

OWASP Top 10 2007	OWASP Top 10 2004	SANS/CWE 25	WASC 24 (+2)*
A1. Cross Site Scripting (XSS)	A4. Cross Site Scripting (XSS)	CWE-79: Failure to preserve Web Page Structure ('Cross-site Scripting')	3.2 Cross-site Scripting
		CWE-89: Failure to Preserve SQL Query Structure ('SQL Injection')	4.5 SQL Injection
		CWE-78: Improper Sanitization of special Elements used in an OS Command	4.4 OS commanding
		CWE-94: Failure to Control Generation of Code ('Code Injection')	4.6 SSI Injection
			4.3 LDAP Injection
A2. Injection Flaws	A6. Injection Flaws		4.7 Xpath Injection
A7. Broken Authentication and Session management	A3. Broken Authentication and Session management		1.1 Brute Force
A8. Insecure Cryptographic Storage	A8. Insecure Storage	CWE-327: Use of a Broken or Risky Cryptographic Algorithm	1.2 Insufficient Authentication
A5. Cross Site Request Forgery (CSRF)		CWE-352: Cross-Site Request Forgery (CSRF)	1.3 Weak Password Recovery Validation
A6. Information Leakage and Improper Error Handling	A7. Improper Error Handling	CWE-209: Error message Information Leak	2.1 Credential/Session Prediction
A10. Failure to Restrict URL Access	A2. Broken Access Control	CWE-285: Improper Access Control (Authorization)	2.3 Insufficient Session Expiration
A4. Insecure Direct Object Reference		CWE-73: External control of File Name or Path	2.4 Session Fixation
A9. Insecure Communications		CWE-319: Cleartext Transmission of Sensitive Information	
	A1. Unvalidated Input	CWE-20: Improper Input Validation	
	A5. Buffer Overflows	CWE-119: Failure to Constrain Operations within the Bounds of a memory Buffer	4.1 Buffer Overflow
	A9. Denial of Service	CWE-404: Improper Resource Shutdown or Release	6.2 Denial of Service
A3. Malicious File Execution		CWE-494: Download of Code Without Integrity Check	
	A10. Insecure configuration Management	CWE-732: Incorrect Permission Assignment for Critical Resource	
		CWE-250: Execution with Unnecessary Privileges	
		CWE-362: Race Condition	
		CWE-642: External Control of Critical State Data	
		CWE-426: Untrusted Search path	
		CWE-665 Improper Initialization	
		CWE-682: Incorrect Calculation	
		CWE-330: Use of Insufficiently Random Values	
		CWE-602: Client-Side Enforcement of Server-Side Security	
		CWE-116: Improper Encoding or Escaping of Output	
			3.1 Content Spoofing
			3.3 HTTP Response Splitting*
			4.2 Format String Attack
			5.1 Directory Indexing
			5.3 Path Traversal
			5.4 Predictable Resource Location
			6.1 Abuse of Functionality
			6.3 Insufficient Anti-automation
			6.4 Insufficient Process Validation

These mappings were compiled by Denim Group, Ltd. More information about the specific classification schemes can be found:

- OWASP Top 10 2007 http://www.owasp.org/index.php/Top_10_2007
- OWASP Top 10 2004 http://www.owasp.org/index.php/Top_10_2004
- SANS CWE/25 <http://www.sans.org/top25-programming-errors/>
- WASC 24 (+2) <http://projects.webappsec.org/Threat-Classification-Previous-Versions>