

OWASP Periodic Table of Vulnerabilities

Perimeter

A1 776,789 SA 35,41,44	A2 307 BL 11
A2 SH 776,789	A2 311,319 IT 4
A2 303 WA 303	A4 639 BP 34,48
A5 16 SM 14	A5 798 AM 15
A5 548 DI 16	A5 200 FP 45
A5 280 IF 17	A6 200 IF 13
134 FS 6	74,444 RG 24,26,27
400 DA 10	626 NB 28
22 PT 33	799 BF 11,21
120,131 BO 7	DS

Generic Framework

A1 89 SI 19	A1 90 LI 29	A1 611 XE 43	A1 88 MI 30
A1 643,652 XP 39,46	A1 91 XI 23	A2 307 BL 11	A2 384 SF 37
A2 640 SH 49	A2 303 WA 303	A2 330 BI 11,18	A2 613 IS 47
A2 640 IR 49	A2 640 IG 49	A3 79 XS 8	A3 79 XD 8
A4 639 BP 34,48	A5 200 FP 45	A6 311,798 ID 50	A6 200 IL 13
A7 691 IP 40	A7 306,862 IA 1,2	A8 352 XF 9	A10 601 UR 38
134 FS 6	120,131 BO 7	626 NB 28	22 PT 33
116 OH 22	434 IH 20	610 RD 32	98 RF 5
799 BF 11,21	190 IO 3	113 RS 25	97 SS 36
693 CJ	362 RC		

Custom Framework

A1 78 OC 31
A4 639 BP 34,48
345 CS 12
799 BF 11,21
116 OH 22
434 IH 20

Custom Code

A1 89 SI 19
A6 200 IL 13
A7 306,862 IA 1,2
A7 691 IP 40
190 IO 3
400 DA 10
840 AF 42
799 BF 11,21
434 IH 20

Legend

OWASP	WASC
XX	
CWE	

=Top 10 2013

Browsers and Standards - Session Management

A2 330 BI 11,18	A2 613 IS 47	A2 311,319 IT 4
A2 303 WA	A2 IG	A2 SH

Browsers and Standards - Content Management

A3 79 XS 8	A8 352 XF 9	A12 345 CS
98 RF 5	74,444 RG 24,26,27	693 CJ

Symbol	Name	OWASP	WASC	CWE	Standards	Perimeter	Generic Framework	Custom Framework	Custom Code
AF	Abuse of Functionality		42	840					X
AM	Application Misconfiguration	A5	15	798		X			
BF	Brute Force (Generic) / Insufficient Anti-automation		11,21	799		X	X	X	X
BI	Brute Force Session Identifier	A2	11,18	330	X		X		
BL	Brute Force Login	A2	11	307		X	X		
BO	Buffer Overflow		7	120,131		X	X		
BP	Brute Force Predictable Resource Location/Insecure Indexing	A4	34,48	639		X	X	X	
CJ	Clickjacking			693	X		X		
CS	Content Spoofing		12	345	X			X	
DA	Denial of Service (Application Based)		10	400		X			X
DI	Directory Indexing	A5	16	548		X			
DS	Denial of Service (Connection Based)					X			
FP	Fingerprinting	A5	45	200		X	X		
FS	Format String		6	134		X	X		
IA	Insufficient Authentication/Authorization	A7	1,2	306,862			X		X
ID	Insufficient Data Protection	A6	50	311,798			X		
IF	Improper Filesystem Permissions	A5	17	280		X			
IG	Implicit Logout	A2			X		X		
IH	Improper Input Handling		20	434			X	X	X
IL	Information Leakage	A6	13	200		X	X		X
IO	Integer Overflow/Underflow		3	190			X		X
IP	Insufficient Process Validation	A7	40	691			X		X
IR	Insufficient Password Recovery	A2	49	640			X		
IS	Insufficient Session Expiration	A2	47	613	X		X		
IT	Insufficient Transport Layer Protection	A2	4	311,319	X	X			
LI	LDAP Injection	A1	29	90			X		
MI	Mail Command Injection	A1	30	88			X		
NB	Null Byte Injection		28	626		X	X		
OC	OS Commanding	A1	31	78				X	
OH	Improper Output Handling		22	116			X	X	
PT	Path Traversal		33	22		X	X		
RC	Race Conditions			362			X		
RD	Routing Detour		32	610			X		
RF	Remote File Inclusion		5	98	X		X		
RG	HTTP Request/Response Smuggling		24,26,27	74,444	X	X			
RS	HTTP Response Splitting		25	113			X		
SA	SOAP Array Abuse, XML Attribute Blowup, XML Entity Expansion	A1	35,41,44	776,789		X			
SF	Session Fixation	A2	37	384			X		
SH	Cookie Theft/Session Hijacking	A2			X	X	X		
SI	SQL Injection	A1	19	89			X		X
SM	Server Misconfiguration	A5	14	16		X			
SS	SSI Injection		36	97			X		
UR	URL Redirector Abuse	A10	38	601			X		
WA	Weak HTTP Authentication Methods	A2		303	X	X	X		
XD	Cross-Site Scripting (XSS) - DOM-Based	A3	8	79			X		
XE	XML External Entities	A1	43	611			X		
XF	Cross-Site Request Forgery	A8	9	352	X		X		
XI	XML Injection	A1	23	91			X		
XP	XPath/XQuery Injection	A1	39,46	643,652			X		
XS	Cross-Site Scripting (XSS)	A3	8	79	X		X		