CWE/SANS Top 25		Releases		
		2019	2020	2021
787	Out of Bounds Write	12	2	1
79	Improper Neutralization of Input During Web Page Generation ('Cross Site Scripting')	2	1	2
125	Out of Bounds Read	5	4	3
20	Improper Input Validation	3	3	4
78	Improper Neutralization of Special Elements used in OS Command ('OS Command Injection')	11	10	5
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	6	6	6
416	Use After Free	7	8	7
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	10	12	8
352	Cross-Site Request Forgery (CSRF)	9	9	9
434	Unrestricted Upload of File with Dangerous Type	16	15	10
306	Missing Authentication for Critical Function	36	24	11
190	Integer Overflow or Wraparound	8	11	12
502	Deserialization of Untrusted Data	23	21	13
287	Improper Authentication	13	14	14
476	NULL Pointer Dereference	14	13	15
798	Use of Hard-coded Credentials	19	20	16
119	Improper Restriction of Operations within the Bounds of a Memory Buffer	1	5	17
862	Missing Authorization	34	25	18
276	Incorrect Default Permissions	X	`41	19
200	Exposure of Sensitive Information to an Unauthorized Actor[1]	4	7	20
522	Insufficiently Protected Credentials	27	18	21
732	Incorrect Permission Assignment for Critical Resource	15	16	22
611	Improper Restriction of XML External Entity Reference	17	19	23
918	Server-Side Request Forgery (SSRF)	30	27	24
77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	X	31	25

Commented [CH1]: 2020 Rank Change +22 from 2021

[1] Renamed from "Information Exposure" on 24th February 2020.

CWE/SANS Top 25 (On the Cusp)	Releases		
	2019	2020	2021
295 Improper Certificate Validation	25	28	26
400 Uncontrolled Resource Consumption	20	23	27
94 Improper Control of Generation of Code (‘Code Injection’) (2019)	18	17	28
269 Improper Privilege Management	24	22	29
917 Improper Neutralization of Special Elements used in an Expression Language Statement (‘Expression Language Injection’)	X	47	30
59 Improper Link Resolution Before File Access (‘Link Following’)	X	40	31
401 Missing Release of Memory after Effective Lifetime	X	32	32
362 Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’)	29	34	33
427 Uncontrolled Search Path Element	X	58	34
319 Cleartext Transmission of Sensitive Information	X	42	35
843 Access of Resource Using Incompatible Type (‘Type Confusion’)	X	45	36
601 URL Redirection to an Untrusted Site (‘Open Redirect’)	32	35	37
863 Incorrect Authorization	33	29	38
532 Insertion of Sensitive Information into Log File	35	33	39
770 Allocation of Resources without Limits or Throttling	39	39	40
426 Untrusted Search Path	22	26	X
284 Improper Access Control	X	30	X
835 Loop with Unreachable Exit Condition (‘Infinite Loop’)	26	36	X
704 Incorrect Type Conversion or Cast	28	37	X
415 Double Free	31	38	X
772 Missing Release of Resource after Effective Lifetime	21	X	X
384 Session Fixation	37	X	X
326 Inadequate Encryption Strength	38	X	X
617 Reachable Assertion	40	X	X

Commented [CH2]: 2020 Rank Change +17 from 2021

Commented [CH3]: 2020 Rank Change +24 from 2021

Commented [CH4]: 2020 Rank Change +7 from 2021

Commented [CH5]: 2020 Rank Change +9 from 2021