

CODE REVIEW CHECKLIST

CATEGORY	DESCRIPTION	PASS	FAIL
General	Are there backdoor/unexposed business logic classes?		
Business Logic and Design	Are there unused configurations related to business logic?		
Business Logic and Design	If request parameters are used to identify business logic methods, is there a proper mapping of user privileges and methods/actions allowed to them?		
Business Logic and Design	Check if unexposed instance variables are present in form objects that get bound to user inputs. If present, check if they have default values.		
Business Logic and Design	Check if unexposed instance variables present in form objects that get bound to user inputs. If present, check if they get initialized before form binding.		
Authorization	Is the placement of authentication and authorization check correct?		
Authorization	Is there execution stopped/terminated after for invalid request? I.e. when authentication/authorization check fails?		
Authorization	Are the checks correct implemented? Is there any backdoor parameter?		
Authorization	Is the check applied on all the required files and folder within web root directory?		
Authorization	Are security checks placed before processing inputs?		
Business Logic and Design	Check if unexposed instance variables are present in form objects that get bound to user inputs. If present, check if they have default values.		
Business Logic and Design	Check if unexposed instance variables present in form objects that get bound to user inputs. If present, check if they get initialized before form binding.		
Authorization	Is there execution stopped/terminated after for invalid request? I.e. when authentication/authorization check fails?		
Business Logic and Design	Are the checks correct implemented? Is there any backdoor parameter?		
Business Logic and Design	Is the check applied on all the required files and folder within web root directory?		
Business Logic and Design	Is there any default configuration like Access- ALL?		
Business Logic and Design	Does the configuration get applied to all files and users?		
Authorization	Incase of container-managed authentication - Is the authentication based on web methods only?		
Authorization	Incase of container-managed authentication - Does the authentication get applied on all resources?		
Session Management	Does the design handle sessions securely?		
Authorization	Incase of container-managed authentication - Is the authentication based on web methods only?		
Authorization	Is Password Complexity Check enforced on the password?		
Cryptography	Is password stored in an encrypted format?		
Authorization	Is password disclosed to user/written to a file/logs/console?		

CATEGORY	DESCRIPTION	PASS	FAIL
Cryptography	Are database credentials stored in an encrypted format		
Business Logic and Design	Does the design support weak data stores like flat files		
Business Logic and Design	Does the centralized validation get applied to all requests and all the inputs?		
Business Logic and Design	Does the centralized validation check block all the special characters?		
Business Logic and Design	Does are there any special kind of request skipped from validation?		
Business Logic and Design	Does the design maintain any exclusion list for parameters or features from being validated?		
Input Validation	Are all the untrusted inputs validated? Input data is constrained and validated for type, length, format, and range.		
Cryptography	Is the data sent on encrypted channel? Does the application use HTTPClient for making external connections?		
Session Management	Does the design involve session sharing between components/modules? Is session validated correctly on both ends?		
Business Logic and Design	Does the design use any elevated OS/system privileges for external connections/commands?		
Business Logic and Design	Is there any known flaw(s) in API's/Technology used? For eg: DWR		
Business Logic and Design	Does the design framework provide any inbuilt security control? Like <%: %> in ASP.NET MVC? Is the application taking advantage of these controls?		
Business Logic and Design	Are privileges reduce whenever possible?		
Business Logic and Design	Is the program designed to fail gracefully?		
Logging and Auditing	Are logs logging personal information, passwords or other sensitive information?		
Logging and Auditing	Do audit logs log connection attempts (both successful and failures)?		
Logging and Auditing	Is there a process(s) in place to read audit logs for unintended/malicious behaviors?		
Cryptography	Is all PI and sensitive information being sent over the network encrypted form.		
Authorization	Does application design call for server authentication (anti-spoofing measure)?		
Authorization	Does application support password expiration?		
Cryptography	Does application use custom schemes for hashing and or cryptographic?		

CATEGORY	DESCRIPTION	PASS	FAIL
Cryptography	Are cryptographic functions used by the application the most recent version of these protocols, patched and process in place to keep them updated?		
General	Are external libraries, tools, plugins used by the application functions the most recent version of these protocols, patched and process in place to keep them updated?		
General	Classes that contain security secrets (like passwords) are only accessible through protected API's		
Cryptography	Does are there any special kind of request skipped from validation?		
General	Classes that contain security secrets (like passwords) are only accessible through protected API's		
Cryptography	Keys are not held in code.		
General	Plain text secrets are not stored in memory for extended periods of time.		
General	Array bounds are checked.		
User Management and Authentication	User and role based privileges are documented		
General	All sensitive information used by application has been identified		
User Management and Authentication	Authentication cookies are not persisted		
User Management and Authentication	Authentication cookies are encrypted		
User Management and Authentication	Authentication credentials are not passed by HTTP GET		
User Management and Authentication	Authorization checks are granular (page and directory level)		
User Management and Authentication	Authorization based on clearly defined roles		
User Management and Authentication	Authorization works properly and cannot be circumvented by parameter manipulation		
User Management and Authentication	Authorization cannot be bypassed by cookie manipulation		
Session Management	No session parameters are passed in URLs		
Session Management	Session cookies expire in a reasonable short time		
Session Management	Session cookies are encrypted		
Session Management	Session data is validated		
Session Management	Session id is complex		
Session Management	Session storage is secure		

CATEGORY	DESCRIPTION	PASS	FAIL
Session Management	Session inactivity timeouts are enforced		
Data Management	Data is validated on server side		
Data Management	HTTP headers are validated for each request		
Business Logic and Design	Are all of the entry points and trust boundaries identified by the design and are in risk analysis report?		
Data Management	Is all XML input data validated against an agreed schema?		
Data Management	Is output that contains untrusted data supplied input have the correct type of encoding (URL encoding, HTML encoding)?		
Data Management	Has the correct encoding been applied to all data being output by the application		
Web Services	Web service has documentation protocol is disable if the application does not need dynamic generation of WSDL.		
Web Services	Web service endpoints address in Web Services Description Language (WSDL) is checked for validity		
Web Services	Web service protocols that are unnecessary are disable (HTTP GET and HTTP POST		