





SSA Knowledgebase




Knowledgebase Search

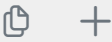
Software Security Test Cases

Rows per page: 30 

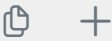
Search



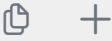
Authentication Testing



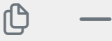
Authorization Testing



Testing Audit Trails



Testing Session Management



Testing Session Management

****1. Test for Predictable Session Identifier****

Objective: To test if session identifiers are generated securely.

Test case ID	Description	Expected results
Session.1.1	Validate if session identifiers are generated using in-house algorithm	Session identifiers are generated using framework methods
Session.1.2	Is any part of session identifier static?	No part of session identifier is static
Session.1.3	Validate if session identifier is generated at client side	Session identifier is generated at server side

Test case ID	Description	Expected results
Session.1.4	Given knowledge of previous session identifier, generation algorithm, validate if it is possible to deduce next session identifier (also known as session brute forcing)	It is not possible to generate next session identifier
Session.1.5	Validate if session identifier length is less than 8 characters	Session identifier length is more than 12 characters
Session.1.6	Check if session identifier is renewed after specified time interval without disconnecting existing session	Session identifier is changed after specified time period
Session.1.7	Check if users are forced to authenticate after very long active session (duration is very long than period used for Session.1.6)	Users are forced to re-authenticate if session is active for a very long time
Section 1.8	Check if users are forced to authentication after specific inactive period (session time out period)	Session timeout feature is implemented with optimum timeout period being set

2. Test for session identifier storage

Objective: To test if session identifiers are stored securely.

Test case ID	Description	Expected results
Session.2.1	Validate if session identifiers are stored in memory	Session identifiers are stored into server memory
Session.2.2	Validate if session identifier is shared with any other system	This is multi server system and session identifier is shared with other servers securely
Session.2.3	At client side if session identifiers stored into persistent cookie?	Session identifier is not stored into persistent cookie

3. Test for session data communication

Objective: To test if session identifiers are communicated securely.

Test case ID	Description	Expected results
Session.3.1	Validate if session identifiers is communicated over encrypted channel	Session identifiers is communicated through encrypted channel
Session.3.2	Validate if each time user authenticated, separate identifier is generated	After successful authentication, new session identifier is generated and after every x minutes new session identifier is generated. Also

Test case ID	Description	Expected results
		"Expires: 0" and Cache-Control: max-age=0 directives are used to protect data
Session.3.3	Validate if session identifier can be cache on proxy?	We used Cache-Control: no-cache and Cache-Control: Private so session identifier is not cached on proxy or local cache
Session.3.4	Check if GET requests carry session data	Get request do not carry session data
Session.3.5	Validate if POST data can be sent via GET request	No, POST data can't be sent through GET request

4. Testing for cookie attributes

Objective: To test if cookies are used securely.

Test case ID	Description	Expected results
Session.4.1	Validate if cookie is set with secure attribute	Cookie is set to secure attribute
Session.4.2	Validate if cookie is marked for httponly attribute	Cookie is marked with httponly attribute so javascript can't access cookie
Session.4.3	Check if domain and path attributes are explicitly set for cookie	Domain and path attributes are explicitly set for cookie
Session.4.4	Validate if persistent cookies are used	No, application uses non persistent cookies

5. Testing for session fixation

Objective: To test if session can be fix by attacker.

Test case ID	Description	Expected results
Session.5.1	Validate if application allow client to supply session identifier?	Application do not allow client to supply session identifier
Session.5.2	Validate if application accept valid session ID supplied by user during authentication?	During authentication, supplied session identifier is invalidated and new identifier is generated for authenticated user.