**CWE Top 25**

| **STRIDE** | **CWE Threat Description** | **CWE Threat** | **Example** |
| --- | --- | --- | --- |
| Spoofing | 13-Improper Authentication | CWE-287 |  |
| 25-Incorrect Default Permissions | CWE-276 |  |
| 20-Missing Authentication for Critical Function | CWE-306 |  |
|  |  |  |
| Tampering | 02-Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-79 |  |
| 03-Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') | CWE-89 |  |
| 05-Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') | CWE-78 |  |
| 16-Improper Neutralization of Special Elements used in a Command ('Command Injection' | CWE-77 |  |
| 06-Improper Input Validation | CWE-20 |  |
| 08-Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') | CWE-22 |  |
| 10-Unrestricted Upload of File with Dangerous Type | CWE-434 |  |
| 09-Cross-Site Request Forgery (CSRF) | CWE-352 |  |
| 14-Integer Overflow or Wraparound | CWE-190 |  |
| 19-Server-Side Request Forgery (SSRF) | CWE-918 |  |
| 23-Improper Control of Generation of Code ('Code Injection') | CWE-94 |  |
| 15-Deserialization of Untrusted Data |  |  |
| Repudiation | 11-Missing Authorization | CWE-862 |  |
|  |  |  |
| Information Disclosure | 18-Use of Hard-coded Credentials |  |  |
| 09-Cross-Site Request Forgery (CSRF) | CWE-352 |  |
| 10-Unrestricted Upload of File with Dangerous Type | CWE-434 |  |
| 11-Missing Authorization | CWE-862 |  |
| 19-Server-Side Request Forgery (SSRF) | CWE-918 |  |
| 19-Server-Side Request Forgery (SSRF) | CWE-918 |  |
| 13-Improper Authentication | CWE-287 |  |
| Denial of Service | 21-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') | CWE-362 |  |
| 01-Out-of-bounds Write | CWE-787 |  |
| 04-Use After Free | CWE-416 |  |
| 07-Out-of-bounds Read | CWE-125 |  |
| 12-NULL Pointer Dereference | CWE-476 |  |
| 17-Improper Restriction of Operations within the Bounds of a Memory Buffer | CWE-119 |  |
| 21-Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |  |  |
| 14-Integer Overflow or Wraparound | CWE-190 |  |
| Elevation of Privilege | 22-Improper Privilege Management | CWE-269 |  |
| 24-Incorrect Authorization | CWE-863 |  |
| 11-Missing Authorization | CWE-862 |  |
|  |  |  |  |

Reference:  
<https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html>