

CWE/SANS Top 25		Releases		
		2009	2010	2011
Insecure Interaction between Components				
89	Failure to Preserve SQL Query Structure ('SQL Injection')	✓	2	1
78	Improper Sainitization of Special Elements used in OS Command ('OS Command Injection')	✓	9	2
79	Failure to Preserve Web Page Structure ('Cross Site Scripting')	✓	1	4
434	Unrestricted Upload of File with Dangerous Type	x	8	9
352	Cross-Site Request Forgery (CSRF)	✓	4	12
601	URL Redirection to an Untrusted Site ('Open Redirect')	x	23	22
319	Cleartext Transmission of Sensitive Information	✓	x	x
20	Improper Input Validation	✓	x	x
116	Improper Encoding or Escaping of Output	✓	x	x
362	Race Condition	✓	25	x
209	Information Exposure Through an Error Message ^[1]	✓	17	x
Risky Resource Management				
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	x	3	3
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	x	7	13
494	Download of Code without Integrity Check	✓	20	14
829	Inclusion of Functionality from Untrusted Control Sphere	x	14	16
98	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP File Inclusion')	x	14	16
676	Use of Potentially Dangerous Function	x	x	18
131	Incorrect Calculation of Buffer Size	x	18	20
134	Uncontrolled Format String	x	x	23
190	Integer Overflow or Wraparound	x	16	24
119	Failure to Constrain Operations within the Bounds of Memory Buffer	✓	x	x
642	External Control of Critical State Data	✓	x	x
73	External Control of File Name of Path	✓	x	x
426	Untrusted Search Path	✓	x	x
94	Failure to Control Generation of Code ('Code Injection')	✓	x	x
404	Improper Resource Shutdown or Release	✓	x	x
665	Improper Initialization	✓	x	x
682	Incorrect Calculation	✓	x	x
805	Buffer Access with Incorrect Length Value	x	12	x
754	Improper Check for Unusual or Exceptional Conditions	x	13	x
129	Improper Validation of Array Index	x	15	x
770	Allocation of Resources without Limits or Throttling	x	22	x
Porous Defences				
306	Missing Authentication for Critical Function	x	19	5
862	Missing Authorization	x	5	6
285	Improper Authorization ^[2]	✓	5	6/15
798	Use of Hard-coded Credentials	x	11	7
311	Missing Encryption of Sensitive Data	x	10	8
807	Reliance on Untrusted Inputs in a Security Decision	x	6	10
250	Execution with Unnecessary Privileges	✓	x	11
863	Incorrect Authorization	x	5	15
732	Incorrect Permission Assignment for Critical Resource	✓	21	17
327	Use of Broken or Risky Cryptographic Algorithm	✓	24	19
307	Improper Restriction of Excessive Authentication Attempts	x	x	21
759	Use of One-Way Hash without Salt	x	x	25
602	Client-Side Enforcement of Server-Side Security	✓	x	x
259	Hard Coded Password	✓	x	x
330	Use of Insufficiently Random Values	✓	x	x

[1] Renamed from "Error Message Information Leak" on 1st December 2009

[2] Renamed from "Improper Access Control (Authorization)" on 29th March 2011