 Improper Translation of Security Attributes by Fabric Bridge, 2194
 Improper Update of Reference Count, 1811
 Improper Use of Validation Framework, 1978
 Improper Validation of Array Index, 347
 Improper Validation of Certificate Expiration, 733
 Improper Validation of Certificate with Host Mismatch, 729
 Improper Validation of Consistency within Input, 2151
 Improper Validation of Function Hook Arguments, 1396
 Improper Validation of Generative AI Output, 2321
 Improper Validation of Integrity Check Value, 883
 Improper Validation of Specified Index, Position, or Offset in Input, 2144
 Improper Validation of Specified Quantity in Input, 2142
 Improper Validation of Specified Type of Input, 2150
 Improper Validation of Syntactic Correctness of Input, 2148
 Improper Validation of Unsafe Equivalence in Input, 2153
 Improper Verification of Cryptographic Signature, 864
 Improper Verification of Intent by Broadcast Receiver, 1841
 Improper Verification of Source of a Communication Channel, 1852
 Improper Write Handling in Limited-write Non-Volatile Memories, 2054
 Improper Zeroization of Hardware Register, 2033
 Improperly Controlled Modification of Dynamically-Determined Object Attributes, 1818
 Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution'), 2216
 Improperly Controlled Sequential Memory Allocation, 2222
 Improperly Implemented Security Check for Standard, 888
 Improperly Preserved Integrity of Hardware Configuration State During a Power Save/Restore Operation, 2188
 Inaccurate Comments, 1964
 Inadequate Encryption Strength, 803
 Inappropriate Comment Style, 1962
 Inappropriate Encoding for Output Context, 1773
 Inappropriate Source Code Style or Formatting, 1927
 Inappropriate Whitespace Style, 1963
 Inclusion of Functionality from Untrusted Control Sphere, 1750
 Inclusion of Sensitive Information in an Include File, 1262
 Inclusion of Sensitive Information in Source Code, 1260
 Inclusion of Sensitive Information in Source Code Comments, 1383
 Inclusion of Sensitive Information in Test Code, 1249
 Inclusion of Undocumented Features or Chicken Bits, 2044
 Inclusion of Web Functionality from an Untrusted Source, 1756
 Incomplete Cleanup, 1106
 Incomplete Comparison with Missing Factors, 1874
 Incomplete Denylist to Cross-Site Scripting, 1528
 Incomplete Design Documentation, 1959
 Incomplete Documentation of Program Execution, 1961
 Incomplete Filtering of Multiple Instances of Special Elements, 1693
 Incomplete Filtering of One or More Instances of Special Elements, 1690
 Incomplete Filtering of Special Elements, 1689
 Incomplete I/O Documentation, 1960
 Incomplete Identification of Uploaded File Variables (PHP), 1385
 Incomplete Internal State Distinction, 926
 Incomplete List of Disallowed Inputs, 466
 Incomplete Model of Endpoint Features, 1067
 Inconsistency Between Implementation and Documented Design, 1915
 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'), 1075
 Inconsistent Naming Conventions for Identifiers, 1948
 Incorrect Access of Indexable Resource ('Range Error'), 298
 Incorrect Authorization, 1796
 Incorrect Behavior Order, 1535
 Incorrect Behavior Order: Authorization Before Parsing and Canonicalization, 1273
 Incorrect Behavior Order: Early Amplification, 1002
 Incorrect Behavior Order: Early Validation, 454
 Incorrect Behavior Order: Validate Before Canonicalize, 457
 Incorrect Behavior Order: Validate Before Filter, 460
 Incorrect Bitwise Shift of Integer, 2247
 Incorrect Block Delimitation, 1167
 Incorrect Calculation, 1507
 Incorrect Calculation of Buffer Size, 361
 Incorrect Calculation of Multi-Byte String Length, 377
 Incorrect Chaining or Granularity of Debug Components, 2166
 Incorrect Check of Function Return Value, 620
 Incorrect Comparison, 1538
 Incorrect Comparison Logic Granularity, 2071
 Incorrect Control Flow Scoping, 1550
 Incorrect Conversion between Numeric Types, 1504
 Incorrect Conversion of Security Identifiers, 2159
 Incorrect Decoding of Security Identifiers, 2155
 Incorrect Default Permissions, 672
 Incorrect Execution-Assigned Permissions, 678
 Incorrect Implementation of Authentication Algorithm, 744
 Incorrect Initialization of Resource, 2292
 Incorrect Ownership Assignment, 1556
 Incorrect Parsing of Numbers with Different Radices, 2275
 Incorrect Permission Assignment for Critical Resource, 1559
 Incorrect Pointer Scaling, 1121
 Incorrect Privilege Assignment, 645
 Incorrect Provision of Specified Functionality, 1514
 Incorrect Register Defaults or Module Parameters, 2005
 Incorrect Regular Expression, 469
 Incorrect Resource Transfer Between Spheres, 1480
 Incorrect Selection of Fuse Values, 2069
 Incorrect Short Circuit Evaluation, 1620
 Incorrect Synchronization, 1731
 Incorrect Type Conversion or Cast, 1547
 Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG), 836
 Incorrect Use of Autoboxing and Unboxing for Performance Critical Operations, 2029
 Incorrect Use of Privileged APIs, 1437
 Incorrect User Management, 698
 Incorrectly Specified Destination in a Communication Channel, 1855
 Inefficient Algorithmic Complexity, 999
 Inefficient CPU Computation, 1980
 Inefficient Regular Expression Complexity, 2243

- Information Exposure through Microarchitectural State after Transient Execution, 2262
 - Information Loss or Omission, 563
 - Information Management Errors, 2333
 - Initialization and Cleanup Errors, 2348
 - Initialization of a Resource with an Insecure Default, 1983
 - Initialization with Hard-Coded Network Resource Configuration Data, 1896
 - Insecure Automated Optimizations, 1881
 - Insecure Default Variable Initialization, 1091
 - Insecure Inherited Permissions, 675
 - Insecure Operation on Windows Junction / Mount Point, 2273
 - Insecure Preserved Inherited Permissions, 676
 - Insecure Security Identifier Mechanism, 2162
 - Insecure Storage of Sensitive Information, 1835
 - Insecure Temporary File, 932
 - Insertion of Sensitive Information Into Debugging Code, 558
 - Insertion of Sensitive Information into Externally-Accessible File or Directory, 1257
 - Insertion of Sensitive Information into Log File, 1250
 - Insertion of Sensitive Information Into Sent Data, 521
 - Insufficient Adherence to Expected Conventions, 1925
 - Insufficient Control Flow Management, 1525
 - Insufficient Control of Network Message Volume (Network Amplification), 997
 - Insufficient Documentation of Error Handling Techniques, 1967
 - Insufficient Encapsulation, 1907
 - Insufficient Encapsulation of Machine-Dependent Functionality, 1954
 - Insufficient Entropy, 828
 - Insufficient Entropy in PRNG, 830
 - Insufficient Granularity of Access Control, 2002
 - Insufficient Granularity of Address Regions Protected by Register Locks, 2010
 - Insufficient Isolation of Symbolic Constant Definitions, 1956
 - Insufficient Isolation of System-Dependent Functions, 1949
 - Insufficient Logging, 1647
 - Insufficient or Incomplete Data Removal within Hardware Component, 2183
 - Insufficient Precision or Accuracy of a Real Number, 2254
 - Insufficient Psychological Acceptability, 1450
 - Insufficient Resource Pool, 1005
 - Insufficient Session Expiration, 1380
 - Insufficient Technical Documentation, 1904
 - Insufficient Type Distinction, 873
 - Insufficient UI Warning of Dangerous Operations, 887
 - Insufficient Use of Symbolic Constants, 1955
 - Insufficient Verification of Data Authenticity, 858
 - Insufficient Visual Distinction of Homoglyphs Presented to User, 1866
 - Insufficiently Protected Credentials, 1234
 - Integer Coercion Error, 489
 - Integer Overflow or Wraparound, 478
 - Integer Overflow to Buffer Overflow, 1502
 - Integer Underflow (Wrap or Wraparound), 487
 - Integration Issues, 2491
 - Internal Asset Exposed to Unsafe Debug Access Level or State, 2048
 - Interpretation Conflict, 1065
 - Invocation of a Control Element at an Unnecessarily Deep Horizontal Layer, 1899
 - Invocation of Process Using Visible Sensitive Information, 556
 - Invokable Control Element in Multi-Thread Context with non-Final Static Storable or Member Element, 1903
 - Invokable Control Element with Excessive File or Data Access Operations, 1933
 - Invokable Control Element with Excessive Volume of Commented-out Code, 1934
 - Invokable Control Element with Large Number of Outward Calls, 1892
 - Invokable Control Element with Signature Containing an Excessive Number of Parameters, 1911
 - Invokable Control Element with Variadic Parameters, 1901
 - Irrelevant Code, 1976
- J**
- J2EE Bad Practices: Direct Management of Connections, 599
 - J2EE Bad Practices: Direct Use of Sockets, 601
 - J2EE Bad Practices: Direct Use of Threads, 942
 - J2EE Bad Practices: Non-serializable Object Stored in Session, 1318
 - J2EE Bad Practices: Use of System.exit(), 940
 - J2EE Framework: Saving Unserializable Objects to Disk, 1341
 - J2EE Misconfiguration: Data Transmission Without Encryption, 1
 - J2EE Misconfiguration: Entity Bean Declared Remote, 6
 - J2EE Misconfiguration: Insufficient Session-ID Length, 2
 - J2EE Misconfiguration: Missing Custom Error Page, 4
 - J2EE Misconfiguration: Plaintext Password in Configuration File, 1279
 - J2EE Misconfiguration: Weak Access Permissions for EJB Methods, 8
 - Java Runtime Error Message Containing Sensitive Information, 1255
- K**
- Key Exchange without Entity Authentication, 795
 - Key Management Errors, 2340
- L**
- Lack of Administrator Control over Security, 1487
 - Large Data Table with Excessive Number of Indices, 1938
 - Least Privilege Violation, 663
 - Limit Access, 2451
 - Limit Exposure, 2452
 - Lock Computer, 2452
 - Lockout Mechanism Errors, 2499
 - Logging of Excessive Data, 1651
 - Logic/Time Bomb, 1225
 - Loop Condition Value Update within the Loop, 1944
 - Loop with Unreachable Exit Condition ('Infinite Loop'), 1766
- M**
- Manage User Sessions, 2453
 - Manufacturing and Life Cycle Management Concerns, 2490
 - Memory Allocation with Excessive Size Value, 1683
 - Memory and Storage Issues, 2493
 - Memory Buffer Errors, 2500
 - Method Containing Access of a Member Element from Another Class, 1939
 - Mirrored Regions with Different Values, 2065
 - Misinterpretation of Input, 286
 - Mismatched Memory Management Routines, 1605
 - Missing Ability to Patch ROM Code, 2191
 - Missing Authentication for Critical Function, 748
 - Missing Authorization, 1789
 - Missing Check for Certificate Revocation after Initial Check, 924
 - Missing Critical Step in Authentication, 745
 - Missing Cryptographic Step, 801
 - Missing Custom Error Page, 1588

Missing Default Case in Multiple Condition Expression, 1149
 Missing Documentation for Design, 1898
 Missing Encryption of Sensitive Data, 764
 Missing Handler, 1051
 Missing Immutable Root of Trust in Hardware, 2224
 Missing Initialization of a Variable, 1096
 Missing Initialization of Resource, 1806
 Missing Lock Check, 1014
 Missing Origin Validation in WebSockets, 2271
 Missing Password Field Masking, 1271
 Missing Protection Against Hardware Reverse Engineering Using Integrated Circuit (IC) Imaging Techniques, 2131
 Missing Protection for Mirrored Regions in On-Chip Fabric Firewall, 2196
 Missing Protection Mechanism for Alternate Hardware Interface, 2174
 Missing Reference to Active Allocated Resource, 1631
 Missing Reference to Active File Descriptor or Handle, 1638
 Missing Release of File Descriptor or Handle after Effective Lifetime, 1640
 Missing Release of Memory after Effective Lifetime, 980
 Missing Release of Resource after Effective Lifetime, 1632
 Missing Report of Error Condition, 958
 Missing Serialization Control Element, 1913
 Missing Source Correlation of Multiple Independent Data, 2161
 Missing Source Identifier in Entity Transactions on a System-On-Chip (SOC), 2185
 Missing Standardized Error Handling Mechanism, 1265
 Missing Support for Integrity Check, 881
 Missing Support for Security Features in On-chip Fabrics or Buses, 2209
 Missing Synchronization, 1729
 Missing Validation of OpenSSL Certificate, 1350
 Missing Write Protection for Parametric Data Values, 2199
 Missing XML Validation, 275
 Modification of Assumed-Immutable Data (MAID), 1129
 Modules with Circular Dependencies, 1891
 Multiple Binds to the Same Port, 1364
 Multiple Inheritance from Concrete Classes, 1900
 Multiple Interpretations of UI Input, 1085
 Multiple Locks of a Critical Resource, 1613
 Multiple Operations on Resource in Single-Operation Context, 1496
 Multiple Releases of Same Resource or Handle, 2258
 Multiple Unlocks of a Critical Resource, 1614
 Mutable Attestation or Measurement Reporting Data, 2140

N

Named Chains, 2580
 .NET Misconfiguration: Use of Impersonation, 1230
 Non-exit on Failed Initialization, 1095
 Non-Replicating Malicious Code, 1221
 Non-SQL Invokable Control Element with Excessive Number of Data Resource Accesses, 1922
 Non-Transparent Sharing of Microarchitectural Resources, 2186
 Not Failing Securely ('Failing Open'), 1409
 Not Using Complete Mediation, 1413
 Not Using Password Aging, 640
 Null Byte Interaction Error (Poison Null Byte), 1403
 NULL Pointer Dereference, 1139
 Numeric Errors, 2333
 Numeric Range Comparison Without Minimum Check, 1776
 Numeric Truncation Error, 507

O

Object Model Violation: Just One of Equals and Hashcode Defined, 1321
 Obscured Security-relevant Information by Alternate Name, 568
 Observable Behavioral Discrepancy, 533
 Observable Behavioral Discrepancy With Equivalent Products, 535
 Observable Discrepancy, 525
 Observable Internal Behavioral Discrepancy, 534
 Observable Response Discrepancy, 530
 Observable Timing Discrepancy, 537
 Obsolete Feature in UI, 1083
 Off-by-one Error, 493
 Often Misused: String Management, 2335
 Omission of Security-relevant Information, 566
 Omitted Break Statement in Switch, 1169
 On-Chip Debug and Test Interface With Improper Access Control, 1989
 Only Filtering One Instance of a Special Element, 1692
 Only Filtering Special Elements at a Specified Location, 1694
 Only Filtering Special Elements at an Absolute Position, 1698
 Only Filtering Special Elements Relative to a Marker, 1696
 Operation on a Resource after Expiration or Release, 1488
 Operation on Resource in Wrong Phase of Lifetime, 1471
 Operator Precedence Logic Error, 1659
 Origin Validation Error, 860
 Out-of-bounds Read, 336
 Out-of-bounds Write, 1669
 Overly Restrictive Account Lockout Mechanism, 1432
 Overly Restrictive Regular Expression, 472
 OWASP Top Ten 2004 Category A1 - Unvalidated Input, 2355
 OWASP Top Ten 2004 Category A10 - Insecure Configuration Management, 2360
 OWASP Top Ten 2004 Category A2 - Broken Access Control, 2356
 OWASP Top Ten 2004 Category A3 - Broken Authentication and Session Management, 2356
 OWASP Top Ten 2004 Category A4 - Cross-Site Scripting (XSS) Flaws, 2357
 OWASP Top Ten 2004 Category A5 - Buffer Overflows, 2358
 OWASP Top Ten 2004 Category A6 - Injection Flaws, 2358
 OWASP Top Ten 2004 Category A7 - Improper Error Handling, 2359
 OWASP Top Ten 2004 Category A8 - Insecure Storage, 2359
 OWASP Top Ten 2004 Category A9 - Denial of Service, 2360
 OWASP Top Ten 2007 Category A1 - Cross Site Scripting (XSS), 2351
 OWASP Top Ten 2007 Category A10 - Failure to Restrict URL Access, 2355
 OWASP Top Ten 2007 Category A2 - Injection Flaws, 2351
 OWASP Top Ten 2007 Category A3 - Malicious File Execution, 2352
 OWASP Top Ten 2007 Category A4 - Insecure Direct Object Reference, 2352
 OWASP Top Ten 2007 Category A5 - Cross Site Request Forgery (CSRF), 2353
 OWASP Top Ten 2007 Category A6 - Information Leakage and Improper Error Handling, 2353
 OWASP Top Ten 2007 Category A7 - Broken Authentication and Session Management, 2353
 OWASP Top Ten 2007 Category A8 - Insecure Cryptographic Storage, 2354

OWASP Top Ten 2007 Category A9 - Insecure Communications, 2354

OWASP Top Ten 2010 Category A1 - Injection, 2377

OWASP Top Ten 2010 Category A10 - Unvalidated Redirects and Forwards, 2381

OWASP Top Ten 2010 Category A2 - Cross-Site Scripting (XSS), 2378

OWASP Top Ten 2010 Category A3 - Broken Authentication and Session Management, 2378

OWASP Top Ten 2010 Category A4 - Insecure Direct Object References, 2378

OWASP Top Ten 2010 Category A5 - Cross-Site Request Forgery(CSRF), 2379

OWASP Top Ten 2010 Category A6 - Security Misconfiguration, 2379

OWASP Top Ten 2010 Category A7 - Insecure Cryptographic Storage, 2380

OWASP Top Ten 2010 Category A8 - Failure to Restrict URL Access, 2380

OWASP Top Ten 2010 Category A9 - Insufficient Transport Layer Protection, 2381

OWASP Top Ten 2013 Category A1 - Injection, 2410

OWASP Top Ten 2013 Category A10 - Unvalidated Redirects and Forwards, 2414

OWASP Top Ten 2013 Category A2 - Broken Authentication and Session Management, 2410

OWASP Top Ten 2013 Category A3 - Cross-Site Scripting (XSS), 2411

OWASP Top Ten 2013 Category A4 - Insecure Direct Object References, 2411

OWASP Top Ten 2013 Category A5 - Security Misconfiguration, 2412

OWASP Top Ten 2013 Category A6 - Sensitive Data Exposure, 2412

OWASP Top Ten 2013 Category A7 - Missing Function Level Access Control, 2413

OWASP Top Ten 2013 Category A8 - Cross-Site Request Forgery (CSRF), 2413

OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities, 2413

OWASP Top Ten 2017 Category A1 - Injection, 2456

OWASP Top Ten 2017 Category A10 - Insufficient Logging & Monitoring, 2460

OWASP Top Ten 2017 Category A2 - Broken Authentication, 2457

OWASP Top Ten 2017 Category A3 - Sensitive Data Exposure, 2457

OWASP Top Ten 2017 Category A4 - XML External Entities (XXE), 2458

OWASP Top Ten 2017 Category A5 - Broken Access Control, 2458

OWASP Top Ten 2017 Category A6 - Security Misconfiguration, 2459

OWASP Top Ten 2017 Category A7 - Cross-Site Scripting (XSS), 2459

OWASP Top Ten 2017 Category A8 - Insecure Deserialization, 2459

OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities, 2460

OWASP Top Ten 2021 Category A01:2021 - Broken Access Control, 2508

OWASP Top Ten 2021 Category A02:2021 - Cryptographic Failures, 2509

OWASP Top Ten 2021 Category A03:2021 - Injection, 2511

OWASP Top Ten 2021 Category A04:2021 - Insecure Design, 2512

OWASP Top Ten 2021 Category A05:2021 - Security Misconfiguration, 2514

OWASP Top Ten 2021 Category A06:2021 - Vulnerable and Outdated Components, 2515

OWASP Top Ten 2021 Category A07:2021 - Identification and Authentication Failures, 2515

OWASP Top Ten 2021 Category A08:2021 - Software and Data Integrity Failures, 2516

OWASP Top Ten 2021 Category A09:2021 - Security Logging and Monitoring Failures, 2517

OWASP Top Ten 2021 Category A10:2021 - Server-Side Request Forgery (SSRF), 2518

P

Parent Class with a Virtual Destructor and a Child Class without a Virtual Destructor, 1889

Parent Class with References to Child Class, 1909

Parent Class without Virtual Destructor Method, 1929

Partial String Comparison, 474

Passing Mutable Objects to an Untrusted Method, 927

Password Aging with Long Expiration, 643

Password in Configuration File, 636

Path Equivalence: ' filename' (Leading Space), 98

Path Equivalence: './.' (Single Dot Directory), 107

Path Equivalence: '//multiple/leading/slash', 101

Path Equivalence: '/multiple/internal/slash', 103

Path Equivalence: '/multiple/trailing/slash/', 104

Path Equivalence: '\multiple\internal\backslash', 105

Path Equivalence: 'fakedir/./readdir/filename', 109

Path Equivalence: 'file name' (Internal Whitespace), 99

Path Equivalence: 'filedir*' (Wildcard), 108

Path Equivalence: 'filedir\' (Trailing Backslash), 106

Path Equivalence: 'filename ' (Trailing Space), 97

Path Equivalence: 'file.name' (Internal Dot), 95

Path Equivalence: 'file...name' (Multiple Internal Dot), 96

Path Equivalence: 'filename....' (Multiple Trailing Dot), 94

Path Equivalence: 'filename.' (Trailing Dot), 93

Path Equivalence: 'filename/' (Trailing Slash), 100

Path Equivalence: Windows 8.3 Filename, 111

Path Traversal: '....' (Multiple Dot), 69

Path Traversal: '...' (Triple Dot), 67

Path Traversal: '....//', 71

Path Traversal: '...//', 73

Path Traversal: './filedir', 55

Path Traversal: '/absolute/pathname/here', 79

Path Traversal: '/dir/./filename', 57

Path Traversal: './filedir', 53

Path Traversal: '\.filename', 62

Path Traversal: '\\UNC\share\name\' (Windows UNC Share), 86

Path Traversal: '\absolute\pathname\here', 81

Path Traversal: 'dir\..filename', 64

Path Traversal: '..filedir', 60

Path Traversal: 'C:dirname', 83

Path Traversal: 'dir/././filename', 58

Path Traversal: 'dir\..\filename', 65

Peripherals, On-chip Fabric, and Interface/IO Problems, 2493

Permission Issues, 2339

Permission Race Condition During Resource Copy, 1521

Permissions, Privileges, and Access Controls, 2337

Permissive Cross-domain Policy with Untrusted Domains, 1857

Permissive List of Allowed Inputs, 464

Permissive Regular Expression, 1400

Persistent Storable Data Element without Associated Comparison Control Element, 1946

PHP External Variable Modification, 1134

Physical Access Issues and Concerns, 2539

Placement of User into Incorrect Group, 1784

Plaintext Storage of a Password, 622

Pointer Issues, 2349
 Policy Privileges are not Assigned Consistently Between Control and Data Agents, 2107
 Policy Uses Obsolete Encoding, 2105
 Power, Clock, Thermal, and Reset Concerns, 2494
 Power-On of Untrusted Execution Core Before Enabling Fabric Access Control, 1995
 Predictable Exact Value from Previous Values, 852
 Predictable from Observable State, 850
 Predictable Seed in Pseudo-Random Number Generator (PRNG), 841
 Predictable Value Range from Previous Values, 854
 Premature Release of Resource During Expected Lifetime, 1743
 Private Data Structure Returned From A Public Method, 1197
 Privilege Chaining, 651
 Privilege Context Switching Error, 659
 Privilege Defined With Unsafe Actions, 648
 Privilege Dropping / Lowering Errors, 660
 Privilege Issues, 2338
 Privilege Separation and Access Control Issues, 2491
 Process Control, 283
 Processor Optimization Removal or Modification of Security-critical Code, 1879
 Product Released in Non-Release Configuration, 2110
 Product UI does not Warn User of Unsafe Actions, 886
 Protection Mechanism Failure, 1529
 Public cloneable() Method Without Final ('Object Hijack'), 1181
 Public Data Assigned to Private Array-Typed Field, 1199
 Public Key Re-Use for Signing both Debug and Production Code, 2157
 Public Static Field Not Marked Final, 1208
 Public Static Final Field References Mutable Object, 1368

Q

Quality Weaknesses with Indirect Security Impacts, 2601

R

Race Condition During Access to Alternate Channel, 1028
 Race Condition Enabling Link Following, 904
 Race Condition for Write-Once Attributes, 2011
 Race Condition within a Thread, 910
 Random Number Issues, 2498
 Reachable Assertion, 1387
 Reflection Attack in an Authentication Protocol, 740
 Regular Expression without Anchors, 1645
 Relative Path Traversal, 46
 Release of Invalid Pointer or Reference, 1608
 Reliance on a Single Factor in a Security Decision, 1448
 Reliance on Component That is Not Updateable, 2231
 Reliance on Cookies without Validation and Integrity Checking, 1292
 Reliance on Cookies without Validation and Integrity Checking in a Security Decision, 1662
 Reliance on Data/Memory Layout, 476
 Reliance on File Name or Extension of Externally-Supplied File, 1434
 Reliance on Insufficiently Trustworthy Component, 2266
 Reliance on IP Address for Authentication, 715
 Reliance on Machine-Dependent Data Representation, 1951
 Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking, 1439
 Reliance on Package-level Scope, 1175
 Reliance on Reverse DNS Resolution for a Security-Critical Action, 870
 Reliance on Runtime Component in Generated Code, 1950
 Reliance on Security Through Obscurity, 1452

Reliance on Undefined, Unspecified, or Implementation-Defined Behavior, 1591
 Reliance on Untrusted Inputs in a Security Decision, 1723
 Remanent Data Readable after Memory Erase, 2234
 Replicating Malicious Code (Virus or Worm), 1222
 Research Concepts, 2596(*Graph*: 2671)
 Resource Locking Problems, 2346
 Resource Management Errors, 2345
 Return Inside Finally Block, 1325
 Return of Pointer Value Outside of Expected Range, 1117
 Return of Stack Variable Address, 1287
 Return of Wrong Status Code, 960
 Returning a Mutable Object to an Untrusted Caller, 930
 Reusing a Nonce, Key Pair in Encryption, 797
 Runtime Resource Management Control Element in a Component Built to Run on Application Servers, 1912

S

Same Seed in Pseudo-Random Number Generator (PRNG), 839
 Security Flow Issues, 2490
 Security Primitives and Cryptography Issues, 2494
 Security Version Number Mutable to Older Versions, 2229
 Security-Sensitive Hardware Controls with Missing Lock Bit Protection, 2023
 SEI CERT C Coding Standard - Guidelines 01. Preprocessor (PRE), 2475
 SEI CERT C Coding Standard - Guidelines 02. Declarations and Initialization (DCL), 2476
 SEI CERT C Coding Standard - Guidelines 03. Expressions (EXP), 2476
 SEI CERT C Coding Standard - Guidelines 04. Integers (INT), 2477
 SEI CERT C Coding Standard - Guidelines 05. Floating Point (FLP), 2478
 SEI CERT C Coding Standard - Guidelines 06. Arrays (ARR), 2478
 SEI CERT C Coding Standard - Guidelines 07. Characters and Strings (STR), 2479
 SEI CERT C Coding Standard - Guidelines 08. Memory Management (MEM), 2479
 SEI CERT C Coding Standard - Guidelines 09. Input Output (FIO), 2480
 SEI CERT C Coding Standard - Guidelines 10. Environment (ENV), 2481
 SEI CERT C Coding Standard - Guidelines 11. Signals (SIG), 2481
 SEI CERT C Coding Standard - Guidelines 12. Error Handling (ERR), 2482
 SEI CERT C Coding Standard - Guidelines 13. Application Programming Interfaces (API), 2483
 SEI CERT C Coding Standard - Guidelines 14. Concurrency (CON), 2483
 SEI CERT C Coding Standard - Guidelines 48. Miscellaneous (MSC), 2484
 SEI CERT C Coding Standard - Guidelines 50. POSIX (POS), 2484
 SEI CERT C Coding Standard - Guidelines 51. Microsoft Windows (WIN), 2485
 SEI CERT Oracle Secure Coding Standard for Java - Guidelines 00. Input Validation and Data Sanitization (IDS), 2465
 SEI CERT Oracle Secure Coding Standard for Java - Guidelines 01. Declarations and Initialization (DCL), 2465
 SEI CERT Oracle Secure Coding Standard for Java - Guidelines 02. Expressions (EXP), 2466
 SEI CERT Oracle Secure Coding Standard for Java - Guidelines 03. Numeric Types and Operations (NUM), 2466

- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 04. Characters and Strings (STR), 2467
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 05. Object Orientation (OBJ), 2467
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 06. Methods (MET), 2468
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 07. Exceptional Behavior (ERR), 2469
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 08. Visibility and Atomicity (VNA), 2469
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 09. Locking (LCK), 2470
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 10. Thread APIs (THI), 2470
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 11. Thread Pools (TPS), 2471
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 12. Thread-Safety Miscellaneous (TSM), 2471
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 13. Input Output (FIO), 2471
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 14. Serialization (SER), 2472
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 15. Platform Security (SEC), 2473
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 16. Runtime Environment (ENV), 2473
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 17. Java Native Interface (JNI), 2474
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 18. Concurrency (CON), 2485
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 49. Miscellaneous (MSC), 2474
- SEI CERT Oracle Secure Coding Standard for Java - Guidelines 50. Android (DRD), 2475
- SEI CERT Perl Coding Standard - Guidelines 01. Input Validation and Data Sanitization (IDS), 2486
- SEI CERT Perl Coding Standard - Guidelines 02. Declarations and Initialization (DCL), 2486
- SEI CERT Perl Coding Standard - Guidelines 03. Expressions (EXP), 2487
- SEI CERT Perl Coding Standard - Guidelines 04. Integers (INT), 2487
- SEI CERT Perl Coding Standard - Guidelines 05. Strings (STR), 2488
- SEI CERT Perl Coding Standard - Guidelines 06. Object-Oriented Programming (OOP), 2488
- SEI CERT Perl Coding Standard - Guidelines 07. File Input and Output (FIO), 2489
- SEI CERT Perl Coding Standard - Guidelines 50. Miscellaneous (MSC), 2489
- Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade'), 1589
- Self-generated Error Message Containing Sensitive Information, 546
- Semiconductor Defects in Hardware Logic with Security-Sensitive Implications, 2060
- Sensitive Cookie in HTTPS Session Without 'Secure' Attribute, 1382
- Sensitive Cookie with Improper SameSite Attribute, 2123
- Sensitive Cookie Without 'HttpOnly' Flag, 1863
- Sensitive Data Storage in Improperly Locked Memory, 1338
- Sensitive Information in Resource Not Removed Before Reuse, 569
- Sensitive Information Uncleared Before Debug/Power State Transition, 2116
- Sensitive Non-Volatile Information Not Protected During Debug, 2046
- Sequence of Processor Instructions Leads to Unexpected Behavior, 2136
- Serializable Class Containing Sensitive Data, 1206
- Serializable Data Element Containing non-Serializable Item Elements, 1918
- Server-generated Error Message Containing Sensitive Information, 1272
- Server-Side Request Forgery (SSRF), 1829
- Servlet Runtime Error Message Containing Sensitive Information, 1254
- Session Fixation, 943
- Seven Pernicious Kingdoms, 2578(*Graph: 2637*)
- SFP Primary Cluster: Access Control, 2407
- SFP Primary Cluster: API, 2403
- SFP Primary Cluster: Authentication, 2406
- SFP Primary Cluster: Channel, 2408
- SFP Primary Cluster: Cryptography, 2408
- SFP Primary Cluster: Entry Points, 2406
- SFP Primary Cluster: Exception Management, 2403
- SFP Primary Cluster: Failure to Release Memory, 2503
- SFP Primary Cluster: Faulty Resource Release, 2503
- SFP Primary Cluster: Information Leak, 2405
- SFP Primary Cluster: Malware, 2408
- SFP Primary Cluster: Memory Access, 2404
- SFP Primary Cluster: Memory Management, 2404
- SFP Primary Cluster: Other, 2409
- SFP Primary Cluster: Path Resolution, 2405
- SFP Primary Cluster: Predictability, 2409
- SFP Primary Cluster: Privilege, 2407
- SFP Primary Cluster: Resource Management, 2404
- SFP Primary Cluster: Risky Values, 2403
- SFP Primary Cluster: Synchronization, 2405
- SFP Primary Cluster: Tainted Input, 2406
- SFP Primary Cluster: UI, 2409
- SFP Primary Cluster: Unused entities, 2403
- SFP Secondary Cluster: Access Management, 2414
- SFP Secondary Cluster: Ambiguous Exception Type, 2420
- SFP Secondary Cluster: Architecture, 2427
- SFP Secondary Cluster: Authentication Bypass, 2415
- SFP Secondary Cluster: Broken Cryptography, 2419
- SFP Secondary Cluster: Channel Attack, 2418
- SFP Secondary Cluster: Compiler, 2428
- SFP Secondary Cluster: Covert Channel, 2425
- SFP Secondary Cluster: Design, 2428
- SFP Secondary Cluster: Digital Certificate, 2416
- SFP Secondary Cluster: Exposed Data, 2421
- SFP Secondary Cluster: Exposure Temporary File, 2423
- SFP Secondary Cluster: Failed Chroot Jail, 2429
- SFP Secondary Cluster: Failure to Release Resource, 2431
- SFP Secondary Cluster: Faulty Buffer Access, 2426
- SFP Secondary Cluster: Faulty Endpoint Authentication, 2416
- SFP Secondary Cluster: Faulty Input Transformation, 2437
- SFP Secondary Cluster: Faulty Memory Release, 2425
- SFP Secondary Cluster: Faulty Pointer Use, 2426
- SFP Secondary Cluster: Faulty Resource Use, 2431
- SFP Secondary Cluster: Faulty String Expansion, 2426
- SFP Secondary Cluster: Feature, 2439
- SFP Secondary Cluster: Glitch in Computation, 2440
- SFP Secondary Cluster: Hardcoded Sensitive Data, 2417
- SFP Secondary Cluster: Implementation, 2429
- SFP Secondary Cluster: Improper NULL Termination, 2427
- SFP Secondary Cluster: Incorrect Buffer Length Computation, 2427
- SFP Secondary Cluster: Incorrect Exception Behavior, 2420
- SFP Secondary Cluster: Incorrect Input Handling, 2438
- SFP Secondary Cluster: Information Loss, 2439

SFP Secondary Cluster: Insecure Authentication Policy, 2417
 SFP Secondary Cluster: Insecure Resource Access, 2415
 SFP Secondary Cluster: Insecure Resource Permissions, 2415
 SFP Secondary Cluster: Insecure Session Management, 2424
 SFP Secondary Cluster: Life Cycle, 2432
 SFP Secondary Cluster: Link in Resource Name Resolution, 2430
 SFP Secondary Cluster: Missing Authentication, 2417
 SFP Secondary Cluster: Missing Endpoint Authentication, 2418
 SFP Secondary Cluster: Missing Lock, 2432
 SFP Secondary Cluster: Multiple Binds to the Same Port, 2418
 SFP Secondary Cluster: Multiple Locks/Unlocks, 2433
 SFP Secondary Cluster: Other Exposures, 2424
 SFP Secondary Cluster: Path Traversal, 2430
 SFP Secondary Cluster: Protocol Error, 2419
 SFP Secondary Cluster: Race Condition Window, 2433
 SFP Secondary Cluster: Security, 2439
 SFP Secondary Cluster: State Disclosure, 2424
 SFP Secondary Cluster: Tainted Input to Command, 2434
 SFP Secondary Cluster: Tainted Input to Environment, 2437
 SFP Secondary Cluster: Tainted Input to Variable, 2438
 SFP Secondary Cluster: Unchecked Status Condition, 2421
 SFP Secondary Cluster: Unexpected Entry Points, 2442
 SFP Secondary Cluster: Unrestricted Authentication, 2418
 SFP Secondary Cluster: Unrestricted Consumption, 2432
 SFP Secondary Cluster: Unrestricted Lock, 2434
 SFP Secondary Cluster: Use of an Improper API, 2441
 SFP Secondary Cluster: Weak Cryptography, 2419
 Signal Errors, 2343
 Signal Handler Function Associated with Multiple Signals, 1758
 Signal Handler Race Condition, 905
 Signal Handler Use of a Non-reentrant Function, 1154
 Signal Handler with Functionality that is not Asynchronous-Safe, 1746
 Signed to Unsigned Conversion Error, 501
 Singleton Class Instance Creation without Proper Locking or Synchronization, 1945
 Small Seed Space in PRNG, 847
 Small Space of Random Values, 834
 Software Development, 2576(*Graph: 2627*)
 Software Fault Pattern (SFP) Clusters, 2592(*Graph: 2654*)
 Source Code Element without Standard Prologue, 1963
 Source Code File with Excessive Number of Lines of Code, 1930
 Spyware, 1226
 SQL Injection: Hibernate, 1290
 Stack-based Buffer Overflow, 320
 State Issues, 2342
 Static Member Data Element outside of a Singleton Class Element, 1886
 Storage of File With Sensitive Data Under FTP Root, 562
 Storage of File with Sensitive Data Under Web Root, 560
 Storage of Sensitive Data in a Mechanism without Access Control, 1834
 Storing Passwords in a Recoverable Format, 625
 String Errors, 2331
 Struts: Duplicate Validation Forms, 252
 Struts: Form Bean Does Not Extend Validation Class, 257
 Struts: Form Field Without Validator, 259
 Struts: Incomplete validate() Method Definition, 254
 Struts: Non-private Field in ActionForm Class, 1369

Struts: Plug-in Framework not in Use, 262
 Struts: Unused Validation Form, 265
 Struts: Unvalidated Action Form, 267
 Struts: Validator Turned Off, 269
 Struts: Validator Without Form Field, 270
 Suspicious Comment, 1266
 Symbolic Name not Mapping to Correct Object, 949
 Synchronous Access of Remote Resource without Timeout, 1937

T

The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 10 - Locking (LCK), 2387
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 11 - Thread APIs (THI), 2388
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 12 - Thread Pools (TPS), 2388
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 13 - Thread-Safety Miscellaneous (TSM), 2389
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 14 - Input Output (FIO), 2389
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 15 - Serialization (SER), 2390
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 16 - Platform Security (SEC), 2390
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 17 - Runtime Environment (ENV), 2391
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 18 - Miscellaneous (MSC), 2391
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 2 - Input Validation and Data Sanitization (IDS), 2383
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 3 - Declarations and Initialization (DCL), 2383
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 4 - Expressions (EXP), 2384
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 5 - Numeric Types and Operations (NUM), 2384
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 6 - Object Orientation (OBJ), 2385
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 7 - Methods (MET), 2385
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 8 - Exceptional Behavior (ERR), 2386
 The CERT Oracle Secure Coding Standard for Java (2011)
 Chapter 9 - Visibility and Atomicity (VNA), 2387
 The UI Performs the Wrong Action, 1084
 Time-of-check Time-of-use (TOCTOU) Race Condition, 913
 Transmission of Private Resources into a New Sphere ('Resource Leak'), 984
 Trapdoor, 1223
 Trojan Horse, 1220
 Truncation of Security-relevant Information, 565
 Trust Boundary Violation, 1210
 Trust of System Event Data, 894
 Trusting HTTP Permission Methods on the Server Side, 1441
 Type Errors, 2331

U

UI Discrepancy for Security Feature, 1081
 Unauthorized Error Injection Can Degrade Hardware Redundancy, 2246
 Uncaught Exception, 603
 Uncaught Exception in Servlet, 1352
 Unchecked Error Condition, 955
 Unchecked Input for Loop Condition, 1366
 Unchecked Return Value, 613

- Unchecked Return Value to NULL Pointer Dereference, 1523
 - Unconditional Control Flow Transfer outside of Switch Block, 1924
 - Uncontrolled Recursion, 1493
 - Uncontrolled Resource Consumption, 971
 - Uncontrolled Search Path Element, 1040
 - Undefined Behavior for Input to API, 1138
 - Unexpected Sign Extension, 498
 - Unexpected Status Code or Return Value, 962
 - Unimplemented or Unsupported Feature in UI, 1082
 - Uninitialized Value on Reset for Registers Holding Security Settings, 2115
 - Unintended Proxy or Intermediary ('Confused Deputy'), 1072
 - Unintended Reentrant Invocation of Non-reentrant Code Via Nested Calls, 2100
 - UNIX Hard Link, 120
 - UNIX Symbolic Link (Symlink) Following, 117
 - Unlock of a Resource that is not Locked, 1761
 - Unnecessary Complexity in Protection Mechanism (Not Using 'Economy of Mechanism'), 1411
 - Unparsed Raw Web Content Delivery, 1053
 - Unprotected Alternate Channel, 1025
 - Unprotected Confidential Information on Device is Accessible by OSAT Vendors, 2168
 - Unprotected Primary Channel, 1024
 - Unprotected Transport of Credentials, 1239
 - Unprotected Windows Messaging Channel ('Shatter'), 1029
 - Unquoted Search Path or Element, 1047
 - Unrestricted Externally Accessible Lock, 1007
 - Unrestricted Upload of File with Dangerous Type, 1055
 - Unsafe ActiveX Control Marked Safe For Scripting, 1397
 - Unsigned to Signed Conversion Error, 505
 - Unsynchronized Access to Shared Data in a Multithreaded Context, 1296
 - Untrusted Pointer Dereference, 1732
 - Untrusted Search Path, 1035
 - Unverified Ownership, 685
 - Unverified Password Change, 1392
 - URL Redirection to Untrusted Site ('Open Redirect'), 1353
 - Use After Free, 1019
 - Use of a Broken or Risky Cryptographic Algorithm, 806
 - Use of a Cryptographic Primitive with a Risky Implementation, 2036
 - Use of a Key Past its Expiration Date, 799
 - Use of a Non-reentrant Function in a Concurrent Context, 1461
 - Use of a One-Way Hash with a Predictable Salt, 1598
 - Use of a One-Way Hash without a Salt, 1593
 - Use of Blocking Code in Single-threaded, Non-blocking Context, 2219
 - Use of Cache Containing Sensitive Information, 1240
 - Use of Client-Side Authentication, 1363
 - Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG), 844
 - Use of Default Credentials, 2284
 - Use of Default Cryptographic Key, 2288
 - Use of Default Password, 2286
 - Use of Expired File Descriptor, 1809
 - Use of Externally-Controlled Format String, 371
 - Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection'), 1125
 - Use of Function with Inconsistent Implementations, 1136
 - Use of GET Request Method With Sensitive Query Strings, 1349
 - Use of getlogin() in Multithreaded Application, 1281
 - Use of Hard-coded Credentials, 1699
 - Use of Hard-coded Cryptographic Key, 792
 - Use of Hard-coded Password, 630
 - Use of Hard-coded, Security-relevant Constants, 1267
 - Use of Implicit Intent for Sensitive Communication, 1846
 - Use of Incorrect Byte Ordering, 510
 - Use of Incorrect Operator, 1157
 - Use of Incorrectly-Resolved Name or Reference, 1553
 - Use of Inherently Dangerous Function, 593
 - Use of Inner Class Containing Sensitive Data, 1183
 - Use of Insufficiently Random Values, 821
 - Use of Invariant Value in Dynamically Changing Context, 856
 - Use of Less Trusted Source, 866
 - Use of Low-Level Functionality, 1533
 - Use of Multiple Resources with Duplicate Identifier, 1531
 - Use of Non-Canonical URL Paths for Authorization Decisions, 1435
 - Use of NullPointerException Catch to Detect NULL Pointer Dereference, 964
 - Use of Object without Invoking Destructor Method, 1940
 - Use of Obsolete Function, 1146
 - Use of Out-of-range Pointer Offset, 1735
 - Use of Password Hash Instead of Password for Authentication, 1770
 - Use of Password Hash With Insufficient Computational Effort, 1822
 - Use of Password System for Primary Authentication, 761
 - Use of Path Manipulation Function without Maximum-sized Buffer, 1664
 - Use of Persistent Cookies Containing Sensitive Information, 1259
 - Use of Platform-Dependent Third Party Components, 1952
 - Use of Pointer Subtraction to Determine Size, 1123
 - Use of Potentially Dangerous Function, 1498
 - Use of Predictable Algorithm in Random Number Generator, 2042
 - Use of Prohibited Code, 1981
 - Use of Redundant Code, 1884
 - Use of RSA Algorithm without OAEP, 1652
 - Use of Same Invokable Control Element in Multiple Architectural Layers, 1941
 - Use of Same Variable for Multiple Purposes, 1958
 - Use of Single-factor Authentication, 759
 - Use of Singleton Pattern Without Synchronization in a Multithreaded Context, 1263
 - Use of sizeof() on a Pointer Type, 1118
 - Use of umask() with chmod-style Argument, 1282
 - Use of Uninitialized Resource, 1802
 - Use of Uninitialized Variable, 1102
 - Use of Unmaintained Third Party Components, 1953
 - Use of Weak Credentials, 2281
 - Use of Weak Hash, 813
 - Use of Web Browser Cache Containing Sensitive Information, 1242
 - Use of Web Link to Untrusted Target with window.opener Access, 1872
 - Use of Wrong Operator in String Comparison, 1345
 - User Interface (UI) Misrepresentation of Critical Information, 1087
 - User Interface Security Issues, 2341
 - User Session Errors, 2500
 - Using Referer Field for Authentication, 717
- V**
- Validate Inputs, 2454
 - Variable Extraction Error, 1394
 - Verify Message Integrity, 2455
 - Violation of Secure Design Principles, 1454
- W**
- Weak Authentication, 2279

Weak Encoding for Password, 638
 Weak Password Recovery Mechanism for Forgotten Password, 1418
 Weak Password Requirements, 1231
 Weakness Base Elements, 2575
 Weaknesses Addressed by ISA/IEC 62443 Requirements, 2621
 Weaknesses Addressed by the CERT C Secure Coding Standard (2008), 2581(*Graph: 2642*)
 Weaknesses Addressed by The CERT Oracle Secure Coding Standard for Java (2011), 2585(*Graph: 2648*)
 Weaknesses Addressed by the SEI CERT C Coding Standard, 2604(*Graph: 2711*)
 Weaknesses Addressed by the SEI CERT C++ Coding Standard (2016 Version), 2587(*Graph: 2651*)
 Weaknesses Addressed by the SEI CERT Oracle Coding Standard for Java, 2603(*Graph: 2708*)
 Weaknesses Addressed by the SEI CERT Perl Coding Standard, 2606(*Graph: 2714*)
 Weaknesses for Simplified Mapping of Published Vulnerabilities, 2597(*Graph: 2696*)
 Weaknesses in Mobile Applications, 2594
 Weaknesses in OWASP Top Ten (2004), 2580(*Graph: 2639*)
 Weaknesses in OWASP Top Ten (2007), 2572(*Graph: 2625*)
 Weaknesses in OWASP Top Ten (2010), 2584(*Graph: 2647*)
 Weaknesses in OWASP Top Ten (2013), 2595(*Graph: 2669*)
 Weaknesses in OWASP Top Ten (2017), 2599(*Graph: 2704*)
 Weaknesses in OWASP Top Ten (2021), 2614(*Graph: 2726*)
 Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS, 2617(*Graph: 2732*)
 Weaknesses in Software Written in C, 2574
 Weaknesses in Software Written in C++, 2574
 Weaknesses in Software Written in Java, 2575
 Weaknesses in Software Written in PHP, 2575
 Weaknesses in the 2009 CWE/SANS Top 25 Most Dangerous Programming Errors, 2583(*Graph: 2645*)
 Weaknesses in the 2010 CWE/SANS Top 25 Most Dangerous Programming Errors, 2584(*Graph: 2646*)
 Weaknesses in the 2011 CWE/SANS Top 25 Most Dangerous Software Errors, 2593(*Graph: 2668*)
 Weaknesses in the 2019 CWE Top 25 Most Dangerous Software Errors, 2608(*Graph: 2718*)
 Weaknesses in the 2020 CWE Top 25 Most Dangerous Software Weaknesses, 2615(*Graph: 2731*)
 Weaknesses in the 2021 CWE Most Important Hardware Weaknesses List, 2613
 Weaknesses in the 2021 CWE Top 25 Most Dangerous Software Weaknesses, 2610(*Graph: 2723*)
 Weaknesses in the 2022 CWE Top 25 Most Dangerous Software Weaknesses, 2618(*Graph: 2735*)
 Weaknesses in the 2023 CWE Top 25 Most Dangerous Software Weaknesses, 2621(*Graph: 2755*)
 Weaknesses in the 2024 CWE Top 25 Most Dangerous Software Weaknesses, 2622(*Graph: 2756*)
 Weaknesses Introduced During Design, 2579
 Weaknesses Introduced During Implementation, 2579
 Weaknesses Originally Used by NVD from 2008 to 2016, 2573
 Windows Hard Link, 124
 Windows Shortcut Following (.LNK), 122
 Wrap-around Error, 345
 Write-what-where Condition, 329

X

XML Injection (aka Blind XPath Injection), 220