BST	PF	GF	CF	CC	Vulnerability/Weakness
	✪	✪	✪	✪	Brute Force (Generic) / Insufficient Anti-automation
		✪	✪	✪	Improper Input Handling
	✪	✪		✪	Information Leakage
		✪		✪	Insufficient Authentication/Authorization
		✪		✪	Insufficient Process Validation
		✪		✪	Integer Overflow/Underflow
		✪		✪	SQL Injection
	✪			✪	Denial of Service (Application Based)
				✪	Abuse of Functionality
	✪	✪	✪		Brute Force Predictable Resource Location/Insecure Indexing
		✪	✪		Improper Output Handling
	✪		✪		Fingerprinting
✪			✪		Content Spoofing
			✪		Brute Force Login
			✪		OS Commanding
	✪	✪			Buffer Overflow
	✪	✪			Cookie Theft/Session Hijacking
	✪	✪			Format String
	✪	✪			Null Byte Injection
	✪	✪			Path Traversal
✪		✪			Clickjacking
✪		✪			Cross-Site Scripting (XSS)
✪		✪			Cross-Site Request Forgery
✪		✪			Remote File Inclusion
		✪			Brute Force Session Identifier
		✪			Credential/Session Prediction
		✪			Cross Site Scripting (XSS) - DOM-Based
		✪			HTTP Response Splitting
		✪			Implicit Logout
		✪			Insufficient Data Protection
		✪			Insufficient Password Recovery
		✪			Insufficient Session Expiration
		✪			LDAP Injection
		✪			Mail Command Injection
		✪			Race Conditions
		✪			Routing Detour
		✪			Session Fixation
		✪			SSI Injection
		✪			URL Redirector Abuse
		✪			XPath Injection
		✪			XML Injection
		✪			XQuery Injection
✪	✪				HTTP Request/Response Smuggling
✪	✪				HTTP Request Splitting
✪	✪				Insufficient Transport Layer Protection
	✪				Application Misconfiguration
	✪				Denial of Service (Connection Based)
	✪				Directory Indexing
	✪				Improper Filesystem Permissions
	✪				Server Misconfiguration
	✪				SOAP Array Abuse, XML Attribute Blowup, XML Entity Expansion
	✪				Weak Authentication Methods
	✪				XML External Entities