OWASP Periodic Table of Vulnerabilities

Perimeter and Platform

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

Generic Framework

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

Custom Framework

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

Custom Code

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

Legend

=Top 10 2013

OWASP WASC

XX

CWE

Browsers and Standards - Session Management

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

Browsers and Standards - Content Management

A3 8 XS 79	A8 9 XF 352	12 CS 345
5 RF 98	24,26,27 RG 74,444	CJ 693

Symbol	Name	OWASP	WASC	CWE	Standards	Perimeter/Platform	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		