|  |  |  |
| --- | --- | --- |
| Rank | ID | Name |
| [1] | CWE-119 | Improper Restriction of Operations within the Bounds of a Memory Buffer |
| [2] | CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| [3] | CWE-20 | Improper Input Validation |
| [4] | CWE-200 | Information Exposure |
| [5] | CWE-125 | Out-of-bounds Read |
| [6] | CWE-89 | Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| [7] | CWE-416 | Use After Free |
| [8] | CWE-190 | Integer Overflow or Wraparound |
| [9] | CWE-352 | Cross-Site Request Forgery (CSRF) |
| [10] | CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| [11] | CWE-78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| [12] | CWE-787 | Out-of-bounds Write |
| [13] | CWE-287 | Improper Authentication |
| [14] | CWE-476 | NULL Pointer Dereference |
| [15] | CWE-732 | Incorrect Permission Assignment for Critical Resource |
| [16] | CWE-434 | Unrestricted Upload of File with Dangerous Type |
| [17] | CWE-611 | Improper Restriction of XML External Entity Reference |
| [18] | CWE-94 | Improper Control of Generation of Code ('Code Injection') |
| [19] | CWE-798 | Use of Hard-coded Credentials |
| [20] | CWE-400 | Uncontrolled Resource Consumption |
| [21] | CWE-772 | Missing Release of Resource after Effective Lifetime |
| [22] | CWE-426 | Untrusted Search Path |
| [23] | CWE-502 | Deserialization of Untrusted Data |
| [24] | CWE-269 | Improper Privilege Management |
| [25] | CWE-295 | Improper Certificate Validation |