**List of vulnerabilities**

* Allocation of Resources Without Limits or Throttling (CWE-770)
* Array Index Underflow (CWE-129)
* Authentication Bypass Using an Alternate Path or Channel (CWE-288)
* Improper Restriction of Authentication Attempts (CWE-307)
* Buffer Over-read (CWE-126)
* Buffer Underflow (CWE-124)
* Buffer Under-read (CWE-127)
* Business Logic Errors (CWE-840)
* Classic Buffer Overflow (CWE-120)
* Cleartext Storage of Sensitive Information (CWE-312)
* Cleartext Transmission of Sensitive Information (CWE-319)
* Client-Side Enforcement of Server-Side Security (CWE-602)
* Code Injection (CWE-94)
* Command Injection - Generic (CWE-77)
* Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') (CWE-362)
* CRLF Injection (CWE-93)
* Cross-Site Request Forgery (CSRF) (CWE-352)
* Cross-site Scripting (XSS) - DOM (CWE-79)
* Cross-site Scripting (XSS) - Generic (CWE-79)
* Cross-site Scripting (XSS) - Reflected (CWE-79)
* Cross-site Scripting (XSS) - Stored (CWE-79)
* Cryptographic Issues - Generic (CWE-310)
* Denial of Service (CWE-400)
* Deserialization of Untrusted Data (CWE-502)
* Double Free (CWE-415)
* Download of Code Without Integrity Check (CWE-494)
* Embedded Malicious Code (CWE-506)
* Execution with Unnecessary Privileges (CWE-250)
* Exposed Dangerous Method or Function (CWE-749)
* External Control of Critical State Data (CWE-642)
* Externally Controlled Reference to a Resource in Another Sphere (CWE-610)
* Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) (CWE-75)
* File and Directory Information Exposure (CWE-538)
* Forced Browsing (CWE-425)
* Heap Overflow (CWE-122)
* HTTP Request Smuggling (CWE-444)
* HTTP Response Splitting (CWE-113)
* Improper Access Control - Generic (CWE-284)
* Improper Authentication - Generic (CWE-287)
* Improper Authorization (CWE-285)
* Improper Certificate Validation (CWE-295)
* Improper Check or Handling of Exceptional Conditions (CWE-703)
* Improper Export of Android Application Components (CWE-926)
* Improper Following of a Certificate's Chain of Trust (CWE-296)
* Improper Handling of Highly Compressed Data (Data Amplification) (CWE-409)
* Improper Handling of Insufficient Permissions or Privileges (CWE-280)
* Improper Handling of URL Encoding (Hex Encoding) (CWE-177)
* Improper Input Validation (CWE-20)
* Improper Neutralization of Escape, Meta, or Control Sequences (CWE-150)
* Improper Neutralization of HTTP Headers for Scripting Syntax (CWE-644)
* Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) (CWE-80)
* Improper Null Termination (CWE-170)
* Improper Privilege Management (CWE-269)
* Inadequate Encryption Strength (CWE-326)
* Inclusion of Functionality from Untrusted Control Sphere (CWE-829)
* Incomplete Blacklist (CWE-184)
* Incorrect Authorization (CWE-863)
* Incorrect Calculation of Buffer Size (CWE-131)
* Incorrect Comparison (CWE-697)
* Incorrect Permission Assignment for Critical Resource (CWE-732)
* Information Disclosure (CWE-200)
* Information Exposure Through an Error Message (CWE-209)
* Information Exposure Through Debug Information (CWE-215)
* Information Exposure Through Directory Listing (CWE-548)
* Information Exposure Through Discrepancy (CWE-203)
* Information Exposure Through Sent Data (CWE-201)
* Information Exposure Through Timing Discrepancy (CWE-208)
* Insecure Direct Object Reference (IDOR) (CWE-639)
* Insecure Storage of Sensitive Information (CWE-922)
* Insecure Temporary File (CWE-377)
* Insufficiently Protected Credentials (CWE-522)
* Insufficient Session Expiration (CWE-613)
* Integer Overflow (CWE-190)
* Integer Underflow (CWE-191)
* Key Exchange without Entity Authentication (CWE-322)
* Lack of Binary Hardening
* LDAP Injection (CWE-90)
* Leftover Debug Code (Backdoor) (CWE-489)
* Malware (CAPEC-549)
* Man-in-the-Middle (CWE-300)
* Memory Corruption - Generic (CWE-119)
* Misconfiguration (CWE-16)
* Missing Authentication for Critical Function (CWE-306)
* Missing Authorization (CWE-862)
* Missing Encryption of Sensitive Data (CWE-311)
* Missing Required Cryptographic Step (CWE-325)
* Modification of Assumed-Immutable Data (MAID) (CWE-471)
* NULL Pointer Dereference (CWE-476)
* Off-by-one Error (CWE-193)
* Open Redirect (CWE-601)
* OS Command Injection (CWE-78)
* Out-of-bounds Read (CWE-125)
* Password in Configuration File (CWE-260)
* Path Traversal (CWE-22)
* Path Traversal: '.../...//' (CWE-35)
* Phishing (CAPEC-98)
* Plaintext Storage of a Password (CWE-256)
* Privacy Violation (CWE-359)
* Privilege Escalation (CAPEC-233)
* Relative Path Traversal (CWE-23)
* Reliance on Cookies without Validation and Integrity Checking in a Security Decision (CWE-784)
* Reliance on Reverse DNS Resolution for a Security-Critical Action (CWE-350)
* Reliance on Untrusted Inputs in a Security Decision (CWE-807)
* Remote File Inclusion (CWE-98)
* Replicating Malicious Code (Virus or Worm) (CWE-509)
* Resource Injection (CWE-99)
* Reusing a Nonce, Key Pair in Encryption (CWE-323)
* Reversible One-Way Hash (CWE-328)
* Security Through Obscurity (CWE-656)
* Server-Side Request Forgery (SSRF) (CWE-918)
* Session Fixation (CWE-384)
* SQL Injection (CWE-89)
* Stack Overflow (CWE-121)
* Storing Passwords in a Recoverable Format (CWE-257)
* Time-of-check Time-of-use (TOCTOU) Race Condition (CWE-367)
* Trust of System Event Data (CWE-360)
* Type Confusion (CWE-843)
* UI Redressing (Clickjacking) (CAPEC-103)
* Unchecked Error Condition (CWE-391)
* Uncontrolled Recursion (CWE-674)
* Unprotected Transport of Credentials (CWE-523)
* Unrestricted Upload of File with Dangerous Type (CWE-434)
* Untrusted Search Path (CWE-426)
* Unverified Password Change (CWE-620)
* Use After Free (CWE-416)
* Use of a Broken or Risky Cryptographic Algorithm (CWE-327)
* Use of a Key Past its Expiration Date (CWE-324)
* Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) (CWE-338)
* Use of Externally-Controlled Format String (CWE-134)
* Use of Hard-coded Credentials (CWE-798)
* Use of Hard-coded Cryptographic Key (CWE-321)
* Use of Hard-coded Password (CWE-259)
* Use of Inherently Dangerous Function (CWE-242)
* Use of Insufficiently Random Values (CWE-330)
* User Interface (UI) Misrepresentation of Critical Information (CWE-451)
* Using Components with Known Vulnerabilities (CWE-1035)
* Violation of Secure Design Principles (CWE-657)
* Weak Cryptography for Passwords (CWE-261)
* Weak Password Recovery Mechanism for Forgotten Password (CWE-640)
* Wrap-around Error (CWE-128)
* Write-what-where Condition (CWE-123)
* XML Entity Expansion (CWE-776)
* XML External Entities (XXE) (CWE-611)
* XML Injection (CWE-91)
* XSS Using MIME Type Mismatch (CAPEC-209)