|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25** | | | **Releases** | | | |
|  | | | **2019** | **2020** | **2021** | **2022** |
|  | 787 | Out of Bounds Write | 12 | 2 | 1 | 1 |
|  | 79 | Improper Neutralization of Input During Web Page Generation (‘Cross Site Scripting’) | 2 | 1 | 2 | 2 |
|  | 89 | Improper Neutralization of Special Elements used in an SQL Command (‘SQL Injection’) | 6 | 6 | 6 | 3 |
|  | 20 | Improper Input Validation | 3 | 3 | 4 | 4 |
|  | 125 | Out of Bounds Read | 5 | 4 | 3 | 5 |
|  | 78 | Improper Neutralization of Special Elements used in OS Command (‘OS Command Injection’) | 11 | 10 | 5 | 6 |
|  | 416 | Use After Free | 7 | 8 | 7 | 7 |
|  | 22 | Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’) | 10 | 12 | 8 | 8 |
|  | 352 | Cross-Site Request Forgery (CSRF) | 9 | 9 | 9 | 9 |
|  | 434 | Unrestricted Upload of File with Dangerous Type | 16 | 15 | 10 | 10 |
|  | 476 | NULL Pointer Dereference | 14 | 13 | 15 | 11 |
|  | 502 | Deserialization of Untrusted Data | 23 | 21 | 13 | 12 |
|  | 190 | Integer Overflow or Wraparound | 8 | 11 | 12 | 13 |
|  | 287 | Improper Authentication | 13 | 14 | 14 | 14 |
|  | 798 | Use of Hard-coded Credentials | 19 | 20 | 16 | 15 |
|  | 862 | Missing Authorization | 34 | 25 | 18 | 16 |
|  | 77 | Improper Neutralization of Special Elements used in a Command (‘Command Injection’) | 🗶 | 31 | 25 | 17 |
|  | 306 | Missing Authentication for Critical Function | 36 | 24 | 11 | 18 |
|  | 119 | Improper Restriction of Operations within the Bounds of a Memory Buffer | 1 | 5 | 17 | 19 |
|  | 276 | Incorrect Default Permissions | 🗶 | `41 | 19 | 20 |
|  | 918 | Server-Side Request Forgery (SSRF) | 30 | 27 | 24 | 21 |
|  | 362 | Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’) | 29 | 34 | 33 | 22 |
|  | 400 | Uncontrolled Resource Consumption | 20 | 23 | 27 | 23 |
|  | 611 | Improper Restriction of XML External Entity Reference | 17 | 19 | 23 | 24 |
|  | 94 | Improper Control of Generation of Code (‘Code Injection’) (2019) | 18 | 17 | 28 | 25 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25 (“On the Cusp”)** | | | **Releases** | | | |
|  | | | **2019** | **2020** | **2021** | **2022** |
|  | 295 | Improper Certificate Validation | 25 | 28 | 26 | 26 |
|  | 427 | Uncontrolled Search Path Element | 🗶 | 58 | 34 | 27 |
|  | 863 | Incorrect Authorization | 33 | 29 | 38 | 28 |
|  | 269 | Improper Privilege Management | 24 | 22 | 29 | 29 |
|  | 732 | Incorrect Permission Assignment for Critical Resource | 15 | 16 | 22 | 30 |
|  | 843 | Access of Resource Using Incompatible Type (‘Type Confusion’) | 🗶 | 45 | 36 | 31 |
|  | 668 | Exposure of Resource to Wrong Sphere | 🗶 | 🗶 | 53 | 32 |
|  | 200 | Exposure of Sensitive Information to an Unauthorized Actor[[1]](#footnote-1) | 4 | 7 | 20 | 33 |
|  | 1321 | Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') | 🗶 | 🗶 | 🗶 | 34 |
|  | 601 | URL Redirection to an Untrusted Site (‘Open Redirect’) | 32 | 35 | 37 | 35 |
|  | 401 | Missing Release of Memory after Effective Lifetime | 🗶 | 32 | 32 | 36 |
|  | 59 | Improper Link Resolution Before File Access (‘Link Following’) | 🗶 | 40 | 31 | 37 |
|  | 522 | Insufficiently Protected Credentials | 27 | 18 | 21 | 38 |
|  | 319 | Cleartext Transmission of Sensitive Information | 🗶 | 42 | 35 | 39 |
|  | 312 | Cleartext Storage of Sensitive Information | 🗶 | 🗶 | 41 | 40 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25 (40+ 2022)** | | | **Releases** | | | |
|  | | | **2019** | **2020** | **2021** | **2022** |
|  | 532 | Insertion of Sensitive Information into Log File | 35 | 33 | 39 | 49 |
|  | 770 | Allocation of Resources without Limits or Throttling | 39 | 39 | 40 | 42 |
|  | 917 | Improper Neutralization of Special Elements used in an Expression Language Statement (‘Expression Language Injection’) | 🗶 | 47 | 30 | 55 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CWE/SANS Top 25 (Including Highest-Ranking Classes)** | | | **Releases** | | | |
|  | | | **2019** | **2020** | **2021** | **2022** |
|  | 400 | Uncontrolled Resource Consumption | 20 | 23 | 27 | 🗶 |
|  | 426 | Untrusted Search Path | 22 | 26 | 🗶 | 🗶 |
|  | 284 | Improper Access Control | 🗶 | 30 | 🗶 | 🗶 |
|  | 835 | Loop with Unreachable Exit Condition (‘Infinite Loop’) | 26 | 36 | 🗶 | 🗶 |
|  | 704 | Incorrect Type Conversion or Cast | 28 | 37 | 🗶 | 🗶 |
|  | 415 | Double Free | 31 | 38 | 🗶 | 🗶 |
|  | 772 | Missing Release of Resource after Effective Lifetime | 21 | 🗶 | 🗶 | 🗶 |
|  | 384 | Session Fixation | 37 | 🗶 | 🗶 | 🗶 |
|  | 326 | Inadequate Encryption Strength | 38 | 🗶 | 🗶 | 🗶 |
|  | 617 | Reachable Assertion | 40 | 🗶 | 🗶 | 🗶 |

1. Renamed from “Information Exposure” on 24th February 2020. [↑](#footnote-ref-1)